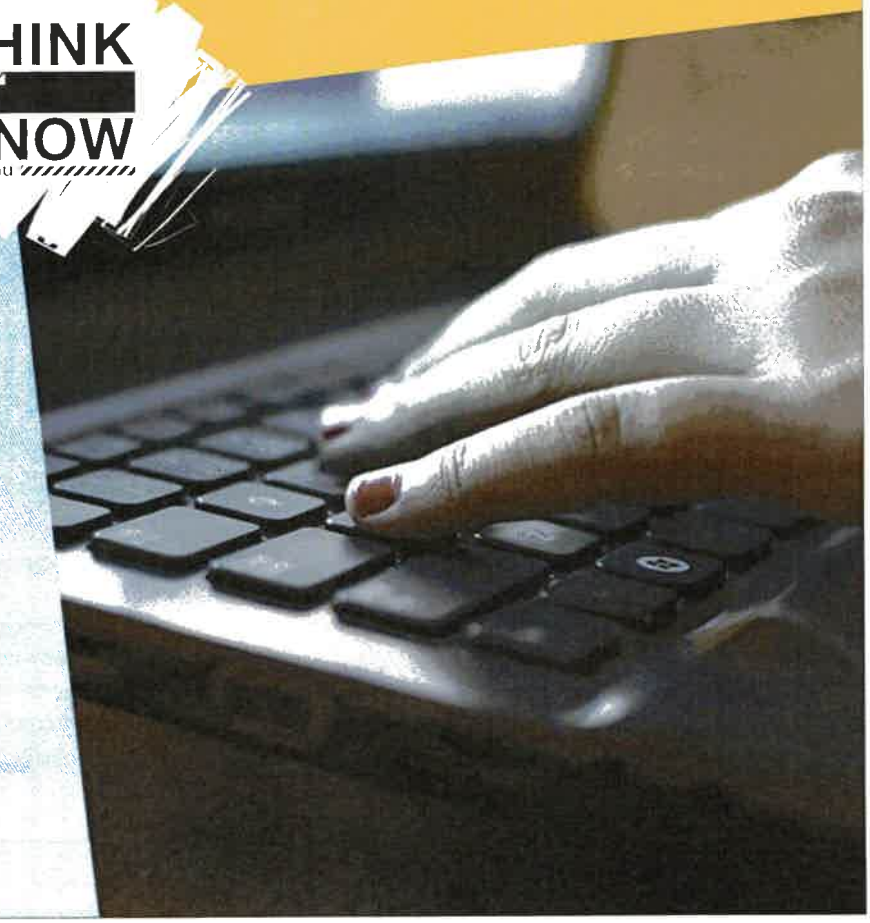
SOS

GUIDE TO CYBER SECURITY

THINK U KNOW
.org.au



THINKUKNOW AUSTRALIA

ThinkUKnow Australia is a partnership between the Australian Federal Police (AFP), Commonwealth Bank, Datacom and Microsoft Australia, which aims to raise awareness of how young people use technology, the challenges they may face and how to help them navigate these challenges.

ThinkUKnow cyber safety presentations are delivered to parents, carers and teachers, and to school grades years three to 12 nationally.

ThinkUKnow is delivered in collaboration with policing partners New South Wales Police Force, Northern Territory Police, Queensland Police Service, South Australia Police, Tasmania Police, Western Australia Police and Victoria Police, as well as Neighbourhood Watch Australasia.

This guide is part of ThinkUKnow's vision to empower every Australian to be safe, respectful and resilient online.

