Digital Security

DIGITAL SECURITY

Digital Essentials

THE UNIVERSITY OF QUEENSLAND LIBRARY

The University of Queensland

CONTENTS

MODULE OVERVIEW

Aims and objectives

This module will:

- outline cyber security issues
- explore ways to protect your privacy online
- provide information and guidance on account security.

After completing this module, you will be able to:

- check cyber security scams and threats
- control the information you provide online to protect your privacy
- understand how accounts are hacked and ways to reduce your risk
- practice proper account and password management.

Module sections

1. Cyber security
2. Online privacy concerns
3. Protect your privacy
4. Have you been hacked?
5. Create secure passwords
6. Account and password management
7. Multi-factor authentication
8. Check your knowledge
9. Conclusion

Download versions are available on the homepage.

Duration:
Approximately 20 minutes

Student partnership

This module was developed with UQ student partners as part of a Student-Staff Partnership project.

Graduate attributes

Knowledge and skills you can gain from this module will contribute to your Graduate Attributes:

Connected citizens

This module is part of Digital Essentials, a series of online modules to help you quickly build your digital skills so you can succeed in study and work.

Return to UQ Library.

1. CYBER SECURITY

- [Cyber security threats](#)
- [Phishing](#)
- [Malware](#)
- [Stay cyber safe at UQ](#)
- [Protect yourself online](#)

Cyber security threats

> ⚠️ Australians lose millions of dollars each year to online scams!
>
> Check the [Scam statistics](#) from Scamwatch.
>
> Anyone can be a target!

Phishing

Phishing is an attempt to acquire sensitive information by baiting the user. A typical phishing attack involves a person using electronic communication, typically email, to induce the user to click on a malicious link or provide sensitive data. The bait might be an attractive subject line, seemingly official layout and branding or an enticing offer. The objective of a phishing attack may be to:

- gain access to your username and password
- obtain financial information
- induce you to download malware.

Spotting a phishing attempt

The Australian Cyber Security Centre (ACSC) recommends users avoid phishing attacks by:

- not opening emails from **unfamiliar** people and companies
- setting up a **spam blocker** on your email client
- **hovering** your mouse over **links** to check the real URL

- checking the message for spelling or grammatical mistakes
- remaining **skeptical** of enticing offers — is it too good to be true?
- not releasing any **personal information** via email — a reputable bank would not ask for personal information via email.

Tips to avoid phishing

Source: Tips to avoid phishing has advice on what you should check to protect against a phishing attack.

Malware

Malware is a combination of the words 'malicious' and 'software'. This software might be downloaded as a result of clicking on a malicious link, for instance as part of a phishing campaign or installing an unknown application.

Click the plus symbol to find out more about each type of malware:

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://uq.pressbooks.pub/digital-essentials-digital-security/?p=81#h5p-3

Stay cyber safe at UQ

Cybersecurity at UQ has information on how to:

- recognise cyber security threats
- report incidents and risks
- access online training (for UQ students and staff)
- stay cyber-secure, including using wifi safely and sharing sensitive information.

Protect yourself online

1. Install anti-virus software

Strongly consider installing anti-virus software to protect yourself against malware, spyware and adware.

PCMag has compared the main antivirus tools for:

- Windows computers – The Best Antivirus Protection of 2023
- Mac computers – The Best Mac Antivirus Protection of 2023

2. Create strong passwords and vary them between services and platforms

- Consider using a password manager (discussed in section 6 of this module).
- Do not use the Login with Facebook option. Researchers have identified security and privacy concerns with this method of authentication.

3. Update your software regularly

Software companies regularly patch security flaws in operating systems and applications. Simply keeping your phone or computer's operating system, web browser, and other applications up-to-date can help protect you and your data.

4. Be alert and guard against phishing attacks

Human error is one of the main causes of security breaches. Take the Spot the scam quiz from the ACSC.

Read Protect yourself by the ACSC.

Malware can be distributed by spam or phishing emails, by visiting malicious websites or downloading legitimate-seeming software.

2. ONLINE PRIVACY CONCERNS

What is privacy?

