The Open University

Introduction to cyber security

OpenLearn | Free learning from The Open University

CYBER_B1

Introduction to cyber security (badged open course)

About this free course

This free course is an adapted extract from the Open University course .

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University –

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Copyright © 2016 The Open University

Intellectual property

Unless otherwise stated, this resource is released under the terms of the Creative Commons Licence v4.0 http://creativecommons.org/licenses/by-nc-sa/4.0/deed.en_GB. Within that The Open University interprets this licence in the following way: www.open.edu/openlearn/about-openlearn/frequently-asked-questions-on-openlearn. Copyright and rights falling outside the terms of the Creative Commons Licence are retained or controlled by The Open University. Please read the full text before using any of the content.

We believe the primary barrier to accessing high-quality educational experiences is cost, which is why we aim to publish as much free content as possible under an open licence. If it proves difficult to release content under our preferred Creative Commons licence (e.g. because we can't afford or gain the clearances or find suitable alternatives), we will still release the materials for free under a personal end-user licence.

This is because the learning experience will always be the same high quality offering and that should always be seen as positive – even if at times the licensing is different to Creative Commons.

When using the content you must attribute us (The Open University) (the OU) and any identified author in accordance with the terms of the Creative Commons Licence.

The Acknowledgements section is used to list, amongst other things, third party (Proprietary), licensed content which is not subject to Creative Commons licensing. Proprietary content must be used (retained) intact and in context to the content at all times.

The Acknowledgements section is also used to bring to your attention any other Special Restrictions which may apply to the content. For example there may be times when the Creative Commons Non-Commercial Sharealike licence does not apply to any of the content even if owned by us (The Open University). In these instances, unless stated otherwise, the content may be used for personal and non-commercial use.

We have also identified as Proprietary other material included in the content which is not subject to Creative Commons Licence. These are OU logos, trading names and may extend to certain photographic and video images and sound recordings and any other material as may be brought to your attention.

Unauthorised use of any of the content may constitute a breach of the terms and conditions and/or intellectual property laws.

We reserve the right to alter, amend or bring to an end any terms and conditions provided here without notice.

All rights falling outside the terms of the Creative Commons licence are retained or controlled by The Open University.

Head of Intellectual Property, The Open University

978 1 47302 487 8 (.kdl)
978 1 47302 488 5 (.epub)

Contents

Introduction and guidance

Introduction

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Introduction to cyber security: stay safe online is an informal, introductory course for people who want to feel more confident about their online safety. This free online course will help you to understand online security and start to protect your 'digital life', whether at home or work. You will learn how to recognise the threats that could harm you online and the steps you can take to reduce the chances that they will happen to you.

Part of this practice will be the weekly interactive quizzes, of which Weeks 4 and 8 will provide you an opportunity to earn a badge to demonstrate your new skills. You can read more on how to study the course and about badges in the next sections.

Like most courses these days, *Introduction to cyber security: stay safe online* has learning outcomes. These are not as complicated as they sound, but are simply what we hope you will achieve by the end of the course. After completing this course, we hope that you will have a better understanding of:

- implementing a plan to protect your digital life
- recognising threats to online safety
- taking steps to reduce the risk of online threats
- concepts including malware, viruses and Trojans
- network security, cryptography and identity theft.

Moving around the course

The easiest way to navigate around the course is through the ‘My course progress’ page. You can get back there at any time by clicking on ‘Back to course’ in the menu bar.

It’s also good practice, if you access a link from within a course page (including links to the quizzes), to open it in a new window or tab. That way you can easily return to where you’ve come from without having to use the back button on your browser.

What is a badged course?

While studying *Introduction to cyber security: stay safe online* you have the option to work towards gaining a digital badge.

Badged courses are a key part of The Open University's mission *to promote the educational well-being of the community*. The courses also provide another way of helping you to progress from informal to formal learning.

To complete a course you need to be able to find about 24 hours of study time, over a period of about 8 weeks. However, it is possible to study them at any time, and at a pace to suit you.

Badged courses are all available on The Open University's OpenLearn website and do not cost anything to study. They differ from Open University courses because you do not receive support from a tutor. But you do get useful feedback from the interactive quizzes.

What is a badge?

Digital badges are a new way of demonstrating online that you have gained a skill. Schools, colleges and universities are working with employers and other organisations to develop open badges that help learners gain recognition for their skills, and support employers to identify the right candidate for a job.

Badges demonstrate your work and achievement on the course. You can share your achievement with friends, family and employers, and on social media. Badges are a great motivation, helping you to reach the end of the course. Gaining a badge often boosts confidence in the skills and abilities that underpin successful study. So, completing this course should encourage you to think about taking other courses.


Introduction to
cyber security

How to get a badge

Getting a badge is straightforward! Here's what you have to do:

- read each week of the course
- score 50% or more in the two badge quizzes in Week 4 and Week 8.

For all the quizzes, you can have three attempts at most of the questions (for true or false type questions you usually only get one attempt). If you get the answer right first time you will get more marks than for a correct answer the second or third time. If one of your answers is incorrect you will often receive helpful feedback and suggestions about how to work out the correct answer.

For the badge quizzes, if you're not successful in getting 50% the first time, after 24 hours you can attempt the whole quiz, and come back as many times as you like.

We hope that as many people as possible will gain an Open University badge – so you should see getting a badge as an opportunity to reflect on what you have learned rather than as a test.

If you need more guidance on getting a badge and what you can do with it, take a look at the OpenLearn FAQs. When you gain your badge you will receive an email to notify you and you will be able to view and manage all your badges in My OpenLearn within 24 hours of completing the criteria to gain a badge.

Get started with Week 1.

Week 1: Threat landscape

1 Online, the new frontline

Introduction

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Welcome to this free course, *Introduction to cyber security: stay safe online*.

Cory Doctorow is your guide through this course. He is a visiting professor at The Open University. He'll meet you at the start of each week to let you know what's coming up and remind you of what you've learned so far to help you make the most of your learning.

About the course

Your journey into the world of cyber security and protecting your digital life has been organised into eight weeks of study. The first three weeks focus on understanding the basics of cyber security. This includes an exploration of the security threat landscape, together with some of the basic techniques for protecting your computers and your online information.

You'll then look 'under the hood', exploring some of the technologies that underpin the internet and cyber security. This will include gaining an understanding of how computers are connected in a network and how the data transmitted across that network is kept secure.

In the final two weeks of the course, you'll look at what can be done if you suffer a successful cyber security attack and how to develop an action plan. As part of this, you'll learn about both the legal and technical aspects of recovering from an attack.

This course will not only help you take steps to protect yourself online, such as how to create a strong password, but also provide an overview of cyber security from the security threat landscape to how the internet works. It will also provide a foundation for further study of this important discipline.

To test your knowledge you can try the end-of-week practice and end-of-course compulsory badge quizzes.

Before you start, The Open University would really appreciate a few minutes of your time to tell us about yourself and your expectations of the course. Your input will help to further improve the online learning experience. If you'd like to help please fill in this optional survey.

Video content is not available in this format.

View transcript - Uncaptioned interactive content

We shop online. We work online. We play online. We live online. More and more, our lives depend on online, digital services. Almost everything can be done online – from shopping and banking to socialising and card making – and all of this makes the internet, also known as cyberspace, an attractive target for criminals.

Large-scale cyber security breaches often make the headlines but about 70% of organisations are keeping their worst security incidents under wraps, so what makes the news is just a small proportion of the breaches that are actually taking place. Britain is being targeted by up to 1,000 cyber attacks every hour.

We all have a responsibility to protect services from being maliciously disrupted or misused, through our vigilance, through our own security measures and through reporting events when they arise.

The knowledge, tools and best practices relating to protecting the computers, communications networks, programs and data that make our digital lives possible are collectively referred to as cyber security, or information security. For the purposes of this course, we use the two terms interchangeably.

Behind the numbers

Cyber security is definitely one of those areas where you need to evaluate the validity of any information you find online before accepting it. The figures about the prevalence and under-reporting of cyber attacks comes from a 2010 CyberSecurity Watch survey carried out in the US by a number of organisations, including the US Computer Emergency Response Team. The survey states that ‘the public may not be aware of the number of incidents because almost three-quarters (72%), on average, of the insider incidents are handled internally without legal action or the involvement of law enforcement.’

The estimate of 1,000 attacks per hour is based on the BIS Cyber Security Breaches Survey 2014. We took the number of organisations that reported that they were attacked ‘hundreds of times a day’ in different ways, and assumed that each of these responses were attacked a minimum of 100 times per day, we worked out that there were at least 24,156 attacks per day across the 1,098 organisations surveyed. Dividing this by 24 suggests that there are a minimum of 1,000 attacks per hour.

Let’s get started by learning some of the basic terminology used when discussing cyber security.

1.1 Talking security: the basics

Figure 1

View description - Figure 1

In any discussion of security, there are some basic terms that will be used a lot. This section will introduce you to the basic terminology of information security.

CIA

The guiding principles behind information security are summed up in the acronym CIA (and we're pretty sure there's a joke in there somewhere), standing for confidentiality, integrity and availability.

We want our information to:

- be read by only the right people (confidentiality)
- only be changed by authorised people or processes (integrity)
- be available to read and use whenever we want (availability).

It is important to be able to distinguish between these three aspects of security. So let’s look at an example.

Case study: PlayStation Network

In April 2011, Sony revealed that the PlayStation Network, used by millions of consumers worldwide, had been breached by hackers. The breach went unnoticed by Sony for several days and ultimately resulted in the theft of up to 70 million customer records. The records included customer names, addresses, emails, dates of birth and account password details. Information which could have enabled additional attacks or identity theft.

In order to assess the scale of the damage and repair the vulnerabilities that led to the attack Sony took the PlayStation Network offline, a move which cost the company, and merchants who offered services via the network, significant amounts of revenue.

In addition to the cost of fixing the breach, Sony was fined £250,000 by the Information Commissioner’s Office as a result of a ‘serious breach’ of the Data Protection Act, stating that ‘The case is one of the most serious ever reported to us. It directly affected a huge number of consumers, and at the very least put them at risk of identity theft.’

The precise financial cost to Sony is unclear but estimates place it at approximately £105 million, excluding the revenue loss by partner companies, damage to its reputation and potential damage to its customers.

So how do the principles of CIA apply to the PlayStation case? Quite obviously, confidentiality was violated: there was a chance that unauthorised people could read the data. However, authorised users still had full access to the data, so it remained available; and the data was not changed, so its integrity was preserved.

Information assets

Time for another definition. When talking about valuable data we use the term ‘information assets’. In the PlayStation case, the information assets were the data about Sony’s customers.

When we consider security of online communications and services, we also need two additional concepts: ‘authentication’ and ‘non-repudiation’.

When we receive a message, we want to be confident that it really came from the person we think it came from. Similarly, before an online service allows a user to access their data, it is necessary to verify the identity of the user. This is known as authentication.

Non-repudiation is about ensuring that users cannot deny knowledge of sending a message or performing some online activity at some later point in time. For example, in an online banking system the user cannot be allowed to claim that they didn’t send a payment to a recipient after the bank has transferred the funds to the recipient’s account.

Malware

Finally, there are a number of terms associated with software that attempts to harm computers in different ways. Collectively these are known as ‘malware’ (a contraction of malicious software).

Depending on what the malware does, different terms are used to in relation to malware. For example:

- **ransomware** is malware that demands payment in order to refrain from doing some harmful action or to undo the effects of the harmful action
- **spyware** records the activities of the user, such as the passwords they type into the computer, and transmits this information to the person who wrote the malware
- **botnets** are created using malware that allows an attacker to control a group of computers and use them to gather personal

information or launch attacks against others, such as for sending spam emails or flooding a website with so many requests for content that the server cannot cope, called a denial-of-service attack.

You'll learn more about malware in Week 3.

Now that you understand some of the basic concepts and terminology, you'll use this knowledge to study real examples of cyber security breaches.

1.2 Obtaining Sophos Threatsaurus

Figure 2

View description - Figure 2

There are lots of technical terms relating to cyber security and it can be difficult to keep track of what's what.

Sophos is one of the major players in the anti-malware business. They publish a Threatsaurus to help you remember and define the terms relating to malware. The Threatsaurus is a plain-English guide, to help IT managers and end users understand the threats posed by malicious software. The Threatsaurus includes:

- an A–Z glossary on computer and data security threats
- practical tips to stay safe from email scams, identity theft, malware and other threats
- a guide to Sophos's security software and hardware.

Download the Sophos Threatsaurus PDF or from the Sophos website.

Save it and print it out if you need to, so that you can refer to it throughout the course. You'll use it again in Week 3.

1.3 Cyber security attacks and phishing

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Britain is being targeted by up to a thousand cyber attacks every hour. For small organisations the worst breaches cost between £65,000 and £115,000 on average and for large organisations may run to many millions of pounds. These costs can occur as direct financial losses due to fraud or theft; the loss of productivity due to time spent recovering from the effects of a successful attack; or the lost of trust and reputation.

Phishing

It may be surprising that many cyber security breaches do not result from technical failures. In fact it is commonplace for attackers to exploit the goodwill and trust of people to gain access to systems, using a form of attack that is known as ‘social engineering’.

Pretending to be technical support personnel or crafting emails that ask for usernames and passwords are common forms of social engineering attacks. You may have heard the term ‘**phishing**’ used to describe these kind of emails. Phishing is a form of social engineering. In the video, course guide Cory explains how it happened to him.

In the next section you’ll find out about three high profile cyber security breaches.

1.4 Examples of high profile cyber security breaches

Figure 3

View description - Figure 3

Cyber security attacks take many forms from obtaining users' personal information, to attacking critical national infrastructure and obtaining companies' proprietary data. Here we describe three high profile cyber security breaches which caused major financial losses and damaged the reputations of the organisations concerned.

Attacking online identities

Adobe Systems is one of the most important companies in the digital economy. Its software is used to produce, publish and present an enormous amount of material – chances are your favourite magazines and books were laid out with Adobe software.

Over the years, Adobe had stored the names, addresses and credit card information of tens of millions of users on its servers. Then, in October 2013, Adobe admitted that data from 2.9 million accounts had been stolen. Later, that number was revised to 38 million accounts, but when the data file was found on the internet it contained no less than 153 million user accounts. Much of this data could be read and soon copies of the stolen accounts were in wide circulation. It also became clear that the people who had stolen user data had also gained access to Adobe's development servers – program code, potentially worth billions of dollars, had also been stolen.

Adobe was forced to change the log in details of every one of its users and to greatly improve its own security. And, of course, users are suing Adobe for not protecting their information.

Is Adobe alone, or are other companies holding valuable data but not protecting it properly?

Attacking industrial systems

Not many people want a uranium centrifuge, but those that do, really want a uranium centrifuge. The centrifuge was developed after the Second World War for enriching uranium so that it can be used either for generating nuclear power, or, as the heart of a nuclear weapon.

Under international treaty it is not illegal for countries to slightly enrich uranium for nuclear energy, but high levels of enrichment are forbidden to all but a handful of countries. As a consequence, centrifuge technology is tightly controlled, but still, centrifuges have gradually spread around the world. Most recently they have been developed by Iran, ostensibly for that country's legal civil nuclear programme; but it is sometimes suspected it might possibly be for the development of an Iranian nuclear bomb.

In the summer of 2010, a new piece of malicious software for the Microsoft Windows operating system was discovered by an antivirus company in Belarus. The software was dissected and found to attack

a very specific set of computer-controlled high-speed motors manufactured by Siemens. Left unchecked, the software, dubbed ‘Stuxnet’, would rapidly increase and decrease the speed of the motors causing irreparable damage to whatever was connected to them – among other things, uranium centrifuges.

The very specific nature of the systems targeted by Stuxnet make many believe that it was developed specifically to disrupt the Iranian uranium enrichment programme. By the autumn of 2010, reports were appearing that the Iranian centrifuge programme was in trouble. The Israeli paper Haaretz reported that Iran’s centrifuges had not only produced less uranium than the previous year, but that the entire programme had been forced to stop and start several times because of technical problems. Other sources reported that Iran had been forced to remove large numbers of damaged centrifuges from its enrichment plant.

Attacking specific targets

In December 2013, the American retailer Target announced that hackers had stolen data belonging to 40 million customers. The attack had begun in late November and continued for several weeks before it was detected. By then it had compromised more than 110 million accounts, including unencrypted credit and debit card information as well as encrypted PIN data. By February 2014, American banks had replaced more than 17 million credit and debit cards at a cost of more than $172 million. The amount of fraud linked to the attack is unknown, as is the damage to Target’s reputation.

Target was not the first major retailer to be hit by hackers, but this attack was different from most; the weakness that allowed the attackers into the Target computers lay outside of the company. The hackers had gained access through computers belonging to one of Target’s heating, ventilation and air conditioning services (HVAC) contractors. Like many large organisations, Target allows other companies to access its internal networks, to submit bills and exchange contracts.

The hack appears to have begun when an employee of the HVAC company received an email from one of their trusted partners. In fact, the email was fake and contained malicious software. Unlike traditional spam email, this message had been targeted at a very specific audience – the HVAC company. It was what is known as ’spear phishing’.

Once the email had been opened, the hidden software went to work and retrieved the HVAC company’s Target network authorisations, allowing them to log on to their real objective. In an ideal system, the HVAC company’s authorisations should have restricted them to a network responsible solely for billing and contracts, but, like a lot of big organisations, Target used a single network for all of its data, allowing the attackers to eventually locate, and steal, customer data.

The Target attack is an example of an advanced persistent threat. Rather than attempting to attack the retailer directly, the hackers had chosen an external company which was much less likely to have the resources to detect and defend against an attack. Their spear phishing email was directly targeted at the contractor, lulling them into a false sense of security and allowing the malware to retrieve the logon credentials needed to attack Target itself.

Activity 1 Describing cyber security breaches

Allow about 10 minutes

Choose one of the three example attacks outlined above. You can choose Adobe, Stuxnet or Target.

Using the terminology you’ve learned so far, try writing a brief description of the attack which might explain it to other learners, and write it in the space below.

Examples of things you might put into your description are:

- the CIA concepts that are relevant to the example you have chosen
- whether malware was involved in the attack, and what type of malware it was

- the asset that was affected by the attack.

Provide your answer...

1.5 Taking stock of your information assets

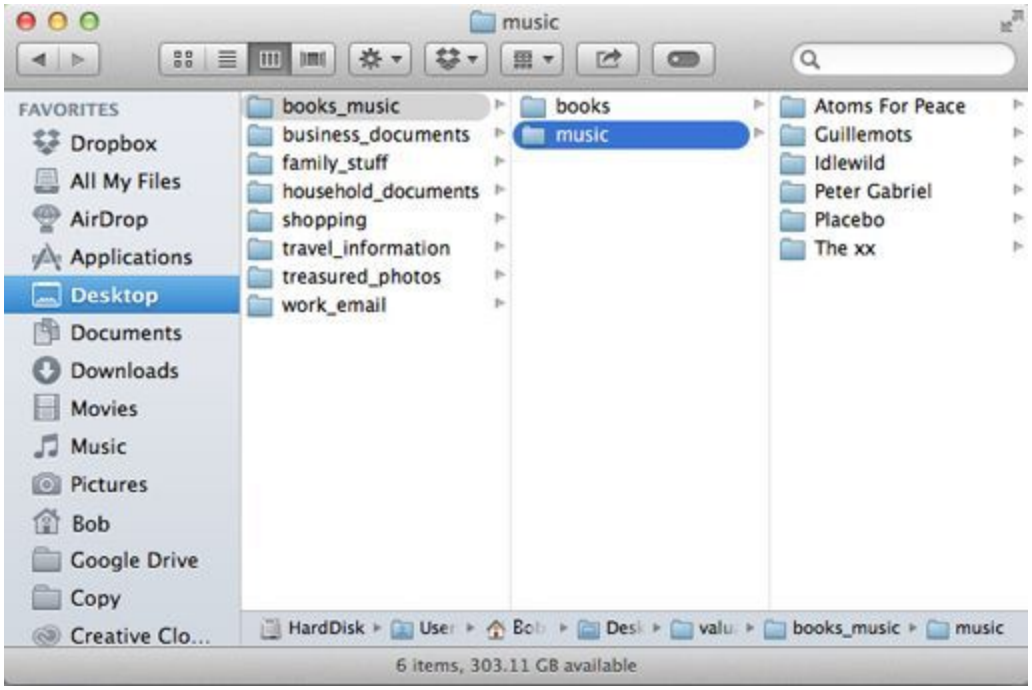


Figure 5

View description - Figure 5

Before you can take steps to protect your corner of cyberspace, you need to know what information you have that needs protection: your information assets.

Activity 2 Your information assets

Allow about 15 minutes

Compile a list, perhaps in a spreadsheet or using one of our templates, of the different types of information you store on your computer or online. For example, you may have personal correspondence, photographs, work documents or personal

details such as your National Insurance number, insurance policy details and passwords for online services.

- Information assets list template (PDF)
- Information assets list template (DOCX).

For each type of information, think of its value to you. Label the most valuable types of information as ‘High’, the least valuable as ‘Low’ and those that are in between as ‘Medium’.

The value could be the cost to replace the information, in time or money, or the impact of its loss on your reputation, for example, all your emails or photographs could all be published online.

Do the same exercise for the online activities you engage in. For example, you might use online banking, shopping or social networking services. This time, label each one with a value based on the potential cost of an unauthorised person gaining access to it.

In the next section, you will use this information as part of a survey that will help you get a picture of your exposure to information security threats but you won’t be asked to share the details of your list. You’ll use this list later in the course, too.

1.6 What are your own safeguards?

Figure 6

View description - Figure 6

It’s time for you to take stock of your own safeguards against data loss, unwarranted access or malicious software. We’d also like to know a bit more about the frequency of computer crime to the average user.

This survey is a series of multiple-choice questions based on your current habits. There are no right or wrong answers so you should choose the answer that most closely matches the way you use your computer.

Don’t worry, the data collected is anonymous and cannot be linked to your OpenLearn profile or email address.

2 Understanding current threats

Figure 7

View description - Figure 7

Now you know what information assets you have, you'll look at how those assets can be compromised.

You will learn about some different kinds of threat, the vulnerabilities that they exploit and some countermeasures that can be put in place to guard against them. When we use those terms we mean:

- **vulnerability** – a point at which there is potential for a security breach
- **threat** – some danger that can exploit a vulnerability
- **countermeasure** – action you take to protect your information against threats and vulnerabilities.

Threats can take many different forms, including unauthorised access to data with the intent of committing fraud against individuals or businesses. At its most extreme, there is the potential for the

systematic disruption of computer networks and services, putting cyber security threats on a par with those associated with terrorism. In 2010, the UK government's National Security Strategy highlighted cyber security attacks on the UK as a 'Tier 1' threat, which means they are one of the highest priorities for action.

New threats are being discovered all the time and they can affect any and every operating system, including Windows, Mac OS, Linux, Android and iOS. To protect ourselves it is important to keep ourselves up to date with the latest cyber security news.

Next, you will explore how a cyber security threat is described in the Windows and Mac OS platforms by watching a video relevant to your computer's operating system if possible.

2.1 Understanding security notices

Windows

Watch this video if your computer runs Windows operating systems. If you have a Mac, you will find a video for the Mac operating system below. You do not need to watch both Windows and Mac videos.

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Large software companies publish security notices when they discover a threat. It can be hard to read these notices to find the important bits. Therefore it's helpful to know where to find them and what to look out for.

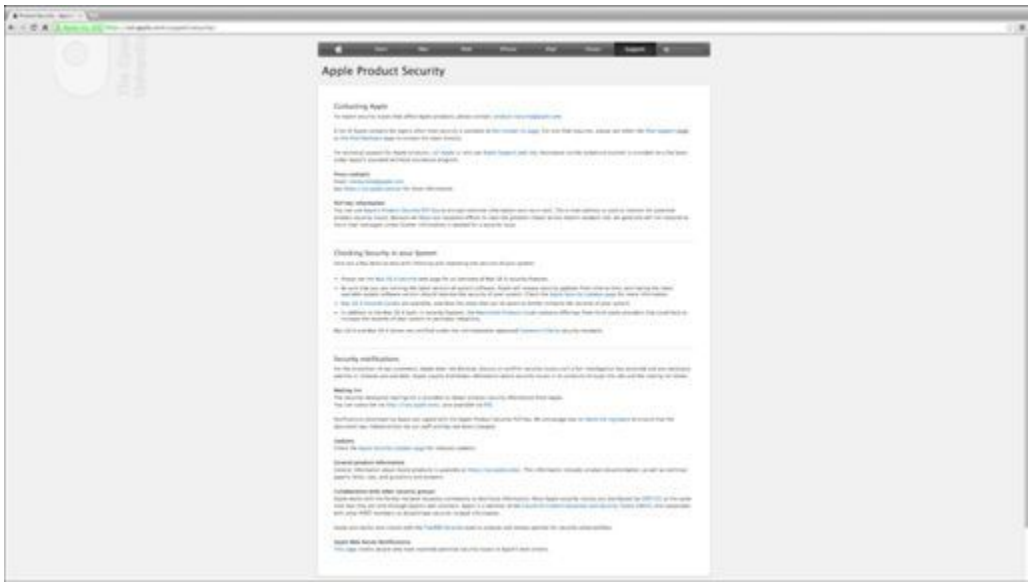
Visit the Microsoft Security Response Center to see the latest security threats.

Mac OS

Watch this video if you have a Mac and run a Mac operating system. (If your computer runs a Windows operating system and you have watched the video in the previous section, you do not need to watch this video.)

Video content is not available in this format.

View transcript - Uncaptioned interactive content



Large software companies publish security notices when they discover a threat. It can be hard to read these notices to find the important bits. Therefore it’s helpful to know where to find them and what to look out for.

Visit the Apple Product Security website to see the latest security notifications.

2.2 How to keep up to date

Figure 8

View description - Figure 8

Attackers are constantly finding new vulnerabilities and ways of attacking computer systems. Therefore, it is important to keep yourself informed and up to date with threats that are relevant to your situation.

There are many sources of news about cyber security. Many of them are extremely technical and are designed for security specialists to communicate their findings with one another, for software developers to improve their programs or academic publications. There are also plenty of free resources, written by journalists, security professionals and enthusiastic amateurs, where you can learn more even if you are new to the field. The Cyber Streetwise website is a good example of this type of online resource.

The links provided below are a selection of others that are available. You are not expected to look at all of them in detail.

News sites

The best places to get started are the major media outlets, most of whom employ technology journalists. These sites will give you readable information intended for as wide an audience as possible. Many of them are updated several times a day, but they will only consider ‘newsworthy’ events such as a major hack or virus outbreak, and some will only cover news in a particular country – so you may need to look at a variety of sites:

- BBC News Technology
- Guardian Online Technology
- The Telegraph Internet security
- Bloomberg Cyber security

Technology sites

Many sites devoted to technology will cover aspects of security on a regular basis. Most of the sites below cover other topics, so you might need to use their search functions to find relevant information.

- Wired – Threat level
- Computer Weekly
- The Hacker News
- Info-Security magazine

Information security companies

There are a large number of companies selling security software to home users and to businesses. Almost all of them maintain regularly updated websites explaining new and emerging security threats and how they can be overcome.

Much of this information is technical and aimed at administrators responsible for large computer systems, but the introductory material is often quite easily understood. These sites can be the best to use when a new security issue is identified.

- Sophos labs

- Microsoft
- Apple

Blogs

- Krebs On Security Brian Krebs is an American journalist and investigative reporter. He is best known for his coverage of profit-seeking cybercriminals. His interest grew after a computer worm locked him out of his own computer in 2001.
- Graham Cluley is an award-winning security blogger, researcher and public speaker. He has been working in the computer security industry since the early 1990s, having been employed by companies such as Sophos, McAfee and Dr Solomon's.
- Bruce Schneier is an internationally renowned security technologist who writes a monthly newsletter, called 'Crypt-o-gram'. He provides commentary and insights into critical security issues of the day. The content of this blog can be accessed in multiple forms, including a podcast and an email newsletter.
- Troy Hunt provides analyses of different system breaches and useful hints on how to avoid being attacked.

Activity 3 Knowing your enemies

Allow about 20 minutes

Carry out some research about different cyber security threats and the types of groups who pose the threat.

Using the information sources above find out about:

- a threat to your information, computers and other devices that arise from malware
- a threat to your communications (such as spam and denial of service (DoS) or distributed denial of service (DDoS) attacks, often launched using botnets).

For each threat, try to identify the type of individuals or organisations that are posing the threat. Which of the following types would best describe them?

- **Cybercriminal:** those carrying out cyber attacks for personal financial gain.
- **Spies:** those engaged in espionage activities on behalf of either commercial organisations or national governments.
- **Hacktivists:** those who carry out cyber attacks as a form of protest against organisations or governments.
- **Insider attacker:** disgruntled or dishonest staff who attack their organisation's computer systems.

If you identify a different type of attacker, how would you describe it?

Spend 10–15 minutes researching, then spend five minutes noting down your findings in the space below.

Provide your answer...

2.3 Staying informed

Figure 9

View description - Figure 9

Hopefully, you now have some ideas of how to stay up to date with the latest developments in cyber security.

Before continuing to the final part of the week, take some time to plan some concrete steps you will take to keep yourself more informed.

For example, you could subscribe to a blog via email or Feedly, or follow updates via Twitter or Facebook.

3 Securing my digital information

Figure 10

View description - Figure 10

What issues arise in doing everyday activities online? As we've already discussed, most of us rely on the internet for everyday tasks such as shopping, working, banking or social networking. We often do this without stopping to think about the security issues that might be involved.

Activity 4 Securing your information

Allow about 15 minutes

Choose one of the following activities and think about the main security issues that might threaten your chosen activity.

- **Online banking** – for example, to check the balance in your account or make a payment.
- **Online shopping** – think particularly about buying something from a new store that you don't recognise and haven't shopped from before.
- **Social networking** – think about whether you would add someone as a 'friend' if you hadn't met them in person.
- **Working from home** – consider the need to transfer documents that contain confidential information between members of your team.

View answer - Activity 4 Securing your information

Questions to consider

Remember that earlier this week we classified security issues under three headings. We want our information to:

- be read by only the right people (confidentiality)
- only be changed by authorised people or processes (integrity)
- be available to read and use whenever we want (availability).

3.1 Threats to your assets

For the final activity this week you'll update your own list of cyber threats.

Activity 5 Your threats

Allow about 5 minutes

Update the list of information assets and online activities you compiled in Taking stock of your information assets. Add any threats that are relevant to your assets.

Save this list to use later in the course.

Next, you have a chance to review your learning in the end-of-week practice test.

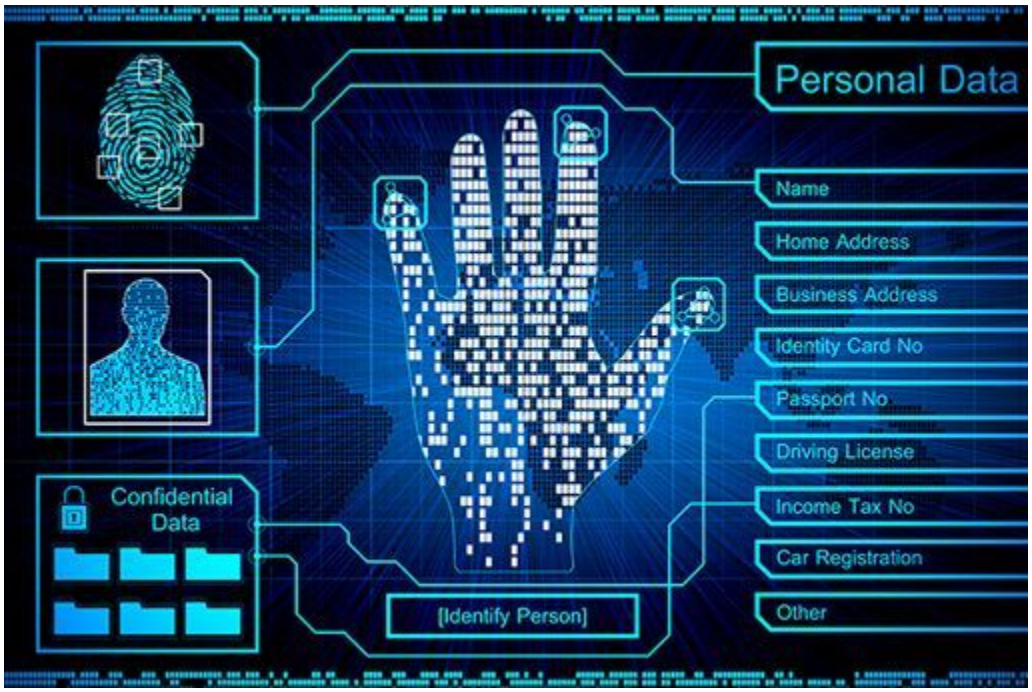


Figure 11

View description - Figure 11

4 Week 1 quiz

This quiz allows you to test and apply your knowledge of the material in Week 1.

Complete the Week 1 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 1

Figure 12

View description - Figure 12

This week you explored the security threats that could affect your digital information and use of online services.

You also learned how to keep your knowledge of these threats up to date and started looking at how these threats relate to your own information assets and online activities. In the coming weeks you will explore the different ways in which these threats can become attacks.

You have also learned about the wider world of cyber security and how attacks can affect a variety of systems. As we enter into an age where most everyday devices are connected to the internet – the ‘Internet of Things’ – we will have to deal with a growing range of threats and cyber security will be increasingly important.

There is some optional further reading relating to cyber security in a business setting in the further reading section.

You can now go to Week 2: Authentication.

Further reading

Microsoft Security Response Centre

Microsoft – Turning automatic updates on or off

Apple Product Security

Cyber governance health check: 2013 A report on the levels of cyber security awareness and preparedness across the FTSE 350, from the Department for Business, Innovation & Skills.

2014 Information security breaches survey A report on cyber security breaches in UK businesses from PricewaterhouseCoopers LLP.

Week 2: Authentication

Introduction

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Cory introduces you to Week 2 of the course.

Last week you explored the security threats that could affect your ability to stay secure online. You also learned how to keep your knowledge of these threats up to date.

This week you'll learn about the purpose of passwords and the different situations in which they are used, the ways in which attackers try to learn your password so they can impersonate you online and ways of improving the security of your passwords and online identification methods.

Important warning: This week, you will be asked to discuss different aspects of password security. It is critical that you never share your actual passwords and only discuss the general principles. If you need an example, please make one up rather than give an actual password!

1 Passwords: what are they for?

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Figure 1

View description - Figure 1

Millions of people use online services every day, and it is crucial that these systems prevent users from accessing each other's information. To do this, they need a way of uniquely identifying each user that prevents users from impersonating each other. This is called identification and authentication.

Passwords and passcodes are the most common way of authenticating users. Examples of their use includes the PIN

(Personal Identifier Number) you use with your credit and debit card as well as the many passwords you are expected to remember when logging in to computer-based services.

An ideal password must satisfy two conflicting aims. It should be:

1. memorable enough that the user can recall it without writing it down
2. long enough and unique enough that no one else can guess it.

As you've almost certainly found out, remembering passwords is hard and it can be even harder to think of one that is secure. For these reasons many services are thinking about replacing passwords – we will return to this later.

First, let's think about how passwords are used and the different ways attackers try to learn our password.

1.1 What happens when you enter a password?

Video content is not available in this format.

View transcript - Uncaptioned interactive content

When a user enters a password it is matched against the password stored by that website. If the passwords match, the user is granted access.

There are a couple of potential weaknesses with this approach that you can probably recognise:

1. The password is *transmitted* as **plaintext** (what you see is exactly what you get; it isn't hidden in any way) – it could be intercepted as it travels across the network.
2. The password is *stored* as plaintext – an attack on the server could not only reveal the user's password, but all the passwords for all the users of the system.

The first problem is usually overcome by encrypting the communication between the user and the server. The most common form of encryption is the SSL standard (Secure Socket Layer). You'll recognise that **SSL** is being used when you see 'https' at the beginning of a web page address instead of 'http', and by a padlock symbol in your browser. (You'll look at encryption and SSL more fully in Week 4.)

The second problem can also be solved using a technique called hashing. A hash is the result of processing plaintext to create a unique, fixed length identifier – you'll find out more in Week 5. It cannot be used to reconstruct the original data – even if the hash falls into hostile hands. In this scheme, a hashing function is used to create a hash of a password, which is stored on the server – the password itself is discarded. When the user enters a password, this is sent over the network and hashed on the server using a copy of the same hashing function. The resulting hash is compared to the hash stored on the password server. Only if they match will the user be granted access. Some implementations of this scheme will hash the user's password before sending it across the network to be compared with the hash stored on the server.

Almost all online services and computer systems store passwords as hashes – but surprisingly, errors still happen. The problems described in the following case study could have been avoided if hashing had been used.

Case study: RockYou

The game and advertising company RockYou suffered a major security breach in 2009 when 32 million user accounts were compromised, revealing that not only did the company store passwords in plaintext, it encouraged insecure passwords by only requiring them to be five alphanumeric characters long.

RockYou's problems were made worse when it became clear that they had known that their database was vulnerable to an attack for more than ten years. The company had previously

been criticised on privacy grounds for sending emails containing complete lists of their advertising partners, and for poor security in issuing passwords through insecure email.

Even when hashing and encrypted communications are used, there are still ways in which attackers can successfully learn your password.

1.2 Attacking passwords

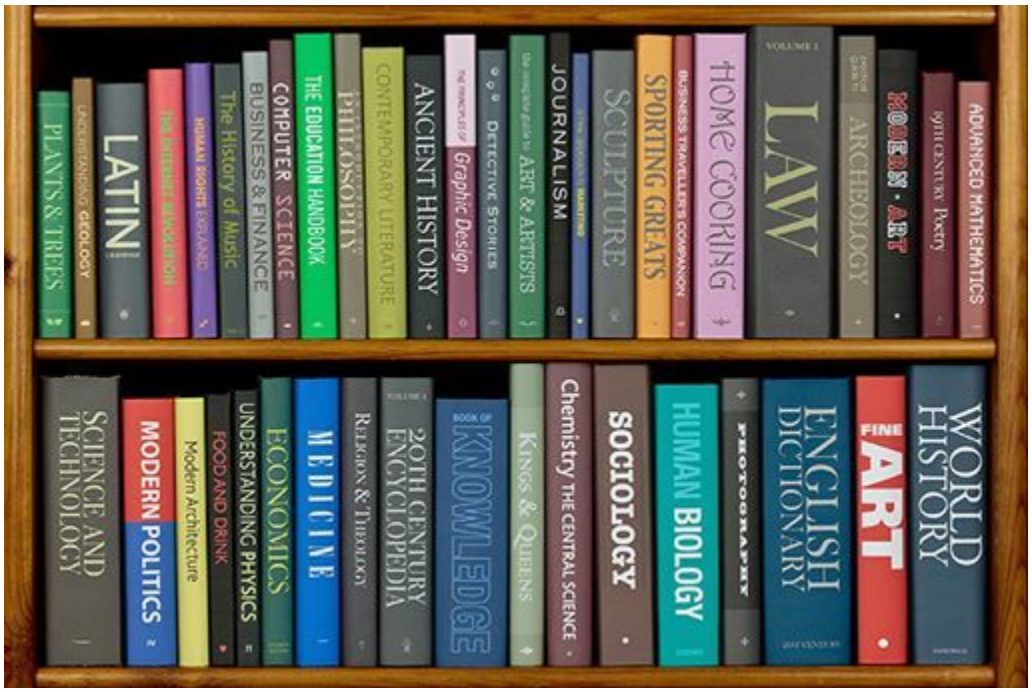


Figure 2

View description - Figure 2

The obvious ways that attackers can find or steal passwords, such as looking over your shoulder when you're using an ATM or credit card machine or trying obvious passwords such as 'abc123' and 'password', are familiar to us.

Almost as long as there have been passwords there have been people attempting to break passwords. One of the oldest methods of automatically breaking into computers is to perform a **dictionary attack**. As its name suggests, a computer will attempt to log into an account by working its way through one or more dictionaries – each entry in the dictionary is one possible password and if it doesn't work, the computer moves on to the next.

Dictionaries need not be the familiar A–Z references that we are familiar with: a concerted dictionary attack will also include more specialised reference works such as atlases, lists of astronomical

bodies and characters from literature, as well as lists of the most commonly used passwords and lists of stolen passwords that are in widespread circulation.

Dictionary attacks can also be performed on the hashed values of words; they may take a little longer, but they will work. Some system administrators might set up dictionary attacks on their own users' passwords to try to identify weak passwords that should be changed.

An alternative, simple attack is a **brute force attack** where a computer will methodically work through all possible passwords (so beginning with 'A', then 'AA', 'AB' and so on …) trying each in turn until it stumbles upon an actual password.

Dictionary and brute force attacks can be foiled by having computers watch for unsuccessful attempts to log in to accounts. Almost all computer systems restrict the number of unsuccessful logins after which the account is locked and can only be accessed after the intervention of an administrator.

Another type of attack on passwords is based on the incorrect configuration of the hashing technique used to store the passwords on the server, which is discussed in the next section.

1.3 Salt to protect

Figure 3

View description - Figure 3

The security of stored passwords can be increased by a process known as salting – in which a random value (called the salt) is added to the plaintext password before the hashing process.

This greatly increases the number of possible hash values for the password and means that even if two people choose identical passwords, their hashed passwords have completely different values.

The hashed password and the relevant salt are stored by the password server. When the user attempts to log in to the computer, their password and the salt are added together, hashed and compared to the stored, hashed value.

Salting is only effective if:

- truly random salts are used for each password (some systems have either used a single salt for all passwords, or have only changed the salt when the computer is restarted)
- the salt is long enough that, when added to a password, it will create enough possible hashed values that an attacker cannot generate a table containing all possible hashes from a salted dictionary. For instance, the passwords used by UNIX in the early 1970s were restricted to eight characters and used a 12-bit salt. When released this was secure enough – it was not feasible to generate the hashes for every possible password each of which had been salted with all 4,096 possible salts. However, the rapid advance in computer power and storage capacity meant that longer salts are required. A typical piece of advice is that the salt should be the same length as the output of the hashing function – so if your hashing function generates 256-bit hashes, a 256-bit salt should be used.