This guide has been developed between ThinkUKnow partners the Australian Federal Police and the Commonwealth Bank.

facebook.com/ThinkUKnowAustralia

twitter.com/ThinkUKnow_Aus

thinkuknow.org.au

THINK U KNOW

CommonwealthBank

CONTENTS

By 2019, the average Australian household will have

24 DEVICES CONNECTED ONLINE

Australians spend almost

1 DAY ONLINE / WEEK

1 IN 2

small and medium business in Australia receive payments online

- Each year, 5% of Australians experience identity crime that results in financial loss, making it more common than assault and car theft
- The annual cost of identity crime in Australia is $2.2b
- 50% of cybercrimes reported to ACORN relates to scams or fraud

Victims' Age

- 6% under 20 years old
- 41% 20 – 40 years old
- 35% 40 – 60 years old
- 18% 60+ years old

Top 3 Targets

- Email
- Social networking
- Website advertising

- Identity theft and romance scams are estimated to cost Australians $55 million a year
- 22% of victims of identity fraud do not know how their personal information was obtained
- In 2015, Australians lost $229 million to scams

References:

Australia's cyber security strategy 2016

Attorney General's Department: Identity crime and misuse in Australia 2016

Scamwatch

Australian Cybercrime Online reporting Network (ACORN)

Keeping yourself secure online

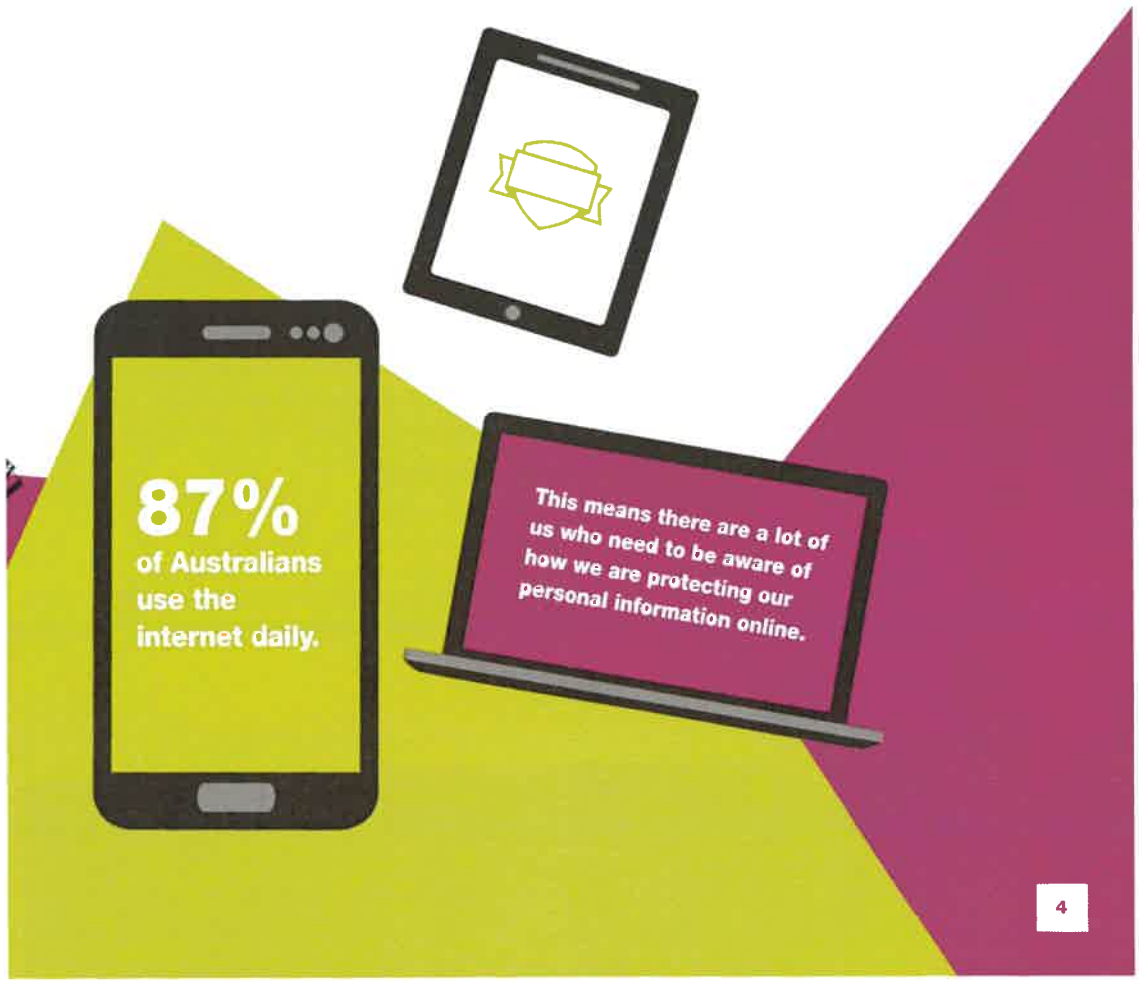
Technology has reached into nearly every part of our lives, including the way we bank, read the news, share images and chat with friends on the internet.