Privacy is a concept which is difficult to define exactly but we intuitively know when it is being threatened or breached. In a digital context, it might be about:

- knowing what is happening to your information, such as where it is stored and how it is being used
- exerting control over your information — to remove it from the internet altogether, or controlling who can view it
- having the ability to block threats to your privacy by controlling what information you provide in the first place
- controlling who can contact you and for what purpose.

Is there a privacy crisis?

"If you are not paying for it, you're not the customer; you're the product being sold"

Andrew Lewis

Helped along by a series of widely reported events, internet users are becoming more aware of the threats that online life can pose to their privacy:

- The Facebook data breach in April 2021, where the details of more than 500 million Facebook users were found online.

- The Optus data hack in 2022.
- Medibank hack also in 2022.

The majority of Australians are concerned about online privacy according to the Australian Community Attitudes to Privacy Survey 2020. Even though we are concerned, few of us take action to protect our privacy. How about you?

Let us know in the following form! The form is set to anonymous. We will get your response data but we won't know who has submitted it.

Check out the responses so far!

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://uq.pressbooks.pub/digital-essentials-digital-security/?p=48

Gathering our data

Governments, organisations and businesses collect data from us. Data can be **used ethically** for research and service improvement, such as for travel and land-use, or to solve social and environmental problems. It can also be used **unethically** for profit.

Personal information requests

Businesses or organisations often request our personal details when we sign up or download their software or tools.

Customer loyalty schemes

The Australian Competition & Consumer Commission (ACCC) warns us to be careful when signing up to customer loyalty schemes. These programs often request personal information. It is possible that they can combine this with information gathered from your social media or web browsing to build a detailed profile about you.

Apps and software

Often when you install an app, it will ask you for access to information on your device, for example, your contacts list, address book, your camera or your photos. The app might also ask to turn on location services.

Try to download from reputable sources and check reviews to verify the safety of an app you wish to use. Try to limit the access and information you provide.

The [Protect your privacy section](#) has more information on steps you can take for personal information requests and installing apps.

Privacy laws

Jurisdictions respond to threats and concerns in varying ways.

Privacy Act

The [*Privacy Act 1988* (Cth)](#) regulates how Australian government bodies, as well as some non-government organisations, must treat your personal information. The *Privacy Act* categorises certain personal information as "sensitive information" and stipulates that organisations provide a greater level of protection. Examples of 'sensitive information' include:

- religious or political affiliation
- sexual preference
- race.

The Act also outlines what should happen if an organisation's data is breached and when the organisation has to notify you.

General Data Protection Regulation (GDPR)

In 2018, the European Union passed the [General Data Protection Regulation (GDPR)](#), perhaps the most comprehensive privacy legislation to date.

Privacy at UQ

The University of Queensland's [Privacy Management Policy](#) specifies that the University must collect, store, provide access to, use and disclose personal information in accordance with the [Information Privacy Act 2009](#).

More information on privacy at UQ can be obtained from the [Right to Information and Privacy Office](#). Learn more about how UQ is required to manage [student privacy](#).

Spam
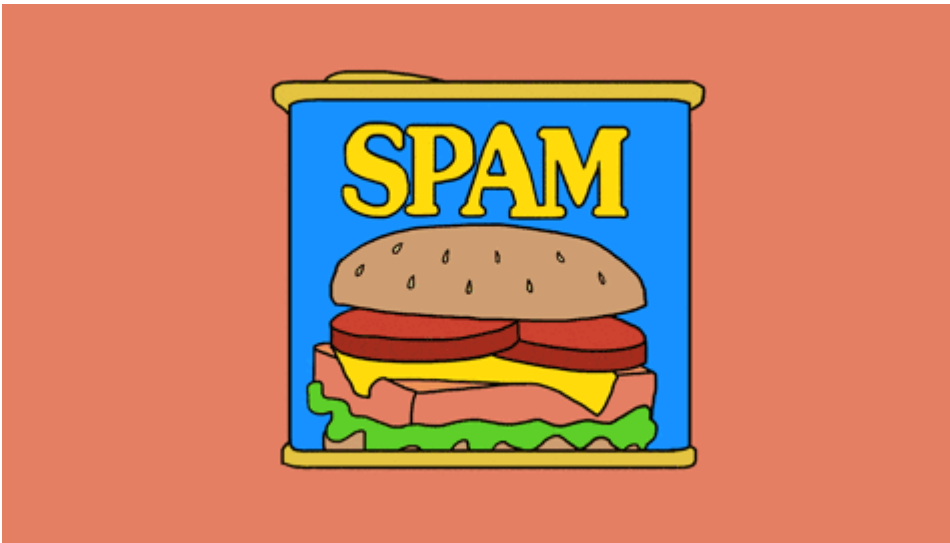
Source: [Luncheon Meat LOL GIF](#)