Case study: LinkedIn

In the middle of 2012, the hugely successful social networking site LinkedIn was attacked by Russian hackers. The passwords to some 6.5 million accounts were stolen, but although they were stored as hashed values, the passwords had not been salted.

The hashing had been performed using the relatively old SHA-1 hashing algorithm which can be performed at very high speed (a desktop computer can calculate several tens of millions of SHA-1 hashes per second).

It was therefore not surprising that within a day, decrypted passwords were being published on the internet and LinkedIn was forced to ask all users to change their passwords.

Preventing the attacks described above depends on the online service taking steps to encrypt the transmission and storage of

passwords. As users, we can help in this protection by choosing passwords that are difficult to attack.

2 Improving password security

Figure 4

View description - Figure 4

Just about every website you sign up to requires a password. What strategies do you use when choosing passwords?

If your passwords are easily guessable, you are effectively giving attackers easy access to your accounts. If your passwords are along the lines of ‘password’, ‘123’ or ‘letmein’, they won’t even need to use their automatic password-breaking tools. This is especially true when people don’t change the default passwords that are used to control access to the settings of certain pieces of equipment such as broadband routers.

Think about your strategies for picking memorable passwords. Consider these questions:

- How many passwords do you use?
- How long are the passwords you use?

- Do you use upper and lower case letters, numbers, other symbols in them?

2.1 How to pick a proper password

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Using your pet’s name, your street’s name or a random word can be easy to remember, but can also be easy to guess.

Even if the website uses hash functions, if the passwords are dictionary words, the attacker can generate lots of possible passwords, hash them and see whether any of them match a stored one. Attackers always start with dictionary words and variations thereof, as most passwords are normal words.

So your accounts will be more secure using passwords made up of a collection of numbers, letters and symbols that don’t resemble a dictionary word. One way of coming up with such passwords is first to choose a memorable phrase and convert it in the way described in the video above.

Strong passwords – long, non-dictionary words that are not easily guessable – are vital. The other thing to remember is to use a

different password for every account.

The majority of cases in which someone's password has been compromised have occurred when an attacker has cracked someone's password on a low-value, low-security site, and that user used the same password for another, higher-value site. The attacker either knows or guesses the target's username on the higher-value site and then tries the cracked password on it.

For more advice about how to choose strong passwords read the Good password checklist. It might be useful to print off and keep this.

Good password checklist

- Don't use simple, easy to guess passwords such as names of friends, family and pets. Don't use words from the dictionary or commonly used passwords such as 12345 or QWERTY.
- Don't share passwords with other people. If they need access to data they should be given their own login.
- Don't leave passwords lying around in notebooks, or on sticky notes close to your computer, or in files on your computer where they can easily be read.
- Before you enter a password into a website, make sure it is using a secure connection beginning with https:// (it might also show a small padlock close to the address) this means the site is using a secure link that cannot be intercepted by attackers.
- When you register with some online services they will send you a password so that you can log in. Many sites force you to change the password when you first log in, if they don't, change it when you first visit the site.
- If possible, change the default password on devices such as your internet router. This is programmed at the factory and some companies have a single password for all their devices. An attacker only needs to know the make of your router to gain access.

- If you have trouble remembering passwords try a password manager program that not only stores passwords, but can generate new, highly complex passwords for you.
- Two-factor authentication gives you additional protection as it requires two pieces of information (such as a password and a random number sent by SMS) to provide access to your data. If a company offers two-factor authentication, you should use it.

In the next section you'll get to test the strength of your passwords.

2.2 Checking the strength of a password

Figure 5

View description - Figure 5

So you've learned to pick strong passwords that are easier to remember, to use different passwords for different organisations and to change them periodically.

When you create a new password you will sometimes see an indication of how weak or strong a password is. There are also apps that can help us to create and manage our passwords. We will look at these a little bit later, but let us start by getting some understanding of how to measure the strength of a password.

Construct an example password using the place name of the city, town or village where you live using only lower case letters – no capitals, spaces, dashes, and so on.

Test it using the password strength checker on the OpenLearn site and make a note of the score. Open the link in a new window so that you can refer back to it as you continue with this section. If you live in a place with a short name such as Ayr, just repeat the name a few times until you have met the minimum length requirement for the password checker.

Modify it into a very strong password using the technique for converting a phrase into a password that you learned earlier.

Think about why the security of the two passwords was different and what makes a very strong password. Things to consider include:

- password length
- the range of characters you used
- whether any personal information is recognisable in your passwords (and could be guessed)
- how easy or difficult it is for you to remember the new password.

2.3 Password managers

Figure 6

View description - Figure 6

While it is possible to create your own strong passwords, it can sometimes be difficult to remember each one, especially if you use a number of online services.

A password manager is an application running on your computer that stores passwords for you. Very simple password managers allow stored passwords to be copied and pasted into login boxes. More sophisticated managers let users launch and log in to an application or website by clicking on their entry in the manager itself, while some password managers include browser ‘plug-ins’ so that you can complete a login on a web page simply by pressing a button.

The majority of password managers also offer password generation facilities. Since computers can remember arbitrarily long pieces of nonsense text, say MHpKQCvpYoouTAaPiiWuFKjpNe7qnsbwkrvq3s3cX, password

managers have no problems with creating passwords that are highly resistant to both brute force and dictionary attacks. Since a password manager contains a great deal of extremely valuable information it represents an attractive target for an attacker. Before choosing a manager you should check that:

- The password manager itself requires a password to use it. This prevents an attacker simply starting the password manager and accessing your passwords.
- The password manager should lock itself after a period of inactivity. This stops an attacker accessing the passwords if you have previously used the password manager and then left your machine unattended.
- The passwords themselves should be encrypted on your computer. This prevents an attacker reading your passwords without needing to open the password manager.

Most modern web browsers offer to remember passwords when you enter them into web forms, providing password management for websites you visit using the browser. This can be very convenient for frequently visited sites where you regularly have to enter details. The security of this password storage is strong and your data will not be visible to casual inspection, but you should be **extremely** careful using them on any computer that you do not own or have sole control of, since your data will be stored on the machine and could be misused by another user or an administrator.

You should only consider using a browser’s password storage on a machine that you are the sole user of, or one where you entirely trust the other users. Under no circumstances should you store passwords in the browsers of public machines in places such as cafes, libraries and workplaces.

When using a password manager check that the password manager’s security functionality has been evaluated by a reputable independent organisation. Additionally, make sure you select a very strong password for controlling access to the password store. This will minimise the risk of attackers having access to your passwords, even if they do manage to steal the encrypted password store, either

from your machine or from online storage provided by the password manager software.

2.4 Installing and using a password manager

Figure 7

View description - Figure 7

Alternatives to a browser’s password management are dedicated password management applications.

Before choosing any product to manage your passwords, you should make sure that it meets your requirements – in particular:

- Is the software available for your computer?
- Does it manage passwords on one machine or more than one computer?
- Can it synchronise passwords between multiple machines?
- Does it have a good reputation?

Check that the password manager software has a good reputation by making sure that it has been evaluated by a reputable organisation. Don’t depend on anecdotal evidence.

Some examples of password manager applications are:

- LastPass is available for a range of operating systems, including mobile devices. It can generate and store passwords, and manage them across multiple devices.
- 1Password is available for Windows and Mac computers as well as mobile devices running iOS, Android and Windows Phone. As well as generating and storing passwords, 1Password can be used to hold other confidential documents. It offers password synchronisation through the free Dropbox cloud service where encrypted copies of all 1Password data are shared between your machines.
- KeePass is available for Windows, Mac and Linux operating systems. It is an open source password manager, which makes it easier for security experts to check its program code and identify potential security problems.

The protection offered by a password manager is only as good as the password you select to control access to it – the ‘master password’. Therefore, make sure to select a long, hard to guess password – ideally a phrase or combination of random words. This will prevent attackers from getting access to all of your passwords, even if they steal the password store from your machine or an online password system. For example, in June 2015 attackers were able to steal a large number of password stores from LastPass, putting those users with very weak master passwords at risk of having all their passwords used by hackers.

2.5 Alternatives to using password managers

Figure 8

View description - Figure 8

Using a password manager makes your life much simpler because, rather than having to remember a multitude of passwords, you only need to remember a single password and the computer does the rest.

But what if you forget that password? All of a sudden all of your passwords are unavailable. And what if your password manager's data file falls into the wrong hands? You'd better hope your password is strong, otherwise all of your passwords are accessible to an attacker. But, what are the alternatives?

For an increasing number of websites it is possible to use your existing online accounts, such those provided by Google or Facebook, to register and log in. This approach for managing users'

account details depends on an authentication mechanism called OAuth (i.e. Open Authentication).

This method of checking a user's identity requires the website to ask the user's computer for some proof that the user's identity has been authenticated by the OAuth provider (e.g., Google). This requires the user's computer to first contact the OAuth provider where the user can input their username and password. The OAuth provider provides a digitally signed token that confirms the user's identity.

You will learn more about digital signatures in Week 5 of the course, but for now it is sufficient to understand that in this case the digitally signed token cannot be created or modified by anyone other than the OAuth provider. Once it receives the token all the website needs to do is to check that the signature on this token is valid to confirm the identify of the user.

So using OAuth can simplify your password management because all you need to remember is the username and password for your account with the OAuth provider. However, just as with password managers, if you forget this password you will no longer have access to any of the accounts. Additionally, if an attacker gets access to this password, they will be able to access all the online systems you are able to access using your OAuth account details.

So while password managers and online authentication services like OAuth can simplify the management of your online accounts, they are not complete solutions. Next, we will look at another way of improving the security of the authentication mechanisms we use.

3 Two-factor authentication

Figure 9

View description - Figure 9

So, if a password isn't secure enough, perhaps having two pieces of information is more secure? This is known as two-factor authentication and you've almost certainly used it without realising.

When you take money out of an ATM you have to give the bank two pieces of information – the first is the data stored on your bank card, the second is the PIN. Individually, neither can access your account, but when brought together they allow you to withdraw money.

Some banks have given similar two-factor authentication to online banking customers – in this case accounts need to be unlocked with the combination of a password and a four or six digit number generated on a hardware security token. If you use online banking and don't have a hardware token it will be well worth finding out if your bank offers them to customers, and if they do not, consider switching to a more secure banking service.

Hardware security tokens

These devices contain a clock and a number generator which creates a new one-time password every minute or so. The bank synchronises the token with a master computer before issuing it to customers so the token and the master computer generate new passwords in time with one another. When the user is asked to enter the one-time password into their browser, they press a button on the token and enter the four or six digit number shown on the screen. The master computer will have also generated the same number. The two values are compared, and if they match, the user is allowed into their account.

Two-factor authentication on the web

A number of companies, including Apple, eBay, Google and Microsoft support two-factor authentication to improve the security for their web users. Rather than a single password, two-factor authentication requires the user to enter two pieces of information – their password and a changing value which is either sent by the website to their mobile phone, or generated by a companion application on the user's own computer.

Depending on the site, it might be necessary to enter the two values every time (which is inconvenient), or after a period of inactivity, or it may be possible to tell the site that the computer which has already been authenticated should be trusted in future and a single password will be sufficient to allow you to use the site (although this raises a security weakness if the machine should be stolen).

Another place where you might have come across two-factor authentication is if you've ever connected to a virtual private network (VPN), which is a type of encrypted network connection. (You will cover VPNs in more detail in Week 5.)

The organisation that owns the network you are connecting to will give you a card or device, often called a VPN token, that can be used to generate a sequence of random characters. When you try to connect to the VPN, you will first be asked for your password (the secret based on something you know) and then will be challenged to provide some information from the VPN token (the secret based on something you have).

3.1 Setting up two-factor authentication

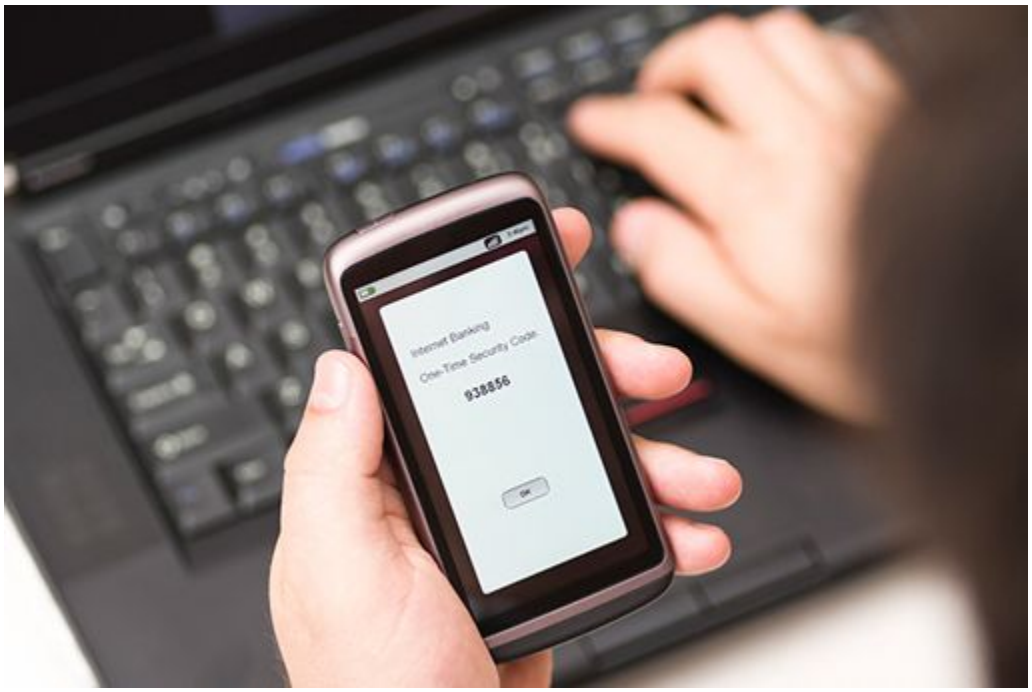


Figure 10

View description - Figure 10

Two-factor authentication is available on many websites such as Google and Facebook and it’s very easy to set up. Follow the instructions to add two-factor authentication to your accounts.

Two-factor authentication on Google

If you have a Google account it is a good idea to set up two-factor authentication.

Google’s two-factor authentication sends authentication codes to your mobile phone. You will need a phone that only you have access to, as otherwise someone who has stolen your details could use it to gain access to your Google account.

You can find out more at Google's 2-Step page and set it up using the following instructions.

- Log into your Google account using your usual username and password.
- Click your profile picture then click 'Account' to take you to your settings page.
- Enter your phone number, choose SMS or voice calls.
- Go to the 'Security' tab.
- In the 'Password' box click to setup 2-step verification.
- Click **Send code.**
- Google will send a six figure authentication code, enter it into the box.
- Google will ask if you want to trust the current computer so it doesn't require two-factor authentication again. Only click this box if you are the only user of this computer, or if it is secured. Click **Next.**
- Google will let you amend the list of trusted computers from your user account. You can also change your phone number from the account settings.
- Click **Confirm** to finish.
- You might also want to add a backup phone number in the event you lose, or are not with, your main mobile phone.
- Non-Google applications, running outside of the browser (such as mobile apps, email programs and instant messaging clients) require new, application specific, passwords to work with two-factor authentication. Google will prompt you to create them now. Enter the new passwords into your applications, following Google's instructions.

Two-factor authentication on Facebook

Facebook also supports two-factor authentication (which it calls Log in Approvals). Facebook's two-factor authentication process is activated whenever you log in from a new computer. An SMS is sent to your phone containing a unique security code, which you will need to enter into Facebook before you can log in.

Set it up using following the instructions:

1. Log into Facebook with your normal username and password.
2. On the top blue bar, click your **Timeline** button (it will contain your photo and name). Then click the **Update Info** button which appears near the right-hand side of the window.
3. Any phones registered with Facebook are listed in your ‘Contact Information’ details. If you don’t already have a mobile phone registered, you will need to register one now by clicking on the **Add Mobile** Phone button.

   Take care when completing your telephone number. There is an option (shown by a small padlock) which allows you to customise who has access to your phone number; Facebook has an option to make your number public, but we’d recommend choosing the ‘Only Me’ option from the menu.
4. Once your details have been registered, your number will be listed in your ‘Contact Information’. You still need to verify your telephone number, click the **Verify** link next to your mobile phone number, then choosing how Facebook will send you the verification code.

   If you choose to receive it by text you will get an SMS, otherwise you can opt to receive an automated telephone call. In either case you will receive a six figure authentication code. You will need to enter this number back into Facebook and click Confirm to complete registration.
5. Return to the top blue bar and click the small downward pointing arrow at the top right of the window – this is Facebook’s main menu. Choose ‘Settings’ from the pop-up menu.
6. Choose ‘Security’ from the left-hand menu, then click the **Edit** button next to the ‘Log in Approvals’ options. Make sure the box labelled ‘Require a security code to access my account from unknown browsers’ is checked and follow the straightforward instructions. At the end of the process, Facebook will need to send you another SMS message to confirm that two-factor authentication has been activated.
7. You might want to take this opportunity to increase your security by having Facebook notify you if an attempt has been made to

access your account. Still on the ‘Security’ section, choose the ‘Log in Notifications’ **Edit** button.

8. Facebook offers to send you emails or text messages when your account is accessed from a previously unknown machine. These notifications will be triggered when you log in on a new machine, but also if someone else is using your account details to gain access. Choose which methods you want to use, then click the **Save Changes** button.

Other two-factor authentication services

As well as many online banking systems, other websites support two-factor authentication, most of which rely on SMS messages. Services include:

- **Apple**
- **Dropbox** – a cloud file sharing service
- **Evernote** – a cloud-based document and note taking service
- **Microsoft Accounts** – used by the Microsoft App Store and its OneDrive cloud storage service
- **PayPal** – online payments used by many small web retailers and eBay
- **Steam** – online game delivery
- **Twitter**

Look out for two-factor authentication on other websites. Set it up to better secure access to your data.

3.2 Other services supporting two-factor authentication

Figure 11

View description - Figure 11

You may be surprised at the range of services and products that provide two-factor authentication. You'll consider these in the next activity.

Activity 1 Two-factor authentication

Allow about 15 minutes

Consider the questions below and see what you can find out.

- Does your bank or credit card company use two-factor authentication, either online or via telephone banking? If so, what form does it take?

- What kind of two-factor authentication is used by shops that you use, either online or in the high street? One example is putting in the security code from the back of your credit card (the last three digits) to prove that you have the card in your possession.
- Can you find examples connected with your work, for example to access the company VPN or different areas of the building?

Write a short comment about the type of methods and devices you came across that offer two-factor authentication in the space below. Then discuss the questions with colleages and add to your notes any other methods and devices you have learned about.

Provide your answer...

Next, you will have an opportunity to review your learning in the end-of-week practice test.

4 Week 2 quiz

This quiz allows you to test and apply your knowledge of the material in Week 2.

Complete the Week 2 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 2

Figure 12

View description - Figure 12

This week you explored how authentication works and the role of passwords in the operation of authentication mechanisms.

You learned how weak passwords could threaten the security of digital information and your online identity. You also learned about different ways of improving your password security, including techniques for coming up with strong passwords, using password managers and two-factor authentication.

Of course attacking passwords are not the only way that attackers can gain access to systems. They can also exploit vulnerabilities in software, making it important that you keep systems up to date with the latest security fixes/patches. Attackers might also try to execute malicious software, ‘malware’, on your systems. These topics will be covered in the week ahead.

You can now go to Week 3: Malware.

Week 3: Malware

Introduction

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Video content is not available in this format.

View transcript - Uncaptioned interactive content

The two biggest threats to consumers online are malware and phishing. Cory introduces you to malware, which is the focus of this week.

Malware is the collective name for software that has been designed to disrupt or damage data, software or hardware. There are several types of malware, such as viruses, worms and Trojans, which you'll learn more about in the next few sections.

However, as malware has evolved from its beginnings as demonstrations of prowess by individual programmers to sophisticated technologies developed by organised crime, the boundaries between the different categories are beginning to blur.

1 Viruses

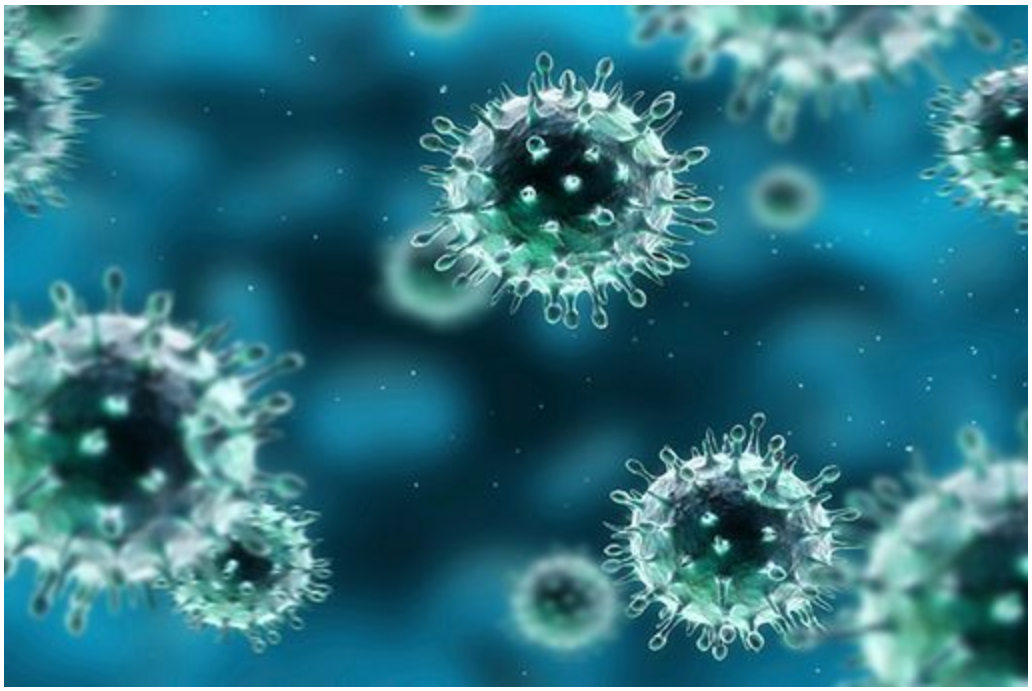


Figure 1

View description - Figure 1

The best-known type of malware is probably the virus; although many pieces of malware are called viruses, they are nothing of the sort.

A virus is a piece of software that has been written to insert copies of itself into applications and data and onto crucial parts of a computer’s hard disk. Viruses are said to be self-replicating programs and date back as far as the early 1970s, but they only became well known with the advent of microcomputers and later, the internet.

Viruses attach themselves to specific applications on a computer and are activated when the program is first run. At that point, the virus may make a copy of itself on the hard disk and continue to run, or it may only run each time the application is used. Early viruses, relying on floppy disks for transmission, spread quickly as infected

data disks were shared around an office, or pirated software was passed around a playground. Nowadays, viruses rely on devices such as flash memory cards or are transmitted through internet connections.

Although some viruses are not intended to cause harm, the majority of these programs are designed to harm users, by corrupting their data or attacking the operating system itself or providing an exploitable ‘back door’, giving attackers access to the computer. Even where no harm is intended, viruses consume memory, disk space and processing power.

1.1 Worms

Figure 2

View description - Figure 2

Another type of self-replicating malware is the worm; like a virus it is designed to make copies of itself, but unlike a virus, a worm is a standalone application.

Worms spread through network connections, accessing uninfected machines and then hijacking their resources to transmit yet more copies across the network.

There are four stages in a worm attack:

1. The first stage is when the worm probes other machines looking for a vulnerability that can be exploited to copy itself to.
2. The second stage is to penetrate the vulnerable machine by performing the operations for exploiting the vulnerability. For example, the worm might detect an open network connection,

through which it can get the remote machine to execute arbitrary instructions.
3. In the third stage, the worm will download itself to the remote machine, and store itself there. This is often called the ‘persist’ stage.
4. In the final stage, the worm will propagate itself by picking new machines to attempt to probe.

Worms were invented as a curiosity and have even been suggested as ways of testing networks or distributing software patches across a network; however their drawbacks far outweigh their benefits. Even the most ‘benign’ worm consumes resources and can affect the performance of a computer system.

1.2 Trojans

Figure 3

View description - Figure 3

The final major type of malware is the Trojan (or Trojan horse) – named after the wooden horse that supposedly smuggled Greek soldiers into the ancient city of Troy.

A Trojan disguises itself as an entirely legitimate program (such as a screensaver), but behind the scenes it is causing damage – perhaps allowing someone else to gain control of the computer, copying personal information, deleting information, monitoring keystrokes, or using email software to pass itself on to other computers. Unlike viruses and worms, Trojans are not self-replicating − they rely on their apparent usefulness to spread between computers.

Some Trojans work in isolation. Some, however, rely on networks, either to transmit stolen information – such as passwords, bank account details or credit card numbers – or to act as back doors to compromised computers. They allow attackers to bypass the

operating system’s security features and gain access to data or even control the machine over a network.

1.3 Defining terms

Figure 4

View description - Figure 4

In addition to the types of malware described in the previous sections, ‘Adware’, that forces users to view advertising, and ‘Spyware’, malware that attempts to access personal information and user passwords, are other examples you may have heard about.

From the Sophos Threatsaurus PDF, look for a term that you have not come across before.

Try to think of a way to define the term in your own words.

You could also look at examples or information from the sources recommended in Week 1, Section 2.2, How to keep up to date.

2 How malware gets into your computer

Figure 5

View description - Figure 5

Malware can get into a computer through a variety of mechanisms, most of which involve exploiting a combination of human and technical factors.

For example, a malware creator might get you to download their malware by putting a link in an email, or attaching the malware to an email. Alternatively, malware might be packaged with illegal copies of standard software so that it can get into the machines of people who choose to use these illegal copies rather than pay for the genuine versions.

However, before looking in detail at how malware gets into your computer, it’s worth thinking about why it does. What is malware for?

2.1 What is malware for?

Figure 6

View description - Figure 6

There are many reasons why malware is created including intellectual curiosity, financial gain or corporate espionage.

Many programmers thrive on the challenge of seeing what is possible, and set out to create a malware program even if they do not intend to do harm. Perhaps the most famous of these experiments was the 1988 Morris Worm – the first worm to spread over the internet. The supposed intent of this worm was to gauge the number of machines connected to the network. However, the result was to slow down the operation of infected machines to the point of being unusable.

Worms continue to represent a major threat, as shown by the case of the Conficker Worm of 2008.

Case study: Conficker

In 2008, Microsoft Windows computers began being infected by an advanced worm called Conficker, which spread when users shared files, either over networks or via USB flash memory drives. The malware disabled important security features, such as antivirus software and automated update systems and blocked users from downloading fixes. At the same time, Conficker would exploit a weakness in Microsoft's server software to infect computers on the same network.

Conficker became the fastest-spreading malware known then, eventually being found in almost every country. Conficker outbreaks were reported from (among others) the armed forces of the UK, France and Germany, as well as the British House of Commons and UK police forces. In the US, Conficker's impact was sufficiently serious that the Department of Homeland Security set up a Conficker Working Group of security experts tasked with creating strategies that could be used against similar outbreaks in the future.

Conficker's authors were clearly not amateurs. They released new variants of Conficker on a regular basis to overcome weaknesses in the original malware and took steps, (including using digital signatures), to ensure that no one else could hijack their program.

Although Conficker caused a great deal of nuisance, it did not appear to do any actual harm to data, however, the program could have delivered other malware that would have attacked users. In many ways, Conficker was a harbinger of the advanced criminal malware – such as Cryptolocker – that is a major threat to today's users.

2.2 Phishing

Figure 7

View description - Figure 7

Phishing is any attempt by attackers to steal valuable information by pretending to be a trustworthy party – a form of social engineering attack.

So an attacker might impersonate a bank to obtain credit card numbers or bank account details. It gets its name from ‘fishing’ – as in ‘fishing for information’, the process of luring people to disclose confidential information.

Phishing relies on people trusting official looking messages, or conversations with apparently authoritative individuals, as being genuine. It is widespread and it can be enormously costly to people who find their bank accounts emptied, credit references destroyed or lose personal or sensitive information.

Email phishing

The use of electronic technologies to perform phishing attacks was described in the late 1980s, but the term did not become commonplace until the mid 1990s when a program called AOHell allowed AOL users to impersonate other people (including the founder of AOL itself).

Phishing became increasingly common as more and more people connected for the first time and began receiving official looking messages that looked very much like those sent out by genuine organisations such as banks, stores and government departments. What most of these users did not realise was that not only could email addresses be faked, but that electronic data can be easily copied – just because an email claims to come from your bank and has your bank's logo doesn't mean that it is genuine.

Phishing emails may be indiscriminate. A phisher will create an email asking the user to get in touch with a bank or credit card company claiming that there is a problem with the account or that the bank may have lost some money. These sorts of messages make people justifiably worried and more likely to follow the instruction. The phisher will then include some plausible looking details such as the bank's logo and address and then send it to millions of individuals. Among all the recipients, a few people will have accounts with that bank and will click the link in the message, or telephone a number, which will begin the process of eliciting further personal information.

What to do

If you do receive an email that worries you from an organisation such as a bank or shop that you use, do not click on or follow the links in the message. Get in touch with their customer services department, or log in to your account through their website. Type in their web address or use the address in your list of favourite sites, or use their published phone number. Most organisations will have a published policy of not asking for sensitive information such as your password

through email or over the phone so you should be suspicious of anything that contravenes this policy.

Social media phishing

Although email still accounts for the majority of phishing attacks, the technique is also used in social media sites as well as in text messages. The same rules apply – if in doubt, go to the official site and make contact with the company through their published links.

As we saw in the first week of the course, phishing can sometimes be targeted at individuals or specific parts of an organisation. These attacks, commonly called a ‘spear phishing attack’, will depend on detailed information about the target. For example, an attacker might use information gleaned from recent emails to craft a plausible reply that appears to come from colleagues of the targeted user.

Attackers may also include links to malware-infected software in personal messages posted in social media. This is especially common after major disasters or during fast-breaking news when people are likely to click on interesting looking links without thinking carefully.

2.3 Trapping phishing emails

Figure 8

View description - Figure 8

Phishing is just one type of spam email which clutters our mailboxes and often delivers unsuitable or even illegal content to individuals.

Spam

Spam is yet another consequence of the early internet being developed by people who trusted one another. Just as we have had to protect computer networks against hackers – which you'll cover in Week 6 – as more and more people have accessed the internet, email has become a tool that anyone can use for good or bad.

Most internet email is moved around the world using the Simple Mail Transfer Protocol (SMTP) which defines a standard template of commands and formatting that allow different mail programs, on a huge range of computers, to understand one another. Protocols are used to specify a set of special messages that should be exchanged between computers to achieve a particular functionality, in this case the delivery of email.

SMTP was defined when the internet had only a tiny number of users, so the original specification did not include any way for computers to authenticate one another, i.e. there was no way of knowing if the message claiming to come from TrustedBank actually came from TrustedBank's computers. This weakness was addressed in a later extension to SMTP called SMTP-AUTH, but crucially it was not required, and so almost all mail servers still accept unauthenticated messages.

Spoofing

Spammers can attack a mail system by changing the information stored in email 'envelopes' which enclose the messages themselves. This is known as 'spoofing' and allows a spammer to disguise their actual address by writing new addresses for the sender (such as replacing their own address with that of TrustedBank) and the destination for receipts. Since SMTP servers do not perform any authentication, they simply pass on the email without checking that it was sent out by TrustedBank.

Simple spoofing is now being challenged by technologies that allow genuine senders to authenticate messages which can be checked by the recipient's mail server, however only about half of all mailboxes have any protection against spoofing.

Provided a spammer has access to a fast network (or increasingly to a botnet), spam costs the sender almost nothing and although only a tiny fraction of users will respond to a spam message, sufficiently vast numbers of emails are sent that the rewards far outweigh the costs. It has been estimated that seven TRILLION spam messages, making up more than 85% of all email, were sent during 2011 alone.

Such is the torrent of spam that internet service providers and companies have to buy far more bandwidth and storage than they will ever need for legitimate purposes.

2.4 Spotting a phishing email

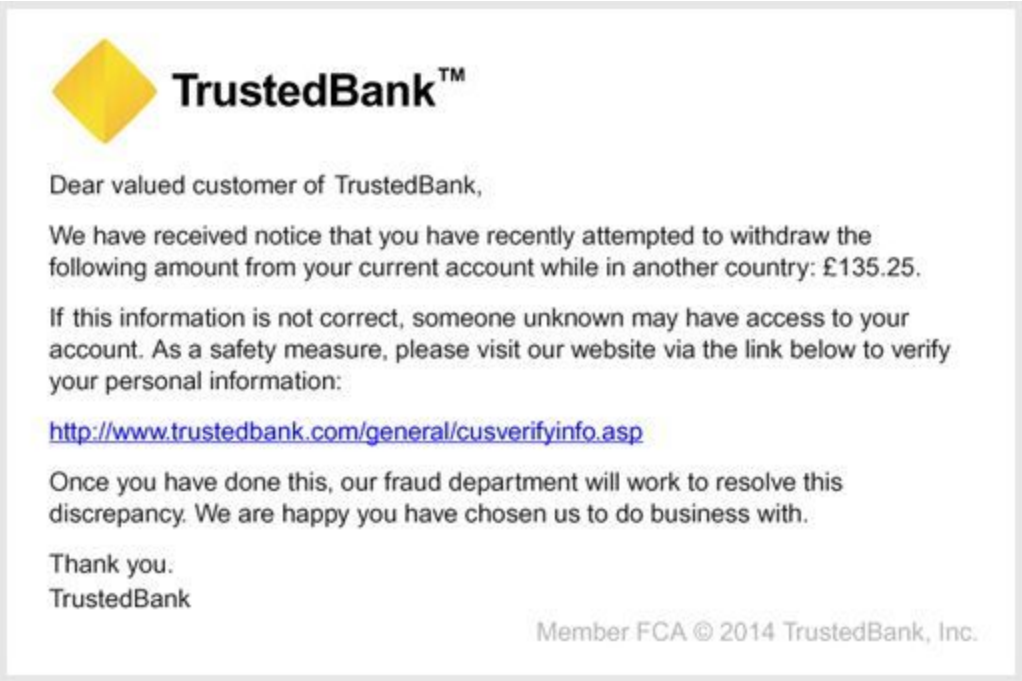


Figure 9

View description - Figure 9

Although a phishing attack may appear plausible at first glance, there are some tell-tale signs that should make you very cautious about clicking on any links or giving any personal information to the supposed sender.

Read through the points below to find out what to look out for.

- **Spelling mistakes**: Most English-language phishing expeditions are sent from countries where English is not the primary language. Attackers often give themselves away by imprecise use of English, even with quite common phrases, and including spelling errors. So read the message carefully.
- **Who is it to?** Many, but not all phishing attacks do not use your name in the introduction – preferring ‘Dear valued customer,’ or ‘Dear user,’. This is because they cannot personalise the emails

sufficiently. Your bank or online store can do this and should address you as ‘Dear Bob,’ or ‘Dear Mrs Jones,’ (or whatever your name is).

- **Poor quality images**: Sometimes, the images used in the emails are fuzzy, or your information may appear as an image rather than type. These images have been copied from screens and would not be used by original companies. It is easy to obtain images every bit as good as the originals though, so a high quality image should not persuade you the message is genuine.
- **Content of the email**: In almost all countries, banks and other financial bodies will not email you to tell you about problems with your account. They recognise that email is fundamentally insecure and that personal information should not be sent by email. So, even the method of communication will give you a clue about whether it’s genuine. The email may give a false sense of urgency, claiming that your account is at risk if you do not act quickly. This is not the case.
- **Links**: The text of a web link is not the same as the destination of the link itself – the link might say it is taking you to, for example http://www.trustedbank.com, but in fact it can take you anywhere on the web – including to a phisher’s computer impersonating that of a reputable company. You can easily spot a fake link by hovering your mouse pointer over the link – but do not click the button. The actual destination of the link will appear at the bottom of the window or in a small floating window next to the link. In a phishing email, the link will probably be to an address you aren’t familiar with.

The example message below claims to come from a fictional site called ePay and is about unauthorised activity on the account. The link says it goes to ePay’s site, but the address is slightly different and is unlikely to be owned by ePay.

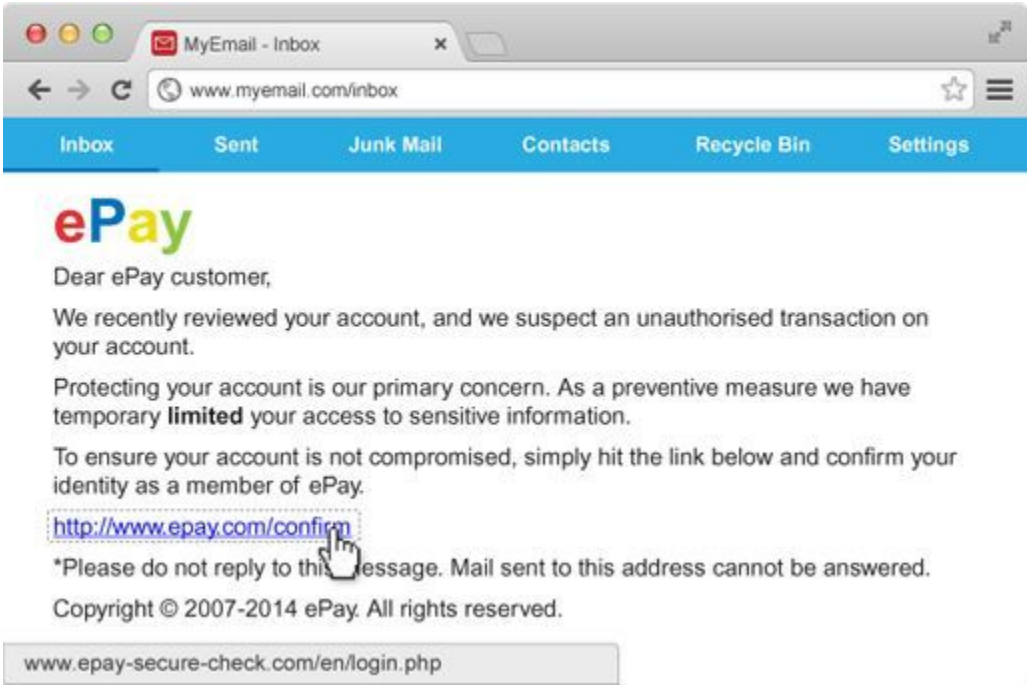


Figure 10 A phishing email claiming to come from the fictional ePay site

So the rules are to be suspicious and to look at the details of the message, the language, the quality of the images and where the links actually take you. Banks and shops will always prefer you to call them and check rather than risking your security.

2.5 Emails are not the only phish

Figure 11

View description - Figure 11

Please don’t think that malware is spread solely through email. Malware will be spread through any means possible.

Malware can be distributed by including it with pirated material such as illegal copies of software, video games and movies. Malware can also be installed on your computer by clicking links on websites – especially sites that distribute illegal copies of software, videos and pornography – or by annoying pop-up windows that claim to have identified problems with your computer (quick tip – they probably haven’t! But it’s a great prompt to run your antivirus software and remind yourself what a genuine alert looks like on your computer).

A recent trend is for malware to be spread through social networking services, like Cory’s experience of the direct message on Twitter that you heard about in Week 1. Once it is on a machine running social networking software, the malware masquerades as the real user and

posts messages containing links to sites that distribute yet more malware.

Once again, this type of malware relies on social engineering to multiply – users of social networks are highly likely to click on links they think have come from friends and spread the infection. Most of these social networking infections have exploited weaknesses in client software rather than the web versions of the networks, so it is important to keep social networking client software, such as the Facebook App for mobile devices, up to date.

2.6 The role of malware in click fraud

Figure 12

View description - Figure 12

The majority of modern malware has been designed with malicious intent; to cause damage to a computer's operating system or its data, or to steal information from a user, or increasingly, from online advertisers.

As you will have seen, many large websites rely on advertising for their revenue. The amount of money spent on online advertising is growing rapidly with more than $32 billion spent in the US alone during 2011. Advertisers like online advertising because it can be relatively cheap compared to a printed advertisement and because software allows for individuals to be targeted with specific adverts for products they are likely to buy.

The most common type of advertising is 'pay per click' where advertisers only pay the owners of a site when a user clicks on an advert. This system can be subverted by either generating clicks that

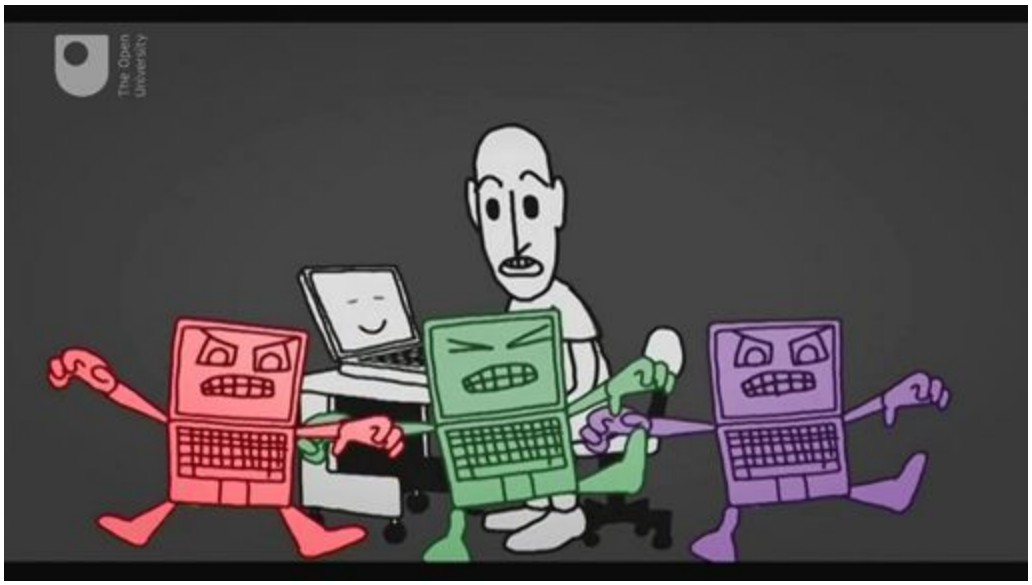
don’t come from genuine customers, or by hijacking a click intended for a genuine advertiser. This is known as click fraud, it accounts for more than 20% of all clicks and it can be aided by malware. Computers all around the world, operating as a botnet, can generate false clicks, siphoning money from advertisers through multiple layers of publishers and redistributors to hide its eventual destination.