Learning how to stay safe and secure online can sound a bit daunting (or time consuming). Sometimes, learning how to use technology can be hard enough without thinking about safety and security!

The constant evolution and changes in technology, such as in social media and online shopping, can unfortunately make us a target for a range of criminal activity.

With this guide, our aim is to give you easy to understand information and tips to keep yourself and your information safe and secure online.

We want you to take all the necessary steps to ensure your information is safe and secure online. This includes your devices, such as your phone and computer, the sites you visit, web browsing, your privacy and the apps you use.



Know the challenges

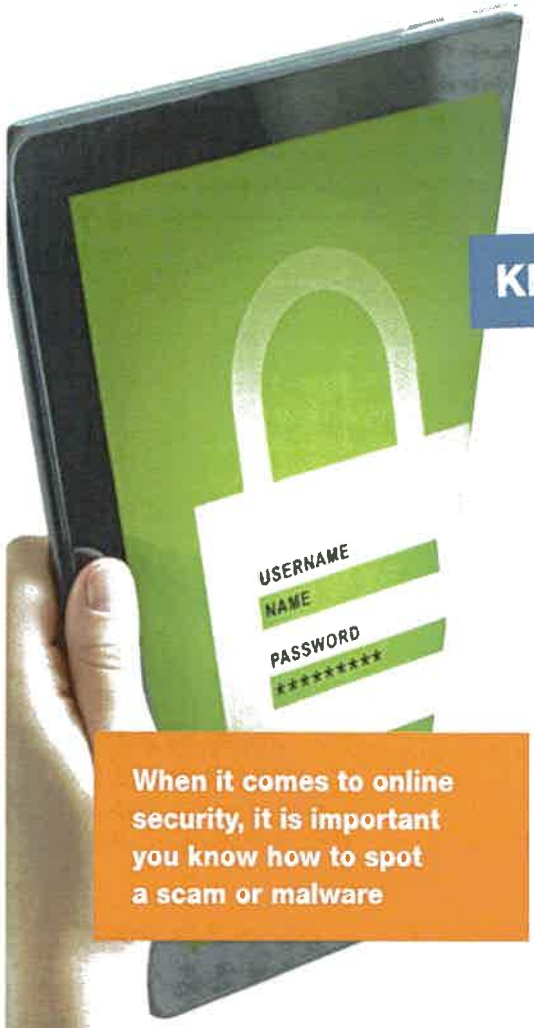
Because technology changes so much and so often, it is important to stay up to date.

In this guide, we've got lots of tips to secure your information, your software, your hardware, your identity and your privacy.

Before we teach you how to protect yourself, it is important to know the common culprits.

KNOW THE CHALLENGES

SCAMS



When it comes to online security, it is important you know how to spot a scam or malware

Some examples of online scams include unexpected money or winnings, fake charities, dating and romance scams, or the buying and selling of illegitimate products.

The most common type of scam through email is known as 'phishing'.

Whatever the scam, the important thing to remember is to never give out your personal information online unless you are sure it is safe and secure to do so. The things that sound too good to be true usually are.

Going Phishing?

Phishing is when scammers send what seems like a legitimate email which either contains links to fool you into installing software, or attempts to trick you into providing personal information, particularly financial details, to enable them to commit fraud.

Spear phishing

Spear phishing is a targeted phishing attack, where scammers send an email using personal details to make it look legitimate. For example, it may contain your social media details or details of family members.

Most spear phishing attacks go after login details for your accounts or accounts known to hold highly confidential, or a large amount of information.