In Australia, the [*Spam Act 2003* (Cth)](#) prohibits organisations from sending spam.

Spam is defined as the sending of unsolicited messages without your consent. You can consent to commercial messages by providing your contact information by filling out a form, over the phone, or during face-to-face communication. Even if you have provided consent, all messages must include a [unsubscribe facility](#).

3. PROTECT YOUR PRIVACY

- [Limit the amount of personal information you share](#)
- [Share information through appropriate channels](#)
- [Don't use the same password between services and platforms](#)
- [Share information through appropriate channels](#)
- [Block third-party cookies and trackers](#)
- [Review your browser settings](#)

Limit the amount of personal information you share

The simplest way you can protect your privacy online is to limit the amount of information you share in the first place. Be particularly careful about sharing **personal information** (date of birth, address, phone numbers) online.

Protect your personal information online

This task shows tips from the [eSafety Commissioner on protecting your personal information online](#).

> An interactive H5P element has been excluded from this version of the text. You can view it online here:
> *https://uq.pressbooks.pub/digital-essentials-digital-security/?p=50#h5p-4*

Downloading and installing apps

The eSafety Commission has [eSafety guides](#) for different apps with tips on how to protect your personal information and security.

Before you get an app check:

1. Whether it is from a reputable source
2. Online reviews to verify its safety
3. Your privacy and security settings.

When you install the app:

1. Don't use the same log in details you use for other apps e.g. your Facebook account
2. Read the installation messages carefully
3. Turn off in-app purchases
4. Pay attention to any notices or emails you receive for the app, in case there are changes.

If you have concerns but are required to install an app or software on your device for work or study:

1. Check your privacy settings prior to installation
2. Make sure you have installed antivirus software and it is up to date
3. Log out of any programs you don't want running at the same time
4. Consider temporarily removing any sensitive data to another location, such as a hard drive or another device
5. Make sure to fully uninstall the app when you are finished:

    ◦ [Delete apps on your Mac](#)
    ◦ [Uninstall or remove apps and programs on Windows](#)

Alternative facts!

[Don't be phish food!](#) recommends giving 'alternative facts', rather than your real details, for platforms that require you to complete a user profile but have no good reason for needing that information.

Don't do this for official websites that need your real data, such as banking, educational institutions or government sites as that would have legal implications.

Social media privacy settings

Regularly check your social media privacy settings:

1. Set your profile to private
2. Only accept friend requests from people you know and trust
3. Disable location sharing.

Don't use the same password between services and platforms

Read our section on [password management](#) and consider using a password manager.

Share information through appropriate channels

Some online tools are not appropriate places to share information. Personal information should generally not be shared on **unencrypted** services or websites.

You may want to consider setting up a **virtual private network** (VPN), which creates a point-to-point secure connection. UQ has a [VPN available for UQ student and staff](#).

📖 Read [The Best VPN Services for 2023](#) by PCMag and scroll down to watch the video on how a VPN works.

When choosing a VPN, you may need to consider factors such as:

- cost
- speed
- location
- device and operating systems compatibility.

Block third-party cookies and trackers

Consider installing a browser extension to stop internet tracking. Reputable extensions are:

- [DuckDuckGo Privacy Essentials](#)
- [Privacy Badger](#)
- [HTTPS Everywhere](#)

Note**:** Blocking [third-party cookies](#) can cause issues accessing your lecture recordings, Turnitin or the ePortfolio system. If you are concerned about privacy, an alternative to allowing third party cookies is [allowing exceptions to individual websites](#).