While an individual click will only raise a tiny amount of money, done millions of times, click fraud can raise serious amounts of money. In 2011, the FBI broke a click fraud operation based in Estonia that had infected more than four million computers in 100 countries and stolen in excess of $14 million from advertisers.

2.7 Botnets

Video content is not available in this format.

View transcript - Uncaptioned interactive content



You heard about botnets briefly in Week 1, when we said that botnets are created using malware that give an attacker control over a group of computers and commonly use them to gather information from the computers (e.g., usernames and passwords), launch attacks against others. These attacks might be sending spam emails, or flooding a website with so many requests for content that the server cannot cope, which is known as a denial-of-service attack.

A single piece of malware can cause enormous damage, but when thousands, or even millions of computers run the same program, their effects can be devastating. So a botnet is a group of computers that coordinate their activity over the internet. There are a number of harmless botnets used for such purposes as the Internet Relay Chat (IRC) text messaging program, but the vast majority are created by malware.

Botnets spread through viruses and worms and once installed on the victim's computer they use the internet to make contact with a control computer. At this point, the infected computer (often called a zombie) will do nothing more except periodically check for instructions from the control computer. Over time, more and more computers are recruited to the incipient botnet until it may contain tens of thousands of zombies, but they don't raise suspicion as they appear to be doing nothing.

At some point in the future, the control computer will issue a command for the botnet to wake up and begin doing something. Often the people who created the botnet itself have either sold or rented the botnet to another group who want to use its capabilities.

Botnets have been used to flood the internet with spam messages, to commit fraud against advertisers and to perform so-called distributed denial-of-service attacks on companies and governments. Botnets are so large, and so widely distributed across the internet that they can be very hard to tackle and the effects of a coordinated attack on critical parts of the network can mean even very large websites struggle to remain online while the botnet targets their computers.

2.8 Confessional

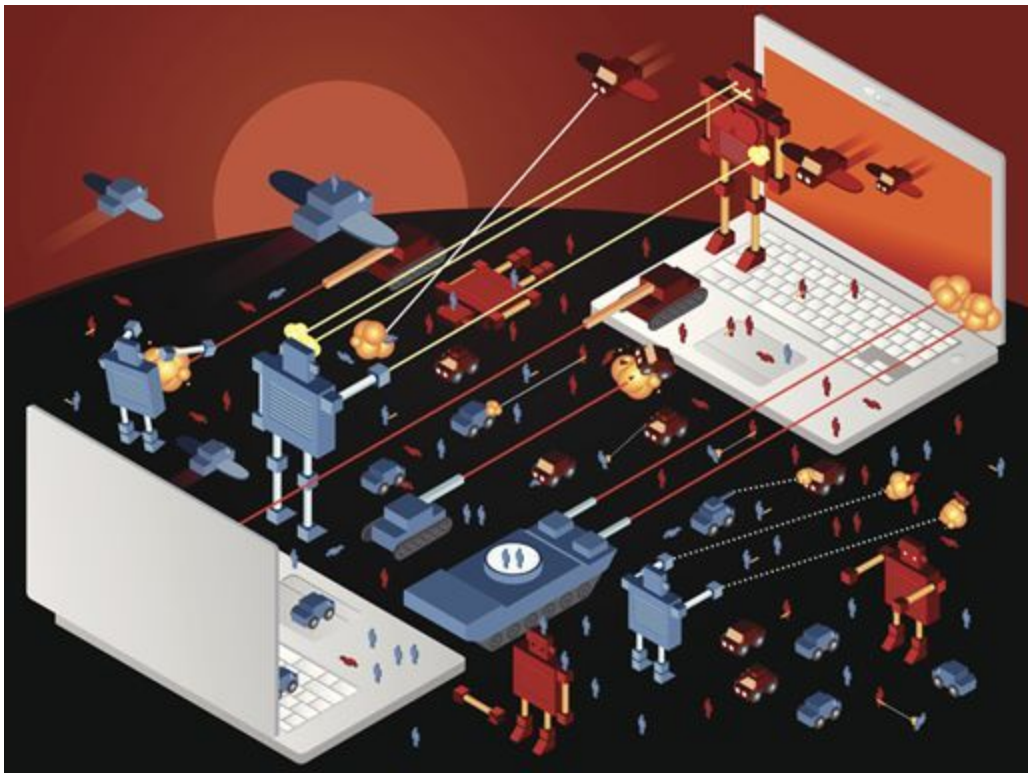


Figure 13

View description - Figure 13

It’s time to confess! Think about the following:

- Has your computer ever been infected with malware?
- Do you know the name of the malware that was involved?
- Was it a virus, worm or Trojan?
- What happened, and what were the consequences?

If you discuss this with others, remember not to share any personal information including the name of the company you work for.

3 Keeping yourself protected

Figure 14

View description - Figure 14

The growth in malware has been accompanied by an explosive growth in software designed to prevent it spreading.

So-called antivirus software (which actually targets a range of malware) is a multi-billion pound business with a large number of commercial and free packages available for all computer users ranging from individuals to large corporations.

At the same time, the developers of computer operating systems are incorporating a wider range of security features that try to stop malware running at all.

And there is a lot you can do yourself to keep yourself protected such as installing antivirus software, keeping your software up to date, looking out for the signs of phishing emails and implementing new security developments.

3.1 Antivirus software

Figure 15

View description - Figure 15

Antivirus software aims to detect, isolate and if necessary, delete malware on a computer before it can harm data. Antivirus software uses several techniques to identify malware – the two most common are known as signatures and heuristics.

Signatures

A malware's signature is a distinctive pattern of data either in memory or in a file. An antivirus program may contain thousands of signatures, but it can only detect malware for which a signature has been identified and published by the antivirus program's authors. As a result there is a period between a new piece of malware being released 'into the wild' and when its signature can be incorporated into antivirus products. During this period, the malware can propagate and attack unprotected systems, exploiting the so-called

‘zero day’ vulnerabilities that exist until the systems are fixed and antivirus signatures are updated. It is not uncommon for several variants of a malware program to be published at intervals, each sufficiently different that they possess different signatures.

A second weakness of signatures is that more sophisticated malware has the ability to change its program (it is said to be polymorphic or metamorphic), disguising itself without affecting its operation.

Heuristics

Complementing signatures, heuristics use rules to identify viruses based on previous experience of known viruses. Heuristic detection may execute suspicious programs in a virtual machine (a software recreation of a physical computer) and analyse the program for operations typical of known malware (such as replicating itself or attempting to overwrite key operating system files); or it might revert the program back to its original source code and look for malware-like instructions. If the heuristic analysis considers that the file acts in a malware-like manner, it is flagged as potentially dangerous.

Unlike signatures, heuristics do not require specific knowledge about individual types of malware – they can detect new malware, for which signatures do not exist, simply by their behaviour. The drawback of heuristics is that they can only draw conclusions based on past experience; radically new malware (which appears all too regularly) can pass unnoticed.

Issues with antivirus software

Although antivirus software is an essential part of protecting your computer, it is not a complete solution to malware problems.

Despite the best endeavours of its makers, antivirus software has occasionally proved to contain bugs with consequences like being inaccurate, failing to update itself or simply consuming huge amounts of computer power. Fortunately, these problems are rare,

easily fixed and much less serious than the risk from a malware attack.

3.2 Installing antivirus software

Figure 16

View description - Figure 16

If you don’t already have antivirus software on your computer, it should be a high priority to install some.

There are a number of good, free packages available but you should always check that it meets your needs before installing it. Some important features to consider are:

- **Is it compatible with your computer?** You will have to make sure the antivirus software is appropriate for the operating system and computer that you have.
- **Does it come from a reputable source?** For example, it may have been developed by one of the major computer security companies, such as Norton, Kaspersky, Sophos or AVG. Alternatively, it may have been provided or recommended by your bank or internet service provider.
- **Does it provide updates that allow it to protect you against the latest malware?** New malware is being developed all the time, and it is important that you use an anti-malware application that will update itself.

Use the above criteria to research antivirus products available so that you can choose the one that is best for you. If you already have an antivirus application, answer the questions for the program you have.

3.3 Keeping your software up to date

Figure 17

View description - Figure 17

Computer operating systems and application programs are so large that they inevitably contain bugs, some of which could compromise your security.

The majority of companies issue regular updates to their programs to fix known problems. Major operating systems and some application packages (such as Microsoft Office and the Adobe productivity suite) automate most of the process of updating software by automatically checking for updates, prompting the user to install them and then actually performing the update itself. This process is sometimes called ‘patching’.

Activity 1 Keeping your software up to date

Allow about 15 minutes

How do you go about keeping one of the software applications on your computer or device up to date? Reseach the application online to find out if there is any additional information about keeping it up to date.

3.4 End-of-life software

Figure 18

View description - Figure 18

Software is continually being developed and replaced by a new version. The lifespan of software begins when it is released and ends when it’s no longer supported and updated.

Software doesn’t become completely unsafe as soon as it reaches the end of its lifespan; in many cases you can continue to use it, but you should be aware that security risks may not be addressed by its authors. If you work for an employer, you may be required to move to an updated version of the software as part of their security management process.

The first effect you will feel from end-of-life software is that companies will cease telephone and internet support for queries. So if you have problems using a product you won’t get any help. The manufacturer may also withdraw bug reporting, so you won’t be able to tell them about problems. At the same time you might also find

that cheap upgrades to later versions of paid software are no longer available.

Most large software companies will continue to offer critical software support to obsolete products for a period of time. However, they will not prioritise these programs, instead they will concentrate on fixing problems in up to date software and releasing patches; only then testing older products to see if they are affected and if they can be fixed. This means that users of older products might be exposed to vulnerabilities for longer than those using more modern software. Developers of malicious software, who know about unpatched bugs in older products, are likely to attack these older, weaker programs in preference to more secure programs.

For example, Windows XP is now no longer supported by Microsoft (since April 2014), despite being widely used. In the chart below, you can see that Windows XP and Windows Vista, the two oldest operating systems, have much higher incidences of infection than the newer operating systems that feature much greater levels of security.

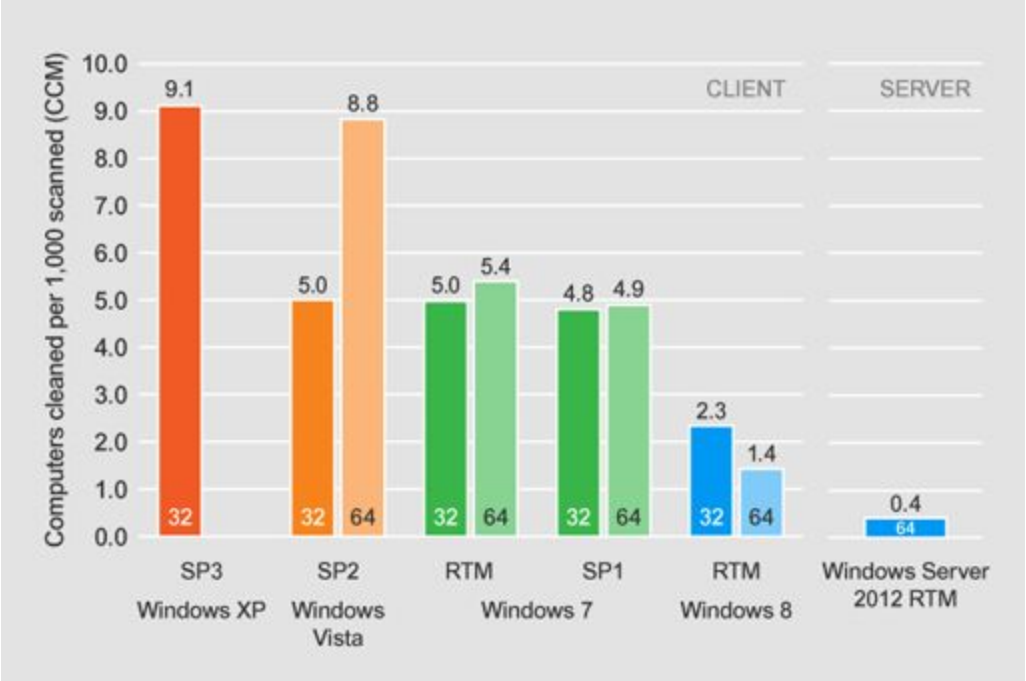


Figure 19 A chart showing infection rates per thousand computers of various versions of Microsoft Windows

If you are using end-of-life software, security applications such as up-to-date firewalls and antivirus software are essential as well as keeping up to date with key applications, such as web browsers and email programs which are used to send and receive personal data. Good information security will help keep you safe. Even if you take these precautions, you should begin planning for a transition to more modern applications. Upgrades are relatively cheap from one version to another (or even free), and any expense should be considered in the light of what you stand to lose if you do not use more secure software.

3.5 Sandboxes and code signing

Figure 20

View description - Figure 20

In addition to keeping software up to date and using antivirus products, there are other technological innovations that can help mitigate the threats of malware.

Sandboxes and code signing are examples of some of the technologies that developers are integrating into the software we commonly use to help protect our computers.

Sandboxes

A software sandbox is a way for computers to run programs in a controlled environment. The sandbox offers a constrained amount of memory and only allows very limited access to resources such as operating system files, disks and the network. In theory, the software cannot break out of the sandbox and affect other parts of the

computer, so even if malicious software attempts to overwrite parts of the disk, the sandbox will prevent it from doing so.

Sandboxing is widely used in modern web browsers, such as Internet Explorer 10 onwards, and Chrome, to prevent internet content causing damage to files on the computer. Similar sandboxes exist for most browser plugins and the Adobe Acrobat PDF viewer.

Code signing

Code signing is a use of cryptography where software companies issue digitally signed copies of their programs that can be checked by recipients for its authenticity. You'll discover more about digital signatures in Week 4.

Code signing is used by the designers of all three major operating systems (Microsoft Windows, Mac OS and Linux) to guarantee that operating system updates are genuine even if they are distributed using flash memory cards rather than directly from the publisher.

Microsoft Windows uses code signing on operating systems components, such as hardware drivers, which have direct access to the heart of the operating system. Apple has taken code signing even further. Versions of Mac OS from 10.8 onwards can restrict users to only running programs that have been certified by the Apple App Store. While this does offer greater security against malware, it may also restrict choice and prevent users from running certain unsigned apps from third parties.

Next, you have an opportunity to review what you've learned in the end-of-week practice test.

4 Week 3 quiz

This quiz allows you to test and apply your knowledge of the material in Week 3.

Complete the Week 3 practice quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 Summary of Week 3

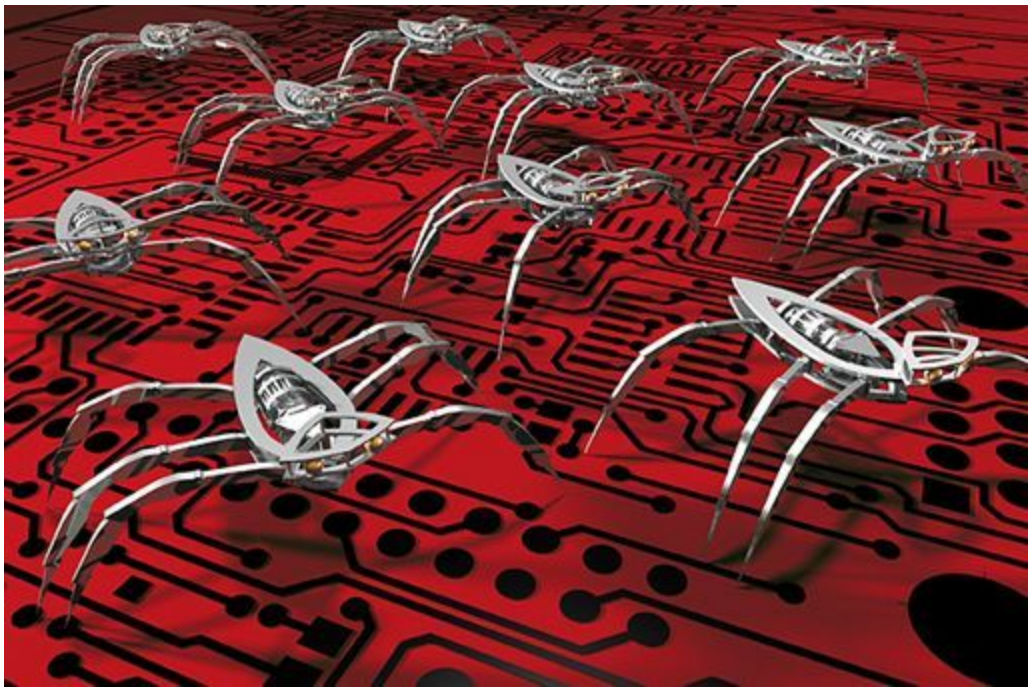


Figure 21

View description - Figure 21

You have also taken a closer look at ways of keeping attackers from impersonating you online or infecting your devices with malware.

In the next part of the course, you will delve a little deeper into the technologies that underpin information security, first focusing on how to protect the networks that we depend on for transmitting our digital information and accessing online services.

There is some optional further reading in the next section relating to some basic precautions you should take before you go online.

You can now go to Week 4: Networking and communications.

References

Microsoft (2012) ‘Microsoft Security Intelligence Report’, vol. 14, issue July – December, pp. 57, [online]. Available via http://download.microsoft.com/download/ E/0/F/E0F59BE7-E553-4888-9220-1C79CBD14B4F/Microsoft_Security_Intelligence_Report_Volume_14_Running_Unprotected_English.pdf (Accessed 6 June 2014).

Week 4: Networking and communications

Introduction

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Cory introduces the networking and communications topic.

You'll learn how data is transmitted across the networks, including wireless networks and understand the difference between the internet and the world wide web.

1 What is the internet?

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Figure 1

View description - Figure 1

The internet is not a single entity with a single owner; instead it comprises a hierarchy of individual networks that have been connected to one another. These networks range from local area networks (LANs) that can be found in many businesses and universities to the telephone and data networks that link cities and countries by fibre optic cables and satellite links.

A definition often used is that the internet is a network of networks. Before looking at the design of the internet in more detail, let’s hear

from Vinton Cerf, one of the engineers who was involved in the creation of one of the earliest computer networks:

Audio content is not available in this format.

View transcript - Uncaptioned interactive content

Two key factors in the design of the internet were:

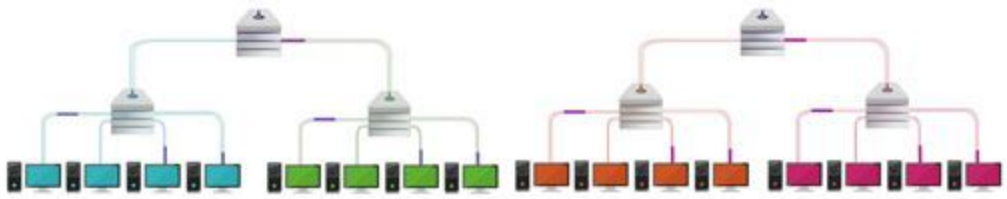
1. The network would not have a central controlling computer. Each computer on the network would be assumed to have the same authority as every other computer.
2. The network should be able to deliver information between any two computers on the network even if some of the machines in the network had failed (or given its Cold War origins, been blown to pieces). There would be a large number of alternative routes through the network, so it was not necessary for information to travel by the most direct route, instead it could travel in a roundabout route, avoiding the damaged parts of the network.

In the next section, you'll see how this works.

1.1 How data moves around the internet

Video content is not available in this format.

View transcript - Uncaptioned interactive content



The video explains how data is routed across a network of computers and how the internet is resilient to failures of individual computers, known as nodes of the network, or connections between computers, known as the links.

Instead of using a dedicated circuit for all of the information, internet traffic is split up and may take any number of routes through the network moving from its origin to the destination by a series of hops.

Note: Early in the above the video [2:05], an example packet is shown with destination address 6.7.8.104. However, there are subsequently two separate examples of different packets being routed. In the first example, the packet is being sent to a host on the local network, 1.2.3.104 and in the second example it is being sent to a remote host, 6.7.8.101.

1.2 Introducing the datagram

Figure 2

View description - Figure 2

When data, such as a picture, movie or a document is sent over the internet, it is not sent as a single chunk. Instead it is split up into small, uniformly sized blocks called ‘datagrams’, also sometimes called ‘packets’.

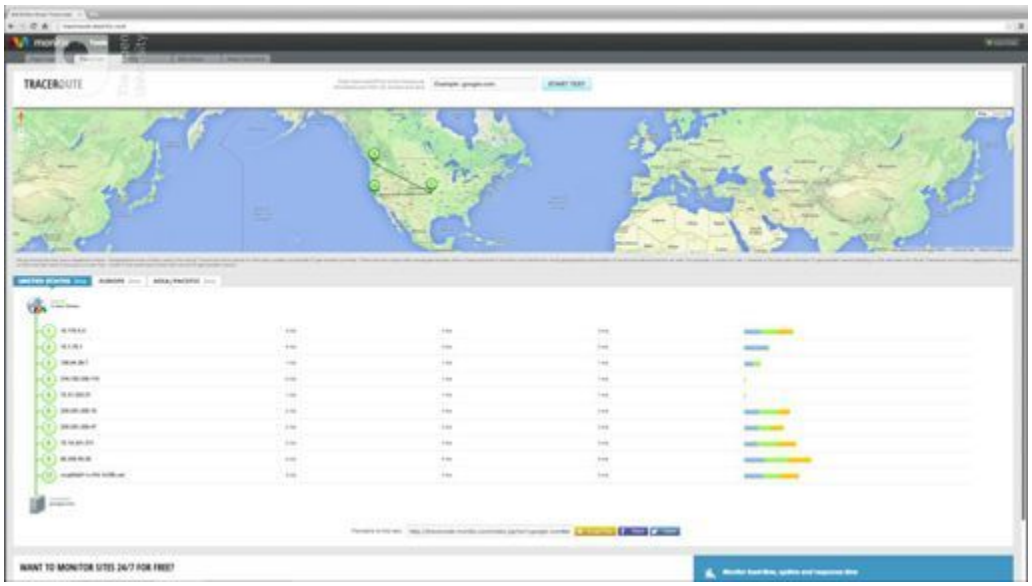
Imagine that you have a large book that you want to post to a friend, but you only have small envelopes. One way to post the book is to tear it into a number of pieces, placing each piece in a different envelope. Each envelope is addressed to the recipient. It makes sense to label each envelope with a number to tell your friend where the pages belong in the whole book. When the envelopes are put in the postal system they may all travel through the same sorting offices and arrive on the same day, or they might take different routes and arrive on different days. However, your friend should be able to recreate the book when they receive all the envelopes.

A number of different datagrams are used by data travelling over the internet, but they all have a similar structure. One envelope and its contents correspond to a single datagram. The envelope (which is called the ‘header’) contains the sender and recipient’s addresses, a unique number, a date stamp and some error correction information, while the contents (called the ‘payload’) contains the actual information being delivered.

1.3 Datagrams on the move

Video content is not available in this format.

View transcript - Uncaptioned interactive content



We have seen how, in theory, datagrams of information move around the internet. It's actually possible to see this in action, often with surprising results.

You've seen the route the datagrams took in the video, now try it yourself.

Activity 1 Datagrams

Allow about 15 minutes

Using Visual Trace Route, spend about 10 minutes exploring the routes to some of the following Australian organisations:

- the University of Sydney
- the Sydney Morning Herald newspaper.

Keep in mind that the route being shown by the Visual Trace Route tool starts from the location where the tool is running, not your local computer. However, you can look at the routes from different regions, USA, Europe and Asia/Pacific, by switching between the tabs.

Be warned! You might be surprised at what you find – information is not necessarily coming from where you might expect it to. Also, bear in mind that things change frequently when it comes to the internet; not only might the route be different if you look at the same destination at different times, but even the location where the information comes from might be different.

View discussion - Activity 1 Datagrams

1.4 Wireless networks

Figure 4

View description - Figure 4

Early computer networks depended on wires to move their data around the world, but engineers quickly realised that it would be useful to be able to use wireless (radio) connections.

Nowadays, wireless internet (abbreviated to wi-fi) is commonplace. If you have a laptop, tablet or smartphone, it probably has wi-fi access. Wi-fi is also being incorporated into an ever wider range of consumer goods including eBook readers, smart televisions, burglar and smoke alarms.

Wi-fi enables devices such as computers and printers to be connected together wirelessly to form a local area network (LAN). Instead of the signals going through cables and wires, they are sent through the air instead as radio waves.

The name ‘wi-fi’ refers in particular to wireless local area networking technology that is compliant with a particular family of standards maintained by the Institute of Electrical and Electronics Engineers (IEEE) and called the 802.11 family. You will see different variants of this standard on wireless routers, for example 802.11b, 802.11g and 802.11n.

In wireless LANs, the individual laptops, mobile phones and other devices, or nodes, are usually referred to as stations, acknowledging the fact that each communicating device acts as a radio station with a transmitter and a receiver.

In order to connect to a wi-fi network, a station needs to know the name of the network. This is also known as the service set identifier (or SSID) of the wireless LAN. The ‘service set’ referred to here is the set of wireless devices to be served by a particular wireless LAN.

The SSID allows the nodes on a wireless LAN to distinguish themselves from nodes on other wireless LANs that may be operating in the same physical space. For example, in many airports mobile phone companies provide free wireless LAN services to their customers and use the SSID to ensure that customers connect to the appropriate wi-fi network.

When you are trying to connect to an available network, you will see a list of SSIDs that are reachable from your device, some of these will have padlocks against them – more about what that means later.

2 Is your private information really private?

Video content is not available in this format.

View transcript - Uncaptioned interactive content

We all hope that the information we send wirelessly is private, but is that always the case?

Channel 4 News was able to learn personal information about unsuspecting people by intercepting their, supposedly private, but in reality completely public, wireless internet signals.

The attack shown in the video was possible because the hackers had set up their own wi-fi hotspot that either advertised the name of a common wireless hotspot provider, or the users chose to connect to a ‘free’ wi-fi network. The lesson here is to be careful about the public wi-fi networks you connect to, and the types of information you access using these networks.

2.1 Network security challenges

Figure 5

View description - Figure 5

Internet routers are designed to move datagrams to their destination but how secure are they?

They have been programmed with strategies to overcome problems such as congestion or the failure of a part of the network. These strategies involve re-routing datagrams via any alternative direction, as you saw from using Visual Trace Route. Therefore, it is impossible to state with any assurance which route will be taken by a datagram travelling outside a local network.

The datagram may travel directly, or, more probably, travel through several routers located anywhere in the world. These routers will most probably not belong to either the sender or the recipient, but a third party. In most cases this will not matter, but datagrams can be copied, and their security compromised, as they pass through a router without alerting either the sender or receiver.

The process is known as packet sniffing and it has many legitimate purposes including analysing network performance and for law enforcement, but packet sniffing software is readily available to anyone who chooses to use it. In the past, packet sniffing required a computer that was wired to the network, but wireless networking means this is no longer the case.

2.2 Encryption in wireless networking

Figure 6

View description - Figure 6

Since wireless networks transmit data over a medium that is shared by everyone, anyone with a compatible receiver or transceiver is able to eavesdrop on the radio signals being sent.

Ensuring that the eavesdropper is not able to convert these signals into the original message is a desirable security property of any wireless network, referred to as ensuring *confidentiality*. (This was one of the three security essentials we mentioned earlier, along with integrity and availability.)

Another security problem with using a shared medium for transmission is that malicious users could interpose themselves between a sender and a receiver and modify the messages being exchanged or even destroy them entirely. This is sometimes called a ‘man-in-the-middle attack’, and it compromises the *integrity* of the data being transmitted across the network.

Finally, an attacker could transmit lots of random data on the frequency being used by the wireless network, congesting the network and thus preventing other users from sending data. As we saw earlier in the course, this is called a ‘denial-of-service’ (DoS) attack and is an example of an attack on the *availability* of the network.

How encryption can help

So how do wireless networks address these potential security issues?

One commonly used security mechanism is **encryption**, which can help to ensure both the *confidentiality* and the *integrity* of data. The idea of encryption is to take the information you wish to protect and transform it into a different form, such that only the people who are supposed to receive the information are able to reverse the transformation and recover the original information. This is like having a key to unlock a door; only a person with the right key can open it.

Encryption can help ensure:

- **Confidentiality** – When a message is encrypted using a particular key, it can only be decrypted to recover the original information if the same key is used. This ensures that messages are confidential between the sender and the receiver.
- **Integrity** – Encryption can prevent messages from being modified without the receiver’s knowledge.
- **Authentication** – Encryption can contribute to the process of proving the identities of the sender and receiver.

You will look at encryption and decryption in more detail next week when we explain how cryptography works.

Encryption in wi-fi

Since wi-fi was first introduced, a number of security techniques have been used to protect wi-fi networks from unauthorised users

and to ensure that the data transmitted across them is secure. The most common methods are based on encryption, using a key known only to the nodes in the wireless network.

The first of these mechanisms was called Wired Equivalent Privacy (WEP), which (as the name suggests) aimed to provide confidentiality comparable to that of a wired network. Since 2001, a number of serious problems have been identified in WEP that allow the encryption key to be computed within a few minutes, using readily available software. Many wireless devices still support WEP to ensure compatibility with older equipment such as old modems, but wherever possible users should switch to a more modern form of encryption.

At the present time, the recommended security mechanism for wi-fi networks is Wi-fi Protected Access 2 (WPA2), which uses a more secure key to encrypt the transmitted data. This security mechanism has become the default configuration for wi-fi networks, and must be supported by all wi-fi devices in order for them to be compliant with the 802.11 standard.

In the next section you’ll consider how you might use wi-fi more securely.

2.3 Using wireless networking securely

Figure 7

View description - Figure 7

Use the network connection tool on your computer to identify how many wireless networks are within range of your current location.

How many of them use secure connections? If your home wireless network is not configured to use WPA2, find out how to set this up and make sure to do this. The user manual for your wireless router or your internet service provider's website should have information that will help.

Consider how you connect to the internet when you are on the move. Do you connect to your home wi-fi network, your mobile service provider, the free wi-fi in a coffee shop?

Go through the online services you identified in Week 1. Which ones would you choose not to access using public wireless networks?

3 Why we need standards on the internet

Figure 8

View description - Figure 8

As you've learned, when you send data over the internet it is sent across several hierarchies of networks, using different technologies from many different providers and operated by different organisations.

These networks must use a standard form of communication so information from one network can be passed across to another network.

To some extent, the way any one of these separate networks works internally is nobody's business but the owner and users of that network. However, where a network joins to other networks, where it becomes part of the internet, it has to conform to the standards of the internet.

The internet is not owned by a single organisation, so there is no one authority that dictates how it works. Yet all the different people and organisations with their own networks that together make up the internet have to work to common standards, or data would be unable to move between the different networks.

In the next section you'll find out about the TCP/IP protocols.

3.1 Introducing the TCP/IP protocols

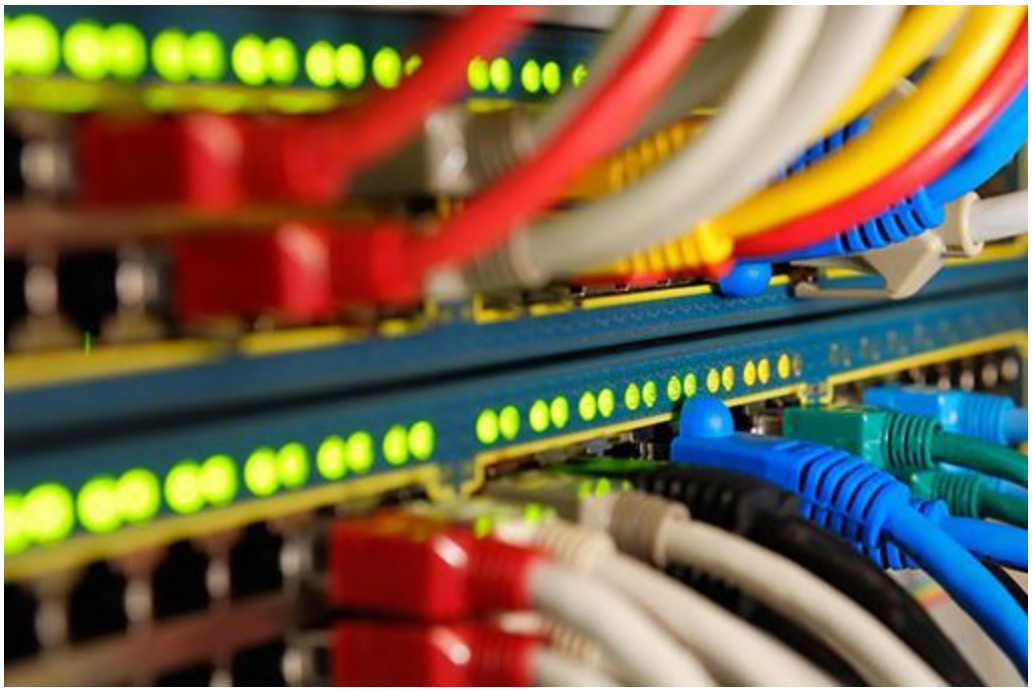


Figure 9

View description - Figure 9

The standards that allow different networks and differing communications equipment to talk to one another are formalised in digital rules known as ‘communications protocols’.

For the internet the two most important are the Transmission Control Protocol (TCP), and the Internet Protocol (IP). They are so inextricably linked that they are often written together as TCP/IP.

TCP

The TCP protocol is responsible for ensuring data can be sent reliably over the internet. It works through a number of software ports that act to keep data separate on the same computer – so it is possible to browse a web page, collect email and listen to streaming music at the same time.

To understand how TCP works you need to know something about ports. A port can mean different things depending on the context. A port can be a physical connection on a device such as the USB port into which you plug your printer or flash drive. Here, it means a number which indicates how data is handled when it reaches its destination. Many ports represent specific protocols such as port 80 representing the well-known port of HTTP.

Common TCP ports include the following:

- port 20 and 21 – File Transfer Protocol (FTP) for sending and receiving files (port 20) and control (port 21)
- port 22 – Secure Shell (SSH) for secure logins to computers
- port 25 – Simple Mail Transfer Protocol (SMTP) for sending email
- port 80 – HyperText Transfer Protocol (HTTP) for browsing web pages.

Data being sent from an application on your computer is divided into TCP datagrams each containing the TCP port number. The TCP application running on the recipient's computer will then examine this port number to determine which application should receive the information in the datagram.

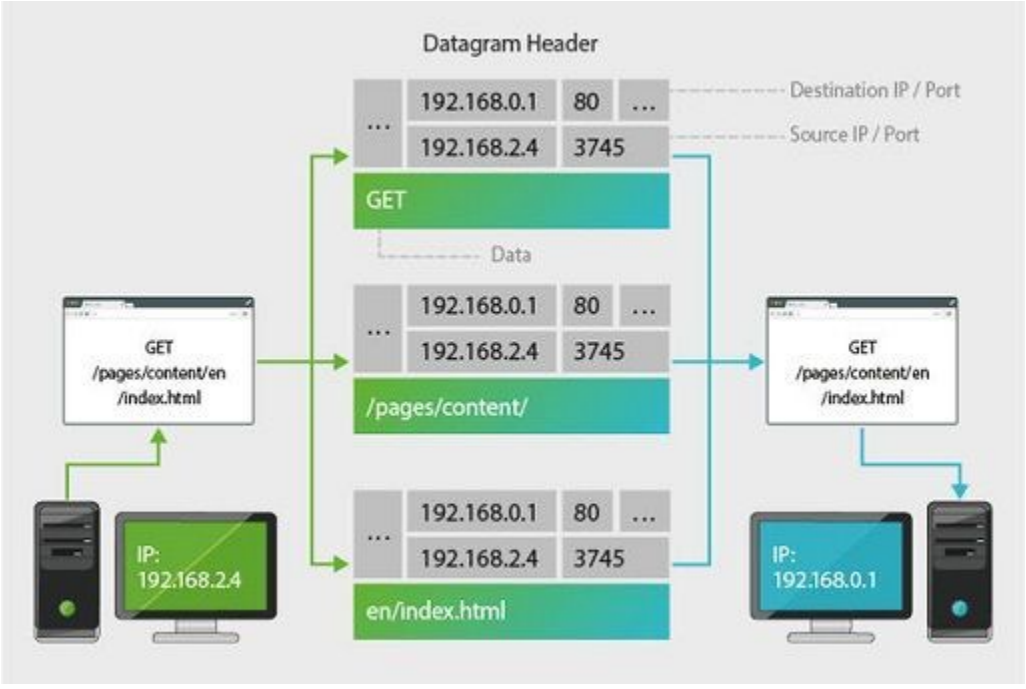


Figure 10

TCP’s second major task is ensuring that all data sent from a computer is received by its destination. It waits for acknowledgements from the remote computer, and in the event that a datagram gets lost or damaged in transit, it can resend the missing datagram. For this reason TCP is reliable – but relatively slow.

Applications where timeliness is more important than absolute accuracy – such as streaming media, video games and video conferencing – will use less reliable, but faster, protocols such as UDP (User Datagram Protocol) to send and receive their data.

If you are receiving an email, you want the whole message to arrive with no gaps, but if you are streaming a TV programme, it doesn’t greatly matter if a few datagrams get lost.

TCP is not responsible for sending and receiving information; that is performed by a second protocol – most commonly, IP, that we will look at next.

3.2 The internet protocol and IP addresses

Figure 11

View description - Figure 11

The Internet Protocol (known as IP) does the hard work of actually moving data across the internet. IP is only concerned with moving data, it doesn't actually check that data actually arrives (that's handled by TCP).

When IP receives data from TCP to be sent on to the internet it wraps the TCP datagram in its own IP datagram containing a sender's and a receiver's address as well as some other information.

When IP receives data from the internet, it removes the IP datagram information and passes it to TCP which will perform the checking of the contents and reordering of information before it can be passed through the appropriate port to an application.

IP addresses

The internet addresses used by humans (such as www.open.edu) are purely for our convenience, as computers use numeric addresses known as ‘Internet Protocol’ addresses (or IP addresses, or sometimes IP numbers) for communication. Every computer directly connected to the internet has a unique Internet Protocol (IP) address.

There are two major forms of IP address: IPv4 and IPv6.

IPv4 (Internet Protocol version 4)

This is the most familiar form of IP address consisting of four numbers, each ranging from 0 to 255, separated by full stops (periods) in the form 192.168.0.1. IPv4 has long underpinned the internet although it is now in urgent need of replacement (see below) because the number of devices connected to the internet has nearly exhausted the total number of available IPv4 addresses.

IPv6 (Internet Protocol version 6)

IPv6 is a a replacement for IPv4, originally outlined in 1998, to accommodate the increasing demand for IP numbers as more people and devices were connected to the internet. It can support a theoretical 3.4×10^{38} devices meaning it is suitable for any conceivable demand.

IPv6 is intended to replace IPv4; however this is an extremely complex process and it has taken a long time with even the most developed countries still far from completing the transition. A measure of compatibility exists in the form of IPv4-mapped IPv6 addresses where IPv4 addresses are stored in the IPv6 format.

Reserved IP numbers

Not all of the numbers in the IPv4 address range are actually available for use. As well as large blocks reserved for specific users in the early days of the internet, some are specifically used for ‘private’ networks outside of the internet.

10.0.0.0 to 10.255.255.255
169.254.0.0 to 169.254.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

Your computer will allocate itself an IP address beginning 169.254… if it is unable to connect to a local network. If you have a connection to the internet from your home your computer will almost certainly have an address beginning 192.168… In this case your network hub has a genuine IP address, your computer and other devices attached to the modem have private addresses. Your modem alters IP addresses on packets as they are sent to and from your home network and the internet.

3.3 From numbers to names

Figure 12

View description - Figure 12

When we type an address (such as www.open.edu) into a browser, the address is translated into a unique IP address by a name server, called a Domain Name Server (DNS), located somewhere on the internet. This IP address is attached to every IP datagram destined for the Open University server.

As an example we will use an IP datagram belonging to an email being sent to Bob who works in the coffee bar at Big University in America (Bob's address is bob@coffee.big.edu). The address is sorted from the most general part of the address to the most specific. First of all, the name server on the sender's machine makes a request across the internet to a computer which holds the addresses of all American universities (most of which use .edu at the end of their address) asking for the IP number of big.edu. Assuming that

big.edu exists, the .edu name server then responds with the IP number for the name server at Big University.

The sender’s machine then uses that IP number to make a link to the name server at Big University and requests the IP number of the coffee shop computer used by Bob. The big.edu name server will then respond with the address of the coffee shop. The IP datagrams can then all be addressed correctly and sent into the network.