Prize notification, lottery and inheritance scams

Ever been told you have won a maybe prize, or a large amount of cash? Or a relative you've never heard of has left you a lot of money? You may have also won a lottery in a country you've never visited. In return for the 'prize', these scams may ask for some personal information or access to your banking details.

Romance scams

This is also known as 'catfishing'.

Romance scams take advantage of people who are looking for romantic partners, often via social media or dating sites. They pretend to be interested in the person in order to gain money and information. In some cases, it can be hard to tell if the person is real or not. In many cases, they may go to elaborate lengths to make the person believe they are real.

Money muling

Online scams can be used to transfer money around Australia or overseas. The unsuspecting 'money mule' may have signed up for a monthly service, or answered a job advert, and is unaware they are moving money around, often illegally.

Get rich quick

These types of scams offer opportunities to earn lots of money. The earnings are often dependant on selling something to others, or providing personal information, such as birth dates and addresses.

BEWARE!

It used to be quite easy to pick a scam. Poor spelling and grammar, or low resolution pictures, often gave them away. Now, those scammers are getting smarter and better at what they do. Scams aren't always so easy to pick. Scammers may even pretend to be the police, or your bank. They can use technology to create emails which look like legitimate correspondence.

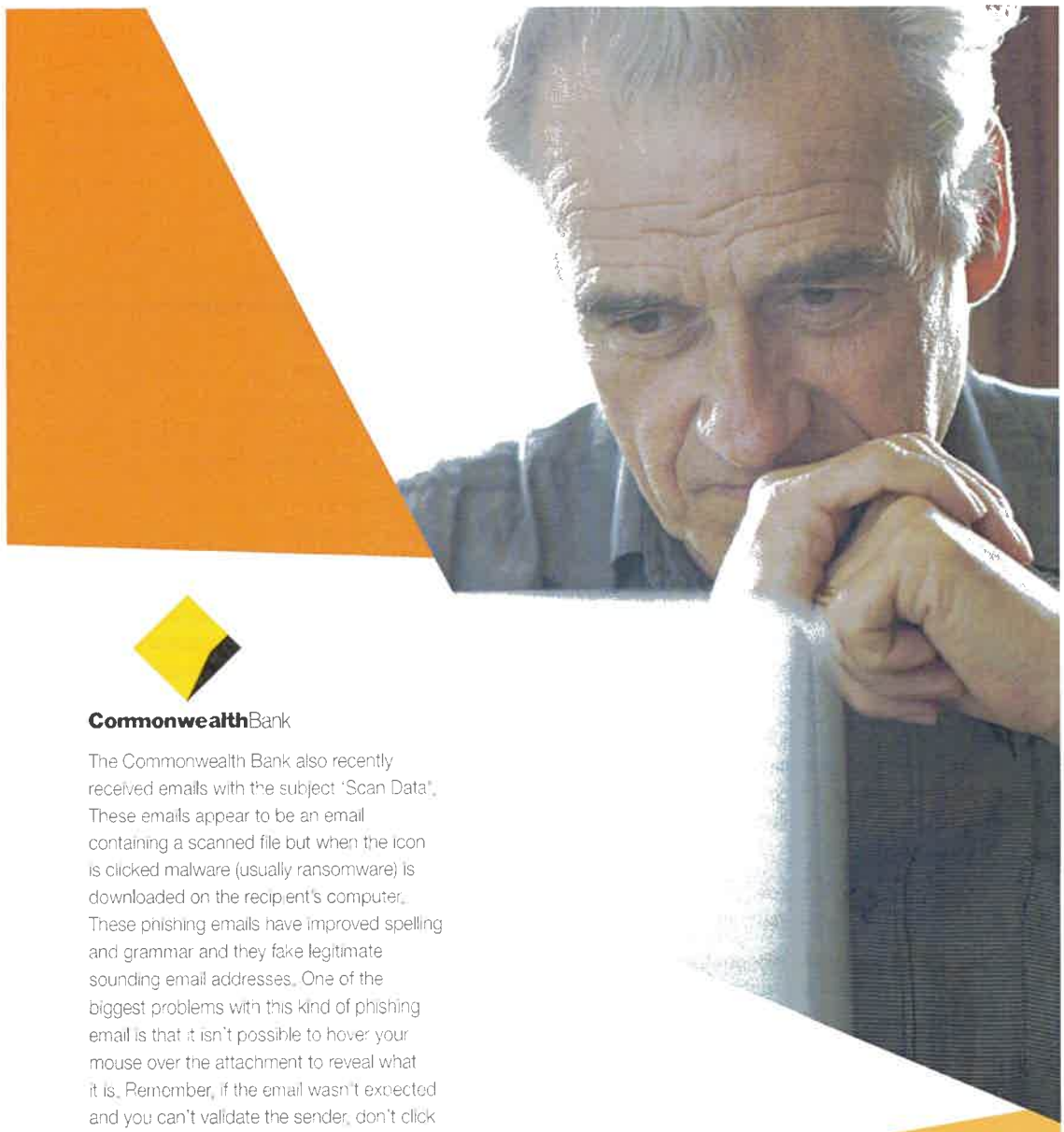
WHAT DO I NEED TO LOOK OUT FOR?