Review your browser settings

- Your browser settings can be adjusted to provide extra protection against cookies and trackers.
- It also helps to **regularly delete cookies** that you may have collected during browsing, to stop websites remembering your past behaviour.
- Make sure you regularly <u>update your browser to the latest version</u>.

Read the eSafety Commissioner's information on <u>Web browsers</u>.

They cover a number of ways to help protect yourself while online.

4. HAVE YOU BEEN HACKED?

- [Data breaches](#)
- [Stopping data breaches](#)
- [Check if your data has been breached](#)
- [How hacking happens?](#)

Data breaches

A data breach happens when personal information is accessed, disclosed without authorisation or is lost.

Source: [Data breaches](#) by the Office of the Australian Information Commissioner.

Examples of data breaches

CSO Australia has tracked the [15 biggest data breaches of the 21st century](#) (dated 6 November 2022). They include:

1. Yahoo, 2013, 3 billion accounts
2. Aadhaar, 2018, 1.1 billion of identity information
3. Alibaba, 2018, 1.1 billion of user data
4. LinkedIn, 2021, 700 million users
5. Sina Weibo, 2020, 538 million accounts.

The Office of the Australian Information Commissioner publishes statistics on [notifiable data breaches](#).

Stopping data breaches

It is up to organisations and their employees to reduce the risk of data breaches occurring.

[Data breaches: How they occur and how to prevent them](#) has information and tips on how to prevent data leaks at UQ.

As an individual, you can reduce the impact a data breach will have by practising sound password and

account management such as using secure passwords and two-factor authentication (this is covered later in the module).

Check if your data has been breached

Have you been pwned?
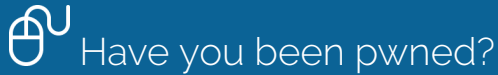
Check your email address on Have I been pwned!

It will tell you if websites associated with your email address have been breached.

This site was created by Troy Hunt, an Australian who works as a Microsoft Regional Developer. The site has an About section and an FAQ section explaining how the site works, along with information on it's history and purpose.

If your email is connected to a security breach, and you reuse passwords for multiple sites, you may be **at risk**.

Groups or individuals will take large numbers of email addresses and associated passwords and start trying them on major websites like Facebook, Gmail, Instagram,Twitter etc. They try these email and password combinations to get access to the accounts of anyone who uses the same password across all websites.

Recommendations:

- Don't use the same password everywhere
- Be vigilant in checking your account security regularly
- Don't use the same password for extended periods of time (2+ years).

The UQ Information and Communication Technology Policy states that if your password is less than 12 characters you should change it every 12 months.

How hacking happens?

Data breaches can occur in a variety of ways, but the common element is someone gains access to a database of user information and either steals or copies and then sells or releases the data.

Brute force

Brute forcing in its simplest form is someone typing in a password of aaaa, aaab, aaac etc until they find the right combination. With today's technology, a computer can check over 1 million password combinations a second. A lot of websites restrict how many passwords can be tried in a certain time frame before the account is locked or temporarily suspended.

When hackers breach a collection of users' information, what they find and steal usually isn't stored in plain text on the system. Instead, the cache of passwords is often converted into cryptographic hashes, random strings of characters into which the passwords have been transformed to prevent them from being misused. It is these hashes that are brute forced to reveal your username and password.

Interested in learning more, check out this article from <u>Hive Systems – Are your passwords in green?</u> (updated for 2023) on how to make more secure passwords.

Stopping brute force attacks

You can make it take longer to brute force your password by increasing the **length** and **complexity** of your password.

'Abcdefghijklmnopqrstuvwxyz' may be long, but it is not complex.

Most password cracking software uses what's known as a dictionary attack to check popular words or phrases first, such as abc123, trustno1, drowssap, password123 etc

Social engineering

Social engineering can be an effective method for some individuals to access a variety of accounts. Social engineering is the manipulation of people so that they give up personal information about themselves or others. This personal information is then used to access systems the person uses.

<u>What is Social Engineering? (YouTube, 2m4s)</u>:

> *One or more interactive elements has been excluded from this version of the text. You can view them online here: https://uq.pressbooks.pub/digital-essentials-digital-security/?p=52#oembed-1*

How to avoid social engineering

1. Avoid having all your eggs in one basket (or the dreaded "single point of failure"):
   Do not use the same email address for every site or service you use online. The more intertwined and dependent your accounts are the more widespread the damage a security breach can cause you. For example, don't use your Gmail address for every service's password recovery option.