3.4 The internet is not the world wide web

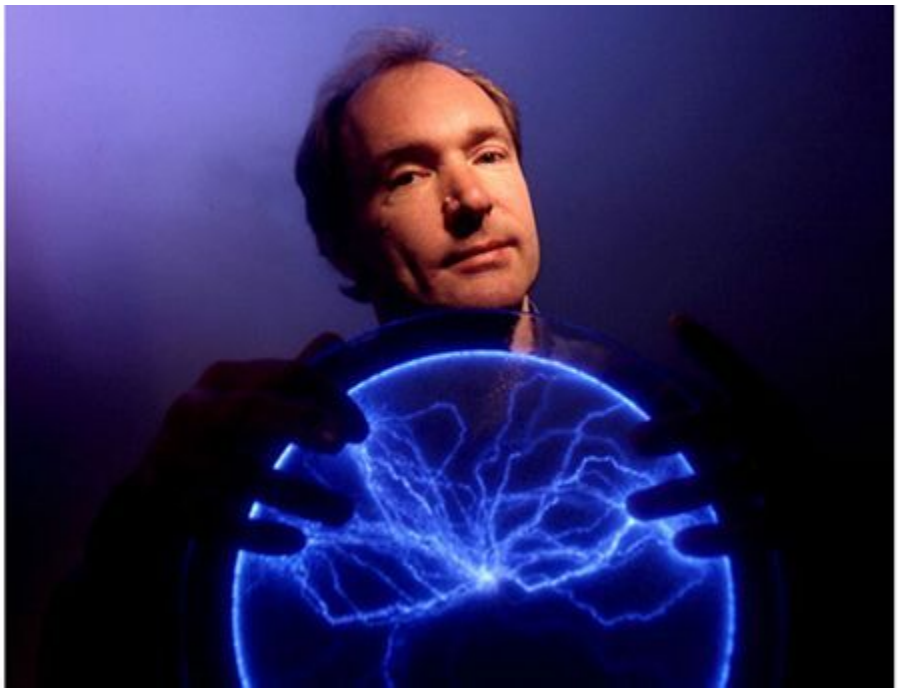


Figure 13 British physicist-turned-programmer Tim Berners-Lee devised the specifications for URIs, HTTP and HTML – technologies that underpin the internet as we know it

We've all done it. We've all been browsing a website and said 'I'm on the internet!'.

This is true, but misleading, if for no other reason than the internet dates from 1982 (with its roots as far back as 1969) but the world wide web only came into being in 1990 thanks to Sir Tim Berners-Lee.

Before the advent of the world wide web, not only did fewer people use the internet (it took until 1998 for 100 million people to log on for the first time), but it wasn't anything like the world wide web we know today – almost all commands had to be typed in – often using cryptic instructions, and what you got back – if you got anything at all – was plaintext. The world wide web not only meant that it was possible to use the internet's resources without learning a whole new language,

but it allowed for rich text, graphics, animation and sound to be delivered quite literally at the click of a button.

Part of the internet

At its simplest, the world wide web is nothing more than the part of the internet that can be accessed through the HyperText Transfer Protocol (HTTP) – another one of those standards that helps glue the internet together. HTTP allows two computers to exchange information as a series of requests (e.g. a request from your computer for a copy of the To do list page for this course) and responses (e.g. an Open University server delivers the contents of that page).

HTTP relies on TCP to set up the connection between the two machines, and it in turn uses IP to send and receive data. The most common applications that understand HTTP messages are web browsers such as the one you are using right now.

The world wide web is an example of hypertext – documents joined together using links. Every time you click on a link, HTTP is used to request a new page from a web server using TCP port 80. The content for the page is delivered to your computer, again through port 80 and interpreted by a web browser which formats the data in a human readable manner.

Designed to be open

The world wide web was designed from the very start to be an open environment which encouraged people to set up their own web servers and to write web pages. To encourage its uptake, all of the documentation that explains HTTP, and other standards that have grown up around the web, are publicly available to anyone wishing to develop software for the web. Likewise, the computer language used to format web documents, the HyperText Mark-up Language (HTML) is not only fully documented online, but is extremely easy to use.

Apart from the world wide web, the internet itself is used for a much wider range of services including email, instant messaging and file

transfers. The internet’s flexibility comes down to the flexibility of the underlying protocols – so long as information can be stored in IP datagrams – and just about anything can – it can be moved around the internet.

Interview with Tim Berners-Lee

Audio content is not available in this format.

View transcript - Uncaptioned interactive content

Listen to this interview. Towards the end, Tim Berners-Lee mentions a number of things that will be needed to make the world wide web achieve its full potential. One of these is digital signatures, which can be achieved using cryptography – our topic for next week.

Next, you have an opportunity to review your learning of the course so far in the Week 4 compulsory badge quiz.

4 Week 4 quiz

This quiz allows you to test and apply your knowledge of the material in Week 4.

Complete the Week 4 compulsory badge quiz now.

Open the quiz in a new window or tab then come back here when you’re done.

5 Summary of Week 4

Figure 14

This week you have learned the basics of computer networking and communications, gaining an understanding of how data is transmitted across the networks, including wireless networks.

You are now aware of some of the networking standards that allow different devices to connect to the network and exchange information.

Additionally, you have learned about the difference between the internet and the world wide web, and can describe some security problems that affect networks.

You can now go to Week 5: Cryptography.

Week 5: Cryptography

Introduction

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Cory explains the focus for this week: cryptography.

Cryptography is a specialised area of mathematics concerned with protecting information so that it can be transmitted and received securely even when there is a risk that a hostile third party might intercept or modify the data. You will recognise it as it's been mentioned before as a technique that can help with protecting information.

We are now going to look at this important aspect of cyber security in a little more detail.

1 The secret of keeping secrets

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Figure 1

View description - Figure 1

There have been many applications of cryptography throughout history, ranging from simple ciphers used by Julius Caesar to send military orders to his generals, to the more sophisticated medieval ciphers that withstood most attacks until the late ninteenth century and the famous Enigma codes of the Second World War.

The development of computers in the twentieth century allowed for far more complex means of encryption. Computers could perform:

- the mathematical operations that underpin all cryptography
- much more complex mathematics than could be reasonably expected of a human
- much faster than a human
- on much more data than a human could handle.

Any data that could be represented in binary format, i.e. using 0s and 1s, can be encrypted by a computer. It is not an exaggeration to say that encryption makes much of the modern world possible. Some commonplace applications for cryptography include:

- secure banking and payments systems – cryptography ensures your money is safe when it is transferred between accounts, issued at ATMs or used to shop online
- protecting conversations made over mobile telephones
- safeguarding wireless networks that give access to the internet
- securing files on hard disks and memory sticks
- authenticating electronic documents
- electronic voting
- securing media files such as music or movies from piracy, where it is known as Digital Rights Management (DRM).

1.1 Plaintext and ciphertext

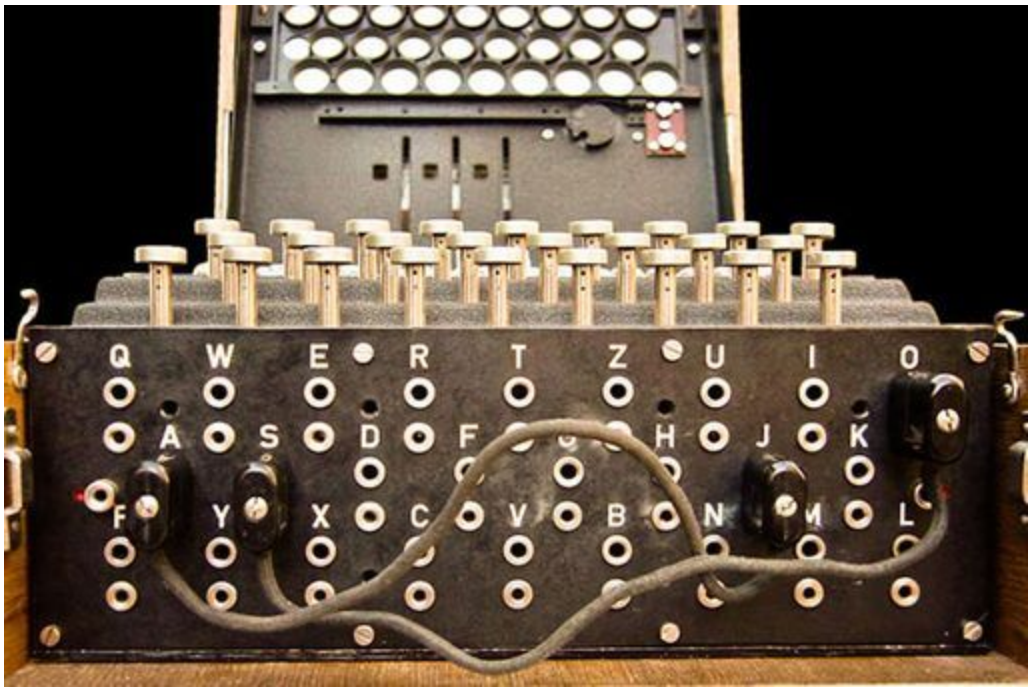


Figure 2

As in previous weeks, there is some terminology we need to introduce:

- **plaintext** – information that can be directly read by humans or a machine (this article is an example of plaintext). Plaintext is a historic term pre-dating computers, when encryption was only used for hardcopy text, nowadays it is associated with many formats including music, movies and computer programs
- **ciphertext** – the encrypted data
- **a cipher** – the mathematics (or algorithm) responsible for turning plaintext into ciphertext and reverting ciphertext to plaintext (you might also see the word ‘code’ used – there is a technical difference between the two but it need not concern us now)
- **encryption** – the process of converting plaintext to ciphertext (occasionally you may see it called ‘encipherment’)

- **decryption** – the process of reverting ciphertext to plaintext (occasionally ‘decipherment’).

1.2 Encryption keys

Figure 3

View description - Figure 3

Keys are pieces of information that determine the output from an encryption (or decryption) process. A single cipher can produce an almost limitless number of different outputs with different key values, allowing secure communication even if the cipher itself is known to hostile third parties.

It might surprise you to know that almost all ciphers are published in the scientific press or in standards documents; having them available for widespread scrutiny allows many people to check that they are secure and do not contain weaknesses which could be exploited to compromise the security of the data encrypted using that cipher.

A computer encryption key is nothing more than a string of bits where each bit can have a value of either 0 or 1. The number of possible values for a key is simply the total number of values that the key can have. So our one-bit long key can only have two possible

values – 0 and 1. If we choose to have a two-bit key it could have one of four possible values – 00, 01, 10 and 11. In fact every time we increase the length of the key by one bit we double the number of possible keys – so a three-bit key has eight possible values – 000, 001, 010, 011, 100, 101, 110 and 111.

The total number of keys can be written in scientific form as $2^{key\ length}$; so a key with a length of eight has 2^8 – that is 256 – values.

But how long should a key be? How short is too short?

The problem with short keys

Short keys are vulnerable to what is known as a brute force attack, just like you learned in Week 2 about passwords. A brute force attack is where a computer, or a number of computers, try every possible value for a key until they produce recognisable plaintext.

Since computers can work through key values extremely rapidly, keys must be sufficiently long that they offer a very large number of possible values.

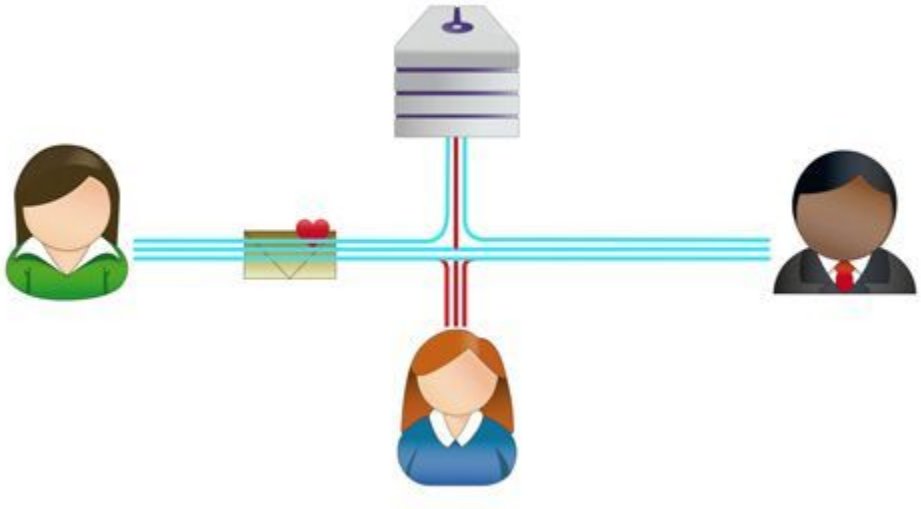
Keys may be known to the user in the form of passwords, or they may be stored in a computer's hardware (such as the decryption keys stored on a DVD player that allow it to play the encrypted data stored on the movie disk), or they can be generated by a computer as and when they are needed (such as conducting a secure transaction on a shopping site).

Next, you'll learn about the key distribution problem.

1.3 The key distribution problem

Video content is not available in this format.

View transcript - Uncaptioned interactive content



Traditionally, symmetric encryption suffered one enormous shortcoming – it was necessary for either the sender or the recipient to create a key and then send it to the other party. While the key was in transit, it could be stolen or copied by a third party who would then be able to decrypt any ciphertexts encrypted with that key.

Another problem is that a large number of key pairs are needed between communicating parties. This quickly becomes difficult to manage the more there are. This can be calculated as n(n-1)/2 where n is the number of communicating parties.

For example, if ten parties want to communicate with each other securely they would need 45 different key pairs: 10(10-1)/2 = 45. This would increase to 4,950 if there were 100 communicating parties!

This problem, called the **key distribution problem**, affected anyone wishing to use encryption until the 1970s when a method of distributing keys without actually sending the keys themselves was developed independently by GCHQ in the United Kingdom and Whitfield Diffie and Martin Hellman in the United States. The British discovery was kept secret for many years, so today the solution is known as the Diffie–Hellman key exchange method.

Symmetric encryption methods have the advantage that encryption and decryption is extremely fast, making them ideal for transmitting large amounts of secure data. In the video you saw how key distribution was achieved between two people, Alice and Bob.

1.4 Asymmetric or public key cryptography

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Asymmetric cryptography, better known as public key cryptography, side-steps the key distribution problem as each user creates their own keys:

- the **private key** which they keep safe and never distribute
- the **public key** which can be sent to anyone with whom they want exchange encrypted information.

Together the two keys are known as a **key pair**, which is what was used by Alice and Bob.

Unlike symmetric encryption, the two keys behave differently; the public key is the only key that can decrypt ciphertext encrypted using the corresponding private key and the private key is the only key capable of decrypting files encrypted with the corresponding public

key. Crucially, the value of one key cannot easily be determined from the other, so even if the public key falls into hostile hands, the value of the private key cannot be determined.

Public keys can be distributed using email attachments or through public key chain servers which act as distributors for large numbers of public keys. The creator of a public key uploads their key to the key chain server and it is freely available to anyone who wants to use it.

Although the mathematics behind public key cryptography is incredibly complex, the process of using it is relatively simple. To send a message using public key cryptography is simple. The sender obtains a copy of the recipient's public key, either by email or from a key chain server, and uses it to encrypt the message. The resulting ciphertext is then sent to the recipient who uses their corresponding private key to restore the original plaintext.

Public key cryptography is popular because there does not have to be any initial secure exchange of secret keys for an encrypted message to be sent (remember, users only ever exchange their public keys). However, it is generally far slower than symmetric encryption; and because of a quirk in the underlying mathematics, traditional public key cryptographic techniques require far longer keys to offer the same level of protection as symmetric encryption.

A newer type of public key cryptography, known as 'elliptic curve cryptography', can be just as secure as symmetric encryption using similar key lengths.

In the next section you'll discover why these encryption methods aren't used to keep the internet more secure.

1.5 Why isn’t the internet encrypted?

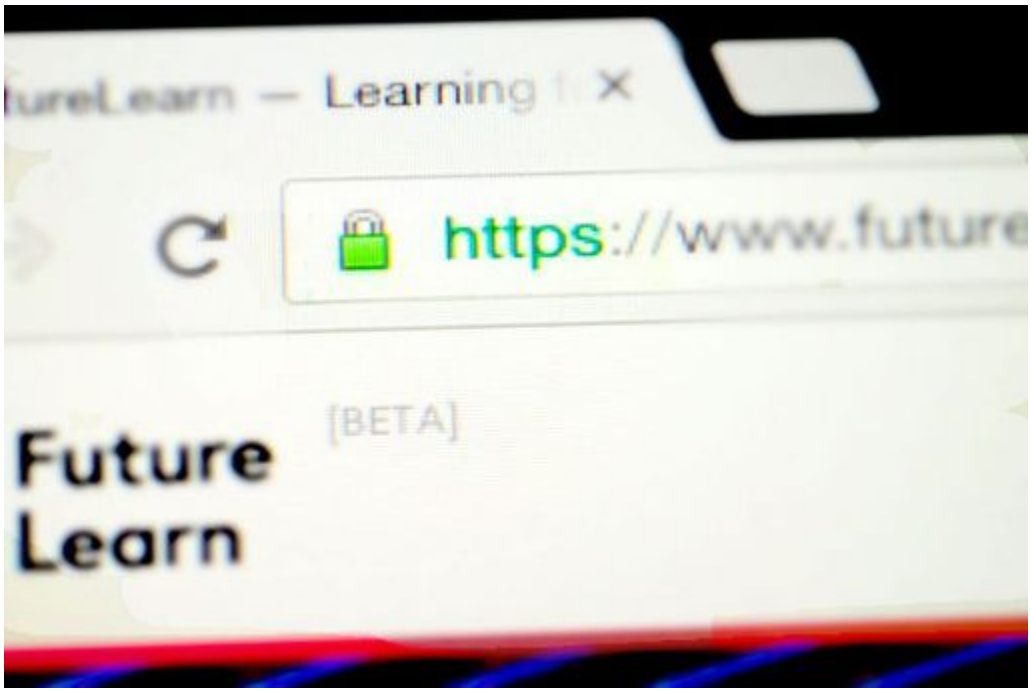


Figure 4

View description - Figure 4

Crucially, one part of everyday life that is not routinely protected by cryptography is the internet itself. The majority of emails and web pages are sent in plain view and can be intercepted and read by a malicious third party.

In theory, the whole of the internet could be protected using cryptography, but this is unlikely to happen because it takes a certain amount of computer power to encrypt and decrypt information so there would be significant costs if it were to be used throughout. Also there are a range of web applications, such as reading news sites or browsing online shops, that do not involve any sensitive information and therefore do not need to use encryption.

Applications running over the internet selectively use cryptography for key tasks (such as processing payments for online shopping) and

users may choose to use cryptography for additional purposes (such as securing email).

Some websites you visit are encrypted. This is sometimes shown by a padlock symbol in the address bar of the web browser. You'll learn more about this later in the course.

Review the list of digital information and online services you compiled in Week 1 of the course. Based on the threats you associated with each item in your list, think about some examples of how you could use cryptography to improve your security.

2 Putting cryptography to use

Figure 5

View description - Figure 5

So far this week you have studied the basic cryptographic techniques that can be used to protect the confidentiality and integrity of your information. Now let's examine how these techniques can be used in practice.

Many websites, such as those for internet banking and online shopping, routinely use encryption to ensure that the data sent to and from your computer is safe from eavesdroppers. However, configuring the same technologies to protect activities such as email communication can be quite difficult because the tools involved are complicated to install and configure.

Most tools depend on a collection of cryptographic techniques, commonly called 'Pretty Good Privacy', PGP for short. PGP includes algorithms for symmetric and asymmetric cryptography. In order to help software vendors develop systems that can easily exchange

encrypted information, a standard called OpenPGP was developed and agreed on by the Internet Engineering Task Force (IETF).

Some examples of tools available for encrypting emails include:

- GPG4Win – provides a set of standalone tools that can be used to encrypt and digitally sign emails, documents and other files. It provides some plug-ins to integrate these features into standard email software, such as Microsoft Outlook and Mozilla Thunderbird.
- GPGMail – this tool is designed to integrate with the Mail software provided by Apple. It can be used to both encrypt and digitally sign your email. It is easier to configure and use than the Windows tools, but is only useful if you use a computer running OSX.
- Enigmail for Thunderbird – this is a plug-in for the Thunderbird email client software that works across all operating systems. However, it requires manual installation of the GNUPG software, an open source implementation of the OpenPGP standard.
- Mailvelope – this is a plug-in for Google's Chrome browser that uses an implementation of the OpenPGP standard. It works with a variety of web-based email systems, such as Gmail or Yahoo Mail.

The effort of installing and configuring these tools puts many people off the idea of encrypting and digitally signing their email. Recognising this, there are ongoing efforts by companies to make encryption easier. For example, in 2014 Google announced that it would be adding PGP capabilities to its free email service, Gmail. The company have now released the software for its Chrome end-to-end encryption plug-in for review by developers. However, at the time of writing, this software has not been made available to the general public.

In the next few steps we will explore an alternative way of using cryptography to protect your email communications.

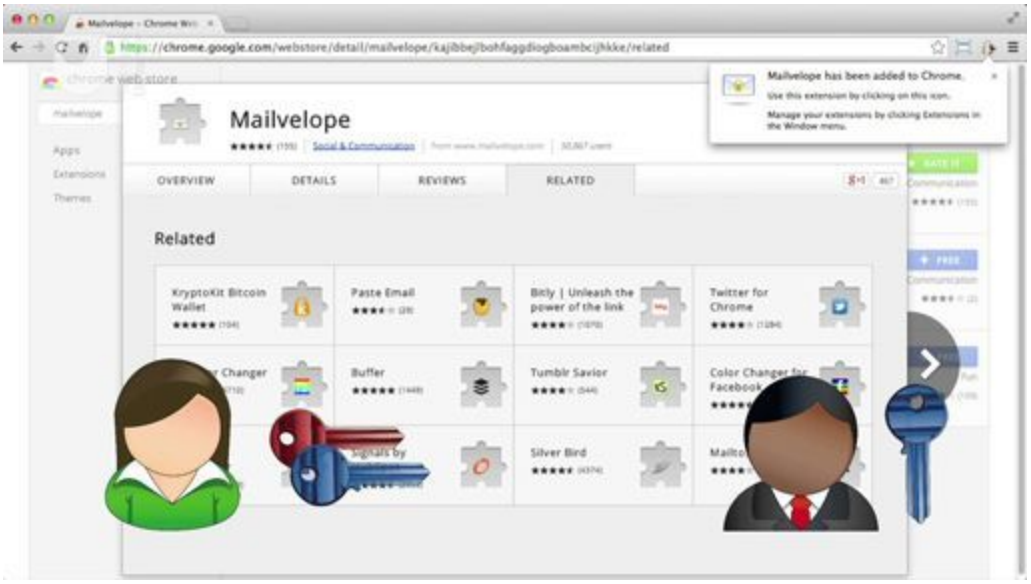
2.1 Setting up Mailvelope

You have learned that using cryptographic tools for email is not particularly straightforward and there is no single tool that works across all computer systems.

The video describes the steps required (also available in a PDF) to download and install the Mailvelope software. This software enables sending an encrypted email through existing web-based email accounts such as Gmail or Yahoo mail. The next section describes how to use Mailvelope.

Video content is not available in this format.

View transcript - Uncaptioned interactive content



The public key for the email address described in the video is as below.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Mailvelope v0.10.2
Comment: Email security by Mailvelope -
https://www.mailvelope.com
```