- Emails from people you don't know promising you something exciting like a prize.
- You are offered a reward, such as a holiday or a computer.
- You are asked to send money to help someone. For example, they may ask for money to pay for their children's food or schooling.
- They may pressure you to act urgently.
- If you receive a suspicious email from your bank, or other service provider, check it is legitimate. Your bank will not send you an email asking you for your logon credentials, to unlock accounts or to provide personal information. Always contact your financial institution using public listed numbers if you are unsure.
- Outsmart the scammers! Search online for something you may think is a scam.

CASE STUDIES

Here are two case studies of phishing emails that were sent to Commonwealth Bank of Australia staff and customers.

The first example looks like an electricity bill but if you click the link, you will discover it's much more sinister. It is a real example of a phishing email that installs 'malware' (malicious software) on the recipient's device which then monitors online banking activities. One of the tell-tale signs is the poor use of language and grammar. The email message also doesn't include any of the usual attributes of a genuine energy bill such as a customer account number or payment method option such as BPAY.



CommonwealthBank

The Commonwealth Bank also recently received emails with the subject 'Scan Data'. These emails appear to be an email containing a scanned file but when the icon is clicked malware (usually ransomware) is downloaded on the recipient's computer. These phishing emails have improved spelling and grammar and they fake legitimate sounding email addresses. One of the biggest problems with this kind of phishing email is that it isn't possible to hover your mouse over the attachment to reveal what it is. Remember, if the email wasn't expected and you can't validate the sender, don't click on the attachment.

KNOW THE CHALLENGES

MALWARE

MALicious softWARE.

Malware is software designed to do harm to computers and devices.

Spyware, adware, Trojans, worms and viruses are all types of malware. The trouble is, it is often disguised as legitimate software, so it is hard to know whether you have become a victim. For example, you may download a new version of software, thinking it is a legitimate download, but in fact it contains malware.

Adware

If your computer has been infected with adware, advertisements will automatically be on your computer. This includes, pop-up ads on websites you visit and ones that pop-up automatically on your computer.

Ransomware

Ransomware encrypts your device, so it freezes and forces you to pay a 'ransom' to have it unlocked.

These programs may be sent to you through websites or pop-ups which you can click on, or through email or social media.

Bot

A bot is also known as a zombie because it is a compromised computer that has become infected with malware that automatically runs tasks over the internet. 'Bots' can sometimes work together in something called a botnet, a network of compromised computers, which are used to coordinate a network attack, such as a Denial of Service attack.

Spyware

Spyware spies on a user's activity without their knowledge. It can spy on your keystrokes, your data, and your information.