2. Use different logins for each service:
   Never use the same password more than once. And make sure your passwords are strong.

3. Use two-factor authentication:
   After you have entered in a correct username and password you are prompted to confirm your identity in another way

4. Get creative with security questions:
   The additional security questions websites ask you to fill in are supposed to be another line of defence, but often these questions are easily guessed or discoverable. You can shift the letters in your answer or use your own special coding system to make sure only you know those security answers, for example pordwass.

5. Frequently monitor your accounts and personal data:
   To be on the lookout for both identity theft and credit card fraud, check in with your account balances. You can use Google Alerts to check if your details have been posted online anywhere.

6. Avoid falling victim to phishing emails:
   Phishing emails are becoming harder to detect, and easier to fall victim to.

5. CREATE SECURE PASSWORDS

Creating a secure password and practising good password management are the most important things that you can do to secure your accounts.

(?) Do you know what makes a secure password?

An interactive H5P element has been excluded from this version of the text. You can view it online here:
https://uq.pressbooks.pub/digital-essentials-digital-security/?p=54#h5p-5

Tips to secure your online accounts

- **Don't just use one password** – use a different password for every account
- **Use a passphrase** – instead of a singular word, try a sequence of words for instance, *DogsandCatsareawesome.* Note*: Do not use this as your password!*
- Include **numbers, capital letters** and **symbols**
- The **longer the password**, the better
- **Don't write passwords** down
- Turn on **two-factor authentication**.

UQ password management

You can change your password via the Information Technology Services (ITS) website. You will be asked to provide your UQ username and current password when you do this. ITS have also created a guide on creating good passwords and managing your account.

If you have forgotten your password, you can use the password reset page on the ITS website. To do

this you will be asked to provide your UQ username and the mobile number recorded in your mySI-net account.

UQ students can contact the Library's [AskUs](#) service if you need password help.

Note: In order to reset your UQ password you will need an Australian mobile number listed in your mySI-net account. Check what number you have listed in your [mySI-net account](#).

6. ACCOUNT AND PASSWORD MANAGEMENT

- [Account management](#)
- [Password management](#)

Account management

Creating a secure password is important, but no matter how secure your password is you can still be vulnerable if your account management is lacking.

An example of bad account management would be using the same secure password and email address across multiple accounts. If one account gets hacked and your username and password are stolen, hackers can use that information to then access your other online accounts.

On websites like Spotify, you can conveniently 'Login with Facebook' so that you don't need to create a separate account for every site you use. However, this convenience comes at a cost, because every time you use your Facebook login to access another service, you are giving that other service access to your personal data stored by Facebook. This also allows an attacker to only require access to your Facebook account to start getting access to everywhere else that you associated that Facebook login. By using the 'Login with Facebook' option you are essentially using Facebook as a password manager to remember your username and password for a number of sites and services.

> Ever noticed after doing some online shopping, adverts in other websites showing similar items to the ones you just searched? This is a demonstration of your personal data being sold and exchanged to target you.
>
> Read [No boundaries for Facebook data: third-party trackers abuse Facebook login](#) on Freedom to Tinker.

? Log in using the same account?

> An interactive H5P element has been excluded from this version of the text. You can view it online here:
>
> *https://uq.pressbooks.pub/digital-essentials-digital-security/?p=56#h5p-6*

Password management

Password managers provide a similar level of convenience to "Login with Facebook" but are much safer. Password managers create an encrypted database of all your usernames and passwords, that only you can access with a master password. This means you only need to remember one password to have access to all of your accounts.

Most password managers will include the ability to generate secure passwords that you can use for new or existing account logins. Because you only need to remember one master password, you can generate and store complex passwords for your needs. This way, you are not relying on your memory and easy passwords to remember many different account login details.

[BitWarden](#) password generator function

To make website logins easy, most password managers have browser extensions that either insert the information into required login fields automatically or allow you to copy and paste the details. Not all websites and apps allow automatic login filling or pasting into login fields.