```
xsBNBFRTk80BCACZvweJjzZdkQMGukYklmKC+57ER4d8WG0lYz4x7DX+4ZZn
NCMMPIWTi3f4dXJ8IJLsgNuksFOqdGVSqFWPNwDuAx+cKgKIzdMfUTqaUkwG
hNCWbLgUfpKzrc5nxbceaaczM8CcEM5DRR/RUXsb8PdF/+qUXGMD/dULbaZF
y3kWjM8eKtk34/Ddhl1BTrdsuqWc0Sd3T5fAunXmt5OVwJfQH4e0A80rYlv/
6x132fvTrc1O2PuhehOYis5GbIIdmEne3uLf2+qY1atituAsITNVeRv1lH9k
vLElIDAx7pg9wzMPS6TCipcy7/Y0A4b/PosRr98Ivxqro/PjmYVtXYdjABEB
AAHNM0N5YmVyIFNlY3VyaXR5IE1PT0MgPGN5YmVyc2VjdXJpdHktbW9vY0Bv
cGVuLmFjLnVrPsLAcgQQAQgAJgUCVFOT2AYLCQgHAwIJEKcfnOAlYdbMBBUI
AgoDFgIBAhsDAh4BAADp0gf+PPYfgJyisnXgpKH/Iac4RH+xX17bVfQ5hbFk
p2cSPTLExba2OBgFT1QnuHfJex2arVEv5Iz/lm09BTzQSBSqrNnbmuAc9qif
mlJVvElvQ+5w0qA5Zllo9XrocLzTyjW4nLTWZLrdfAJo9CB1D/q60xE8KFYD
vX7zRplTdZsRc85PM3yfKFt4jsAY+Uv1gTHUfT2CBgi8wsnq6r1rPFE+1w5r
SNlQbugUzUzbjCzD4RqUL6DVbp3T04ZiPvlHh4j3yLKtCNg6OhcLZ3NfRjL4
aD8YAI17uB9FEYSC9Z10xWO/knRHBYWjj7sp/IAzuIki0+67XYMaTBEQVCMI
nBUBn87ATQRUU5PYAQgAzZFiDoNzvSzrBzOpjIGdg24aC/nA0kxZgnHbTFD3
81gic6DkJ1wS3oN5kNT7WDsCRVM2vNEZ+dLGu3aR1AntbZFxsd7k7iTPNCeC
VV0X59cX9x5WCUuygl4rK4dDW8NUk1E6ef5eFAo4YPkaaSPqr+RcurS4mWa+
9zLvvrIxG7J4xPbC1FSe5GSCi+CyjzxDV+lCI3h985DuIDNXShlUrSjhz+xy
TfVpLcjRODom8frO+7K4n04qUAvqoiqHaIdeC2lrasURWDHpuhBpaSQeWtEF
NlMwBPjkQ3LS2vqqCTpugjZzLI0YzpUOFJKlvoX0c0wyCE0f01nFISkEQjFB
0wARAQABwsBfBBgBCAATBQJUU5PhCRCnH5zgJWHWzAIbDAAAY7IH/2qzhjzB
lFnw2boWlYvUQwhaTUB8+DkGk0hXAOy8TspJQ6ph/8jC1ajSe4iElfqhI4nj
q+a2YhpVxMuXBIGPMdoG4fV/rJayKKSPR8w0Fyd/8+LeiHdiHmYrog0ds0Hb
hT6G3mXzlqXixaKMCADFv3yWYLhbgtNU90eBTblLW+b1hMXocmgWS4jHxePy
abjLUzBcjOlJ1dDsoxg2BIJT/1okvZa7c+uzcbTrm5wC+TLWqMbUDcGnPmid
7NUL8696ZKhrOeVc1ieOvc9v8Ax3Co5qQWh78/f3XS2pmv/reGPPPhaTSfmt
QAbFlDORGdx9/rkjhtrPyl1YtMeuVNAHflA=
=RTLt
-----END PGP PUBLIC KEY BLOCK-----
```

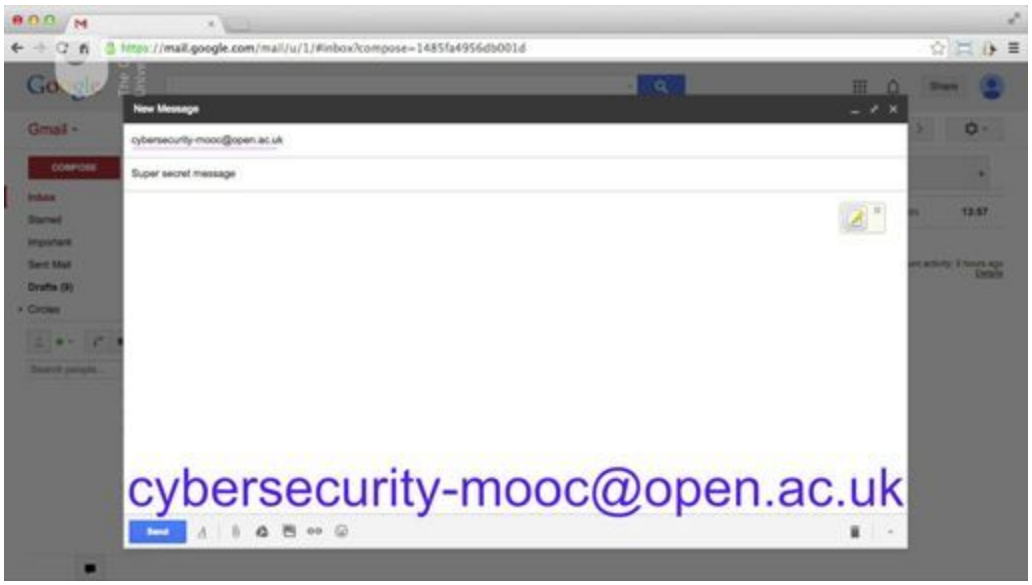

Disclaimer: The Open University and partners associated with this course have found this software to be robust at the time of checking. However, installing software is done at your own risk and The Open University and their partners cannot be held responsible for any resulting damage to your computer.

2.2 Sending signed and encrypted email

This video describes how to use the Mailvelope tool to send a signed and encrypted email (these steps are also available in a PDF).

Video content is not available in this format.

View transcript - Uncaptioned interactive content



Please note: Mailvelope has recently updated their interface and there are some changes from what is shown in the video. Instead of a swirly pen symbol, it is necessary to click ‘Sign’ at the bottom of the box, select the key created earlier and then click ‘Transfer’ to return the message to the email window. This hasn’t encrypted it yet though, just signed it.

To encrypt it, the steps are as follows: click the notepad icon again. Instead of the padlock sign shown in the video, click ‘Encrypt’ at the bottom of the box and select the key for ‘cybersecurity-mooc@open.ac.uk’. The message is now ready to be sent.

If you use this tool, you may notice the coloured shape in the top right of the Mailvelope message window, which has a short code in it. Don’t worry if yours isn’t the same as in the video. This is the security token that you can use to verify that the window you’re entering your message into isn’t a fake pretending to be Mailvelope. This code and colour can be set in the ‘Security’ options, under ‘Settings’.

To find out more about Mailvelope’s features or get help with specific problems visit Mailvelope help.

In the last few sections you have explored what is involved in using cryptography to encrypt and sign email communications.

- What seemed to be the hardest parts of the process?
- What would you want to improve to make it easier?

You may find it useful to compare your experience with the instructions for one of the other tools mentioned in Section 2, Putting cryptography to use.

3 Comparing different cryptographic techniques

Figure 6

View description - Figure 6

The field of modern cryptography is steadily growing with its increased use in everyday life when surfing the internet, using your card in a cash machine etc.

There are hundreds of different cryptography schemes each with different applications, some of the most notable are described below.

DES (Data Encryption Standard)

DES was first developed in the 1970s and was adopted by the United States National Bureau Of Standards as the US government standard for encrypting sensitive information. It is a symmetric cipher using 56-bit keys.

Due to DES's relatively small key size it was discovered that it was possible to crack the encryption with a brute force attack. Although this was a theoretical risk when first proposed, the great increases in computing power over recent years have shown that DES can be brute forced in less than a day. It was this weakness that led to official adoption of other encryption standards, such as AES, by the US government.

A variant of DES, called Triple DES was developed to provide additional security, and be compatible with the previous version, without the requirement to develop a completely new cipher. Triple DES uses three rounds of DES encryption and three separate 56-bit DES keys.

Triple DES is widely used in e-commerce and online payment applications as well as securing data in Microsoft Outlook. By current projections of the growth in computer power, Triple DES will remain secure from a brute force attack until at least 2030.

AES (Advanced Encryption Standard)

The realisation that the DES standard was no longer adequate led the United States government to call for a replacement. After an open competition lasting five years, AES was adopted as a US government standard in 2001. AES uses a combination of symmetric ciphers and either 128, 192 or 256-bit keys providing enhanced security over DES. Although some potential weaknesses have been identified in AES, most are theoretical, with the encryption being easiest to break in a situation where it has not been implemented correctly rather than in the case of a brute force attack where every possible key combination must be tried.

AES is now widely used in commercial applications since the underlying specification is freely available for personal or commercial use. It is used to protect archive files, encrypting computer file systems (such as Windows 2000 onwards), encrypting hard disks and for secure file transmission. Such is its importance that many microprocessors now include AES in their instruction sets to speed up encryption and decryption.

Blowfish

Blowfish was developed in the early 1990s as a potential replacement for DES, though AES ultimately became the agreed standard form of encryption. It is a cipher supporting variable key lengths from 1 to 448 bits. To date there has been no known successful attempt to break the encryption in its full implementation, although weaknesses have been identified when Blowfish is used with relatively weak keys. The related twofish and threefish ciphers have been designed to overcome these weaknesses, although most users have switched to AES.

Next, you'll find out how cryptography is used to prove identity online.

3.1 Using cryptography to prove identity

Figure 7

View description - Figure 7

Cryptography isn’t just used to hide secrets, it can also be used to authenticate data sent on an insecure network – such as the internet. The process begins by checking that your copy of a piece of data is an exact match for the one you requested.

Hashing

Hashing is the mathematical process of converting data of any size into data of fixed length known as the ‘hash’ (alternative names include message digest, hash codes, hash sums or hash values).

Hashing operates in one direction only, making it impossible to deduce the original data from the resultant hash. The intention of hashing is not to preserve the contents of the data but to create a

unique identifier for every single piece of data. When a file is published on the internet, the author may choose to publish the hash value for that file. For instance, here is some information published by the GnuPG encryption software authors on their website:

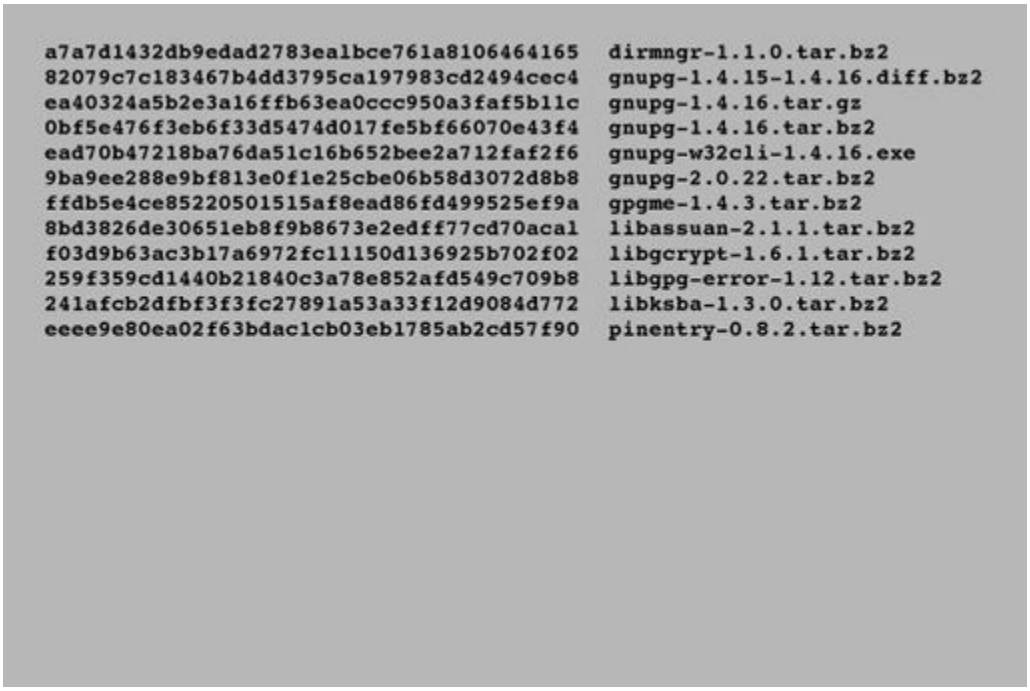


Figure 8

View description - Figure 8

Each long line of numbers and letters on the left is a hash (in this case from a hashing program called SHA-1), the text on the right is the name of the file. If you download one of these programs, you can then run your own copy of SHA-1 on your download and obtain a hash – if your file exactly matches the original the two hashes will be identical.

A variation of a single bit of data between two otherwise identical files will result in vastly different hash values, so any edits to a file between two hashing operations will result in different hash values revealing that the data has been tampered with and should not be trusted.

A large number of hashing algorithms have been developed; the most widespread are algorithms called MD5, SHA-1 and SHA-2.

Although MD5 and SHA-1 are in common use, both have been found to be flawed. Under certain circumstances ‘collisions’ can occur where two pieces of different data can generate the same hash value (albeit under specifically controlled conditions).

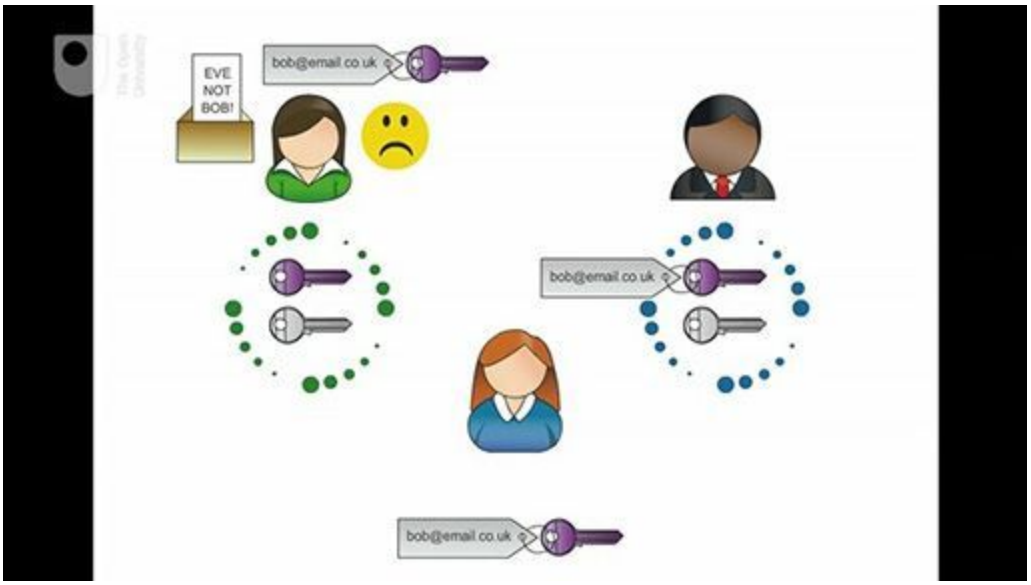
This weakness in the MD5 hashing algorithm has been used in malware targeting Microsoft Windows computers. Since neither algorithm can be guaranteed to generate unique hashes they can be considered ‘broken’ and should not be used. The United States government requires all hashes to be generated using the newer SHA-2 algorithm which has not shown any such weaknesses.

Next, you’ll find out how digital signatures and certificates use cryptography.

3.2 Digital signatures and certificates

Video content is not available in this format.

View transcript - Uncaptioned interactive content



Hashing can show that data has not changed in transmission, but on its own cannot demonstrate that the data originated with its supposed author. To do that, a digital signature should be used.

Digital signatures use the sender’s private key to encrypt the hash. Previously, you learned how documents can be encrypted with a public key which can be used by anyone, but can only be decrypted using the corresponding private key known only to the owner.

Encrypting data using the private key isn’t suitable for securing secrets (as anyone with access to the public key could decrypt it). However, it is perfectly possible to encrypt a hash using the private key so that the hash can be decrypted and compared by anyone possessing the matching public key. This can be used to provide authenticity since the encrypted hash must have been produced by the holder of the private key – hence the name digital signature.

Case study: Alice and Bob

Imagine that Alice wants to send the company's quarterly profit statement to Bob, who works in the financial markets, for public announcement. Both Alice and Bob want confidence that the quarterly profit statement has not been intercepted by Eve en route and altered.

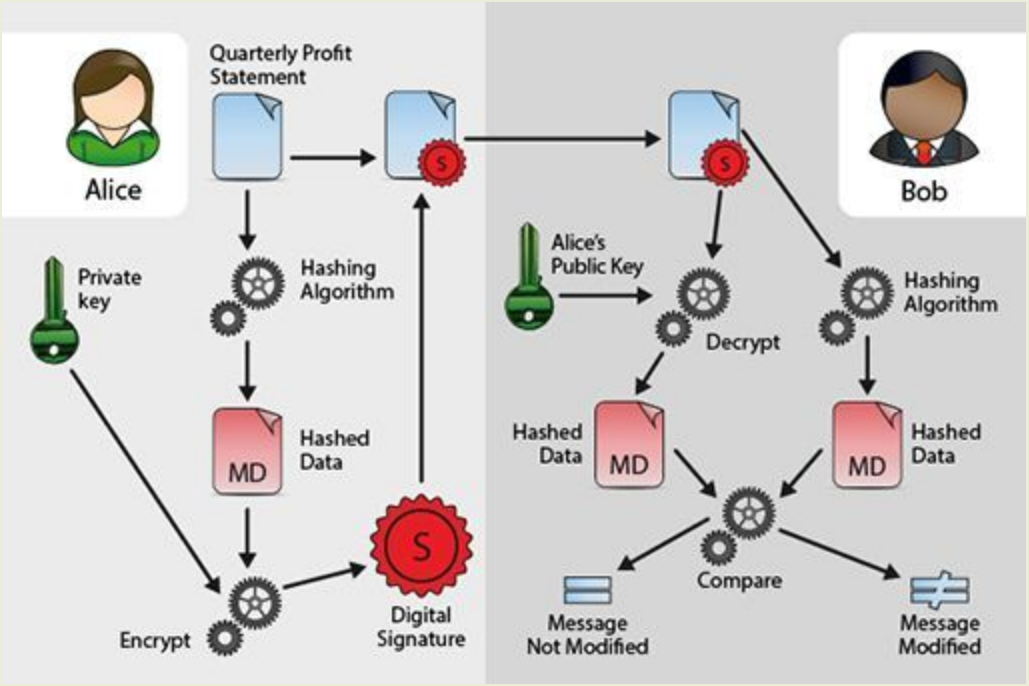


Figure 9

View description - Figure 9

Alice will therefore produce a hash of the quarterly profit statement and then encrypt this with her private key to produce a digital signature. Alice will then include the digital signature with the quarterly profit statement and send this to Bob, (depending on any time-bound sensitivities she may or may not encrypt this with Bob's public key).

Upon receipt Bob will decrypt the digital signature using Alice's corresponding public key to reveal the hash, (again depending on any time-bound sensitivities he may initially decrypt the

entire message using his private key). Bob will then calculate a hash of the quarterly profit statement and then compare this with the encrypted hash that he received from Alice. If the hashes are the same then both Bob and Alice can be confident that the quarterly profit statement was not altered en route by Eve.

Digital signatures do not provide us with complete confidence of the author or originator. Just because a digitally signed document claims to come from a person or a company it doesn't mean that it actually did, a malicious individual could masquerade as the sender by producing their own public/private key pair and using these to produce digital signatures.

Case study: Alice and Bob

Imagine that a digitally signed business invoice arrives in Alice's mailbox from Bob. She uses Bob's public key from a public key server to decrypt the digital signature and validate the business invoice by comparing the hashes. Alice, assuring herself that it is Bob (as the hashes are the same), follows the instructions and transfers money to the account details in the business invoice.

A few weeks later, Alice receives an angry email from Bob because he has not been paid. After a bank investigation she finds out that she had transferred the money to Eve by mistake – so what went wrong?

It's clear that the business invoice and the associated signature did not come from Bob, instead the signed business invoice actually came from Eve. Eve used Bob's personal information to create a new key pair in Bob's name and placed a copy of the public key on a public key server. Eve then used her corresponding private key to sign the business invoice and send it to Alice.

Alice, convinced that the document was a genuine business invoice from Bob (as it included what she believed to be his digital signature), followed the instructions and paid money into an account belonging to Eve – oh dear!

Digital certificates help us overcome this problem. A digital certificate is a means of binding public keys to their owner. These are issued by Certificate Authorities (CAs) who validate the owners of public keys. The CA does this by validating (through various processes), the identity of the owner of the public key. Once it has done this it will bind the public key to a digital certificate and sign it using its private key to attest authenticity. The CA's public key is available to all parties who need to validate the CA's assertion of public key ownership.

Case study: Alice and Bob

So, this prevents Eve from creating a key pair of her own, and claiming that the corresponding public key is Bob's. If Eve were to now send a business invoice appearing to be signed by Bob, when Alice uses Bob's validated public key to try and decrypt the hash and compare them, this will not work; she would know that something was wrong, and (hopefully), not transfer money to Eve.

3.3 Encrypted network connections

Figure 10

View description - Figure 10

As you learned earlier, web traffic is not encrypted by default. Web pages pass as plaintext across the internet and are vulnerable to interception.

Obviously, this was a problem when companies first began to consider online shopping. At first companies had to ask customers to browse online and then make a telephone call so the company could accept credit card information.

The solution came in 1995 when the web browser pioneer Netscape announced the Secure Socket Layer (SSL) protocol (this has now been replaced by Transport Layer Security (TLS)), which would allow web browsers to exchange secure data. It is supported by all modern browsers and allows confidential information to be exchanged over an insecure link.

TLS/SSL

TLS/SSL uses a combination of asymmetric and symmetric encryption to exchange data. When a web browser connects to a server and requests a secure communication the two computers first engage in what is known as a handshake and agree how future communications will be conducted, including the type of cryptography that will be used.

After agreeing how to communicate, the server transmits its own public key and a digital certificate of authenticity to the user's computer which checks that the certificate is genuine and has not expired. If the certificate is genuine, the user's computer then generates a master secret, encrypts it with the copy of the server's public key and sends that to the server.

The server decrypts the encrypted master secret with its own private key. Both the server and the computer now have copies of the secret and use that to generate identical copies of a symmetric encryption key. Crucially, the key itself has not been transmitted across the network.

Each computer now informs the other that all other transactions in this session will be conducted using the symmetric key (called the session key), by sending 'finished' handshake messages using each other's session keys. The two computers can now perform the secure transaction itself, including sensitive information such as bank account details, addresses, credit card numbers and receipts using the high-speed symmetric key.

At the end of the secure session, the two computers say goodbye to one another and each deletes their copies of the symmetric session key. If the user starts another secure session a completely new key will be used.

As well as e-commerce sites, TLS/SSL is supported by other websites that supply confidential information including banks and some email clients. Its use means that end users can benefit from the confidentiality and integrity provided by cryptography without

having to worry about the technical details of configuring their software or managing keys.

In the next section you'll see TLS/SSL in action.

3.4 How secure is your browsing?

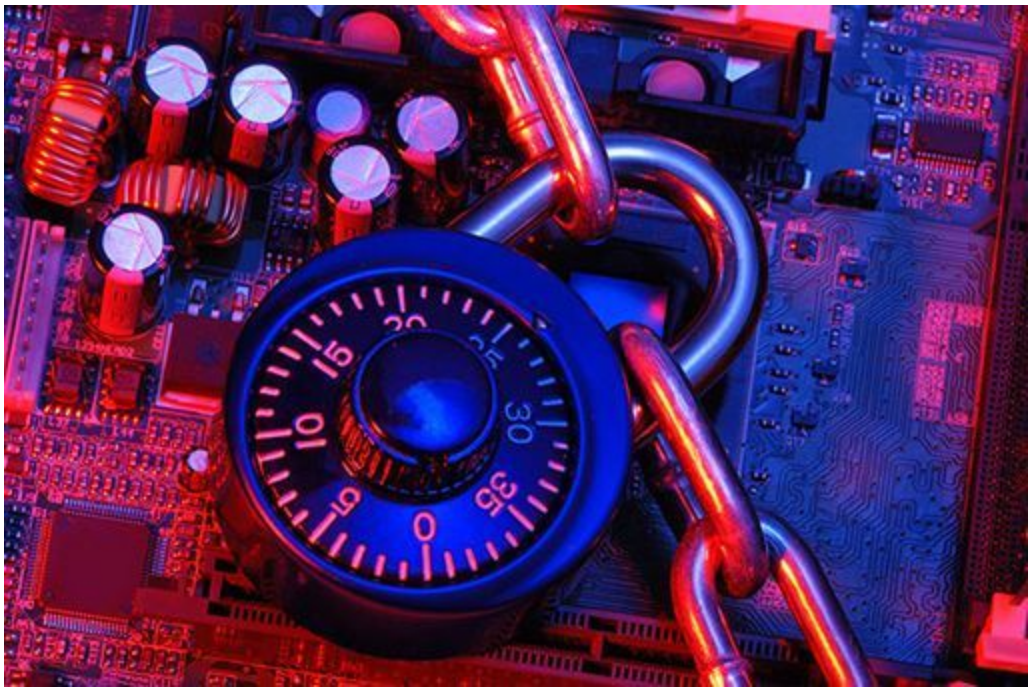


Figure 11

View description - Figure 11

Web browsers have made it easy to determine if a website is using TLS/SSL by:

- Making all secure addresses begin ‘https://’ (rather than ‘http://’) with the s standing for ‘secure’. Examples include Gmail, at https://mail.google.com/; Google defaults to Google Safe Search at https://www.google.com/, which means that your search requests and results cannot be seen by others.
- Showing a closed padlock symbol in or near the top of your browser window.

Activity 1 Your own browsing security

Allow about 15 minutes

Visit a website that you use regularly (it could be this one!) and find a page that you would expect to use a secure network connection. A common example would be your webmail account or online banking website. Use your browser’s help feature and click on the padlock icon to find out about its meaning.

Research browsing security online. You might find that your browser shows different versions of the padlock to highlight potential problems with the secure connection.

4 Week 5 quiz

This quiz allows you to test and apply your knowledge of the material in Week 5.

Complete the Week 5 practice quiz now.

Open the quiz in a new window or tab then come back here when you’re done.

5 Summary of Week 5

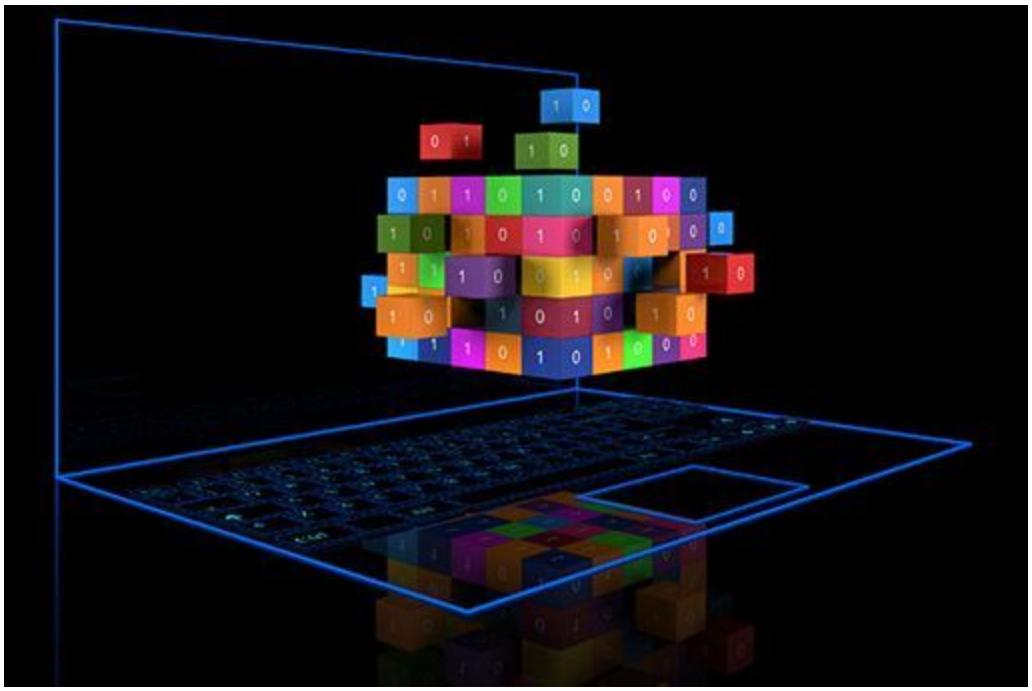


Figure 12

View description - Figure 12

This week has focused on cryptography – a key security technique that allows you to ensure confidentiality and integrity of your data.

You have learned how to use cryptography tools to secure your email and can explain the use of cryptography in common applications, such as the world wide web. As a result, you should now be able to identify where you could use cryptography to improve the protection of your digital life. One example of this, the use of cryptography to protect computer networks, is the topic for the next week of the course.

You can now go to Week 6: Network security.

Week 6: Network security

Introduction

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Your course guide, Cory, explains that earlier in the course, you looked at a range of security techniques and technologies aimed at protecting your online identity, as well as your digital information, from malware.

This week explores different ways of protecting the underlying communication networks and computers we use from attack and you'll also configure a firewall for the computers you use.

1 Firewall basics

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Figure 1

View description - Figure 1

In a building, a firewall is a reinforced masonry wall that is designed to prevent a fire spreading through the structure, allowing people time to escape. Similarly, in a computer network, a firewall is a barrier that blocks dangerous communications from spreading across a network, either from the outside world into a local network, or from one part of a local network to another.

Firewalls can be supplied as dedicated network devices or they may form part of a network router. A firewall might also be included as part of a computer's operating system.

The internet existed for a long time before firewalls were invented. The first discussion of the necessary technologies took place late 1988, and came about after several attacks from organised groups of hackers and the very first malicious software.

At their simplest, firewalls block network communications by looking at the addressing and protocol information in the data packet's header. As a data packet (or datagram) arrives at the firewall's interface, the addressing (usually IP) and protocol information (usually TCP or UDP) is compared to rules programmed into the firewall's software. These rules can be supplied by the firewall's manufacturer, or more often they are created by an administrator or sometimes the user.

So if a packet originating from a hacker conducting a scan of your network or computer arrives at a firewall, it will inspect its addressing and protocol information and then compare this against its set of rules. If the set of rules say that packets from an unknown address (the hacker) are to be blocked, then the firewall may either discard the packet 'silently' or 'close' the connection with the hacker.

Most firewalls store the state of connections to determine if they represent new or existing connections. They will only allow packets belonging to a known, active connection to pass (provided the rule set allows this). More advanced firewalls can identify the applications responsible for sending and receiving packets, allowing network managers to block applications that use excessive bandwidth – such as media players, or those widely used for distributing copyright infringing content – such as BitTorrent applications, as well as protecting from application attacks.

You'll learn what a personal firewall protects against in the next section.

1.1 Personal firewalls

Figure 2

View description - Figure 2

Most operating systems come with a firewall that is installed as part of an operating system.

This firewall is only able to protect the computer it is installed on (and any devices attached to it) from an attack, so it is called a personal firewall. It is not intended to replace a network firewall which prevents attacks from outside of the network (such as from the internet).

Personal firewalls are especially useful for people with portable computers which will inevitably be connected to a wide range of computer networks. While we all hope and, to some extent, trust the people responsible for maintaining these networks to maintain a safe system, we cannot be sure that these networks are not compromised. The personal firewall on our own computers therefore

adds a layer of protection between our personal data and a potentially untrustworthy (but useful) network.

Personal firewalls are the responsibility of individual computer users. If you have complete access to your computer’s settings then it is entirely possible to turn off the personal firewall and leave your computer vulnerable.

In the next sections, you’ll learn how to check that your default personal firewall installed with your computer is running correctly.

1.2 Configuring your own firewall

In this section you will locate the personal firewall on your own computer and, if necessary, make modifications to its settings to provide the best possible protection.

You will need to have Administrator level access to the computer you use as you will be making changes to important parts of the operating system. If you do not have these permissions, request temporary administrator rights from the machine's owner.

If your computer is in an office environment, or is supplied by your employer, please check that you are permitted to change the firewall settings before attempting this section. Many employers have preferred settings that are maintained by specialist staff and you should not attempt to change them without permission.

If you use Windows 7 or Windows 8, continue with the next part 'Configuring your own firewall (PC)'.

If you use a Mac, go straight to 'Configuring your own firewall (Mac)'.

Configuring your own firewall (PC)

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Locate the personal firewall on your own computer and, if necessary, make modifications to its settings to provide the best possible protection.

Download the PDF of these instructions to keep as reference.

You can skip the next part, unless you also own a Mac and want to configure a firewall for this as well.

Configuring your own firewall (Mac)

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Locate the personal firewall on your own computer and, if necessary, make modifications to its settings to provide the best possible protection.

Download the PDF of these instructions to keep as reference.

Other firewalls

Other firewalls are available either to download or as software packages that can be bought from retailers.

You may prefer to use one of these programs, but if you do, please remember:

- you should only keep one firewall running at a time since multiple firewalls will not offer significantly better protection and can interfere with one another
- you must keep one firewall running at all times.

Once you've set up your personal firewall, identify a type of traffic that you might want to allow (or deny) on your computer.

2 VPN basics

Figure 3

View description - Figure 3

You've just learned how firewalls can protect individual computers and local networks from attack. Next, you'll learn about the uses of virtual private networks (VPNs).

In some ways, our local networks resemble forts sitting in the Wild West of a Hollywood movie. Inside strong walls, life goes on as normal, with data being exchanged freely between trusted machines. Meanwhile, beyond the firewall there is the lawless frontier of the internet; traffic crossing the internet must make a risky journey largely unprotected.

The problem of secure data transmission is especially acute for organisations based in several physical locations, such as those who need to exchange information with sub-contractors or those with a dispersed workforce such as sales teams or home workers.

Traditionally, companies invested in private communications links (usually called leased lines) whose cost might run to thousands of pounds per month. Most organisations cannot justify such an investment and in any case, leased lines cannot serve a mobile or highly dispersed workforce. So the lawless frontier of the internet is our only choice – this is where VPNs come to the rescue!

A VPN, as the name implies, is a means of creating a private network across an untrusted network such as the internet. VPNs can be used for a number of different purposes such as:

- to securely connect isolated local area networks (LANs) across the internet
- to allow mobile users remote access to a corporate network using the internet
- to control access within an intranet environment.

VPN concepts

VPNs are typically implemented using dedicated network devices (sometimes this might be a firewall) and software. There are two parts to the software; the first, called a **VPN client**, is installed on the computer of anyone who wants to be part of the VPN. The client is responsible for connecting users to the VPN so that it can send and receive information in a secure manner with, in this example, a corporate network. The second part is the **VPN server** which is part of a dedicated network device, usually located on the perimeter of an organisation's network. The server software typically performs the authentication of users and route traffic to the corporate network.

The VPN software creates a path known as a 'tunnel' between the VPN client and the VPN server. It can establish this 'tunnel' by using any third party or untrusted network such as the internet. Unlike other paths through the internet, information which passes through this 'tunnel' can be encrypted to protect it from inspection or modification. So we can use these tunnels to protect our data while it crosses the lawless frontier of the internet back to the safety of our forts!

2.1 Securing the tunnels

Figure 4

View description - Figure 4

The VPN path or tunnel between the VPN client and the VPN server relies on encryption to protect the data from interception or modification as it travels across the internet.

Encryption

In a VPN, encryption and decryption is typically performed by the client and server software. Early VPN solutions used proprietary encryption techniques, but shortcomings in many of these methods has forced a switch to public encryption standards.

Authenticity and integrity

It is vital to ensure that information can be trusted – that it is coming from an authenticated user and that it has not been altered in transit.

VPNs use a number of methods to ensure authenticity:

- **hashes** (see Week 5)
- **digital signatures** (see Week 5)
- **message authentication codes (MACs)**.

MACs are appended to messages and act as an authenticator. They are similar in principle to digital signatures, but the hash is encrypted and decrypted using the same secret key (symmetric encryption).

VPN protocols

There are three main forms of VPN protocol currently in use:

PPTP (Point to Point Tunnelling Protocol)

PPTP was designed in a consortium led by Microsoft, which included an implementation of the protocol as a standard component of Windows NT 4. Microsoft also released PPTP as a free add-on to Windows 95 and Windows 98, allowing users of (at the time) the most popular version of Windows to access corporate networks.

PPTP proved unsuited to large companies (being limited to 255 connections per server), but more seriously, the PPTP standard did not settle on a single form of user authentication or encryption; therefore two companies could offer software supporting PPTP, yet each product would be incompatible with the other! From Windows 2000 onwards, Microsoft replaced PPTP with L2TP (see below).

L2TP (Layer 2 Tunnelling Protocol)

This is an adaptation of a VPN protocol known as L2F originally developed by Cisco to compete with PPTP. In an attempt to improve L2F, a successor was devised by a group composed of the PPTP Forum, Cisco and the Internet Engineering Task Force (IETF). L2TP combines features of both PPTP and L2F.

IPSec (Internet Protocol Security)

IPSec was designed by an international committee (*The Internet Engineering Task Force* (IETF)) in 1992 with a first draft standard published in 1995, the revised standard was published in 1998. IPSec is now the most widely supported protocol with backing from Intel, IBM, HP/Compaq and Microsoft (among others).

IPSec has gained a reputation for security thanks to its use of well-known and trusted technologies. Rather than invent new techniques for encryption, the designers of the protocol built their system on top of existing encryption technologies, which had, in themselves been subjected to intense scrutiny.

In the next section you'll discover how secure VPN access can be.

2.2 Security risks of VPN

Figure 5

View description - Figure 5

VPNs might sound like a panacea to a number of problems as they can extend, in our example, a corporate network across a wide geographic area via the internet. However, in doing so, they raise a number of new problems.

Security of remote machines

When a remote machine is part of a VPN it effectively creates a new frontier between the ‘secure’ corporate network and the internet. This remote machine now offers a direct route into a corporate network. Previously, it had been relatively simple to secure machines within a corporate network; now the remote user might be using their own computer, network connection, operating system and software – none of which are controlled by the organisation. Worse still, they might be sharing the machine with a number of other users, some of

which might not be employed by the organisation. Perhaps the same PC is used to manage corporate documents, as well as downloading pirated music from the internet and playing video games!

The remote machines must themselves be secured from abuse. That may mean enforcing certain minimum standards with regards to operating system, antivirus software, firewalls and so on. Employers may have to stipulate that antivirus software is kept up to date, and that all patches and service packs are installed.

Security of the VPN implementation

As you learned earlier, the security of various VPN implementations has come under scrutiny. Protocols themselves might be well designed and apparently secure, but the method of implementation, where programmers have taken shortcuts or offered ‘additional convenience’ to the user, may compromise the protection offered.

For instance, there are no major problems with the PPTP protocol, but Microsoft’s implementation of PPTP was found to have a number of serious defects. Microsoft’s implementation of PPTP was introduced in 1996, and hacker software exploiting weaknesses began circulating the following year. Papers describing the weaknesses appeared in 1998, it was only after publication that Microsoft addressed the most serious weaknesses in PPTP by releasing a patch (DUN 1.3), and even then some issues remained unresolved.

In addition to errors in protocol implementations, security vulnerabilities can be introduced if the design or configuration of the overall VPN solution is done incorrectly.

Security of interoperation

VPN is still a relatively immature technology with a number of competing standards, often supported by different vendors. Mixing and matching hardware and software might cause problems. Until technology matures (which is happening at a rapid rate), it might be necessary to use a single technology provider.

Security of network availability

Since VPNs typically rely on the internet for delivering information there are no guarantees about the reliability. The internet cannot guarantee delivery of information from one location to another.

In the next section you are invited to find out more about VPN and share your findings.

2.3 Putting VPN to work

Figure 6

View description - Figure 6

VPN technologies have a range of applications in the real world.

Activity 1 VPN applications

Allow about 30 minutes

Find out about some VPN applications. What are the potential security problems associated with some of the applications? Note down your thoughts in the space below.

Provide your answer...

3 Intrusion detection system (IDS)

Figure 7

View description - Figure 7

So what happens when there’s an attack on a computer network? Chances are that you’ve seen a movie or TV programme where the administrators rush to their keyboards and frantically begin typing, lights flash, sirens sound – it’s all very exciting – but does anything like this happen in real life?

As you might suspect, the answer is, no, not really. Computer networks are regularly attacked, but the response is rarely as exciting as filmmakers would like you to believe.

Intrusion detection systems (IDS) may be a dedicated device or software and are typically divided into two types depending on their responsibilities:

- **Network Intrusion Detection System (NIDS)**, which is responsible for monitoring data passing over a network.

- **Host Intrusion Detection System (HIDS)**, which is responsible for monitoring data to and from a computer.

An IDS can support a network firewall. Ideally the firewall should be closed to all traffic apart from that which is known to be needed by the organisation (such as web traffic, email and FTP). An IDS can then be used to scan any traffic passing through the firewall for potential attacks using a NIDS, as well as being able to detect those coming from within – such as from a personal computer infected with malware – using a HIDS.

Intrusion detection may be considered passive; it identifies that an intrusion is taking place and informs an administrator who must take appropriate action. However, they can also be reactive – as well as informing the administrator, the IDS can actively attempt to stop the intrusion, in most cases by blocking any further data packets sent by the source IP address. These systems are also referred to as an Intrusion Prevention or Protection System (IPS).

Weaknesses

Automated intrusion detection systems have a number of weaknesses. They can be too sensitive, falsely reporting that an intrusion is under way, for example if a network is incorrectly configured or a buggy program begins issuing large numbers of packets.

Conversely, they are sometimes not sensitive enough to certain types of attack that proceed very slowly and do not generate enough traffic data to raise the alarm. Finally, signature IDS relies on the software suppliers issuing regular updates to the list of known signatures, until the IDS receives the update it is effectively blind to the attack.

In the next section you'll learn how IDS works in practice.

3.1 IDS techniques

Figure 8

View description - Figure 8

Intrusion detection typically uses one of two techniques: anomaly detection or misuse detection.

Anomaly detection

Anomaly detection depends on the system having a model of the expected ‘normal’ network behaviour of users and applications. The basic assumption of anomaly detection is that attacks differ from normal behaviour. This approach has the advantage of being able to detect previously unknown attacks by simply looking for patterns that deviate from the expected normal behaviour.

For example, consider a user who normally logs on to his computer at 9am each weekday and spends most of the morning accessing an order processing application, before taking a break for lunch.

Subsequently the user accesses a number of supplier websites each afternoon before logging off at 5pm. If the intrusion detection system logs the user accessing the system at 3am and installs new software on his machine, the anomaly detection algorithm would flag this activity as suspicious.

Of course a potential disadvantage of this approach would be that some legitimate activities might be incorrectly identified as being suspicious.

Misuse detection

Misuse detection depends on the system having a set of attack patterns, or ‘signatures’, against which all network activity can be compared. The patterns of normal behaviour and attacks are configured by an administrator. Whenever there is a match between users’ activities and one of the attack signatures, or a mis-match between users’ activities and a configured normal use pattern, the system will flag that an attack is underway.

This approach has the advantage of minimising the occurrences of legitimate activity being identified as being suspicious. However, it also has the disadvantage of only being able to identify attacks where there is a known pattern, so attacks of a new unknown pattern can be easily missed.

To find out more about attacks, honeypots are used.

3.2 Honeypots

Figure 9

View description - Figure 9

Sometimes network administrators want to study attacks, either so the attackers' methods can be understood more fully and countermeasures prepared, or as part of an investigation that might lead to civil or criminal prosecutions.

One method of safely studying an attack is to deflect attackers towards an isolated computer or network which appears to be completely legitimate, but is in fact a closely-monitored trap known as a honeypot. There, every action performed by the attacker can be recorded and analysed without risking important data.

Honeypots are also used by researchers to identify new attacks that are circulating in the hacking community, as well as by anti-spam organisations which use them to identify the location and identities of spam email senders.

Next, you'll have the opportunity to review your learning in the end-of-week practice quiz.

4 Week 6 quiz

This quiz allows you to test and apply your knowledge of the material in Week 6.

Complete the Week 6 practice quiz now.

Open the quiz in a new window or tab then come back here when you’re done.

5 Summary of Week 6

Figure 10

View description - Figure 10

This week has focused on techniques for network level protection of your digital life.

In particular you have learned the role of firewalls in protecting networks and configured a personal firewall for the computers you use. You have also learned how cryptography can be used to maintain the confidentiality, integrity and authenticity of network traffic and how networks can be automatically monitored to detect potential attacks.

You can now got to Week 7: When your defences fail.

Week 7: When your defences fail

Introduction

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Over the past few weeks, you've learned about technologies that can help improve the security of your digital information. You now have an understanding of how cryptography helps keep information private and prevents information from being modified and how to protect networks from attack.

But, as Cory explains, information cannot be protected by technology alone and it is important to have a good awareness of what kind of

things can go wrong when an attack on your information has been successful.

This week will help you to recognise the signs of an attack, to know how and where to report the problem, and to consider what you can do to recover from the security breach and stop it happening again.

1 Identity theft

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Identity theft is a type of fraud in which an attacker uses stolen personal information to impersonate another person. This video shows an extreme, though by no means unique, example of the possible consequences of identity theft for an individual.

Traditionally, this type of fraud was achieved by an attacker intercepting postal deliveries which contain personal information such as names, addresses, bank account details and so on. Attackers could then open credit card accounts and apply for loans in the victim's name. Victims have had their financial security and lives ruined by identity theft.

The online world has opened up a new, lucrative source of information for fraudsters. Many users have been quite relaxed about sharing their information with online services and other users, but even security conscious individuals are threatened by malware

designed to sniff out personal information on a computer, or phishing attacks that persuade users to divulge personal information. Additionally, as we have seen, hacking attacks on big retailers can make millions of personal records available for potential abuse.

Online identity theft still only makes up a tiny proportion of all cases of identity theft and it is actually quite a rare occurrence, but it is a growing threat.

Preventing identity theft

You can greatly limit your risk of online identity theft by following simple security procedures such as running an antivirus program, keeping it up to date and by not responding to phishing emails.

Detecting identity theft

Online identity theft may pass unnoticed for some time, during which great damage can be done to your financial security. Some signs that a victim might notice are:

- unexplained bank withdrawals or credit card charges
- bills and other expected official letters don’t arrive
- cards or cheques are declined
- debt collectors make contact about debts the victim knows nothing about
- they receive notice that their information was compromised by a data breach at a company where they do business or have an account
- their bank or credit card provider makes contact about suspicious behaviour on their account.

Next, you’ll learn about what data loss can mean for organisations.

1.1 Loss of data

Figure 1 US Army Private Chelsea (then Bradley) Manning, who was at the centre of a controversial data leak to the Wikileaks website in 2009

Data loss can mean several things ranging from the destruction and deletion of data, to making unauthorised copies that are no longer under your control.

Data can be stolen by people who have direct access to a computer, such as by copying data to a flash memory drive, and also by attackers gaining access over a network connection.

Insider attacks

The hardest attack to defend against is when an attacker has direct access to a computer, especially in an organisation where many people might have access to a single computer, and one, or more, of them might not have the organisation's best interests at heart. Security risks posed by employees (or ex-employees) of an organisation to their employers are known as insider threats.

A 2013 Forrester survey of businesses employing two or more people in the UK, US, Canada, France and Germany found that 36% of information security breaches were caused by insiders and represented the leading threat to organisational security. These findings were supported in a survey of attendees to the Infosecurity Europe conference where 37% of respondents said the biggest threat to their information security came in the form of ‘rogue employees’. This placed insider threats ahead of cyber attacks (19%) and device security (15%).

Case study: Stealing data

In 2012, a programmer for the Federal Reserve Bank of New York was sentenced for stealing source code used to develop the bank’s computer systems.

Bo Zhang was a third party contractor for the bank with privileged access to software that was under development. He pleaded guilty to copying the code to personal computers in violation of his contract of employment although there is no evidence that he intended to share the programs with anyone.

Similarly, in 2013, the social networking game developer Zynga settled a lawsuit with a former employee, Alan Patmore, who had copied hundreds of files, including unreleased game designs, to a Dropbox cloud storage folder before taking up employment with a rival company. Patmore expressed deep regret for his actions and agreed to ensure all copies of the data were destroyed in exchange for Zynga dropping charges against him.

The case of Chelsea Manning is one of the more significant insider attacks involving the loss of data. It is another example where the attacker simply copied the data and shared it with others, depriving the data owners of control over the confidentiality of the information.

Case study: Chelsea Manning

Chelsea Manning (born Bradley Manning) was a United States Army soldier who leaked confidential information, including 250,000 United States diplomatic messages and 500,000 United States Army reports as well as videos of military action in Iraq, to the WikiLeaks website.

Manning obtained copies of classified materials during service in Iraq in 2009, copying them directly to a data CD disguised as a music disc, from which the materials were transferred to a laptop and then to the WikiLeaks servers for dissemination.

The reports were widely published around the world and caused enormous diplomatic embarrassment for the United States government. Manning was eventually identified after confessing in an online chat to Adrian Lamo, who informed the Army. Manning was charged with 22 offences, including that of aiding the enemy, and pleaded guilty to 10 charges. She was found guilty in 2013 and sentenced to 35 years in military prison.

Next, you'll find out about the risks of data loss.

1.2 Risks of data loss

Figure 2

View description - Figure 2

As the case studies showed, there are serious consequences of losing data.

These consequences can be expressed as a series of costs, such as:

- the cost of recreating the lost data – either by buying new hardware and software or re-entering the lost data (which may not always be possible)
- the cost of continuing without that data (availability)
- the cost of informing others about the loss.

The costs cannot just be expressed in terms of money. For instance, the last cost, of informing others, is not just limited to, for example, postage and email charges. A company that suffers a data loss can also suffer a loss in its reputation as a professional organisation.

This problem is greatly magnified if personal data belonging to other people has been lost.

Case study: JournalSpace

At the end of 2008, the blog provider JournalSpace went into liquidation after the crucial database containing its customers' blogs was corrupted by a disgruntled former employee. This criminal action should not have proved fatal, but it became clear that the six-year-old company had not been keeping complete backups of their data.

JournalSpace customers were able to recover some of their data using copies of their postings held in Google's giant cache, but JournalSpace's reputation was ruined. JournalSpace was later reborn under new management, but by then it had lost most of its users.

The risk of data loss cannot be completely eliminated, but it can be minimised. The 2013 Forrester report suggested that malicious actions by disgruntled employees was the leading cause of internal breaches, but a significant number of security threats are caused inadvertently by employees who are unaware of the risks of their actions, such as copying data to external devices or websites, opening infected emails, clicking malicious links, installing software and so on. Better staff training could reduce the risk of accidental data loss.

The Infosecurity Europe survey revealed that while a slight majority of companies had implemented an internal information security policy to secure computers, networks and data, only a minority had provided staff training to raise awareness of potential security risks. Another important way of minimising the effect of any loss is by backing up data – making secure copies of data either on to a separate device, to a separate disk, or even to a different location.

Think about identity theft and loss of data. Have you ever been affected by these issues? Reflect on your personal experience.

2 Laws and computers

Figure 3

View description - Figure 3

Now that you have a broader understanding of the kind of things that can go wrong, you'll look at some of the most important laws in the UK that help to protect us against these cyber security threats. These are the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, the Computer Misuse Act 1990 and the Fraud Act 2006.

First though, we'll start with a brief introduction to the UK legal system. If you live outside the UK (or work with a multinational organisation) you'll also get a chance to find out what legal frameworks exist in your own country. It is still useful to learn about the UK laws so that you can look for the equivalent in your country.

Criminal and civil law

Law in Britain can be broadly divided into two categories:

- **Criminal law** is concerned with punishing behaviour that is considered unacceptable (murder, serious injury, fraud and so on). The majority of criminal cases are brought by the State against individuals and companies and require a high standard of proof to secure a conviction (‘beyond reasonable doubt’). Criminal cases can punish guilty parties with either fines or imprisonment, depending on the nature and severity of the offence.
- **Civil law** is concerned with disputes and these are usually brought before the court by individuals. Civil cases concern (among other things) property law, contracts and noise. There is a lower standard of proof (‘on the balance of probabilities’) than with criminal law and punishments are usually financial in nature.

Bills, Acts and Laws

An **Act of Parliament** is a law that has been approved by the British Parliament (Britain has a second type of law that has not been passed through Parliament known as Common Law).

An Act starts as a draft called a **Bill** which is debated in the elected House of Commons. If it is approved, the Bill is passed to a specialist committee made up from Parliamentarians for revision. Their changes are discussed further in the House of Commons and possibly revised further.

After a formal vote, the Bill passes from the House of Commons to the House of Lords for further scrutiny and possible amendments. The Lords will vote on the Bill before returning it to the House of Commons which considers their amendments. If the two houses agree (and sometimes they do not), the Bill is given Royal Assent and becomes an **Act**.

Some Acts take immediate effect, but often there is a delay between enactment and implementation as there may need to be processes put in place in order to achieve compliance.

So a Bill does not become law until it becomes an Act.

Keeping up with threats

It is worth remembering that cyber security is a fast moving area and therefore, legislation is constantly being revised based on new threats and court cases. In particular, the outcomes of trials can result in changes to the interpretation of existing laws as well as prompting creation of new laws. Additionally, because cyber threats are global, they can be affected by legislation from other jurisdictions.

Case study: Gary McKinnon

In 2002, the British hacker Gary McKinnon was accused of ‘the biggest military computer hack of all time’ against US Department of Defence and NASA computer systems, resulting in a demand for his extradition to the United States.

McKinnon fought extradition for 10 years, including an appeal to the House of Lords and the European Court of Human Rights, until the British Government blocked extradition in late 2012. He was not prosecuted in the UK due to the logistics of moving evidence and witnesses from the United States, the passage of time and the difficulties of bringing a case in England and Wales.

2.1 The Data Protection Act 1998 (DPA)

Figure 4

View description - Figure 4