Trojan or Trojan Horse

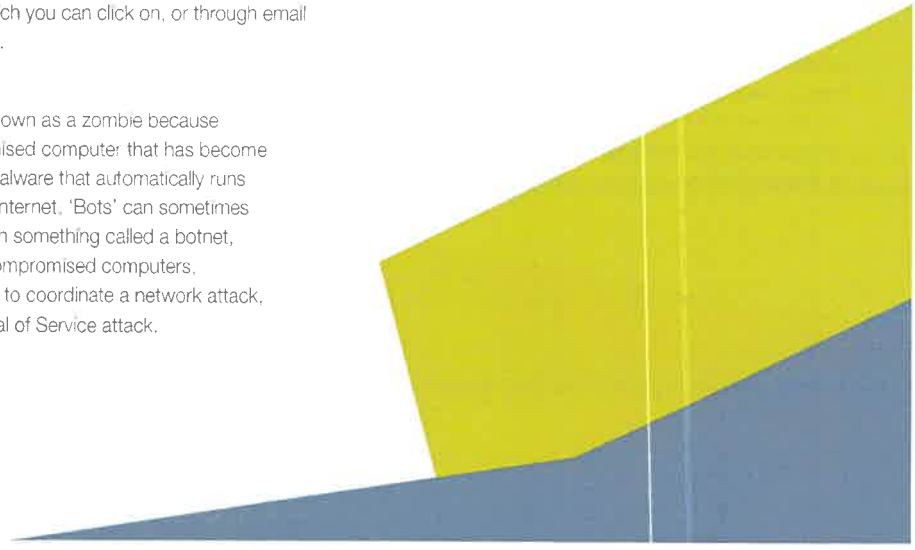
Trojan is a malicious program, disguised as useful software. Once on your device it will steal files, damage data, monitor user activity or perform other actions.

Virus

A computer virus is like a flu virus. It attaches itself to a program or file allowing it to spread from one computer to another, leaving infections as it travels. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but usually requires a person to run or open it to trigger the infection. Viruses can be used to steal information, corrupt files, spam your email contacts, and even take over your computer.

Worm

Worms spread from computer to computer, but unlike a virus, they have the capability to travel without any human assistance. A worm takes advantage of files or information transport features on your system, which allows it to propagate unaided.



BEWARE!

If you think your computer has been infected with malware, install and run anti-malware and firewall software. This may fix a minor infection, however the best course of action is to reinstall the operating system and recover your files from a trusted backup. In some cases, you may need to seek a computer support expert for help.

WHAT DO I NEED TO LOOK OUT FOR?

- Your computer or web browser speeds are slow.
- Your computer is freezing or crashing.
- Files have been deleted or modified.
- Icons or strange files which you cannot remember downloading.
- Emails or messages are being sent from your accounts without your knowledge.

KNOW HOW TO BE SECURE

Knowing how to secure everything—from your passwords to your hardware—is an important part of keeping yourself safe and secure online.

In this section, we're giving you tips on how to secure the most important parts of what you do online.

Secure your passwords

Secure your identity

Secure your privacy

Secure your devices

Know how to — Secure your passwords

It sounds like such a simple thing to do, but many people don't use secure passwords. Using a secure password, and using different passwords for each account, is one of the best steps you can take to secure your information.

ThinkUKnow?

If someone has the password to your email, and you use the same password for your banking or social media accounts, they can gain access to those!

How strong is your password?

Use a passphrase instead! It's best to use 16 characters or more, including letters, numbers and symbols

ThisIsaHelpfulGuide2CyberSecurity!

Did you know there are also Apps and programs that can securely store your passwords? Do your research before selecting one.

Know how to — Secure your identity

Stolen and fraudulent personal information continues to be highly sought after by criminals, with a large amount of personal information obtained online through email, social media, scams or data breaches.

People can be tricked into giving out their personal information online to fake websites, phishing, scams, or information may have been stolen through a network breach.

While identity theft is not restricted to just online, criminals have migrated to the online space, and are using technology to gain your information.

"Some 22 per cent of victims of identity fraud do not know how their personal information was obtained"

Check out page 9 for information on malicious software, which is used to gather private information, disrupt computer operations or gain unauthorised access to computers.

WHAT CAN I DO?