What to consider when choosing a password manager

There are a large number of password managers available for use. You need to research which service you want to use. A lot of these solutions have reports or blogs on their site discussing how it works and what they do to protect your details, for instance 1Password has a [white paper (PDF, 831 KB)](#) going into a lot of depth on their service and mission.

Some points to consider when making a decision:

1. Is my password **stored only on my computer** or is it **backed up in the cloud**?

     ◦ Given the growing popularity of using password managers, they are a prime target for a data

breach due to the sheer amount of account information they may store. You have to decide between maximum security vs usability and convenience. If a password manager stores passwords in the cloud, they often have a phone app and browser extension allowing syncing across devices. This means that your information is being sent across the internet to allow your other devices access, making that less secure than never being sent across the internet.

2. If they are backed up in the cloud, is the information **encrypted before or after it is backed up**?

    ◦ If the information is encrypted after it has been backed up in the cloud, then it was potentially sent over the internet as plain text and is a lot easier for attackers to gain access to.

3. Are there any **recorded breaches** of the password manager in the past, and **how did the service react**?

    ◦ LastPass suffered a security breach in 2022. LastPass publicly addressed the breach, how it occured and what was stolen. This type of communication is important because it allows users to change their password, usernames etc to avoid trouble in the future.

The following list is a mix of open-source and commercial services. Make sure to do your own research and decide which will work best for you:

- [1Password](#)
- [Bitwarden](#)
- [Password Safe](#)
- [iCloud Keychain](#)
- [Keepass](#)

7. MULTI-FACTOR AUTHENTICATION

- Single-factor authentication
- Two-factor and multi-factor authentication
- MFA at UQ

Single-factor authentication

Single-factor authentication requires only one type of log in method, such as a username and password. This has previously been the usual way to log in to accounts on many websites and platforms.

This method can reduce your account security as anyone who gets access to your log in details will be able to get into your account.

Two-factor and multi-factor authentication (MFA)

In recent years, two-factor authentication (2FA) and MFA have become more common ways to login to online accounts to help protect users from data breaches.

After a user has entered their normal login details (username and password), they are prompted to confirm their identity in another way, i.e. entering a code sent via text or email, confirming the login attempt via an app on their phone or entering a code generated by an authentication device.
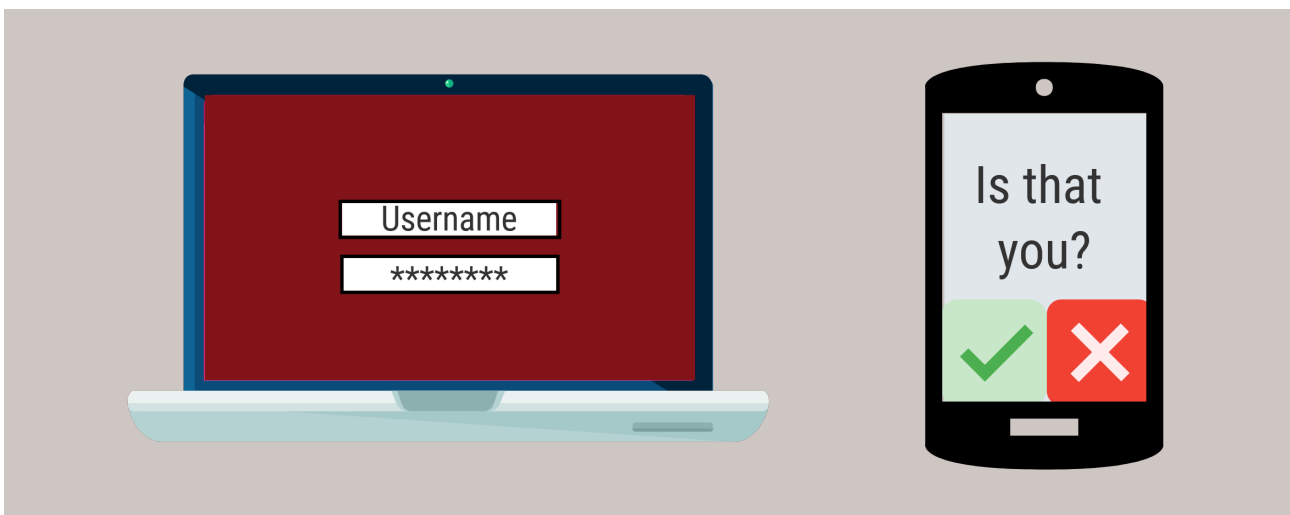
Two methods of authentication

2FA requires two methods of authentication and MFA requires two or more methods. Examples of other multi-factor authentication options are biometrics like FaceID by Apple and fingerprint scanning.