The original Data Protection Act (DPA) became law in 1984. Organisations were legally obliged to act responsibly with respect to personal information, which relates to data on any living individual, held in computer databases.

It was replaced by the Data Protection Act 1998 which was implemented in two stages in 2000 and 2003. This change was needed to reflect the changes in technology that had passed since the original DPA. The 1998 Act is currently in force and will be for the foreseeable future.

The Information Commissioner’s Office is an independent supervisory authority appointed by the government to oversee and enforce compliance with the Act in all dealings with personal

information and to ensure access is freely available to recorded information held by public authorities. The Office reports directly to the UK Parliament. Note that the Scottish Information Commissioner's Office promotes and enforces freedom of information in Scotland.

The DPA enforces strict rules on the storage and processing of electronic data that can uniquely identify a living person. It is designed to stop data being obtained or stored unnecessarily, to prevent it from being exchanged without good reason, to ensure it is held under secure conditions and to give individuals redress if they feel their personal data has been misused.

So, all organisations that store information on living individuals must comply with the Data Protection Act. The Information Commissioner maintains a public register of these organisations called the Data Protection Register.

Before you look at the Act in more depth, let's define what is meant by 'information' and 'data' and how are they different?

- **data** is a representation of information so that it can be conveyed, manipulated or stored
- **information** is the meaning that we give to data in particular contexts.

So data cannot really be considered as information until it is given meaning and is interpreted by us. Opinion polls, where members of the public are asked their opinion on particular subjects, are good examples of where data is collected, stored and manipulated to show the resulting information as statistics. They may demonstrate how we might vote in the next parliamentary election, or whether one brand of food is preferred to another.

In terms of the DPA, data controllers are people who are employed by any organisation that stores, manipulates and retrieves personal information held on computers.

The DPA is based around eight fundamental principles of good information handling. Data controllers are legally required to act in accordance with these rules, the details of which are explained in

the Principles of the DPA (PDF). The case study below describes an example of the data protection act being used.

Case study: The British Pregnancy Advisory Service

The British Pregnancy Advisory Service is a charity offering confidential advice to pregnant women, including information about abortion and sterilisation.

In early 2012, a hacker defaced the charity's site, claiming to have obtained records of nearly 10,000 people who had contacted BPAS and threatening to post their details online. Police were able to determine the IP number of the attacker's computer and James Jeffery was arrested the next day in the West Midlands. No confidential data was released, although copies of the BPAS data were found on Jeffery's computer.

BPAS had initially acquired the names through a 'call back' form where people could leave details so they could be contacted later, but had chosen to not continue with the 'call back' because of security concerns. However, unbeknownst to BPAS, the data was retained on the site and inadequately secured from attacks.

BPAS was fined £200,000 for the breach, although at the time of writing it was contesting the fine. In April 2012, James Jeffery was sentenced to 32 months in prison under the Computer Misuse Act.

Inadvertent breaches of the Data Protection Act may be prosecuted although no harm was intended.

Case study: Hertfordshire County Council

In June 2010, Hertfordshire County Council breached the DPA on two occasions when its childcare department accidentally

sent faxes to incorrect numbers.

On the first occasion, documents intended for lawyers were sent to members of the public, and on the second occasion, information including personal information about two children in council care, criminal convictions of two people and domestic violence records were sent to a legal practice unconnected to their case.

The council correctly alerted the Information Commissioner to the two breaches, but was fined £100,000 because of the seriousness of their mistake which could have had serious consequences for the safety of children in the council's care.

Next, you'll learn about The Regulation of Investigatory Powers Act.

2.2 The Regulation of Investigatory Powers Act 2000 (RIPA)

Figure 5

View description - Figure 5

The Regulation of Investigatory Powers Act 2000, usually known as RIPA, governs the use of surveillance technologies by public bodies such as the police, the intelligence services and local authorities.

RIPA ensures intrusive powers are subject to strict safeguards. These covert surveillance powers include intercepting communications, using bugs, covert CCTV and undercover agents.

The use of RIPA is overseen by three commissioners: the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner. The Investigatory Powers Tribunal, which comprises independent senior lawyers and members of the judiciary, can hear complaints relating to the exercise of powers under the Act.

RIPA allows certain public bodies to access communications records from communication providers, such as telephone companies and internet service providers, when necessary and proportionate to do so for a specific investigation. These records may include the names, addresses and telephone numbers of individuals, the time and duration of calls, the source and destination of emails and the location of mobile devices.

More intrusive techniques are subject to higher levels of authorisation. Another section of RIPA stipulates that the interception of the contents of communications (such as telephone calls and emails) must be authorised under a warrant issued by the Secretary of State.

In 2014 the UK enacted the Data Retention and Investigatory Powers Act, also known as DRIP, in response to a ruling by the European Court of Justice that existing EU Data Retention Directive was unlawful. DRIP extends the communications intercept powers of RIPA to non-UK communications companies, leading some to criticise it for extending the surveillance capabilities of the government. However, like RIPA, DRIP includes oversight by an independent board to ensure that its use does not erode civil liberties. Also, both RIPA and DRIP have ‘sunset’ clauses that means that parliament will have to debate and vote on them again in December 2016.

Next, you’ll find out about The Computer Misuse Act.

2.3 The Computer Misuse Act 1990 (CMA)

Figure 6

View description - Figure 6

The Computer Misuse Act 1990 (CMA) is one of the most influential pieces of legislation relating to computers. It has been the inspiration for similar laws being introduced in other countries.

It came about, in part, because of a 1988 case where two hackers broke in to the British Telecom Prestel network and obtained access to user accounts including that of Prince Philip.

Prestel was a text-based interactive information system developed by the UK Post Office in the late 1970s. Users could browse numbered pages of text (similar to the contemporaneous Ceefax and Teletext information services) on their television as well as send electronic messages to other Prestel users. Prestel services were expensive and the system did not become widely used, although

Prestel technology was sold to many other telecom companies. Prestel was gradually sold off in the early 1990s as the internet became available to domestic users.

The two hackers were originally tried and convicted under a law concerned with forgery and counterfeiting, but the conviction was overturned by higher courts who concluded that the Forgery and Counterfeiting Act 1981 had never been intended to be used for this purpose. This led the majority of legal experts to conclude that hacking was not actually illegal in Britain at the time.

The CMA was drawn up hurriedly and was criticised at the time for not being adequately scrutinised, but its central aims have stood the test of time. The original Act introduced three new criminal offences:

- unauthorised access to computer materials
- unauthorised access with intent of committing or aiding further offences
- unauthorised modification of computer material.

Note that ‘unauthorised’ in this context means that the attacker must be aware that they are not intended to use the computer in question. So using another person’s account details, or breaking in to a computer by a password attack are clearly unauthorised use of the computer.

The CMA has been amended a number of times to cover new offences including denial-of-access or denial-of-service to legitimate users (making denial-of-service attacks a criminal offence in the UK), and criminalising the creation and supply of software and hardware that might aid an attack on a computer. This not only criminalises the development of programs designed to break passwords or the development of certain types of malware, but it could potentially criminalise tools used by forensics experts to investigate computer systems which can be abused by attackers.

The CMA has been successfully used in a wide range of criminal cases including denial-of-service attacks against Kent Police, Oxford University, the United States Air Force, the CIA, Sony and Nintendo; fraudulent activities in online games; illegal access and disclosure of

confidential emails and personal information; theft from online banks; stalking; hoax calls to emergency telephone numbers and piracy.

The next act you'll find out about is The Fraud Act.

2.4 The Fraud Act 2006

Figure 7

View description - Figure 7

The Fraud Act 2006 was introduced to simplify a notoriously complex Act of Parliament called the Theft Act.

The previous law defined a large number of types of fraud, often tied to specific circumstances, that made for complex cases that were difficult to prosecute and for juries to understand. In fact, it wasn't until 1996 that obtaining money from a fraudulent bank transfer was specifically illegal in the UK!

The Fraud Act defines fraud in three ways:

- false representation
- failing to disclose information
- abusing power.

In each case, the defendant's conduct must be dishonest with the intention of making a gain, or must cause a loss (or the risk of a loss)

to another person or individual. Crucially, no actual gain or loss needs to be proved – the fraud might have been unsuccessful or it was stopped before it could take place.

The Fraud Act can be used against anyone attempting to perform fraud whether or not it takes place over the internet. However, Section 11 of the Act makes specific reference to electronic fraud and can be used to prosecute in response to:

- dishonestly obtaining electronic communications services such as a telephone, ISP or satellite television subscription
- cloning mobile phones so that calls made on one handset are billed to another
- reprogramming mobile phones to interfere with their operation or change their unique identifier information
- breaking encryption on encrypted communications services such as subscription television services or telephone conversations.

In the next section you'll learn about Lawful Business Practice Regulations.

2.5 Lawful Business Practice Regulations

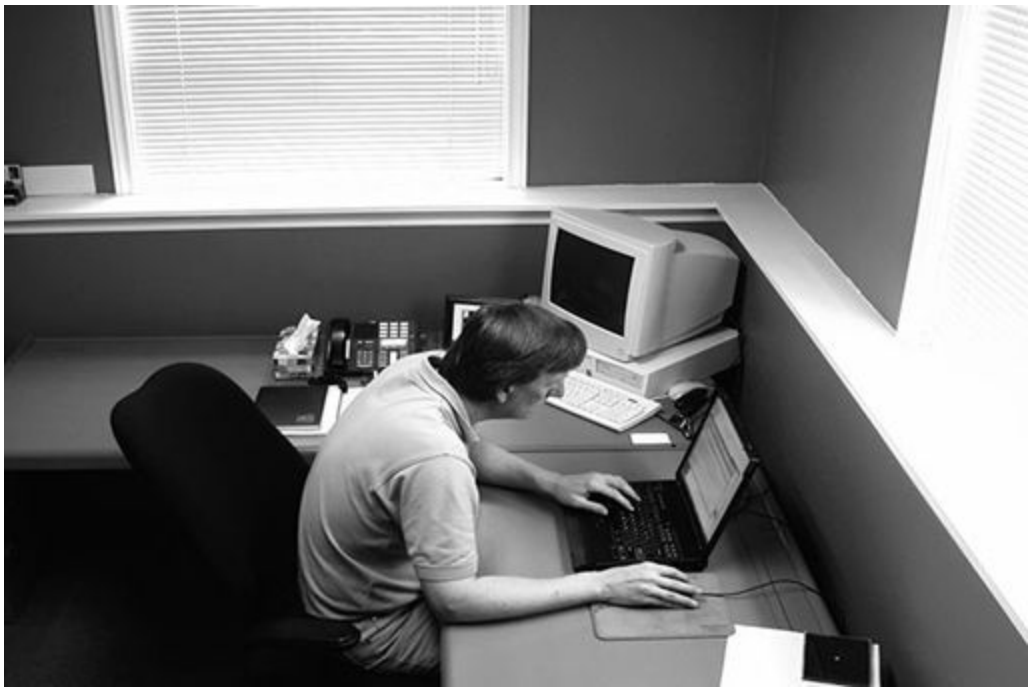


Figure 8

View description - Figure 8

Under UK law, employers have certain rights to monitor communications made by their employees.

They are authorised to do so under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699 (sometimes abbreviated to IC Regs). Monitoring can take many forms including recording telephone calls, storing telephone numbers, email addresses and website addresses, storage of email and the inspection of any email attachments.

The regulations exist so that employers can ensure that their networks are used in a manner that does not bring the company into disrepute (such as sending offensive emails would), be used for illegal activities (such as transmitting copyright materials without

licence), or to check that company resources are not used for personal reasons.

Companies may also have to monitor their networks to meet legal regulation – such as in the case of financial organisations where ‘health warnings’ must be offered to customers – and in extreme cases, monitoring may take place in support of national security.

The IC Regs are an exception to the general understanding that it is unlawful to intercept any communications unless an individual or organisation is specifically authorised to do so. This is codified in RIPA – see Section 2.2 The Regulation of Investigatory Powers Act 2000 (RIPA). The IC Regs allow interception to be made under specific conditions, but only if both parties in the communications consent to it happening. Such consent may be a necessary condition of employment, or it might be an additional agreement between an employer and their employees.

Monitoring of employees is an activity that must be done with care since it has the potential to erode trust between management and workers as well as being intrusive. Employers must abide by legislation including the Human Rights Act and the Data Protection Act to ensure that interceptions take place in a proportionate manner that any intercepted data is used for the correct purposes and that personal information is stored and processed appropriately.

Next you can complete an activity to check what you’ve learned about cyber security and the law.

2.6 Cyber security and the law

Check what you've learned about cyber security and the law by completing this activity.

Activity 1 The law

Allow about 5 minutes

Q1. Consider a scenario:

A hacker steals the customer database of an organisation by exploiting a well-known vulnerability in their computer systems. This vulnerability hadn't been fixed by the organisation despite the IT department being aware that there was a patch to fix the problem.

In the UK, under which of the following laws would the organisation have committed an offence?

- Computer Misuse Act
- Data Protection Act
- RIPA
- Fraud Act

Q2. Thinking about the same scenario:

A hacker steals the customer database of an organisation by exploiting a well-known vulnerability in their computer systems. This vulnerability hadn't been fixed by the organisation despite the IT department being aware that there was a patch to fix the problem.

In the UK, under which of the following laws would the hacker have committed an offence?

Computer Misuse Act

Data Protection Act

RIPA

Fraud Act

Next, you'll think about European laws and consider laws that apply in other countries.

2.7 The European Economic Area

Figure 9

View description - Figure 9

It’s worth remembering that the UK is also subject to European laws.

Part of that reciprocation is the subscription to a Europe-wide legal jurisdiction through the adoption of EC directives. This means that all the member states will have roughly the same law in relation to anything covered by an EC directive. However, there is some leeway in the interpretation of the directives, which is why countries still have their own laws and why there may be slight differences between them.

In the next section, you’ll be invited to find out about similar laws in a country of interest and share your results with other learners.

2.8 What laws apply in your country?

Figure 10 British hacker Gary McKinnon, accused of accessing US Department of Defence and NASA computer systems, seen here outside the Royal Courts of Justice in January 2009 as he was fighting extradition charges

If you live or work outside the UK, or work in a multinational organisation or have links with another country, you might be wondering if there is an equivalent set of laws in your country of interest.

Activity 2 Laws in other countries

Allow about 20 minutes

Carry out some research into similar laws that might exist in the country you are interested in and note down the results in the space below.

Look for laws that address one of these aspects of information security:

- data protection relating to living individuals
- misuse of computers
- investigatory powers
- fraud.

Find out:

- if equivalent laws exists
- what are they called
- what the differences are.

Based on your research, does it seem that the laws in other countries are similar, different or non-existent?

Provide your answer...

3 Who should you contact?

Figure 11

View description - Figure 11

So far this week, you've taken a broader look at the threat landscape that was introduced in Week 1 and learned how to recognise when you've suffered a successful attack on your information security. You've also learned about the laws in the UK (and in your own country) that are in place to protect you.

The rest of this week focuses on how to recover from the attack and what you can do to prevent a similar attack being successful in the future.

First, let's consider who you need to tell about the attack and what they need to know.

Responding to identity theft

If you have lost important documentation (such as passports, driving licences, credit cards and cheque books) you should report them immediately to the issuer so that they can be blocked and new copies can be issued to you. You should also report their loss to the police and ask for a crime reference number.

Report any unexplained transactions to your bank or credit card issuer so that they can be investigated by the company's fraud team. You may not be liable for any losses provided that you have acted in a responsible manner and without fraudulent intent.

Almost everyone has a credit report registered with a credit reference companies. A credit report is used by financial agencies to determine your suitability for financial services such as a credit card, bank loan or mortgage. Every time a user (or an impersonator) requests a new financial product, a credit search is made and included in the credit report. You can ask for a copy of your credit report from a credit reference agency (in the UK they are Callcredit, Equifax and Experian) which will list all searches made on that account, who authorised the search, what type of search was made and when it was performed.

Credit reference agencies can also provide a credit report checking service (for which they may charge) which keeps a track of any changes to your credit report.

For more information see ActionFraud.

Personal data and security

If you have accidentally opened a suspicious email message

If you aren't sure if a website is secure, look for the little padlock symbol showing a secure (SSL) connection. Look back at Week 5, Section 3.3, Encrypted network connections. If you are unsure of a site's authenticity, or if you can't see the padlock, then don't enter any personal details!

Bank card fraud

If you notice a charge on your card account that you didn't authorise, contact your card issuer as soon as possible. It may be that you've paid for goods you've not received or are suspicious about a website you've used. Give the card issuer as much information as possible – the name of the website, how much you spent, when you did it and so on.

The card issuer will investigate all cases of possible fraud and give you guidance which you should follow exactly. You may have legal protection, which means you're not liable for any losses, as long as you took reasonable care and did not act fraudulently.

You should also contact the police and complete a crime report. Visit The UK Police's website for reporting online fraud at ActionFraud.

Next, you will find out how to get your computer working again after an attack.

3.1 Getting your computer working again

Figure 12

View description - Figure 12

You've realised you have been the victim of a cyber security attack, you've reported it, now what? How do you get your computer working again? The next sections offer some advice.

Recovering from a virus or other malware

Your aim is to update your antivirus software then isolate your computer so that the malware doesn't spread. You can then start the computer in 'SafeMode' and remove the virus.

1. Make sure your antivirus software is up to date. Sometimes the automatic updating doesn't work reliably, or a paid subscription to an antivirus program might have expired. If downloads aren't

working correctly, try getting the latest update from the antivirus software manufacturer's website.
2. Now disconnect your computer from the network (including wireless networks). This will isolate it, preventing it from sending or receiving any more data; it cannot infect any more machines, nor can it receive data from elsewhere.
3. Restart the computer and start it in 'SafeMode' – on a Windows computer, press the F8 key as soon as the computer restarts and hold it down until the 'Advanced Boot Options' menu appears. Choose 'SafeMode', (not 'SafeMode with Networking'. 'SafeMode' is a special setting on the computer which restricts the number of applications that can run and stops it talking to networks even if they are plugged in. 'SafeMode' stops most malware from doing more damage to your computer.
4. When the computer finishes booting, open your antivirus software and tell it to perform a complete scan of the disk. This will take a considerable amount of time! At the end of the process, the antivirus program will report what it has found. It might also make recommendations about how to deal with the problem – follow its suggestions. When the virus scan is complete, restart your computer as normal.

Once you have completed these steps, spend a few minutes thinking about how the malware might have got on to your computer. Did you visit a suspicious website, download a suspicious program or simply click on an attachment in an email message? These are common ways to receive malware, so think about what you can do differently to prevent it happening again.

Recovering from accidentally deleting a file

Deleting a file isn't necessarily permanent. If you have simply moved a file to the trash can (Recycle Bin on Microsoft Windows), then you can recover it by simply dragging the file out of the trash. However, if you have since emptied the trash you will need specialised software to recover the file. The good news is that the data is still on the disk, the bad news is that the operating system cannot find it again. Fortunately, special file recovery software exists that can restore

deleted files. Find out about the software available from *About Technology*'s article 19 Free Data Recovery Software Tools.

Stop using the computer immediately you realise the file has been deleted. The less time that has elapsed between deleting a file and trying to recover it, the greater your chance of recovering the whole file. If significant amounts of time have passed, only a partial recovery may be possible, or it may not be possible to recover the file.

You then need to install a file recovery program (some file recovery applications can be run from an optical disk or a flash memory drive). A good selection of free file recovery applications can be found on *About Technology*. Run the file recovery application once you've installed it.

Note: Because of a difference between the way in which Microsoft Windows and Apple Mac OS store files on a disk, file recovery is much easier for Windows computers than Macs. A number of file recovery applications exist for the Mac, but there is much less selection than for Windows.

Once you've got your file back you might want to review your data backup strategy to prevent a future accident.

Recovering from a lost computer, disk or flash memory drive containing confidential data

The first question to ask is, was the data encrypted using a form of strong encryption? If it was, does it require a strong password to decrypt it? Is the password known only to you?

If the answer to any of these questions is 'no' then you may have a problem as the data is potentially vulnerable. If the lost property contains personal information, then you have an obligation to act under the Data Protection Act. Larger companies will have staff responsible for ensuring compliance with the DPA and you must get in contact with them as soon as possible so that steps can be taken

to protect individuals. Alternatively, you can contact the Information Commissioner's Office for guidance.

If you have lost material containing confidential information about a company or other organisation, or which is sensitive, then you need to contact the organisation which owns the data so they can take necessary steps. In certain circumstances, this may also require the involvement of the police or security services.

If the data is securely encrypted, then the data is almost certainly safe. You should still contact the relevant authorities to inform them of the loss.

Recovering from an operating system failure

If you use a recent version of Microsoft Windows (XP or later), you could use the 'Restore Point' feature to revert your computer to a previous working state. Windows automatically saves its configuration daily, when it updates itself and also when certain events, such as the installation of an unsigned driver for a peripheral device, occur.

Recent versions of Mac OS (10.5 or later) include a feature called Time Machine, which can be used to backup both files and system configurations. If you have Time Machine enabled it is possible to restore your Mac to a previous state, with hourly backups available for the past day, daily backups for the past month and weekly backups for anything older.

In the next section, you'll consider how to make your information less vulnerable to attack.

3.2 Making your information less vulnerable

Figure 13

View description - Figure 13

Some simple steps to make your information less vulnerable to attack in the future.

User accounts and passwords help secure data so that it can only be seen and used by authenticated users. Without a user account and password, an attacker is forced to use much more time-consuming techniques to break into the machine, greatly increasing their risk of being caught.

If you haven’t already done so, it is time to configure your computer and mobile devices so that they require a login or passcode when you switch them on and that that they lock when left for a certain period. This will prevent anyone tampering with them or impersonating you on social media if you leave them unattended.

A network firewall installed on a router and a personal firewall on the computer itself will stop hackers from getting into your computer. Likewise, up to date antivirus software can stop malware from deleting, encrypting or transmitting your files over the network.

If you have very important files that cannot be shared, then you should consider encrypting documents when they are not actively being edited. However, encryption can be troublesome when files must be shared since that requires sharing of keys which is generally considered inadvisable.

User accounts

All modern operating systems allow for different user accounts to be created with different levels of access. These range from a guest who can only perform a small number of tasks and cannot change any important settings, through to an administrator who can install new applications, see any data on the computer and make major changes to settings. In between, are user accounts that have limited access and do not usually allow users to install new software – helping to prevent malware infections.

Even if you are the only user on a computer it can make sense to use a user account for day to day purposes, only using the administrator account as and when new software needs to be installed or the operating system is updated.

User accounts can be used to restrict access to files, printers and other resources on a local area network.

File permissions

Every file and folder on your computer has a set of permissions that tell the computer’s operating system what can be done with that file:

- write permission – the file can be edited
- read permission – it can be copied
- execute – the file can be executed as a program (if applicable).

Different users have different sets of permissions – so you may have read and write access to an important document, but you can restrict others to read only (i.e. they cannot edit the file), and deny access entirely to people outside of the group.

Remember, read permission allows a file to be copied and to be read. An attacker can still then use copy and paste to copy important information from a document, or to make a copy of the original and to edit that instead.

Disabling ports

Almost all modern computers come with one or more USB ports through which data can be stolen using flash memory drives, a plug-in hard disk or smart phone or media player. It may be necessary to disable these ports for security reasons.

Data Loss Prevention (DLP) software can temporarily disable the USB ports, or monitor or restrict the copying of files to USB devices.

Locks

The easiest way to steal a large amount of data is to simply steal the computer itself. Most computers and some external devices have sockets into which a lock, usually attached to a flexible metal chain that is secured to a wall or a desk, can be attached.

Obviously, if you are working in a shared environment, locking doors and windows is an obvious deterrent to attackers, as is challenging unknown individuals who might be wandering around.

In the next section, you'll create a personal recovery plan.

3.3 Protecting your data for the future

Figure 14

View description - Figure 14

If you have not already done so, now is the time to consider investing in computer backups.

Backups protect us from threats including:

- accidentally deleting a file or program
- losing disks, computers or memory cards
- hardware failures such as a hard disk crash
- software bugs that prevent data being written to a storage device or cause it to be corrupted as it is written
- disasters such as fire or flooding
- crimes including terrorism, theft and acts of sabotage such as hacking.

Activity 3 Protection for the future

Allow about 30 minutes

Grab the list of digital information that you compiled in Week 1 and develop a plan to recover your data in the event that it is lost in a computer security breach.

For each type of information on your list, consider how you might go about recovering the data. Form a plan for each type of information.

3.4 Backup media

Figure 15

View description - Figure 15

Depending on the amount of data you need to backup, a range of technologies are available:

Optical storage

Optical storage is the same technology used for CDs, DVDs and Blu-Ray.

The most common technology for optical storage is writeable DVD standards including DVD-R, DVD+R, DVD-RW, DVD+RW and DVD-RAM. Most of these DVD formats can store 4.7 GB on a single disc, although newer, so-called, dual layer discs and drives can store twice that. Blu-Ray technology offers 25 GB and dual layer (50GB) formats with three layer 100GB discs, although they are expensive.

Advantages

- Optical drives and media are extremely cheap and widespread. Most computers have an optical drive or can accept a USB driver and the discs can be bought in supermarkets.
- There are a large number of manufacturers, so there should be no problem with future supplies of discs.
- More modern optical disc technologies (such as Blu-Ray) also support most older types of disc such as DVD and CD.
- The media is relatively small. Large amounts of data can be stored in a very small space.
- The media is robust. Discs can be posted and are able to survive regular use or being dropped. They are resistant to extremes of temperature and humidity, and immune to strong magnetic fields.

Disadvantages

- Optical drives are relatively slow compared to hard disks, especially when writing data.
- There are a large number of types of disc (especially recordable DVDs). Some of these discs are not widely supported.
- Their capacity is relatively low compared to hard disks. A 1TB hard disk is commonplace on modern computers, so it would take more than 200 DVDs to make a complete backup of the disk. Consequently, DVDs might be best suited to making backups of key data.

Magnetic disks

The magnetic hard disk at the heart of most computers can also be used as a backup device. Most PCs have sufficient internal space for a second hard disk that can be devoted to backups, or a relatively cheap external hard disk can be connected to a USB or Firewire port on a computer.

More expensive disks can be connected directly to a network using Ethernet or wi-fi in which case they are known as Network-Attached

Storage (NAS). Disks can be made more resilient to failure by combining several disks together with copies of data stored on multiple disks so that even if one copy is damaged or the disk fails, it is not lost forever; the most common type of this ‘redundant’ storage is called a Redundant Array of Independent Disks (RAID).

Advantages

- Disks are relatively cheap and capacities are growing rapidly.
- External hard disks can be easily moved between computers.
- There are many disk manufacturers, all of whose products can be used in almost any computer.
- There are a large number of backup programs designed to be used with hard disks. Many external disks are sold with applications to ease the backup process, or offer a ‘one touch’ backup button.

Disadvantages

- Hard disks are fragile and easily damaged if dropped or exposed to extremely high temperatures or magnetic fields.
- If hard disks are used once to make a backup then archived, the replacement cost is much higher than for tape or optical media.

Solid State Disks

Solid State Disks (SSDs) are storage devices that can store data in memory chips without the need for a power source. The name is somewhat misleading because these devices don’t actually contain physical disks. They can be commonly found in the USB memory sticks used for sharing files between computers. As the technology has advanced to increase the storage capacity of SSDs they are now being used in laptops and mobile devices as substitutes for magnetic disks.

Advantages

SSDs have the same advantages as magnetic disks when compared to optical storage technologies. Some additional advantages are:

- SSDs are more robust and are unlikely to be damaged if dropped or exposed to magnetic fields.
- It is possible to read and write data from SSDs much faster.
- There is no noise produced when SSDs operate because they have no moving parts.

Disdvantages

- SSDs are more expensive than equivalent capacity magnetic disks.
- At the moment, the maximum capacity of SSDs available on the market is 1TB although this will increase as the technology advances.

Next, you'll learn about remote backups.

3.5 Remote backups

Figure 16

View description - Figure 16

Large businesses and organisations insure themselves even further against failure by storing backups away from their centre of operation.

In the event of a disaster, there is much greater likelihood that they can return to normal operations within a short period of time – after all, it is much easier to buy new computers than recreate all of the records.

Offsite backups

Specialised companies offer specialised facilities where companies can hire storage space or machinery to hold backups. These offsite facilities might be nothing more than an extremely secure vault where tapes or disks can be deposited; but increasingly they are

large server farms connected to extremely high-speed networks. Users can copy files to these servers as if they were part of their own network; the only bottleneck is the speed of the network between the offsite facility and the user.

The UK's largest such site is Telehouse UK in London's Docklands which has partner sites in the United States and Japan. The London facility covers some 45,000 square metres and is used by over 700 large companies and internet service providers.

Backing up to the cloud

For many years, offsite backup was restricted to organisations which could afford relatively large monthly fees. cloud technology allows anyone to have offsite storage, and in many cases a certain amount of storage is completely free. Most cloud services are designed for convenience, to allow users to share files between computers, and with other users, rather than specifically as backup services, but they can also offer you some additional security (especially when you encrypt files before putting them in the cloud) if your computer is stolen or stops working.

One strong word of warning if you do use the cloud as a backup, with only a few exceptions, these services will not protect you if a file is deleted. Most cloud services are synchronised – that is, when a file is deleted on your computer, the copy on the cloud server is either immediately, or very shortly afterwards, also deleted.

Cloud backups are obviously limited by the bandwidth of your internet connection. If you have a slow uplink (that is sending data to the cloud) you may not be able to make backups of all your data in a reasonable amount of time. Instead you might have to prioritise which data is backed up to the cloud and which is stored locally.

Cloud security

Unless you take further steps, once data is stored in the cloud you can no longer be sure that it is entirely secure from prying eyes. Most suppliers have policies claiming that your data will be secure,

but they cannot provide absolute insurance from attackers, as experienced by some celebrity users of Apple's iCloud service in 2014. You can read more about this incident, if you are interested, via the link in the Further reading section at the end of this week.

Some businesses have policies forbidding employees from storing information in the cloud as it may not be secure, or it may be stored outside the legal protection of the company's country of origin.

Using encryption to scramble the contents is the only way you can guarantee that your data is safe in the cloud.

In the next section, you'll consider your own backup procedures.

3.6 Do you backup your data?

Figure 17

View description - Figure 17

For this activity thin about how you backup your own data.

Activity 4 Do you backup?

Allow about 15 minutes

Write a short description of how you backup data. Describe the different technologies you use, how often you backup and what risks remain.

If you don’t perform backups, but you work for an organisation who does, briefly explain their backup procedure (you might need to talk to the person in charge of the company’s computers).

If neither of these situations applies, briefly explain what sort of backup procedures you think would offer you a reasonable amount of security.

Warning: Do not identify your company or organisation if you discuss this with others.

Provide your answer...

In the next section, you'll examine archiving data.

3.7 Archiving data

Figure 18

View description - Figure 18

In a perfect world, each of us would keep a backup of every piece of data we ever use, but it is simply impractical for most of us to buy enough media to store our backups.

Instead, most media are reused after a certain period of time with old backups written over by new data. Businesses, in particular, must retain backups for a number of years (for legal and tax purposes) before media can be recycled.

Important files, especially those of historic or legal interest should be archived so that they are never overwritten. In many countries, it is a legal obligation for companies to archive data for auditing purposes. Governments around the world are recognising the importance of archiving data and authorising national bodies to store important digital records. In Britain, this work is managed by the National Archives and the British Library.

Next, you'll have an opportunity to review your knowledge in the end-of-week practice quiz.

4 Week 7 quiz

This quiz allows you to test and apply your knowledge of the material in Week 7.

Complete the Week 7 practice quiz now.

Open the quiz in a new window or tab then come back here when you’re done.

5 Summary of Week 7

Figure 19

View description - Figure 19

While most of this week's learning is about how to recover from a disaster, it is worth spending a few minutes reminding yourself what can be done to minimise the risk of a breach in your security.

These relatively easy measures will greatly increase your computer and mobile device security and we have covered many of them over the past few weeks:

- each user has their own personal accounts when using a computer
- use strong passwords (and perhaps a password manager application)
- set your computer and mobile devices to require a login or passcode when you switch them on and when they lock after being left for a certain period
- keep your operating system and key applications up to date

- install antivirus software and keep it up to date
- protect wireless networks using modern (e.g. WPA2) encryption
- enable a personal firewall on your PC and a router firewall.

You could also take these measures, which might require some assistance, or if you are in a business environment, the approval of a system administrator:

- encrypting your hard disk
- using encrypted flash memory drives.

Look at the list of security measures above. Do you think any of them apply to you and your computer and mobile devices? Make a note of the security measures that apply to your situation and make some notes on how you could implement them.

You can now go to Week 8: Managing security risks.

Further reading

Apple toughens iCloud security after celebrity breach

Week 8: Managing security risks

Introduction

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Cory introduces the final week of the course.

Over the past seven weeks, we have explored different cyber security threats together with actions we can take to prevent these threats from causing harm to our digital lives.

This final week of the course focuses on how to assess the security risks associated with your digital life so that you can effectively plan to protect yourself from attacks.

1 Information as an asset

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – www.open.edu/openlearn/science-maths-technology/introduction-cyber-security-stay-safe-online/content-section-0

Figure 1

View description - Figure 1

You'll remember from Week 1 that, when thinking about computer security, it helps to think of information as an asset. Just like money in the bank, it is valuable, possibly irreplaceable, and crucially it can be lost or stolen.

When we think about our assets, traditionally we consider tangible things such as money, property, machinery and so on. Increasingly, it is recognised that information itself is an asset, crucial to adding

value. In today’s digital world, it is increasingly apparent that information is the most important asset, for both businesses or individuals – just think of the value of music to a media company or a games program to a video game company.

Considering information as an asset allows us to create strategies for protecting information and minimising the consequences of any disaster.

Case study: San Francisco Medical Center

In October 2002, the University of California, San Francisco Medical Center received an email message from someone who claimed to be a doctor working in Pakistan and who threatened to release patient records onto the internet unless the money owed to her was paid. Several confidential medical transcripts were attached to the email.

UCSF staff were mystified, they had no dealings in Pakistan and certainly did not employ the person who sent the email. The Medical Center began an immediate investigation, concentrating on their transcription service, which had been outsourced to Transcription Stat, based in nearby Sausalito. It transpired that Transcription Stat farmed out work to 15 sub-contractors scattered across America. One of these sub-contractors was Florida-based Sonya Newburn, who in turn employed further sub-contractors, including Tom Spires of Texas. No one at Transcription Stat realised that Spires also employed his own sub-contractors, including the sender of the email. The sender alleged that Spires owed her money, and had not paid her for some time.

Newburn eventually agreed to pay the $500 that the email sender claimed was owed to her. In return the sender informed UCSF that she had had no intention of publicising personal information and had destroyed any records in her care. Of course, there is no way to prove that the records have actually been destroyed.

Naturally, you would not wish your own medical records to be publicised: they should be secure. This threat cost the organisation little in monetary terms, but how much in reputation? Just what is a reputation worth? Or, to put it another way, how much should you invest in information security to protect a reputation?

Information in this context is a very broad term and it applies to large and small organisations as well as to individual users. So a doctor’s surgery’s information assets would include things such as personal medical records, telephone contact lists, its emails as well as personal information about its employees. A manufacturing company will have electronic records of order books, correspondence with suppliers and customers, staff records, bank references and so on.

Risk management

Information security risk management assesses the value of information assets belonging to an individual or an organisation and, if appropriate, protects them on an ongoing basis.

Information is stored, used and transmitted using various media; some information is tangible, paper for example, and it is relatively straightforward to put in place strategies to protect this information – such as locking filing cabinets, or restricting access to archives.

On the other hand, some information is intangible, such as the ideas in employees' minds, and is much harder to protect. Companies might try to secure information by making sure their employees are happy, or by legal means such as having contracts that prevent people leaving and going to work for a rival.

Imperatives and incentives

Information security risk management considers the process in terms of two factors: imperatives or incentives. Imperatives are pressures that force you to act. Incentives are the rewards and opportunities that arise from acting.

The imperatives for information security arise from legislation and regulation. The Computer Misuse Act and the Data Protection Act, which we discussed last week, are examples of legislative imperatives. Regulatory imperatives include standards such as the Payment Card Industry Data Security Standard (PCI-DSS), which specifies how merchants should secure all card transactions.

The most important incentive is trust. People and organisations are more likely to work with other people and organisations who have secured their information. Establishing this trust requires that the parties involved examine each others' information security practices to ensure that there are adequate safeguards to protect the information. One way of doing this is to show that the organisation has satisfied the requirements of standards such as PCI-DSS or the ISO27000 family of standards for designing and implementing information security management systems.

In the last few weeks, you have covered all of these aspects – you have learned about a range of threats that confront internet users, you have explored laws that have been drawn up to regulate information and you have seen how the internet is fundamentally underpinned by trust and how technologies such as encryption and signatures can help us feel secure. In the next section, you are invited to apply this to your own information assets.

1.1 Your own information assets

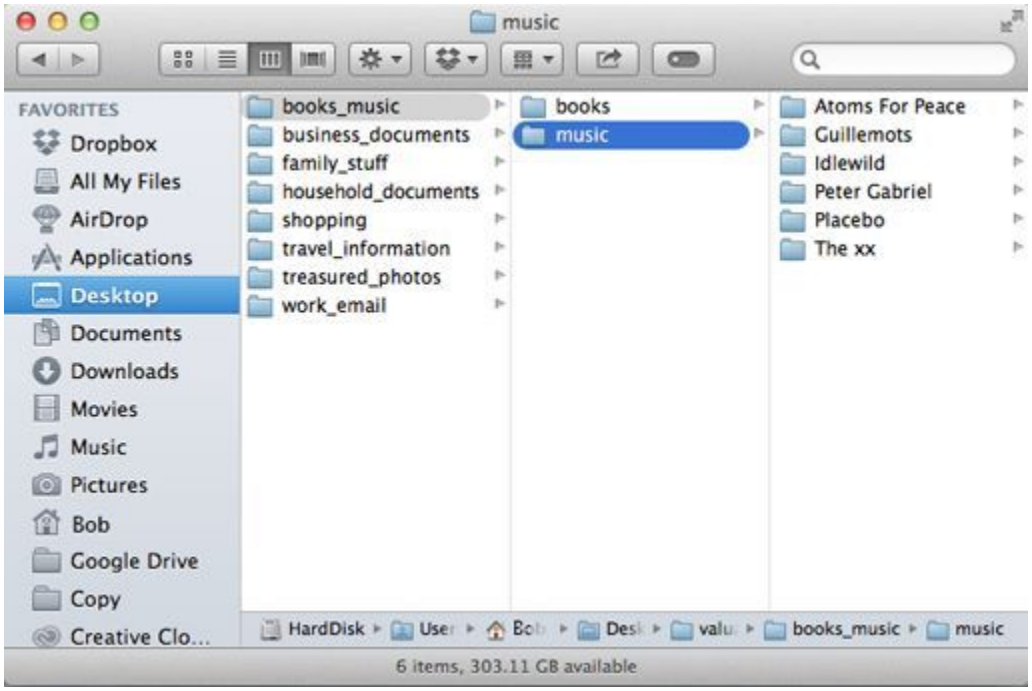


Figure 2

View description - Figure 2

In Week 1, you created a list of information assets that you possess. This was any sort of information that you store on a computer system that you use and which would be expensive, inconvenient, or impossible to replace if it was lost, damaged or stolen.

Spend a few minutes reviewing your list and thinking about whether you need to add anything based on what you have learned over the past eight weeks.

Lewis, a student of The Open University, did the same exercise on his own computers:

- study materials – documents and data relating to his postgraduate studies
- digital photographs – about 20,000 images taken over the last ten years

- music – about 10,000 tracks ripped from CD or bought online
- movies – about 200 films and TV programs
- email – about ten years worth of correspondence
- banking and other financial records
- passwords and account details.

Duplicates of some of these assets could be obtained if he lost the originals, for instance iTunes will allow him to download new copies of any lost music, but it would take a very long time to rebuild the entire library. Some others, such as emails and financial records could be recreated, but only by spending a lot of time asking for information from other people.

Passwords could be changed and other authentication information could be recovered, but again it would take a great deal of time and inconvenience to get back to normal. If these items had been stolen, an attacker might have been able to misuse those assets. The photos would, almost certainly, be lost forever.

Now look back at your own list of information assets. Does Lewis's list prompt you to add any items to yours?

Next, you will learn about risk analysis.

1.2 Risk analysis

Figure 3

View description - Figure 3

We use the term ‘risk’ in everyday speech, but a whole science has grown up around the identification, analysis and management of risks. You will now look briefly at how to apply some of these ideas to identifying, assessing and reducing risks that affect the security of your information.

Risk can be thought of as the chance of adverse consequences or loss occurring. Generally, risks can be identified and the likelihood of them occurring assessed.

The main technique for a qualitative analysis of risk is to construct a likelihood–impact matrix in which the likelihood and impact of each risk event are assessed against a defined scale and then plotted on a two-dimensional grid. The position on the grid represents the relative significance of each risk. The simplest matrix is formed by classifying both likelihood and impact as either high or low, which

leads to a 2 by 2 grid. This basic classification of a high or low value leads to the following rank order for tackling risks:

1. high-impact, high-likelihood risks
2. high-impact, low-likelihood risks
3. low-impact, high-likelihood risks
4. low impact, low-likelihood risks.

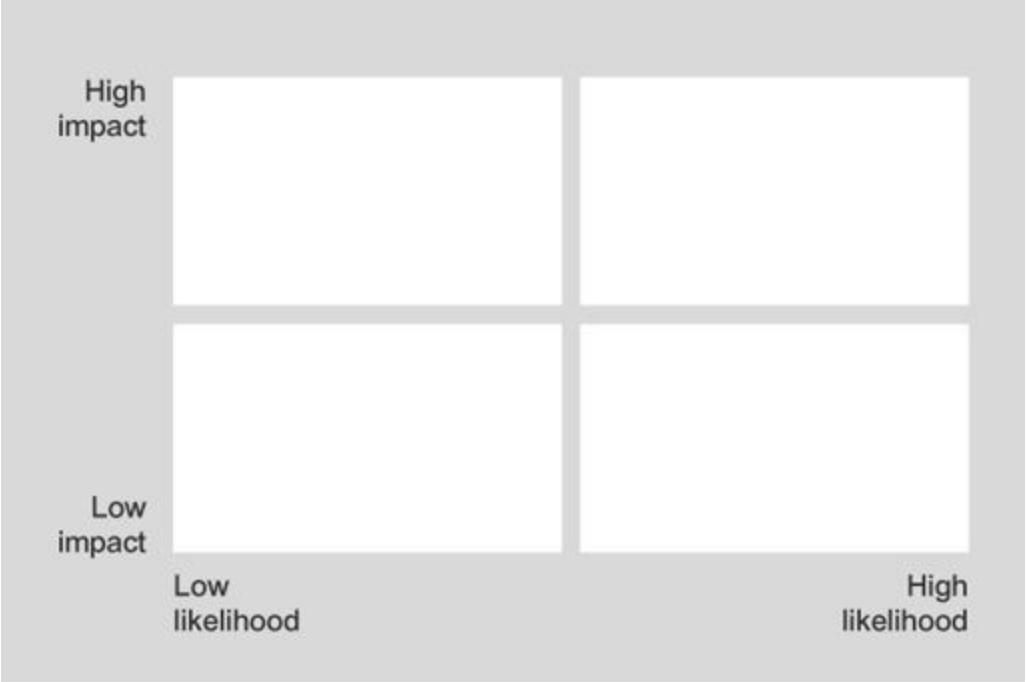


Figure 4 Risk analysis grid

Low-impact, low-likelihood risks are probably not worth expending much effort on (but see the discussion of risk acceptance later this week). You can then look at these high-impact or high-likelihood risks one by one to determine whether there are ways either to reduce the impact if the risk occurs or to reduce the likelihood of the risk occurring, or both.

The next stage is to apply quantitative techniques, based on a financial assessment of the impact of each of the risks, to put the risks into order, with the greatest risks at the top of the list.

It is beyond the scope of this course to discuss these techniques. Sometimes it is hard to reach a decision about the importance of some risks until a corresponding response has been identified as

well as any possible interactions between risk events and responses, so risk management is usually iterative in practice.

Next, you'll do some risk analysis on your information.

1.3 Risk analysis in practice

Let’s think about a practical example of how qualitative risk analysis could be done for Lewis’s information assets.

Any successful attack on email, banking details and password information will have high impact and there is a high likelihood that these attacks will be targeted due to their high value. So they should go in the high-high box.

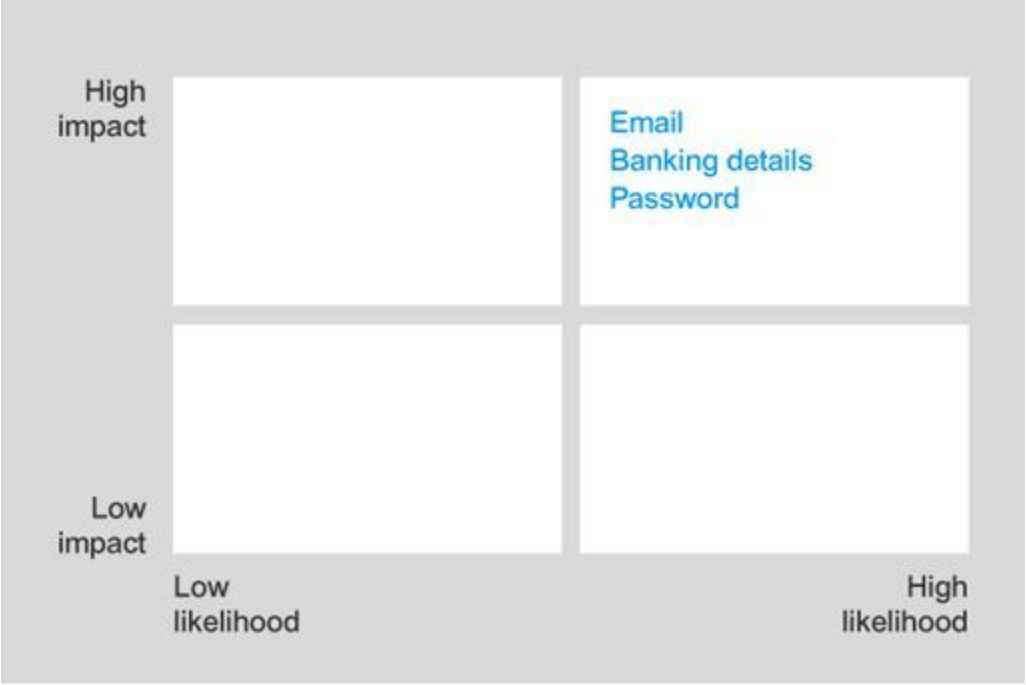


Figure 5

View description - Figure 5

An attack that affects the study materials or digital photographs will have high impact, but there is a low likelihood given that these assets have minimal financial value to an attacker. These should be placed in the high-low box.

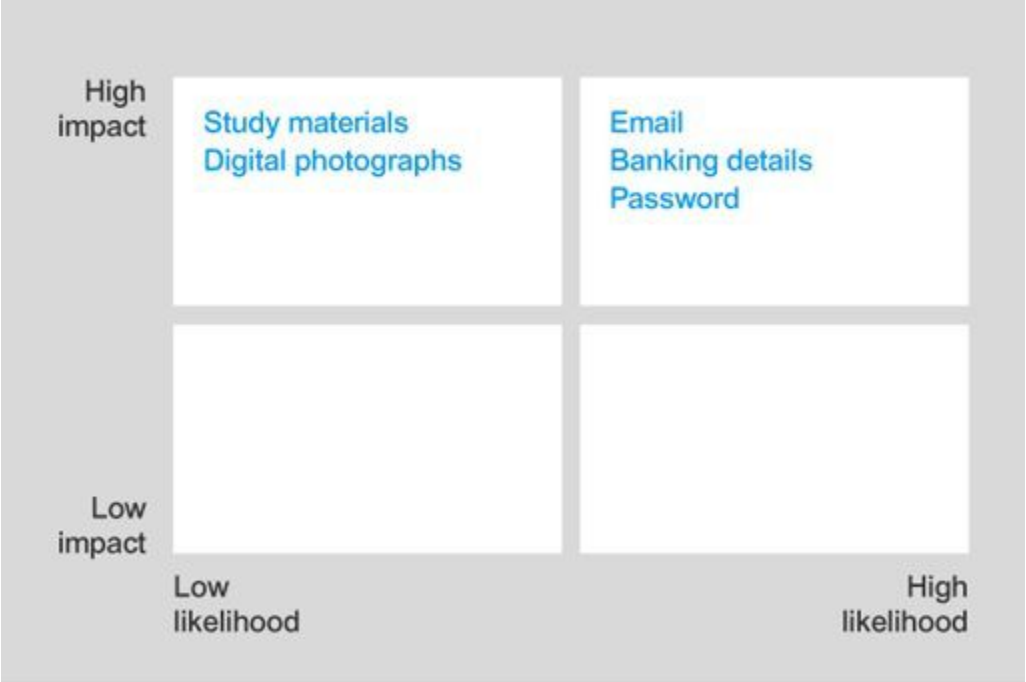


Figure 6

View description - Figure 6

An attack on the digital music or videos will have low impact, since these can be downloaded again easily. However, this will have high likelihood because these assets can be easily copied and sold, this making these attractive to an attacker. Therefore, they go in the low-high box.

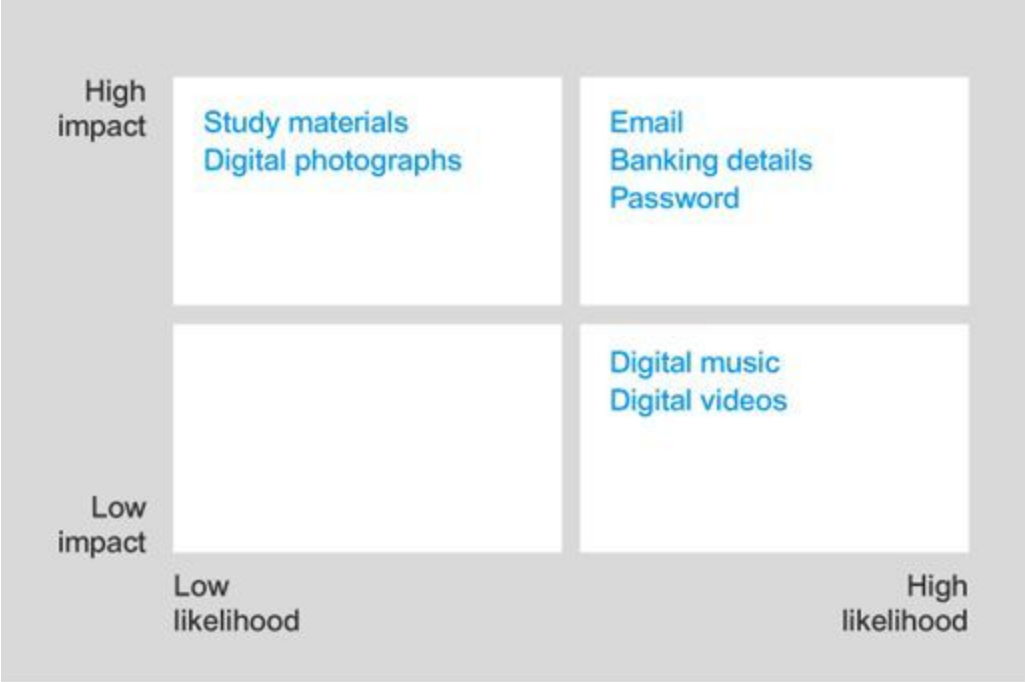


Figure 7

View description - Figure 7

Conducting a risk analysis is an important part of protecting your information assets. Following Lewis's example consider your own list of information assets and carry out a similar risk analysis to determine the impact and likelihood of attack for each type of information.

2 Staying safe online

Figure 8

View description - Figure 8

There are a number of things you can do to stay safe on the internet. Like almost all parts of life, although you hear terrible stories, most people never have serious problems online. By taking a few simple steps, you can make yourself and your computer much more secure.

Stay up to date