- Use a secure password! See page 12 for hints.
- Regularly check your bank and credit card statements for any unusual activity.
- Never share your passwords, or other personal information with others, such as bank or credit card PIN.
- Ensure you have the most up to date firewall, security and operating software on every device you use. This includes your home computer, phone and tablet.
- Ensure all devices you use have anti-virus and anti-spyware software installed.
- Always ensure you are on the official website you are trying to log into. Don't click on links to websites, which could be a fake site set up to try and get login details of unsuspecting victims. We recommend always typing the address into your browser.
- Always use secure websites when shopping online. This is shown by the 's' on https.
- If you are in doubt about an email you've received about your personal or billing information, contact your bank or relevant institution to find out its legitimacy. It is better to be safe than sorry!
- Never use public computers or public Wi-Fi for online shopping or internet banking.
- Don't give out your email address or mobile phone number unless you know how that information will be used.
- Be careful not to click on links in suspicious emails, and don't open emails from people you do not know.

ThinkUKnow how to spot if you've been a victim?

Here are some things to look out for:

- Purchases made on your bank or credit card that you did not make yourself.
- You receive invoices or bills for items you haven't purchased yourself.
- Your friends tell you that they are receiving strange emails or letters from you asking to send money.
- You've received strange emails or phone calls about purchases you did not make yourself.
- You've been refused a financial service, such as a credit card or a loan, despite having a good credit history.

What if it happens to me?

- Call your banking institution and advise them of what has happened. They may need to put a hold on your card, or in some instances, cancel it.
- Report it to police, or to the Australian Cybercrime Online Reporting Network (ACORN).
- If you need additional support, speak to a support service on page 23.

Helpful links

idcare.org

acorn.gov.au

scamwatch.gov.au

Know how to – Secure your privacy

Have you ever thought about how much information you give out online?

We all give out personal information without even meaning to. Every time you browse the internet, you could potentially be giving out personal information.

Policies, Terms and Conditions

Many of us don't often read this fine print! However, Terms and Conditions are the things we agree to when we sign up to a website, game or app. Often, we're giving away rights to our information or photographs without even realising. Some may even state that they can transfer or sub-licence the rights of your content to another company or organisation.

Whenever you sign up to a social media account or download an app, you're asked to agree to the Terms and Conditions of using that service.

Most social media services have four parts to their terms and conditions:

- A licence agreement – This allows the service to change, add to, delete, publicly display, reproduce, copy, distribute, sell and use your personal information including your photos, posts, private messages, comments and videos without your permission.
- Law enforcement disclaimer – This means that these companies can provide your information to police for investigation purposes.
- Community guidelines – These are the rules around how to use the service, and consequences for breaking the rules, such as shutting an account down.
- Privacy policy – This explains what private information the company collects, how it is used and what privacy settings you can use.

Your location

You can give away your location without even knowing. Most devices, including tablets and phones, have a Global Positioning System, which is more colloquially known as a GPS.

When a photo is taken with the GPS (also known as location services) is turned on, location metadata is automatically embedded into the image. This reveals the location it was taken and is known as 'geotagging'. Geotagging can also occur in comments posted on social media, or instant messages.

Privacy settings

Most of us use the standard settings on our social media accounts, but they aren't always the most private.