We recommend that you turn on MFA for your accounts wherever possible.

Protect Yourself: Multi-Factor Authentication from the Australian Cyber Security Centre (ACSC) has links with instructions for setting up MFA on different services, such as email, banking, shopping, gaming and social media.

Enabling multi-factor authentication (Vimeo. 43s) from the ACSC:

> *One or more interactive elements has been excluded from this version of the text. You can view them online here:* *https://uq.pressbooks.pub/digital-essentials-digital-security/?p=135#oembed-1*

MFA at UQ

UQ requires you to use MFA to log in to UQ systems.

The my.UQ Multi-factor authentication (MFA) page explains how to activate and troubleshoot MFA at UQ.

8. CHECK YOUR KNOWLEDGE

All the answers to the quiz questions can be found in this module.

Your response data will **not** be gathered if you answer the questions below. Take a screenshot of **Your result** at the end of the quiz if you are required to show you have completed it.

? Digital Security quiz

There are 8 questions to answer. After you answer a question, click the arrow to move to the next question.

> 🖹 *An interactive H5P element has been excluded from this version of the text. You can view it online here:*
> *https://uq.pressbooks.pub/digital-essentials-digital-security/?p=34#h5p-7*

Note for Teaching staff: You can download and embed both the module and H5P quiz in your course.

Module summary

① Cyber security

- Cyber security threats and scams are prevalent in our digital society.
- A common security threat is phishing, which involves a person using electronic communication, typically email or messaging, to induce the user to click on a malicious link, or provide sensitive data.
- Installing Install anti-virus software is recommended, but there is a range of additional steps you can take.

② Online privacy concerns

- Privacy is reliant on having transparency, security and choice around how your information is collected and used.
- Australian businesses and government departments, especially larger ones, need to comply with the *Privacy Act 1988* (Cth) and the *Spam Act 2003* (Cth).

③ Protect your privacy

- There are steps you can take to protect your privacy online.
- It is important to limit the amount of personal information you share online.

④ Have you been hacked?

- Regularly checking your accounts for any security breaches is an important part to staying safe online.
- Your email address is frequently used as a username across multiple services and sites. If it is breached then access to all it's attached sites and services are at risk.

⑤ Create secure passwords

- One of the most important steps to staying safe online is creating a secure password for each account.
- The longer the password the better.

⑥ Account and password management

- In an effort to stay secure online, multiple passwords and usernames can become hard to track.
- Using proper account management and password managers can make keeping track a lot easier.
- Not every password manager offers the same security or convenience as others, it's important to understand the differences and make an informed decision on which to use.

⑦ Multi-factor authentication

- Sometimes having a super secure password is not enough to stay safe online.
- Enabling multi-factor authentication .creates an additional barrier to secure your account.

9. CONCLUSION

You have completed the **Digital Security** module.

Tell us what you think

Use our <u>Digital Essentials feedback form</u> to give **anonymous** feedback on this module. You can provide your email if you would like us to reply to you.

Digital Essentials modules

Build your digital skills with Digital Essentials. Select modules from the 6 themes that match your interests and will help you succeed in study and work.