Out of date software is one of the biggest problems for computer users. Bugs that have been fixed in newer operating systems or applications may remain unresolved in previous versions, leaving you vulnerable. This is especially important in the case of operating systems, which are responsible for managing files and connecting to the internet.

To keep up to date you will need to check whether your operating system is still supported, so you should consult the software support website such as those provided by Microsoft or Apple.

Many other applications, such as Microsoft Office, the Java programming language (used by a lot of websites), web browsers and so on, also require regular updating to fix security problems.

If you are using an old operating system that is not supported by its manufacturer, or if you need an application, but your current edition is out of date, it is well worth investing in updated software. First, though, check that your computer can run the updated software, if not, it might be time for a new computer.

Do the basics

The basic check list:

- set up a personal firewall
- install an antivirus program (remember, Macs do need antivirus protection)
- get used to making backups
- set up your computer to require passwords to log in and when unlocking the screen
- use hard disk encryption if you have it – especially on laptops.

It will take a couple of hours to perform these steps, but your computer will be significantly more secure.

Fix your email

Most email applications now come with junk mail screening. If it’s not already enabled – turn it on! Your mail program will scan incoming email looking for suspicious messages that might be trying to scam you – or are just annoying spam. It puts any suspect messages into a junk mail folder where you can examine them later, just in case any genuine messages were misfiled.

Most email programs will also let you train the screening process so that any messages that were missed can be treated as junk in the future.

In the next section, you’ll learn some tips to improve your web browser’s security.

2.1 Fix your browser

Figure 9

View description - Figure 9

There are a couple of simple things you can do to improve your web browser’s security.

Cookies are small pieces of data that can be used to track your use of the web and some websites host cookies belonging to organisations you know nothing about – these are called ‘third party cookies’ and they’re no use to you whatsoever.

Find the appropriate sections for the web browsers you have installed from the selection below, and use the browser’s preferences section to locate the cookie preferences and fix them.

Google Chrome

From the **Chrome** menu, make sure the **Settings** page is shown, then choose **Show advanced settings**… at the bottom of the page. In the **Privacy** section, click the **Content Settings** … button then choose '*Block third-party cookies and site data*.' You might also want to block pop-up windows (which are annoying and can also be abused by attackers). Click **Done**.

Then look through the comprehensive list of privacy options, selecting any you wish to set – we recommend the '*Enable phishing and malware protection*' and '*Send a "Do Not Track" request with your browsing traffic*'.

Apple Safari

Go to the **Safari** menu, then **Preferences**, choose **Privacy**. In the **Cookies and other website data** section select the '*From third parties and advertisers*' option. You might also want to select the '*Ask websites not to track me*' option which restricts the ability of websites to follow your progress around the web.

There are some further useful settings in Safari's **Preferences – Security** section. You should make sure all the security settings are turned on.

Finally, in the **Preferences – General** section, make sure the option to automatically open 'safe' files is turned off. Although Safari is very good at checking that files are safe to open, it is possible that a dangerous file could be get through. Turning off 'safe' files just means that you will have to open the file yourself. If you find a file you did not request, delete it just in case.

Mozilla Firefox

From the **Firefox** menu choose **Preferences** … then **Privacy**. Before going any further, select the '*Tell websites I do not want to be tracked*' option, then in the **History** section, choose '*Use custom settings for history*' from the drop-down menu. Make sure the option '*Accept third-party cookies*' is unselected.

You can also find useful settings in the **Security** section. Make sure the '*Warn me when sites try to install add-ons*', '*Block reported attack sites*' and '*Block reported web forgeries*' are all selected. These will prevent unwanted software from being installed on your disk and help stop you visiting hijacked or dangerous websites.

Microsoft Internet Explorer

Click the **Tools** button then choose **Internet Options**. Select the **Privacy** tab. Move the slider from side to side to customise the level of privacy you want (we'd recommend any of **Medium**, **Medium High** or **High**). At the same time select the '*Turn on Pop-up Blocker*' option to stop annoying pop-up browser windows which are often used by advertisers.

Click **OK** when you are finished.

Opera

From the **Opera** menu choose **Preferences** … , the **General** tab has an option to block pop-up windows. Choose '*Block unwanted pop-ups*' if it is not already selected.

On the **Advanced** tab, choose **Cookies** from the left-hand menu and choose '*Accept cookies only from the site I visit*'.

Also on the **Advanced** tab, select **Security** from the left-hand menu and make sure the two options '*Ask websites not to track*

me’ and ‘*Enable Fraud and Malware Protection*’ are enabled.

Click **OK** when you are finished.

Your browsers should now be much better protected!

Next, you will decide what to do about the risks to your digital information and share your resolutions with your fellow learners.

2.2 Risk management in practice

Figure 10

View description - Figure 10

Having analysed the situation, the next stage is to decide what to do about the risks.

For each risk to be managed, we need to identify what cost-effective countermeasures can be applied. Possible countermeasures are:

- **Avoiding the risk** – avoidance would mean stopping the activity that is causing the risk. For example, deleting all banking information and unsubscribing from internet banking would avoid the risks associated with the information assets related to banking.
- **Modifying the risk (likelihood and/or impact)** – this involves choosing and implementing a security mechanism that reduces the likelihood of a successful attack, or the impact that would result from such an attack. For example, installing an up to date antivirus application can prevent the attacker from using

malware to gain access to the computer holding the internet banking information.

- **Transferring the risk to others** – typically involves taking out insurance to cover any losses in the event the threat materialises.
- **Accepting the risk** – would mean choosing not to implement any of these countermeasures, choosing instead to monitor the information asset for any attacks.

Consider risks identified in the qualitative risk analysis. Choose one of your information assets and decide on which countermeasures you would apply in this case.

2.3 Protecting your information assets

Figure 11

View description - Figure 11

Now you've done a risk analysis, it's time to look at how we can better protect our information assets.

You've already thought about backing up data and using encryption to protect information – but have you put any of these measures into practice?

Go back to the list of information assets you used in your risk analysis. What steps have you taken to protect them? Think in terms of what you have studied on this course. For example:

- Have you set up firewalls to protect your networked computers from external attack?
- Are you protected by up to date antivirus software?
- Are your operating system and key applications up to date?
- Is important information protected by encryption?

Note, next to each item on your list, the measure you have taken to protect it. If you have not yet implemented that measure, identify it in some way that will remind you to action it.

In the next section, you are invited to create a plan for implementing and maintaining your information security.

2.4 What should I do next?

Figure 12

View description - Figure 12

You have now taken several simple but very important steps to protect your information. Review your list of information assets and work through what else you need to do to improve your own security.

Based on the risk analysis you have done for your information assets, create an information security action plan detailing the countermeasures you could implement to protect each asset.

Before proceeding, you should implement at least one set of countermeasures. In time, you should implement all the countermeasures and also periodically review your risk analysis and action plan to make sure that you are maintaining your countermeasures.

Next you'll learn about some of the recent developments in cyber security.

2.5 Tracking a moving target

Figure 13

View description - Figure 13

Security is an ever-changing topic. New technologies are always being introduced and they bring new risks, or allow old threats to resurface in a new form.

Old technologies are retired by manufacturers, potentially leaving their users exposed to danger as bugs and security weaknesses remain unaddressed. And there are new threats being discovered every day, as the Heartbleed bug shows only too well.

In April 2014, news broke about a serious bug that affected at least half a million websites. Called ‘Heartbleed’, the bug affects a program used by web servers to establish secure connections for web browsers so that financial or personal information can be safely exchanged over the internet. Heartbleed is a fault in OpenSSL’s heartbeat function which is usually used by the computer on one end of an SSL connection to check that the remote computer is still

connected. However, the bug allows a fake heartbeat message to return a copy of the contents of a chunk of the server's memory which could include the site's certificates (used to prove the site is genuine), unencrypted user passwords, credit card numbers or other personal information.

The Heartbleed bug was introduced into a version of OpenSSL released in early 2012 and was present in all versions of the software until April 2014. For more than two years Heartbleed was present on a huge number of websites, including those of very large organisations such as Yahoo!, the photo sharing site Flickr (owned by Yahoo!) and the slate.com news site, during which it created a security risk for all users.

To the best of our knowledge, Heartbleed was discovered by two groups of researchers, including people at Google, who, as is typical for computer security, worked with the designers of OpenSSL to fix the problem before a public announcement of the bug. However, it is entirely possible these weren't the first people to find Heartbleed and it might have been known to criminals for some time.

At the time of writing, the effects of Heartbleed are still not known. So far, thousands of developers all around the world have been checking and updating web servers, creating new security certificates and in some cases asking all users to change their passwords. Even if no crime is ever committed as a result of Heartbleed it will have cost a huge amount of money to fix.

3 What do you do now?

As we approach the end of the course, it's a good opportunity to reflect on what you have learned and how it has impacted your ability to protect your digital life.

At the beginning of the course, you took a survey on your information security practices. We'd like you to retake it now to see how your practices have changed.

Launch the survey – answer the questions based on your habits **now**. There are no right or wrong answers so you should choose the answer that most closely matches the way you use your computer now that you've completed the course. Don't worry, all the data is anonymous and we will not reveal individual answers.

When you've finished you can compare your answers with those you gave at the start of the course.

When this course was originally run, the results were collated by the author of the course, Arosha, in his blog. You might want to take a look at those results.

3.1 Confessional

Figure 14

View description - Figure 14

In Section 2.4, What should I do next?, we asked that you implement at least one of the countermeasures you included in your security action plan.

Activity 1 A security problem

Allow about 20 minutes

Use the space below to note down the details of a security problem that you spotted and took appropriate countermeasures to address.

Provide your answer...

Next, you’ll have the opportunity to review your learning from the whole course in the end-of-course compulsory badge quiz.

4 End-of-course quiz

You can now take the end-of-course quiz, which consolidates your understanding of all the topics you've studied.

Complete the Week 8 compulsory badge quiz now.

Open the quiz in a new window or tab then come back here when you're done.

5 End-of-course guide and round-up

Video content is not available in this format.

View transcript - Uncaptioned interactive content

Cory says goodbye and summarises the course as it comes to a close.

Over the past eight weeks you have learned about different types of cyber security threats and techniques that can be used to counter them. You should now have a grasp of cyber security concepts such as confidentiality, integrity and availability as well as understanding the basics of cryptography, network security and security risk management.

If you would like to find out more about any of the topics covered in the course we have created an area specifically for exploring more about cyber security on OpenLearn.

6 Next steps

Figure 15

Congratulations, you have completed the course! We hope you have enjoyed your journey into the world of cyber security.

Were you inspired by the course? Would you like to continue your learning with The Open University? Then read on!

If you already have a qualification in computing or relevant work experience in the field and want to specialise in cyber security, The Open University offers the following postgraduate courses:

- M811 *Information security*
- M812 *Digital forensics*
- T828 *Network security*.

If you don’t have a computing background but your introduction to cyber security has inspired you to learn more about computing, you may be interested in The Open University’s BSc (Honours) in Computing and IT, starting with TU100 *My digital life*.

Now you've completed the course we would again appreciate a few minutes of your time to tell us a bit about your experience of studying it and what you plan to do next. We will use this information to provide better online experiences for all our learners and to share our findings with others. If you'd like to help, please fill in this optional survey.

References

Microsoft (2012) ‘Microsoft Security Intelligence Report’, vol. 14, issue July – December, pp. 57, [online]. Available via http://download.microsoft.com/download/ E/0/F/E0F59BE7-E553-4888-9220-1C79CBD14B4F/Microsoft_Security_Intelligence_Report_Volume_14_Running_Unprotected_English.pdf (Accessed 6 June 2014).

Acknowledgements

Introduction and Guidance

This course was written by Arosha K. Bandara and Maria Townsend.

Except for third party materials and otherwise stated (see FAQs), this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Don't miss out:

1. Join over 200,000 students currently studying with The Open University – http://www.open.ac.uk/choose/ou/open-content

2. Enjoyed this? Find out more about this topic or browse all our free course materials on OpenLearn – http://www.open.edu/openlearn/

3. Outside the UK? We have students in over a hundred countries studying online qualifications – http://www.openuniversity.edu/ – including an MBA at our triple accredited Business School.

Week 1: Threat landscape

Introduction and Guidance Images

Course image: Atomic Taco in Flickr made available under Creative Commons Attribution-ShareAlike 2.0 Licence .

Week 1

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Week 1 Images

Figure 1 © Blend Images - Colin Anderson (via Getty Images)

Figure 2 © xxz114 (via iStock photo)

Figure 3 © caracterdesign (via iStock Photo)

Figure 4 © bluebird13 (via iStock Photo)

Figure 5 © agsandrew (via shutterstock)

Figure 6 © Ryan McGinnis (via Getty Images)

Figure 7 © Jasper James (via Getty Images)

Figure 8 © Vetta Collection (via iStock Photo)

Figure 9 © JGI/Tom Grill (Getty Images)

Figure 10 © LeoPatrizi, sb-borg (via iStock Photo); mediaphotos (via Getty Images)

Figure 11 © Danil Melekhin (via Getty Images)

Figure 12 © Jimmy Anderson (via iStock Photo)

Week 1 Video

1 Online, the new frontline © HM Government

1.3 and 2.1 © The Open University

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 2

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 2 Images

Figure 1 © agsandrew (via Fotolia)

Figure 2 © beaucroft (via iStock Photo)

Figure 3 © piotr_malczyk (via iStock Photo)

Figure 4 © dcdp (via iStock)

Figure 5 © dsteller (via iStock Photo)

Figure 6 © Garry518 (via iStock Photo)

Figure 7 © Andrey_Kuzmin (via iStock Photo)

Figure 8 © FredFroese (via iStock Photo)

Figure 9 © lek2481 (via iStock Photo)

Figure 10 © David Clark (via Getty Images)

Figure 11 © pagadesign (via iStock Photo)

Figure 12 © Alan Uster (via Shutterstock)

Week 2 Audio visual

2.1 How to pick a proper password (including transcript) © Sophos

Week 3

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 3 Images

Figure 1 © Eraxion (via iStock Photo)

Figure 2 © JordiRoy (via iStock Photo)

Figure 3 © Colin Anderson (via Getty Images)

Figure 4 © vadimguzhva (via iStock Photo)

Figure 5 © Carol and Mike Werner/Visuals Unlimted, Inc. (via Getty Images)

Figure 6 © Yugi Studio (via Getty Images)

Figure 7 © Stephan Zabel (via Getty Images)

Figure 8 © Trina Dalziel (via Getty Images)

Figure 9 © Andrew Levine http://commons.wikimedia.org/wiki/File:PhishingTrustedBank.png

Figure 11 © Dimitri Otis (via Getty Images)

Figure 12 © enjoynz (via iStock Photo)

Figure 13 © ryccio (via Getty Images)

Figure 14 © aydinmutlu (via iStock Photo)

Figure 15 © John Lamb (via Getty Images)

Figure 16 © Danil Melekhin (via Getty Images)

Figure 18 © FreezeFrameStudio (via iStock Photo)

Figure 20 © webking (via iStock Photo)

Figure 21 © addimage (via iStock Photo)

Week 4

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 4 Images

Figure 1 © Michael Smith (via Getty images)

Figure 2 © bioraven (via Shutterstock)

Figure 3 © Mark Horn (via Getty Images)

Figure 4 © bluebird13 (via iStock Photo)

Figure 5 © olhainsight (via iStock Photo)

Figure 6 © powerofforever (via iStock Photo)

Figure 7 © Bet_Noire (via iStock Photo)

Figure 8 © Scorpions and Centaurs (via Flickr.com)

Figure 9 © no_limit_pictures (via iStock Photo)

Figure 11 © chrisroll (via iStock Photo)

Figure 12 © Pashalgnatov (via iStock Photo)

Figure 13 © Catrina Genovese (via Getty Images)

Figure 14 © John Lund (via Getty Images)

Week 4 Audio Visual

2 extract (including transcript) from Datababy: How easy is it to become a phone hacker? © Channel4/ITN

Week 5

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 5 Images

Figure 1 © Bletchley Park Trust (via Getty Images)

Figure 2 © Bob Lord - Licensed under Creative Commons Attribution-Share Alike 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Enigma-plugboard.jpg#mediaviewer/File:Enigma-plugboard.jpg

Figure 3 © agsandrew (via Shutterstock Photos)

Figure 5 © peterhowell (via iStock Photo)

Figure 6 © GlobalP (via iStock Photo)

Figure 7 © blackie (via iStock Photo)

Figure 10 © Wavebreak (via iStock Photo)

Figure 11 © choicegraphx (via iStock Photo)

Figure 12 © Vertigo3d (via iStock Photo)

Week 5 Audio Visual

2.1 and 2.2 © The Open University

Week 6

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 6 Images

Figure 1 © narvikk (via iStock Photo)

Figure 2 © HAYKIRDI (via iStock Photo)

Figure 3 © Underwood Archives (via Getty Images)

Figure 4 © vmedia84 (via Fotolia)

Figure 5 © RapidEye (via iStock Photo)

Figure 6 © OJO_Images (via iStock Photo)

Figure 7 © belterz (via iStock Photo)

Figure 8 © BaderElbert (via iStock Photo)

Figure 9 © Hugh Threlfall (via Getty Images)

Figure 10 © Isantilli (via iStock Photo)

Week 7

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 7 Images

Figure 10 © Shaun Curry (via Getty Images)

Figure 11 © David Gould (via Getty Images)

Figure 12 © wakila (via iStock Photo)

Figure 13 © scanrail (via iStock Photo)

Figure 14 © Jeff Nagy (via iStock Photo)

Figure 15 © v777999 (via iStock Photo)

Figure 16 © Scorpions and Centaurs (via Flickr.com)

Figure 17 © scyther5 (via iStock Photo)

Figure 18 © kirillm (via iStock Photo)

Figure 19 © Mari (via iStock Photo)

Week 7 Audio Visual

1 extract (including transcript) from 'Inside Out’ (6/2/12) © BBC

Week 8

This course was written by Arosha K. Bandara.

Except for third party materials and otherwise stated in the acknowledgements section, this content is made available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence.

The material acknowledged below is Proprietary and used under licence (not subject to Creative Commons Licence). Grateful acknowledgement is made to the following sources for permission to reproduce material in this course:

Every effort has been made to contact copyright owners. If any have been inadvertently overlooked, the publishers will be pleased to make the necessary arrangements at the first opportunity.

Week 8 Images

Figure 1 © 1joe (via iStock Photo)

Figure 3 © scotto72 (via iStock Photo)

Figure 8 © swilmor (via iStock Photo)

Figure 9 © DonNichols (via iStock Photo)

Figure 10 © ishoot63 (via iStock Photo)

Figure 11 © btrenkel (via iStock Photo)

Figure 12 © mjutabor (via iStock Photo)

Figure 13 © Leena Snidate / Codenomicon (CC0 1.0 Universal license)

Figure 14 © wakila (via iStock Photo)

Figure 15 © Mordolff (via iStock Photo)

Activity 4 Securing your information

Answer

The following case study provides an example for the fourth option above, working from home.

Case study: working from home

When working from home you may need to share a confidential file with a colleague in another location. You could email it to them, but this is not a secure method of transmitting information – email is easily intercepted en route to its destination and there is always the risk that you send it to the wrong person!

You could use an online cloud service such as Dropbox, Google Drive or Microsoft OneDrive to store the file, but you will have to make sure that your colleague can access the uploaded file. You might also be worried about the security of the cloud services against hackers.

You could put the file on a USB flash memory drive and post it to your colleague. But the drive could be lost, stolen or intercepted by an attacker who adds malware to the drive as a way of infecting your organisation's computers.

Or, you could use encryption to lock the file against intruders. You could email the encrypted file safe in the knowledge that no one else could read the document. However, you would have to be sure that your colleague knows how to use encryption software so that they can decrypt the document when it arrives.

Back

Activity 1 Datagrams

Discussion

You will have discovered that the route to the Sydney Morning Herald website did not terminate in Australia.

A URL ending in '.au' is an Australian domain, but that doesn't mean that the computer hosting the site has to be in Australia.

The Australian Domain Name Administrator (auDa) is responsible for licensing users of '.au' names, and it has rules that require the licensees to have some connection with Australia (that is not the case with all countries; some authorities allow anyone to license their names). However, where the website is hosted – which computer the website is stored on – is a different question from who is using the URL. For example, Google (based in the USA) offers a service hosting websites (Google Sites). It's possible to use a service with a '.eu' (European) domain name, with the result that the '.eu' site is in the USA.

In addition, websites that receive heavy usage from a particular location might be cached locally – that is to say, copies of the website's data might be temporarily stored on a computer closer to the location from which the information is being accessed. This saves making heavy use of long-distance connections.

How many stages did your information take? Did anything surprise you about the route your information took?

Back

Figure 1

Description

This is a photograph of a woman's head and shoulders. Going around her head are square images depicting images linked with security.

Back

Figure 2

Description

This is an image of a dictionary being flicked through.

Back

Figure 3

Description

This image is made up of a dark blue/black background, with a yellow dotted line running along the left-hand side, and the word 'DANGER'.

Back

Figure 5

Description

The image is a screenshot showing the files on a person's computer desktop.

Back

Figure 6

Description

This is an abstract image showing an outline of a person's face in profile multiple times.

Back

Figure 7

Description

This is a photograph of dark clouds above a green field.

Back

Figure 8

Description

This is an abstract image of a cityscape with the shadow of a person holding a laptop over it.

Back

Figure 9

Description

This image shows a person's hand holding a mobile device with one finger of the other hand pressing onto the tablet's surface.

Back

Figure 10

Description

This figure is made up of three separate images. Starting top left and going clockwise: the first image is of two small devides, presumably used for online banking, sitting on top of a computer keyboard; the second is off a man taking a photo of a plate of food with a mobile phone; the third shows one person with their hands hovering over a computer keyboard and another person holding a magazine and using a mobile phone.

Back

Figure 11

Description

In the centre of the image is a digital handprint. Coming of the hand there is a close up a finger print, the outline of a person, and a heading 'Personal Data' with entries underneath such as 'Name', 'Home Address', and Passport No'.

Back

Figure 12

Description

This image shows a padlock with a key inserted.

Back

Figure 1

Description

This is an abstract image of an outline of a person's head in profile, showing an outline of their brain. Coming from the brain are different numbers.

Back

Figure 2

Description

This image shows two shelves on a bookcase, both of which are full of books. The titles of the books cover a range of academic disciplines, from Latin to human biology, and from modern politics to medicine.

Back

Figure 3

Description

This is a close-up image of a spoon of salt.

Back

Figure 4

Description

This is an image of a man wearing sunglasses. Reflected in the sunglasses are the words 'Enter password' and a box containing six asterisks.

Back

Figure 5

Description

This image, depicting strength, shows two young men arm wrestling.

Back

Figure 6

Description

This image shows a collection of jumbled up letters and numbers.

Back

Figure 7

Description

This image shows a large wooden filing cabinet with a few draws open.

Back

Figure 8

Description

This image shows a large rock with a crack. Through the crack, blue sky can be seen.

Back

Figure 9

Description

This image shows a computer keyboard and a small device used for internet banking.

Back

Figure 10

Description

In the foreground of this image is a person holding a mobile phone: on the screen is 'Internet Banking. One-Time Security Code' and a set of numbers. In the background the person's other hand hovers over a computer keyboard.

Back

Figure 11

Description

This image shows a USB cable sitting on top of a credit card.

Back

Figure 12

Description

This is an illustration of the palm of a hand, made up of numbers and words such as 'password', 'lifehack' and 'QWERTY'.

Back

Figure 1

Description

This image shows cells associated with a virus.

Back

Figure 2

Description

This image shows a small worm coming out of an apple.

Back

Figure 3

Description

The image depicts a wooden Trojan horse being pulled along on a cart.

Back

Figure 4

Description

The image shows a person using a laptop which is sitting on top of a pile of books.

Back

Figure 5

Description

This abstract figure shows an open laptop and a number of circles and spheres with numbers floating around them.

Back

Figure 6

Description

The image shows a city at night, with curved lines connecting different parts of the city.

Back

Figure 7

Description

This image shows a figurine of a fisherman standing on top of a computer keyboard. On the end of his fishing line is a piece of paper with the word 'Password'.

Back

Figure 8

Description

This is a cartoon showing a fishing boat in the sea. In its net are a number of captured letters and pieces of paper.

Back

Figure 9

Description

This is an example of what could be a phishing email.

Back

Figure 11

Description

This image shows a computer keyboard. Instead of letters and numbers, on each key is an emoji.

Back

Figure 12

Description

This is an image of a pile of notes of different currency, for example American dollars and Euros.

Back

Figure 13

Description

This is an illustration of two laptops sitting opposite each other, with various robots shooting lasers at each other.

Back

Figure 14

Description

This shows a needle being injected into a bottle.

Back

Figure 15

Description

This image shows numerous toy soldiers guarding a laptop.

Back

Figure 16

Description

This image shows six computer screens, each displaying images related to antivirus software, such as images of locks and the words 'privacy, 'password' and 'protection'.

Back

Figure 17

Description

This is an image of a smartphone. On the screen is a calendar alert for a software update.

Back

Figure 18

Description

This image shows an old-fashioned typewriter, but with a DVD drive and a mouse attached.

Back

Figure 20

Description

This is an image of an elaborate sandcastle.

Back

Figure 21

Description

This image shows silver spider-like robots on a patterned image.

Back

Figure 1

Description

This is a photograph of Vinto Cerf.

Back

Figure 2

Description

This is an image of a collection of envelopes of different colours.

Back

Figure 4

Description

The image is of a large mast with a number of satellite dishes attached to it.

Back

Figure 5

Description

This shows the back of a wireless router with a cable going into the port labelled 'INTERNET.

Back

Figure 6

Description

This image shows three large satellite dishes.

Back

Figure 7

Description

The image shows three internet cables sitting on top of a computer keyboard.

Back

Figure 8

Description

This image is a photograph of a complicated road layout, from above.

Back

Figure 9

Description

This image shows the back of a computer with multiple cables.

Back

Figure 11

Description

The image is of a lorry driving along an empty road.

Back

Figure 12

Description

This is a close up of '.uk' on a screen.

Back

Figure 1

Description

This is a black-and-white photograph of a number of women in an office at machines.

Back

Figure 3

Description

This is an abstract image of different coloured numbers and patterns.

Back

Figure 4

Description

This is a screenshot of a web browser - our attention is drawn to 'https' at the start of a web address.

Back

Figure 5

Description

In the background is a large image of a human eye. Overlaying this is a set of number ones and zeroes.

Back

Figure 6

Description

This is an image of a fish.

Back

Figure 7

Description

This is an image showing a a substantial number of numbers in rows, of different colours.

Back

Figure 8

Description

This shows a number of letter and number combinations.

Back

Figure 9

Description

This is an illustration of how Alice would send her quarterly profit statement to Bob. It shows the different stages it would go through.

Back

Figure 10

Description

This shows two people shaking hands (it shows their hands and part of their forearms only). There are symbols around them, for instance @, an envelope, a speech bubble and a padlock.

Back

Figure 11

Description

This shows a padlock with a combination lock, attached to a chain.

Back

Figure 12

Description

This shows a number of coloured blocks, numbered either 0 or 1, on top of each other. This collection of blocks hovers over a laptop.

Back

Figure 1

Description

This is a photograph of a building on fire, with a firefighter looking on.

Back

Figure 2

Description

This shows the startings of a brick wall.

Back

Figure 3

Description

This is a photograph from a film scene in which two people in the Wild West are shooting at each other.

Back

Figure 4

Description

This is an abstract image in which there is a tunnel of different photographs.

Back

Figure 5

Description

This photograph is of an open laptop, but a beach and the sea in the background.

Back

Figure 6

Description

This is a photograph of a man using a laptop.

Back

Figure 7

Description

This is a close-up image of some toy soldiers.

Back

Figure 8

Description

This image shows four different colour lights.

Back

Figure 9

Description

The image shows a computer on a mouse trap.

Back

Figure 10

Description

This image shows a man, from behind, wearing a baseball cap and holding a walkie-walkie. On the back of his jumper reads 'SECURITY'.

Back

Figure 2

Description

This shows an empty office, with rubble on the floor and desk.

Back

Figure 3

Description

This is a photograph of the Houses of Parliament and Big Ben in London, UK.

Back

Figure 4

Description

This shows a judge's gavel on top of a computer.

Back

Figure 5

Description

This is an image of a security camera.

Back

Figure 6

Description

This is an image of a person's hands in handcuffs. Their clenched fists rest on a computer keyboard.

Back

Figure 7

Description

The image is of a person with their hands behind their back, in handcuffs. The person is standing in front of an open laptop with graphs on the screen.

Back

Figure 8

Description

This is a photograph of a man at a desk using a laptop.

Back

Figure 9

Description

This is a map of Europe.

Back

Figure 11

Description

This is a close-up image of a number of credit cards.

Back

Figure 12

Description

This shows three figurines dressed as builders on top of a computer.

Back

Figure 13

Description

This image shows a login screen on a mobile phone.

Back

Figure 14

Description

This image shows a rusty laptop on top of some rocks near water.

Back

Figure 15

Description

This image shows hundreds of discs in front of a computer screen.

Back

Figure 16

Description

This is an image of clouds in the sky.

Back

Figure 17

Description

This is an image of a USB memory stick and a memory card on top of a pile of discs.

Back

Figure 18

Description

This is an image of a number of devices for saving datam for instance memory cards and USB memory sticks.

Back

Figure 19

Description

This image shows a closed padlock.

Back

Figure 1

Description

This image shows a number of documents.

Back

Figure 2

Description

This is a screenshot showing the contents of a computer desktop.

Back

Figure 3

Description

This is an image of a person climbing up a rock. The sea is in the background.

Back

Figure 5

Description

In this risk analysis grid, email, banking details and password are classified as high impact and high likelihood.

Back

Figure 6

Description

In this risk analysis, study materials and digital photographs are classified as high impact but low likelihood.

Back

Figure 7

Description

In this risk analysis, digital music and digital videos are classified as high likelihood but low impact.

Back

Figure 8

Description

This photograph shows a man wearing protective clothing while using a laptop.

Back

Figure 9

Description

This is a photograph of chocolate chip cookies.

Back

Figure 10

Description

This photograph shows three people sky diving.

Back

Figure 11

Description

This photograph shows a young woman sitting on the floor with her laptop. Surrounding her are poloroid images.

Back

Figure 12

Description

This image shows a number of toy soldiers.

Back

Figure 13

Description

This shows a red heart, with the effect of red paint dripping from it.

Back

Figure 14

Description

This shows three figurines dressed as builders on top of a disc.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Hi, I'm Cory Doctorow, and I'll be your guide through this eight week course, catching up with you each week to recap on what we've covered and how it relates to what you'll be learning during the week. I used to be the European director of the Electronic Frontier Foundation. That's a campaigning civil liberties group in San Francisco that, among other things, legalised the use of strong cryptography around the world and continues to be involved in a lot of important struggles. I'm also a visiting professor at the Open University, and I hold an honorary doctorate in Computer Science from the OU.

At the start of the course, you'll learn the basics of information security and how to take some easy steps to secure your digital life. We'll then begin to look under the hood, exploring some of the technologies underpinning the internet and information security. You'll see how data moves between computers over the internet, how it can be attacked, and how it can be kept secure.

What if you are attacked? We'll also be looking at ways to deal with the aftermath, as well as steps you can take to prevent any future attacks from

being successful. By the end of the course, you'll know how to recognise online threats. You'll know what steps to take to reduce any chance of being harmed by them, and you'll know how to feel secure in your digital life. This week you'll be learning some of the basic terminology used when discussing information security. You'll also start to learn about the different threats you'll face online.

Back

Uncaptioned interactive content

Transcript

An estimated 1.6 billion people regularly access the web. And while most people log in, log out and harm no one, some of them do. Among them, criminals, malicious hackers and terrorists. The threats they pose are huge and multiplying. Today, online is the new frontline.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW So there was a time that I actually got phished. I was successfully attacked over the internet. And it really illuminated the fact that security depends on you never making any mistakes, and attacking depends on finding one person who can make a mistake.

So the way that happened was the night before, I'd reinstalled the operating system on my phone, and so every time I logged into a service that normally I'd have a password stored on my phone for, it was prompting me to reenter my password, because I had a new operating system. And also, I had a new browser, and the browser hid part of the URL of the website I was looking at. So that made things bad, too.

I went to the coffee shop after dropping off our daughter at school with my wife, and she sat down to read the free sheet and I stood in the queue, and I fired up Twitter and there was a direct message from a friend of mine that said, was this you? And a URL. And the day before, I had also published a bunch of newspaper editorials, so I was getting a lot of emails and direct messages, saying oh, I saw that, or

how was this, or whatever. And so it seemed kind of plausible. And I clicked on it, and it prompted me for my password. And it brought me to a Twitter login screen and prompted me for a password, which was normal. Everything was prompting me for it. It looked like I was visiting Twitter dot com, because of the way the browser was displaying, and I entered it in.

And then I got three more DMs from other people saying, is this you? And I was like, oooh, they've all been infected by something that presumably I've just been infected by, too. And if nothing else, I just entered my password into this.

The consequences, thankfully, were pretty light, because it happened immediately, and I had good password hygiene that I didn't recycle passwords across services. So I immediately sat down in the cafe, cancelled all my morning meetings, and changed that password and went through and made sure everything looked OK and then ended up blowing out the operating system on that phone and reinstalling it. Luckily, the consequences were pretty slight and nothing bad happened to me apart from losing that morning and feeling like an idiot.

Back

Uncaptioned interactive content

Transcript

Many of the major software companies publish security notices when they discover a threat. In this video, we're going to look at the security notices published on the Microsoft website. The link to the website is provided in the text below. When you visit the website, click on Security Updates, followed by Bulletins, to see the latest security notices. We're going to take a look at the security updates for May, 2014, which list the executive summaries relating to a range of different security issues. The key information to note from this list is the particular software that's affected by each security issue. For example, the first two bulletins are in relation to the security issues in Microsoft Windows and Internet Explorer. Whereas, the third deals with issues with the Windows Server operating system.

Let's look at the details of the second security bulletin listed here. The summary table indicates that this affects Windows and Internet Explorer. It also shows that this is a critical vulnerability that could allow an attacker to execute arbitrary code on the affected machine. The first section of the bulletin is an executive summary

that explains the threat posed by the vulnerability. In this case, it could cause an information disclosure. In other words, it's possible for an attacker to access data from the computer. The summary also explains a number of key points. The attack only works if the attacker has a valid username and password for the machine, and this vulnerability does not allow attackers to get more access rights than the currently logged in user. This means that users with basic, non administrative privileges on the machine will not be as badly affected by the attack as those users with full administrative privileges.

Scrolling down the page, we can see the key sections of the bulletin that list the affected, and not affected, software, as well as instructions on how to update different versions of Microsoft Windows to fix the security issue. Of course, a more simple way to update your Windows operating system is to enable automatic updates, by following the instructions on the Windows Update site. We've provided the link to this site below.

Back

Uncaptioned interactive content

Transcript

Many of the major software companies publish security notices when they discover a threat. In this video, we're going to look at the security notices published on the Apple website. A link to the website is provided in the text below.

This page provides advice on how to report security problems with Apple products together with guidance on how to check the security of your system. However, the section that we're interested in is titled security notifications. You can subscribe to receive emails informing you of security updates. And clicking on the link for the Apple security updates page will take you to a list of security notifications.

The security updates page lists the security issues with the most recent at the top. Each issue is identified by the particular software that's affected by the issue. For example, the issue listed here affects the Safari web browser version 6.1.4 and 7.0.4.

Clicking on this link takes us to the detailed information about this vulnerability. The page includes information on how to update your software to remove the vulnerability and also provides a description of what

could happen if an attacker were to exploit this vulnerability. In this example, the vulnerability could lead to the Safari browser closing down unexpectedly or the execution of arbitrary code.

An attacker could use the execution of arbitrary code to gain complete access to the machine, allowing them to steal information or install malware. It's important to note that the impacts section also notes that an attack that exploits this vulnerability depends on the user visiting a website that has been specially created by the attacker. As mentioned, the security notification page also includes guidance on how to update your software to remove the vulnerability. In this case, it advises using the Apple software update tool, which can be accessed from the Apple menu.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Hello and welcome to Week 2. Last week we looked at online activities and security threats. We saw that many of these threats depend on attackers being able to impersonate us online. For this to happen, the attacker needs to access our online identities.

So this week we're looking at passwords. Many online services use passwords. From social networks to payment systems, passwords are how we identify ourselves and interact with the services that we use. So you'll learn the ways in which attackers will try to discover your password so they can impersonate you online. And you'll learn how you can improve the security of your passwords, and online identification methods that use different techniques and password managers.

But before we get started, a note of caution-- there will be discussions during the course, and just as you should never disclose your PIN, please also take care never to share any of your passwords. If you need an example, make one up.

Back

Uncaptioned interactive content

Transcript

Speaker

When a user connects to the server for the first time, they may be asked to create a password so they can get access to the services available on the server. In this case, the user types in a simple password. To keep things easy, we're using the very simple-- and very bad-- password "apple." Your own passwords should be much harder to guess. The user's password is sent over the network and is stored in a database on the server. At some later date, the user wants to access the server again. They're asked for their password, and type in "apple." The password is sent over the network and compared to the stored password-- also "apple"-- in the server's database. If the two match, they're given access.

Any data passing over a network can be stored or intercepted. It's very easy to copy data on a network, so an attacker could make their own copy of the password. Once they have that, they can then log into the server masquerading as the original user. A second problem is that the database itself might be stolen from the server by hackers-- or even a disgruntled employee. If this were to happen, all of

the passwords belonging to all of the users could be misused.

To prevent passwords being stolen in transit, we use a secure network link between the user's computer and the server which hides data using strong cryptography. One type of secure link is called SSL, which you'll have used, perhaps without knowing it, when shopping online.

It's much harder to stop the server's database being stolen. But we can obscure passwords using a technique called hashing. Hashing is a mathematical technique that scrambles a password to produce a so-called hash. So when the user creates a password, server turns the password into a hash. And rather than storing the password in the database, we store the hash. So when the user logs in next time, they enter their password, which is sent over the network. The server creates a new hash from the password and compares it to the stored hash. If the two hashes match, then the user is allowed into the computer. Crucially, hashing only works one way. It's not possible to simply undo the hashing to recover the original password. Even if the database is stolen, the attackers only have the hashed passwords, rather than the passwords themselves. If the attackers want to find out the original passwords, they'll have to hash every possible password and compare

them to the list of stored hashes. This is an enormously time-consuming process.

Back

Uncaptioned interactive content

Transcript

How to pick a proper password

PAUL DUCKLIN Hello everybody. I'm Paul Ducklin. And this is a two-minute tutorial on How to pick a proper password.

Number one. Make your passwords hard to guess. The crooks have dictionaries, books, movie scripts, song lyrics, Facebook, Twitter, and much more. So avoid passwords based on nicknames, birthdays, quotations, pets, anything of that sort. And don't forget that easy passwords don't get harder if all you do is add some digits on the end. Password cracking programmes can do that, as well.

Point two. Go as long and complex as you can. Random, eight-letter passwords look pretty tough, with 26 to the power 8 possibilities. That's a whopping 200 hundred billion. But a password cracking service costing less than $20,000, under ideal circumstances, can try out more than 100 hundred billion passwords each second. So mix together uppercase, lowercase, digits, and punctuation.

And aim for 14 characters or even longer. That may look terribly complicated, but you can make up a little saying to help you out. If you don't like that approach, some people take

several unusual words and combine them into a meaningless phrase, like the XKCD cartoon's famous correct horse battery staple password. But watch out for words that relate obviously to you. They do need to be unusual.

And Point three. Consider using a password manager. Examples include LastPass, KeePass, and 1Password. Password managers can make up complex, random nonsense for each account, plus they remember which password goes with what website. That also helps protect you from phishing, because you can't put the right password into the wrong page. But do remember, you will need a really good password for the Password Manager itself.

So let's go over the points again. One, make your passwords hard to guess. Two, go as long and complex as you can. Three, consider using a password manager.

And no, we haven't forgotten. Number four. One account, one password. Don't reuse passwords.

Don't make things easy for the crooks. And until next time, stay secure.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Last week we explored how authentication works and the role of passwords in protecting online identities and digital information. Now you're armed with different ways of improving your password security, including password managers and two-factor authentication. This week we'll be looking at another common way the computer systems are compromised, which is through the use of malicious software or malware. By the end of the week you'll be able to describe the different types of malware and their key characteristics, as well as how malware gains access to computer systems, and which steps you can take to prevent your own computer from being infected. 'Til next week.

Back

Uncaptioned interactive content

Transcript

COMPUTER

Hello there. Are you about to click on a link you're not sure about? Well I hope you've taken care. Because if not, I could quite easily drop a Trojan horse, or a drive-by download, or some other sinister malware into your laptop and turn your computer into a zombie. Don't worry, it's not one of those zombies.

But it does mean I could take control of your computer without you knowing and either steal your identity or make your computer do things it shouldn't, like sending out spyware or spam. I can make it happen without you noticing. And it's not only your computer I can do that to. I can make a whole network of them which is called a botnet, or a zombie army.

So, I guess you'll want to know how to avoid it all, won't you? Well, the first thing to do is not to click on any unsafe links or download any attachments that you're not sure of. But if you're worried you may be part of a botnet, check if your computer is running slower than normal, or if starts behaving erratically. Or you might notice some unusual internet activity that you weren't expecting.

You could check your Task Manager to see what it's up to. Disconnect from the

network and see if the computer behaves differently. Looks like you've got a problem. Of course your virus scanner should be telling you as well.

So what can you do to stop it happening? Uh oh, almost right. You need to make sure your antivirus and anti-spyware software is up to date. But use a reputable source. Rogue antivirus software could be malware in disguise. And remember, though that helps, it can't save you if you go and click on an unsafe link anyway. You're learning, but give it a full scan. And make sure your firewall is on too. And, if all else fails, ask an expert to help you. No need to thank me. I was just doing my j-.

[TYPING]

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Over the past three weeks, we've explored the many potential threats to our digital lives. We've also taken a closer look at ways of keeping attackers from impersonating you online or infecting your devices with malware. Now we're going to delve a little deeper into the technology that underpins information security, focusing first on how to protect the internet itself and the network security problems that can affect it.