⌨ UQ systems

<u>Use UQ systems module</u>, includes:

- [Check your IT set up](#)
- [Book rooms](#)
- [Printing at UQ](#)

✎ Assignment essentials

- [Find and use media](#)
- [Information essentials](#)
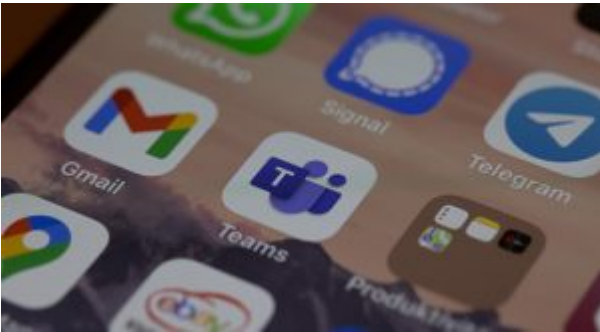- [Write, cite and submit](#)
- [Types of assignments](#)

⚙ Digital creation

- [Accessibility](#)
- [Choose the right tool](#)
- [Intellectual Property](#)

🔒 Digital security and safety

- [Digital security](#)
- [Internet essentials](#)
- [Social media](#)

👥 Professional identity and skills

- [Communicate and collaborate](#)
- [eProfessionalism](#)

📊 Work with information

- [Artificial Intelligence](#)

- [Work with data and files](#)
- [Document your research data](#)

How to use the modules

You can complete entire modules or check the **Module Overview** section to select just the parts you need.

Watch [Using Digital Essentials (YouTube, 1m 37s)](#), created by our student partners, for tips on how to use the modules to build your digital skills.

One or more interactive elements has been excluded from this version of the text. You can view them online here: https://uq.pressbooks.pub/digital-essentials-digital-security/?p=37#oembed-1

Read more about our [Student Staff Partnership project to improve the Digital Essentials modules](#).

Teaching staff – use the modules in courses

Teaching staff can embed or link the modules in courses to help build your students' digital literacy.

- There are interactive elements throughout each module and a short H5P quiz at the end.
- The modules are also available for your students to download in EPUB, PDF and HTML format to make them more accessible.

Import a module into Learn.UQ (Blackboard)

Instructions to embed a module in your course. Email us via dxdc@library.uq.edu.au if you have any questions.

- [Blackboard courses](#)
- [Blackboard Ultra courses](#).

Blackboard courses

[Embed Digital Essentials in Learn.UQ course (YouTube, 1m 55s)](#)

> One or more interactive elements has been excluded from this version of the text. You can view them online here: *https://uq.pressbooks.pub/digital-essentials-digital-security/?p=37#oembed-2*

Text version of video instructions:

1. Go to the module home page
2. Select **Common Cartridge (LTI Links)** under the **Download this book** options.
3. Go to your Blackboard course
4. Go to **Course Management**
5. Click **Import Package/View Logs**
6. Click **Import Package**
7. Click **Select a Package** and navigate to the **.imscc** file you downloaded from the module
8. Scroll down to **Select Course Materials** and select **all** the options
9. Click **Submit**.

In your course site, the module will appear in a new [content area](#) in your course. Each module chapter will be a section. You can [copy, move and delete](#) the chapters in your course.

Blackboard Ultra courses

1. Copy the URL of your Pressbook
2. Go to the Learning Resources section in your Blackboard Ultra course
3. Click +
4. Click **Create**
5. Click **Teaching tools with LTI connection**
   a. Click to edit the title (where it has New LTI Link…) to enter your Pressbook's title
   b. Select Visible to students
   c. At **Configuration URL** enter your Pressbook's URL
   d. Add a **Description**
6. Click **Save**.

Note: You can click the More options dots to go back to make changes to the entry after you have saved it.

Add a weblink in the course menu

- You can provide <u>weblinks to the chapters</u> in the weekly folders in Learning Resources e.g. If you want your students to read the chapters in particular weeks.
- You can also add your book as a <u>weblink in the menu</u>.

Assess student learning

Most modules have a final short quiz created in H5P. You can download the H5P quiz from the module and embed it in your course if you would like to check your students' completions or to allow for the results to be transferred to the Grade Centre in your course.

The H5P quiz content will not record any completion data unless you download and add the H5P quiz directly to your course. Students can screenshot the quiz if they are required to show completion.

Add the final H5P quiz to your course

If you would like to check your students' responses and completion of a module you can:

1. Go to the final H5P quiz in the **Check your knowledge** section of the module
2. Click **Reuse** then **Download as a .h5p file**
3. Then <u>embed</u> or <u>link</u> the quiz in your course. Note: You will need a <u>H5P account</u>.