By the end of the week you'll be aware of some of the networking standards that allow different devices to connect to the internet and exchange information. You'll also be able to explain how data is transmitted across networks. And you'll understand the difference between the internet and the world wide web.

Back

Uncaptioned interactive content

Transcript

SPEAKER

Vinton Cerf is vice president and chief internet evangelist for Google. He has been involved in internet technology right from the very start. Ten years ago, the Open University interviewed him for a series called TheWebStory.com.

His involvement with internet technology started in the 1960s, when he was working on a computer networking project funded by the US Defense Advanced Research Project Agency, ARPA. He is widely known as the ‘father of the internet’.

VINTON CERF

Well I think people have gotten a little carried away at least in our culture there seems to be a need to focus a lot of attention on just one or two people. That’s not right. There are many fathers of the Internet depending on how far back you want to go and the evolution of the technology. At UCLA I was a graduate student along with Steve Parker, John Postel, Bob Braden, and a number of others, all working for Professor Len Kleinrock, who had the network measurement centre at UCLA. And so our job was to put the first computer up on the ARPANET and particularly the one that did network measurement.

SPEAKER The ARPANET was a network of computers set up in 1969 to link research departments in universities around the United States. The big challenge was to get the different computers to talk to each other.

VINTON CERF No one was really in charge of the development of the host protocols to connect computers up to the underlying network that Bolt Beranek and Newman was building, and so the graduate students just sort of gravitated to try to work on that. We always expected that someone would come out who was professional and would run the show. Steve Parker, who was my good friend then and still is, ran the network working group and we always expected that somebody from the East Coast would show up to tell us what to do but they never did. So we just went on and did the best we could.

Protocol is of course it's a diplomatic term. It's something that you establish in agreement between countries and that’s called protocol. It also turns out to come from the Greek word ‘protocollum’, which was the table of contents of a scroll. Well we stole that word for computer communication conventions because packets of information that computers exchange have little headers on them to say where they're going, where they came from and how much there is in that piece. So we called the procedures

computer protocols. They're simply conventions for communications between computers.

SPEAKER To get information between the various computers that formed the ARPANET, the data was chopped up into small ‘packets’. The packet switching protocols Vint and his colleagues devised enabled the packets to be sent by different routes and recombined at the other end to recreate the original data.

VINTON CERF When the first wide area packet switch network was being built the ARPANET there was some uncertainty whether it was going to work at all. That actually worked out quite well. It was a very powerful and useful tool for computer science departments that were part of that system. In fact packet switching was so successful that we at ARPA anyway decided it would explore using packet switching in radio and satellite communication. That led to the development of the mobile packet radio network and an Atlantic satellite net that linked the US to Europe using packet switching technology. Well once those projects were under way Bob Kahn who was at ARPA at the time realised that these networks would ultimately have to be inter connected to each other. And we didn’t have any protocols, no procedures, no conventions that would allow computers that were on different

networks to smoothly intercommunicate with each other. That led to the inter net project which Bob started at ARPA around 1970 – late ’72 or early ’73 and he posed that problem to me when I was at Stanford in March of ’73 and we worked together on solving that problem: how could computers on different networks communicate with each other uniformly. And that led to the design of what is now called TCP/IP.

This really was a back of the envelope moment. I was sitting in San Francisco in a hotel lobby waiting for some session to start at a conference and had an envelope in my pocket and I pulled it out and I was just sketching what the implications were of the architecture that Bob and I had talked about, eventually leading to what we called gateways and are today called routers. And so in a sense the system’s basic architecture was forced on us because we weren't allowed to change any of the networks themselves we had to work outside of them and then figure out a way to achieve uniformity. So that little sketch, which is long since lost, I had no idea it was an important sketch at the time, it was just getting my thoughts in order, was the beginning of at least for me of understanding how the structure would work.

SPEAKER TCP/IP was one of the great technological breakthroughs of the

twentieth century. It allowed the internet to become what it is today.

VINTON CERF

The easiest way to understand how the Internet works is to think of Internet packets as electronic postcards. Just like postcards: they have a 'to' address and a 'from' address and a finite amount of content on them. And the fact that they're electronic means that they go through the system about a hundred million times faster than the postcard that goes through the post office. But they behave just like postcards. They don’t necessarily arrive in the same order they were sent. They might not even arrive on the same day. Some of them get lost. That’s true of the Internet packets as well as postcards and so if you think about Internet packets as postcards you have a pretty good model. To understand TCP you need a little bit more thinking. Suppose that you were sending a novel to someone and the only way you could send it was by sending postcards so you cut the pages of the novel up, put them on postcards and then you realise that you have to number the postcards in order to let the party at the other end put them in the right order. Then you wonder you know if some of them got lost you'd have to re-transmit them so you keep copies to send. Then you realise that you need to find out whether you need to send any copies and you have acknowledgements

coming back in the form of post cards, some of which might get lost. And so you have time outs that say if I haven't heard anything I'll start sending copies. It's basically the way the TCP works. It essentially allows us to send novels in sequenced order on top of postcards except of course we do it electronically and much faster.

SPEAKER So the internet is essentially a giant game of pass the packet, using a set of rules or protocols called TCP/IP. When the protocol was first used to create an inter network from three separate networks, it was a milestone in internet history.

VINTON CERF Interestingly enough there are two big milestones, neither one of which were very noted at the time by anybody except those of us deeply involved. In 1977, late in the year we actually got all three, packet radio, sat net and ARPANET networks to function together using the Internet protocols and gateways in between and that was very exciting for a few of us who were a part of that, but not noted anywhere. We didn’t call a press conference or issue a press release or anything. We just breathed a great sigh of relief. In 1983 in January we actually insisted on the deployment of those protocols by all the computers that were part of the ARPANET and satellite net and packet radio net. And that was a big moment for the people who had to get their

machines up but there were only about two hundred and at most four hundred computers involved. Today there are fifty million computers on the Internet. And so any such similar kind of transformation can't be done in what's called a flash cut. It wasn’t even a flash cut in the Internet’s case. It took several months to get everybody up and running on the new protocols. But that was a forced change. Today you can't force that change.

The only real regret I have is that I didn’t argue that we should have a larger address space for the Internet than we decided on. In 1977 I picked a thirty-two byte address space which was enough to identify up to four billion things. It's now very clear that there will be many hundreds of billions of things on the Internet in the future and we should have picked a bigger address space but at the time it was an experiment and it never dawned on me or most everyone else that we needed anything like the scale that we will ultimately require.

SPEAKER Although he resists being called the father of the internet, Vint Cerf is one of its greatest pioneers. When he first sketched out his ideas for the TCP/IP protocol, did he imagine that the internetworking project would turn out the way it did?

VINTON CERF Certainly not in the form which it has ultimately materialised in. Tim Berners-

Lee’s world wide web is something that’s truly phenomenal at the rate at which it has been absorbed and adopted. We knew however that we were working with very powerful technology. We knew that computing and the distributed programmes that are around the network would be very, very powerful engines. We just didn’t know exactly what they were going to do at the time. Software is sort of the ultimate clay – you can make anything you want to out of software if you can figure out how to programme it and so the Internet simply underscores the possibilities by creating an endless frontier of software that sits on top of the computers in the networks that communicate. So although in detail we didn’t know how this would all evolve and economics has played a big role in the evolution. Lower cost of networking, lower cost of computing making it available to many more people. But I think we knew we were working with something that was very powerful and that ultimately might make a big difference.

Back

Uncaptioned interactive content

Transcript

TEACHER

When we talk about the internet, it's very tempting to think of it as a single computer network. But in reality, it's made up of thousands of separate networks owned by governments, corporations, and individual users. The computers and links that make up the internet are built by a huge number of companies, and use a large range of different technologies to store and transmit information. The internet is made possible, because although there are a large number of different types of computer and networking equipment, they all understand a relatively small number of communications protocols.

The two most common are the Internet Protocol, IP, which is used to transmit information. And the Transmission Control Protocol, TCP, which provides a structure for sending data over a network. The two are so important that they're often written together as TCP/IP. Since all of our computers understand the same protocols, it appears that they all belong to the same network.

The internet is made up of a hierarchy of networks all communicating through TCP/IP. The lowest tier is made up of individual users, who might be

connected together in a local area network. These small networks are connected to the next tier, which is made up from internet service providers or corporate networks who provide access to internet services. These, in turn, are connected to higher tiers, such as telecommunication companies who own the all-important cables that allow data to travel around the world. The topmost part of the internet is sometimes called the internet backbone, or tier one.

Before data can be sent across the internet, the TCP is used to break it into fixed-size chunks. These are known as datagrams, but are sometimes called packets. Each datagram contains a small amount of data, as well as information needed by the internet itself, including the addresses of both the sender and the recipient and a serial number. The addressed datagrams are passed by the sender's computer to a nearby router, such as one on their home network. The local router extracts the destination address of the datagram, and looks for that destination in a table of known addresses. If the destination address is known to the router, then the datagram is sent to the destination computer. However, if the destination address isn't known to the router, it forwards the datagram to a higher-level router, which has a more comprehensive list of addresses. A

datagram 1 might be forwarded all the way up to the routers on the internet's backbone.

The higher-level routers only need to examine the first part of the destination address to determine where the datagram needs to be forwarded. Once its address is found in a router's address table, the datagram can be redirected to a lower-level router, which will in turn forward it to more and more local routers until it eventually reaches its destination.

Routers constantly inform one another about their status and how busy they are. When parts of the internet become congested, or the router becomes unavailable, other routers will find new paths for datagrams that to avoid the problem. IP's ability to constantly reroute data to ensure a reliable flow of traffic means it's entirely possible for datagrams containing parts of the same file to take completely different routes across the internet.

When datagrams finally reach their destination, TCP is responsible for restoring the data to its original condition. The serial numbers on each datagram allow them to be ordered so that the data can be correctly reconstructed. TCP also allows the receiver to request new copies of missing or damaged datagrams from the sender. Between them, TCP and IP offer an extremely reliable way of

sending data over what might be an unreliable network.

Back

Uncaptioned interactive content

Transcript

SPEAKER

We're going to explore the routes taken by datagrams, as they travel across the internet, using a tool called Visual Traceroute. The link to this tool is provided in the text below. When you visit the web page, there's a text box into which you can type the address of the computer we're going to try to send the datagram to. We're going to try to send a datagram to the University of Sydney web server, www.usyd.edu.au.

Clicking the Start Test button will initiate connections from three different locations, in the USA, Europe, and Asia, to this web server. We can zoom and move the map to get a clearer picture of the route taken by the datagram if it is sent from a machine in the United States. Clicking on the Europe tab, located underneath the map, displays the route taken by the datagram when it's sent from a machine in Europe. You can try out some other destination addresses. Does the route taken by the datagram match your expectations?

Back

Uncaptioned interactive content

Transcript

SARAH SMITH

You might think you've got pretty good online security. You've devised long and complicated passwords. You only log onto trusted Wi-Fi networks. So how could anyone access your personal data? Well it doesn't take millions of pounds worth of high tech infrastructure. It's not only state security services that can do it. Anyone, with a bit of inexpensive kit, and a little bit of know-how, could be reading your emails right now. To show how easy it is to hack into just about anyone's emails, we invited a group of students to participate in a short experiment. We promised them a free lunch and that was enough to tempt them in. And we told them it had something to do with mobile phones. We did not tell them precisely what was about to happen.

We've invited you here to ask what your mobile phone says about you. And by the time we're all finished here, I think you're going to be pretty surprised when you find out just how much information your phone is giving away about you, all the time, without you even knowing it.

While they ate some free sandwiches and, inevitably, started playing with

their phones, we started the electronic eavesdropping. They had no idea what we were up to next door. What our volunteers don't know is that hidden behind this bookcase, are our tech security experts. Right now, they are using a bogus Wi-Fi network to connect to our volunteers' phones and access all kinds of personal data.

Glenn and Daniel are here to show us, and our student guinea pigs, just how easy it is to hack into their phones and start reading their emails, tracking where their phones have been, and see what they're looking at online.

GLENN WILKINSON So, Rachel Powell, we've got her Mac address.

DANIEL CUTHBERT Can we find her?

SARAH SMITH Using only a small receiver attached to their laptops, they're able to create Wi-Fi networks that look like the familiar trusted networks the students use all the time. Any of our students might have been wary if they had knowingly logged onto an insecure public network, like you might find at a bar or a coffee shop. But their phones are being tricked into automatically joining what looks like an approved and trusted network, sending all their traffic through our hackers' laptops. They had no reason to suspect anything, but while they dug into the egg and cress.

DANIEL CUTHBERT Her Facebook profile is open. She shows where she lives.

SARAH SMITH Glen and Daniel could see their Facebook pages, check where they'd been, even read their personal emails. Whilst you've been patiently waiting for us here, we have secretly had two tech security experts in the next room trying to find out as much as they possibly can about each and every one of you, without them knowing your names. They don't know your telephone numbers, none of that. But they've still been able to glean quite a lot of information about you.

Our students are about to discover just how much. By leaving their phones switched on, they've inadvertently given away their names, online identities, and allowed access to deeply private communications.

GLENN WILKINSON I'm seeing your Facebook and your email. Your Yahoo mail, it turns out, was, it's not encrypted.

ALLIE KURTZ Are you going through my email?

GLENN WILKINSON We can go through your inbox. At that point, we have control. So Dan was looking at, like, a sent email.

ALLIE KURTZ I do know I have quite an open online profile. But to see the emails come up on the screen, that was a bit shocking, all my work emails, personal things. So that was surprising. It's, like, really scary to know that can happen.

SARAH SMITH And it's not just your email. Our hackers could identify the precise

	locations where our students' 2 phones had previously logged on to Wi-Fi networks.
GLENN WILKINSON	Someone went to the States and connected to a network with a unique name. So that's the only one that's in the database. So I know you've been there. And anyone from Romania or visited Romania?
SARAH SMITH	Did you realise that the phone in your pocket was practically a GPS tracking device?
RACHAEL PELLS	Not to that extent. I didn't realise it was that easy to track my whereabouts, even if, you know, even if they don't have anything on me in the first place, they can just find out everything they need to know through my phone.
GLENN WILKINSON	We are the good guys. We are on your side. This is an example to – if we were the bad guys, we wouldn't be showing you this. We'd be clearing out your bank accounts and running for the border.
DOMINIQUE BRUNDLER	I had no idea, really. We were just talking, eating sandwiches. So really just surprised and shocked.
SARAH SMITH	So at any point, somebody could be hacking into your phone and trying to access all this information about you. And you've realised there's no way you would know that was happening.
DOMINIQUE BRUNDLER	Yeah, basically, I will now turn off my Wi-Fi while I'm around.

SARAH SMITH Worried now? You should be. So how can you carry on, using convenient Wi-Fi hotspots, without giving away all your secrets?

DANIEL CUTHBERT They've got to be more aware of what they're connecting to. Mobile phones and smartphones today leak out a lot of information. The way we use the internet, we give away a lot of what we're doing.

SARAH SMITH You're the white hat hackers. You are doing this for good purposes. Are other people out there using technology like this without quite such good purposes?

DANIEL CUTHBERT Definitely. The criminal market is abusing this kind of technology now. Advanced malware, custom viruses, et cetera. And they're going after people. They want people's email boxes. They want access to computers. Because that way you can then start doing a lot more fraud than you could do with the old fashioned style attack.

Back

Uncaptioned interactive content

Transcript

NARRATOR

In 1980, a young software consultant called Tim Berners-Lee wrote a programme called ENQUIRE. It involved the use of hypertext, links that allow users to jump directly from one computer page to another. It's sowed the intellectual seeds of an information revolution – the world wide web.

In the late 1990s, Tim gave several interviews against rather noisy backgrounds for the Open University series TheWebStory.com.

TIM BERNERS-LEE

The web is an abstract space of information. The web is a space of pages, of documents, of pictures, which are linked together. And the links are abstract links. Now in fact, for the web to exist, all this information about the links and about the documents is transferred over the internet.

NARRATOR

Tim's pioneering idea for the world wide web emerged in 1989, when he was working for CERN, the European organisation for nuclear research.

TIM BERNERS-LEE

I was just frustrated with a lack of interoperability, the fact that people were championing different documentation systems and help systems. And I tried experimenting with actually taking all the documents in one

system and making it appear as though they were in this help system. So I looked at the mapping between the two, and eventually I realised that this little hypertext programme I'd been playing with 10 years before was, in a sense, the key, and that if you made a global hypertext system, any of these systems could be represented in terms of it.

And so suddenly, this was the answer to making any system available without disturbing it, even. That was the key thing. Without putting constraint on somebody, forcing them to use a particular machine, forcing them to store their documents in a particular format.

It just said, all right, let's not force any of those issues. Let's just second-guess them. Let's step above them, and let's say, whatever format you put your document in, let's say that it's part of the one universal space. And let's find a way of making an identifier for it. And once you had that idea, it's really pretty unstoppable.

So when I said, hey, I think we should make a completely general global hypertext system, the very proper answer at CERN was, well, that's fine, but it's not what we're here for. So in fact, it was only because my boss, Mike Sandel, who had a sort of twinkle in his eye, and thought, hm, I don't know what exactly this is about, but I

have a feeling that it sounds kind of exciting.

And he said, well, why don't you spend the next couple of months – you know, I won't complain if you just go and write the programme. If Mike hadn't said that, if I'd had to go through the process of trying to get a formal project approved, it would never have happened.

NARRATOR Tim's brilliant idea was to make documents located on one computer appear to be located in a window on another computer. It took Tim and his colleague Robert Cailliau two years to develop and refine the protocols that could make this happen.

TIM BERNERS-LEE When you're looking at a web page and you click on a hypertext link, then hidden behind the actual text of what's written there is the identifier of some other page. When you click on it, then the programme which shows you that page looks up the identifier. An identifier's one of these things which starts with http://.

Now the http means if you want to get at this thing, this is how you do it. You take the rest of the string, the rest of the characters, and the first bit is something like www.acme.com. And that is the is name of a computer, in fact.

So the first thing you do is you go out to another computer you know which

knows about the native computer and says, hey, where do I find this? And you get back a computer number, like 28.34.6.12. Something looking more like a telephone number of the other computer. Then your computer uses that to start communicating with the other computer, which has got the information.

And what it does, it sends a very simple message. It just says get, and then it gives the rest of all the other characters left. So when you look at something which says http:// – that means use hypertext transfer protocol. www.something.com – that means go to this computer. Slash, gobbledy-gook-gobbledy-gook.

Gobbledy-gook-gobbledy-gook, you don't have to understand. All you do is you know that's what you asked for. So it makes a connection and it sends a very simple command, which is get gobbledy-gook-gobbledy-gook. And the response is that the information about how to put up that page comes back across the internet, across that connection.

So it's really very simple. It's just, get me gobbledy-gook. Here's gobbledy-gook.

NARRATOR: To start with, the web was limited to developments within the CERN community. Then in August 1991, Tim and his colleagues launched the first

publicly available website, a milestone in the history of the internet.

TIM BERNERS-LEE A lot of people ask, what was it like when the web – when it suddenly exploded? When – but it didn't. It didn't suddenly explode. What happened was that it was, for the first two years, a big, hard slog trying to persuade everybody that the idea of global hypertext was not too crazy, or too complicated, or too confusing, or too expensive, or whatever. And in fact, that it was very simple, and in fact, it would save time, et cetera.

So with my fellow evangelist and colleague, Robert Cailliau, we went around to conferences and we went and talked to people individually within the high-energy physics community – which was basically paying our salaries, remember. So I had to persuade them this was important for highenergy physics. And we, at the same time, sent our some emails and some articles to newsgroups and things.

And it was not apparent that it was going to actually make it for a long time. But the interesting thing was that when I looked at the logs of the servers – the first server was called info.cern.ch. And the load on that server, which started off serving 10, 100 hits a day in the summer of '90 – the load on that server went up

exponentially during the next 12 months.

And then when I looked back the year after that and made a graph of the second 12 months, it was again exactly the same-shaped exponential curve. So after a while, I started plotting it on a log scale so that you could see it as it went up from the hundreds to the thousands to the tens of thousands. And the load on that server was just – as the time went on from the summer of '91, summer of '92, summer of '93, summer of '94 – the load on the server just went on increasing by a factor of 10 every year.

NARRATOR But the growing success of the world wide web only partially realised Tim's initial dream of what might be possible.

TIM BERNERS-LEE The first part of it was, wouldn't it be great if we had this universal information space, and everybody could be in equilibrium with it so they could exchange information very fluidly through it? Wouldn't this do something amazing for humankind, if we were connected through this information space? That was the dream, part one.

And the other half of the dream was, suppose you have a situation where any idea which is worth typing in, worth clicking in with a mouse, is in the web? Then maybe we should bring back the computers, the computers which have gotten out the way. The computers

which have hidden, made themselves scarce, and just produced this information for us. Maybe we'll be able to use them again. Maybe we'll be able to write programmes which can analyse what on Earth our society is like, what on Earth we are trained to do.

That was the second part of the dream. And that's not there at all. So that, we need a whole lot more technology in the web. We need machine-understandable information. We need digital signature. We need a web of trust. We need logical reasoning out there on the web. That is going to be yet another revolution.

I think it's going to be as dramatic as the web phase I, if you like. And we haven't started yet. So really, if you think everything's over, you're completely wrong. This is just the start. We're just figuring out how to make these global revolutions using technology, and how to make them be a good thing for humankind. So jump on board now, because it's just speeding up.

ANNOUNCER From the Open University. For more information, go to www.open.ac.uk/use.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Early in the course we looked at the importance of ensuring your digital information is kept secret and not tampered with. We called these goals confidentiality and integrity. This week we'll focus on a key technique called cryptography, which is concerned with securing information so that it can be transmitted safely, even over unsecured networks. You'll be learning the basic terminology of cryptography and how it can be used to achieve different security goals, including securing your emails and protecting your digital life. By the end of the week you'll also be able to explain the use of cryptography in common applications, such as the world wide web.

Back

Uncaptioned interactive content

Transcript

Alice and Bob want to form some kind of relationship. It might be business, it could even be romantic. But whatever else, it must be confidential. The third person in this relationship is Eve. And, as her name suggests, she's an eavesdropper who wants to know what's going on between Alice and Bob. To do that she has to intercept their information.

Alice and Bob might not even be aware that Eve exists, but she as a threat to their confidentiality. First of all, let's remind ourselves how messages are sent over the internet. So we have Alice's and Bob's computers here. Alice has created a document which she wants to send to Bob.

When you send a message across the internet, it may actually look like the message goes straight from one computer to the other. In reality, there's usually at least one more computer, such as a router or a file server in between. So now the message goes from Alice, to the computer in the middle, to Bob.

In fact, it can get even more complicated, and there may be a large number of different computers in between the two of them. Alice's

message is routed from one computer to another until it reaches Bob.

We've drawn the computers in different colours because they don't belong to either Alice or Bob. They might belong to their internet service providers, their employers, or to a big telecom company. Some of the computers may be in a different country, where different laws apply. And some of them might not be trustworthy, which is where Eve comes in.

Here's the same network, except now Eve's going to join in. She will log on and then compromise one of the computers in the middle. One way she could do this is to use a packet sniffer, a piece of hardware or software that makes copies of any messages passing between Alice and Bob, and sends them to Eve. Alice and Bob won't even know these copies are being made, but Eve will have a full transcript of everything that's happening between the two of them.

Alice and Bob can protect themselves using encryption. The most obvious form of encryption is called symmetric encryption, which uses a single key to encrypt plaintext to ciphertext and decrypt ciphertext back into plaintext. Symmetric encryption has been around for thousands of years and is still important today in the form of technologies called DES, triple DES, and AES, which are widely used in

financial transactions over the internet and within banks.

Let's go back to Alice and Bob. Aware that Eve wants to learn their secret, they choose to use symmetric encryption. The first thing for them to do is to generate a shared key and each to make their own copy. One way of doing this is to meet, discuss their secrets, and come up with a key. At the end of the meeting they'll each go away with their own copy of the key. Alice and Bob can now exchange secure messages, each using their own copies of the symmetric encryption key to encrypt and decrypt messages.

However, remember that Alice and Bob don't live locally. They have to travel a long distance, so meeting is not always possible. And it's entirely possible they're in a situation where it's dangerous to share a key.

An alternative is for Alice to generate a key and send it to Bob, perhaps through the post, perhaps over the internet. However, as we all know, things get lost in the post. And that could happen to our encryption key. Or perhaps Eve is waiting by Bob's post box and makes her own copy when it's delivered.

Alice might choose to generate the key herself, then give it to an armed guard, a bit like the way you might use a courier to send a valuable parcel from

one part of the country to the other. Alice generates the key on her computer, hands it over to the armed guard, who then trundles across to Bob and hands the key over.

However, as you can imagine, armed guards are very expensive. Historically, the only people who could afford armed couriers to distribute encryption keys were governments and the very largest companies such as banks and international corporations. This meant that most people were completely unable to use cryptography.

Now you've seen some of the problems of symmetric cryptography, let's see how some of those problems apply to the internet.

Alice and Bob still want to share their secrets. Alice has generated a symmetric encryption key on her computer and needs to send it across the internet to Bob. There are a number of computers in between, one of which has been compromised by Eve. So when Alice sends the key across the network, it passes through the computer now belonging to Eve, who obtains a copy of the key, and so does Bob. Neither Alice or Bob know that the key has been copied. So they can carry on using it, thinking their messages are secure, but in reality Eve is reading each and every one of them.

This is called the key distribution problem. How do we keep keys in the hands of those who need them and not in the hands of criminals or those who would misuse them?

Until the early 1970s it was believed there was no solution to the key distribution problem, hence all those armed guards and couriers. The solution is called asymmetric encryption. Now there are two keys. The first key, called the public key, encrypts plaintext to ciphertext. The second key, known as the private key, decrypts ciphertext back to plaintext.

Back

Uncaptioned interactive content

Transcript

Before we get into the details of how computers use asymmetric cryptography, it's worth spending some time on a small thought experiment.

Here's Alice, here's Bob. Alice has a valuable document. And Bob has gone to his local locksmith and ordered a very large number of identical padlocks, as well as a single key which can open any of those padlocks. If anyone asks Bob for a padlock, he'll send one of them through the post, but he will never give away his key.

Alice asks Bob for a padlock. When she receives it she places her valuable item into a box, closes it, then uses the padlock to lock the Box. At this point, the contents of the box are secure behind the padlock and Alice can't open the box, because she doesn't have a key. It's perfectly safe for Alice to send the box through the post because no one who gets a hold of it can open it unless they have a key. And the only key is in Bob's possession.

When both receives the box all he needs to do is use his key to open the lock, open the box, and there's the original document that Alice wanted to send him.

The boxes and padlock example should make asymmetric encryption easier to understand. The padlocks, which are given to anyone who wants one, represent the public key. The top secret key that can unlock the padlocks is the private key. We'll show the public key as a coloured key on a white background. The private key will be a white key on a coloured background. To keys together are called a key pair, and these are normally held inside a computer on what's called a key chain.

Alice and Bob are now going to use asymmetric cryptography to exchange information. Each of them will independently generate a key pair. A public key, and a private key. The keys are generated using a whole combination of information, such as the user's name and their email address. But to ensure that they can't be created by someone else the program usually asks you to input random information, such as typing away on a keyboard, measuring the amount of traffic passing over a network, or waggling the mouse for a while.

Before they can actually use asymmetric cryptography, Alice and Bob must now exchange their public keys. Each of them sends a copy of their public key to the other. These are added to the key chains on their computers. Alice and Bob are now ready to go.

Alice creates the document she wants to send to Bob. She then, using her encryption program and a copy of Bob's public key, encrypts the document from plaintext into ciphertext. The only way it can be decrypted is using the private key held on Bob's computer. So Eve, or anyone else apart from Bob, can't get at this document no matter how hard they try, which means it's perfectly safe for Alice to send this document over the internet to Bob.

Obviously, the ciphertext needs to be turned back into plaintext. Bob also has a copy of the encryption software. So when he receives the ciphertext the program uses his private key to decrypt the document. Again, this takes a few seconds, but then he's got plaintext. Remember, he's the only person in the world with a copy of his private key, so he's the only one that can actually decrypt this document.

When Bob wants to send a message to Alice he uses his copy of her public key to encrypt the message. Alice uses her securely-stored private key to perform the decryption.

We've seen how asymmetric encryption is used in everyday practice. Now let's look at why it's secure. Remember, asymmetric cryptography uses two different keys – one to encrypt, another to decrypt.

Bob will give his public key to anyone who asks for it, but he always keeps his private key safe and secure. Alice has encrypted a document using Bob's public key and sent it to him over the internet. However, it's been intercepted by Eve, who not only has a copy of the ciphertext, but also a copy of Bob's public key. If Eve tries to decrypt the document using Bob's public key, she's in for a nasty surprise. Eve loads the ciphertext into her encryption program and then uses her copy of the public key to try and decipher it. She ends up with rubbish.

Remember, the document was encrypted with Bob's public key. It can only be decrypted with Bob's private key. And that safe and secure on his computer. No matter how hard Eve tries, she cannot decrypt this document using the public key. She will either have to steal Bob's private key, which is hopefully very secure, or she'll have to use brute force, which could take billions of years to find the correct key. The document is very, very secure.

Back

Uncaptioned interactive content

Transcript

In this video, we demonstrate how to install and use Mailvelope, an extension to the Chrome Web browser which allows you to send an encrypted email through existing web-based email accounts, such as Gmail or Yahoo mail.

To install Mailvelope we first locate it in the Chrome Web Store. Click Add to Chrome and select Add. Once the extension has successfully installed, you can see the Mailvelope icon appear in the Chrome toolbar at the far right-hand side.

We now need to generate a public and private key for ourselves and tell Mailvelope about the public keys of the people we plan to communicate with. We start by generating our own keys. We click the Mailvelope icon in the Chrome toolbar and select Options. This shows our key ring, the set of keys that Mailvelope knows about.

At the moment there are no keys listed. We then click the menu option, Generate Key, from the list at the left of the screen. We are presented with a form asking for the name, email address, and passphrase that will be associated with the generated key. We fill in the information, making sure we

use a strong and memorable passphrase. Mailvelope will ask for this passphrase when we try to use this key to sign or decrypt a message.

Clicking Submit shows a progress indicator and a message that the key is being generated. Once this is complete we see the message 'Success! New key generated and imported into key ring.' at the bottom of the form.

The final part of configuring Mailvelope is to import a public key for the person we want to exchange messages with. We've set up a special email address for this task: cybersecurity-mooc@open.ac.uk.

We start by clicking the Menu option Import Keys from the list at the left of the screen. Public keys can be provided as plaintext. We copy the one for our email address below. Include the lines with "begin" and "end." Paste it into the text area of the Mailvelope Key Import screen. Click Submit. We can now use the Mailvelope tool to send a signed and encrypted email to the cybersecurity-mooc email address.

Back

Uncaptioned interactive content

Transcript

First, we open Google Chrome, log into our email, and start a new message. Here we're using Gmail. We address it to cybersecurity - mooc @ open . ac . uk. To encrypt the message, we click the notepad icon that appears in the message window. We now see the mailvelope message window where we can type our message.

First, we digitally sign our message by clicking the swirly pen icon in the message window. This brings up a dialogue box, where we select the key we created earlier. This modifies the message to include an encrypted signature block.

We now want to encrypt the signed message so that only the intended recipients can read it. To do this, we click the padlock icon at the top right of the window. Mailvelope shows us a dialogue box where we can select the keys associated with the intended recipients.

In this example, we select the key for cybersecurity - mooc @ open . ac . uk, and click Add, followed by OK. The message is modified again.

The final step is to move the signed and encrypted message back to the

web-based email system by clicking Transfer. We can now send the signed and encrypted email.

Back

Uncaptioned interactive content

Transcript

NARRATOR: We've already seen that exchanging encrypted documents using public key means that Alice and Bob each have to generate their own key pairs, comprised of a public key and a private key. Before they can exchange documents, they first need to send one another copies of their public keys. Then, Alice can send secrets to Bob by encrypting documents using Bob's public key, and Bob can share secrets with Alice using her public key. But there's more you can do with public key cryptography than just hiding secrets. It's also possible to encrypt data using the private key, which might sound like a pointless thing to do.

After all, a file encrypted using Bob's private key can be decrypted by anyone who has a copy of his public key. And Bob gives that away to anyone who asks, including evil Eve. So, if encrypting using the private key isn't going to protect any secrets, what's it for? Whilst the encrypted file can be decrypted by any copy of Bob's public key, it can only have been encrypted by the corresponding private key. If Bob has obeyed the rules and not shared his private key, then the documents can only have come from

Bob. Encrypting using the private key is therefore a way of authenticating data.

Now, anyone wanting data from Bob can download a copy of the encrypted document and a copy of his public key. They decrypt the file using the public key and can satisfy themselves the data is genuine. But it’s not quite as simple as that. Bob’s public key is only authenticated by his email address. If Eve can steal Bob’s email address, there is nothing to stop her generating new keys under Bob’s identity. Eve can now send false documents or malware in Bob’s name. Alice will open them, because she trusts Bob. Oh dear. Bob can prevent Eve impersonating him by certifying his public key.

Here, a so-called trusted third party, which can be another individual, a government, or a private company, will confirm that Bob’s key is genuine. To do this, Bob must prove his identity to them using personal information that isn’t readily available to Eve, such as his passport, business registration, or birth certificate. The certification body can either certify the public key itself or provide Bob with a digital certificate containing his public key.

As well as the holder’s public key, a certificate contains a unique serial number, the name of the certificate’s owner, the name of the agency that issued the certificate, the agency’s digital signature, proving it is authentic,

the issue date of the certificate and the date it will expire, after which it can no longer be considered valid, and a hash value used to check that the certificate has not been altered since it was issued. As well as individual use, certificates are used to authenticate software downloads, such as those from app stores. Certificates are also used by websites who presents copies of their certificates to web browsers. The browser checks that the certificate is authentic, proving that the site is genuine.

If the certificate is invalid, the browser will warn the user they may be navigating to a page that has been hijacked, and it will offer them an opportunity to stop. Certificate holders have to be careful to renew their certificates before they expire. Otherwise, they might find users avoiding their websites or that their software downloads are not valid. This happened to Apple in November 2015, when millions of users could not update apps on their Macs. Fortunately, a new certificate was quickly issued, and everything worked again.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Hello. You're now 6 weeks into the course. As we saw a couple of weeks back, computer networks provide the basic infrastructure for the internet and the worldwide web. Therefore, it's important to understand how these networks can be protected from attacks. Building on what you recently learned about networking and cryptography, you can now see how to protect the underlying communications networks and computers you use.

By the end of this week, you'll understand the role of firewalls and protecting networks, you'll be able to configure your own personal firewall on your computer, and you'll be able to describe how networks can be automatically monitored to detect attacks as they occur. You'll also learn how cryptography enables virtual private networks to maintain your confidentiality. When you lock your front door, you protect your valuables and personal space in the real world. Now let’s see how to do the same for your digital life.

Back

Uncaptioned interactive content

Transcript

Configuring your own firewall (PC)

If you have Windows 7, go to the Start menu. Choose Control Panel, and then System And Security.

One of the options is for Windows Firewall. Click it. Click Turn Windows Firewall On or Off. You may need to enter an administrator password depending on how your Windows is set up. If the firewall is not already active, click Turn on Windows Firewall for each of the network types that your computer supports. The Windows Firewall gives you a range of options depending on how much data you wish to allow through the firewall.

When the firewall is first activated, the majority of applications are automatically blocked. But you can overrule this block by checking the Notify Me check box when the Windows Firewall blocks a new app.

From now on, every time an application first attempts to connect to the network, Windows will prompt you, asking if you wish to give it permission to do so. Your choice is remembered by the firewall. You should only give permission if you are sure the application is safe.

If you want to get maximum protection from the firewall, select the Block All Incoming Connections option, including those in the list of allowed apps. This will prevent other computers connecting to your machine unless your computer has requested data. This is a very useful option if you're travelling and using public Wi-Fi networks.

Back

Uncaptioned interactive content

Transcript

On an Apple Mac, you can access the firewall using the System Preferences. Choose Security and Privacy. On the Security and Privacy Preferences pane, select the Firewall tab. If the firewall is not already enabled, click the Turn On Firewall button. You may need to click the padlock icon and provide your password to do this. Once the firewall is enabled, you can access its settings by clicking the Firewall Options button. Clicking the Block All Incoming Connections button will stop network traffic from external computers other than the traffic relating to some basic network services.

The list of software under this check box specifies the programmes that are allowed to send and receive data from the network. Software can be added to this list by clicking the Plus button underneath it. The check box to automatically allow assigned software to receive incoming connections allows those applications that have been digitally signed to send and receive data.

Finally, the Stealth Mode button can be used to prevent your computer from responding to ping messages that are sometimes used by attackers to identify

potential targets. Any changes we make to the firewall settings have to be confirmed by clicking the OK button at the bottom of the window.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Over the past few weeks, we've looked at the threats to your digital information and the technologies available to protect it. Now you know how cryptography can help you keep your secrets and how to protect your network from an attack. But what if you are attacked? This week, we're going to look at what can go wrong when an attack on the security of your information is successful. Using case studies, we'll look at individuals and organisations that have been hit and see what impact it had on them.

This will help you learn to recognise the signs of an attack, arm you with the information on how to recover from a security breach, and how to stop it happening again. Just as importantly, we'll be looking at backing up your data, and the pros and cons of various approaches. 'Til next week.

Back

Uncaptioned interactive content

Transcript

PRESENTER	In this block of flats behind me, a hacker made tens of thousands of pounds in fraud, and all from the comfort of his own home, until he tried to push his luck a little too far. Ian Wood was using Facebook to fund a lavish lifestyle.
DC BILLY JOHNSON	He would generally pose as someone who wasn't himself. For example, maybe as an attractive woman and he would try and befriend men on Facebook who would look at his profile picture and say, 'Oh yeah, I'll be friends with that person'. And what they were essentially doing was allowing this man into their life.
PRESENTER	He discovered people often use the same usernames for different accounts online.
DC BILLY JOHNSON	What Ian Wood did was he used that username, type it into mainstream banking websites, and as soon as he got the message of username correct, password incorrect. Security questions. He was in play then. And he could use information from the social networking sites to try and find a way in to that bank account.
PRESENTER	Once in, he stole 35,000 pounds from online accounts. He then transferred

	the money to bogus accounts until he got cocky.
DC BILLY JOHNSON	As a lot of criminals do, they get more relaxed about their behaviour, and that was when he made the transfer from a bank account into his own in his name. We went to arrest him for that offence and that was when we opened the door basically to all the activity that he'd been involved in.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW Welcome to the final week of the course. Over the past 7 weeks we've explored different information security threats, together with the actions you can take to prevent these threats from causing harm to your digital life. We've looked at some key technologies such as networking and cryptography that underpin the activities we carry out online. We've looked at what can be done in the event of an attack from both a technological and legal standpoint.

Now we'll focus on how to assess the security risks associated with your digital life, so that you can effectively plan to protect yourself from attacks. You'll also have the opportunity to review your information security practises and review on how these might have changed as a result of what you've learned.

Back

Uncaptioned interactive content

Transcript

CORY DOCTOROW That's it for this course. I hope you've enjoyed it and are now feeling more confident about navigating through potential risks to your online security. If you want to find out more or are curious about other courses, please head over to the Open University's website where you'll find modules related to computing in general and some focusing on different aspects of information security.

Back