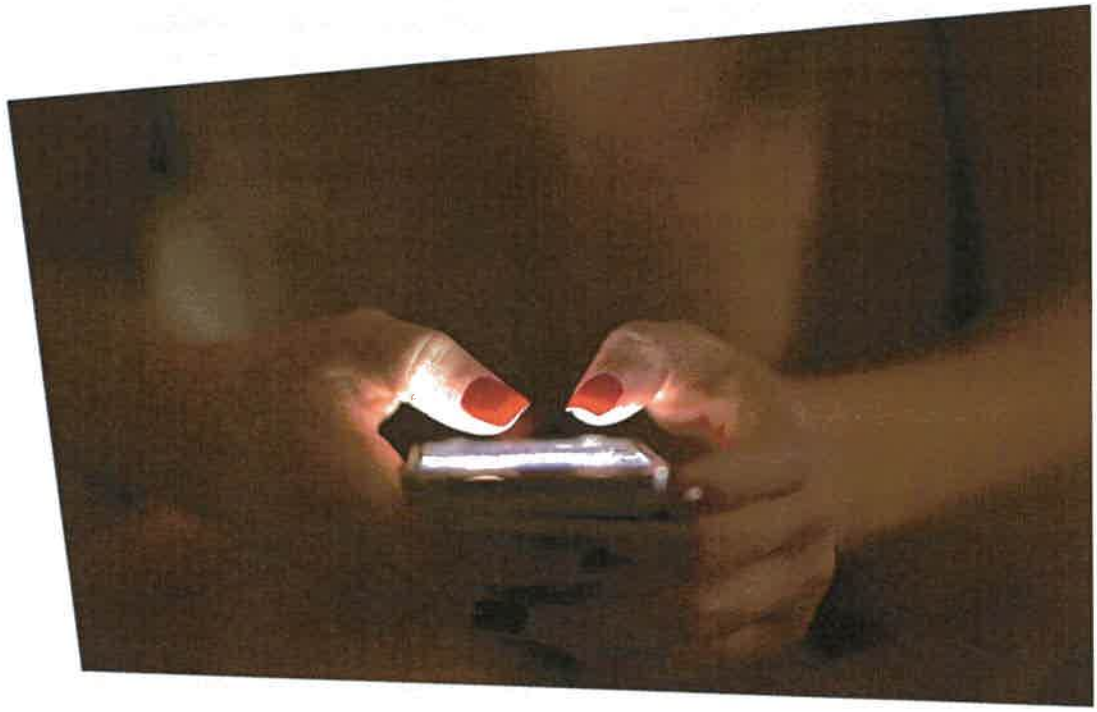
Check what privacy settings you have on each social media app or site you use. Most social media, including Facebook and Twitter, have helpful information on different security settings you can use.

What is personal information?

Personal information can be your full name, address, email, telephone number/s, workplace and job title.

WHAT CAN I DO?

- Check the privacy policies and Terms and Conditions of the sites and apps you use.
- Turn off the location services (GPS) on your phone when it does not require your current location.
- Only download apps from the official stores, such as Apple's App Store or the Android marketplace. Illegitimate app stores or app websites may contain pirated apps or malicious software (malware) which could steal your personal information.
- Before you download and install an app, check which features of your device (such as the GPS function) the app wants permission to access. Disable any features which are unnecessary for the app to access.
- Be careful about sharing too much personal information online. For example, your current location, your name, your age, your address, etc. Sometimes we don't even mean to share this information. For example, your street address may be in the background of that family photo you shared.
- Ensure you have the right security settings on for the social media apps and sites you use. Be aware—the standard privacy settings aren't often the most private!



Know how to – Secure your devices

SOFTWARE

Software can be defined as the information on a computer or device, including an operating system, utilities, programs and apps.

With software, the best rule is always be one step ahead of malware!

The good news is there are some easy things you can do to protect your software.

WHAT CAN I DO?

Install and update security and protection software

Here are some things to look out for:

- Internet security software
- Anti-virus software
- Some security programs will offer anti-virus, anti-spyware and a firewall all in one.

It is important that these are up to date. Don't become a victim because you forgot to update your software!

Secure your Wi-Fi

Sometimes, Wi-Fi can be easy for people to 'hack' into. If it isn't secure, someone could use it to steal your stored online and device information.

- Change the default administrator password on your router, as these passwords are often computer generated and may be publicly available online.
- Ensure remote management is disabled. Remote management allows your modem or router to make changes to your internet connection, including passwords, by logging into your device from the internet.

Install the most up to date operating system

Updating your operating system will minimise your exposure to security risks.

- Make sure it is protected by a secure password! Check out page 12 for hints.
- Turn off file sharing.
- Consider encrypting part or all of your data, especially personal information you may have saved on your computer or device.

HARDWARE

We store a lot of information on our computers. From family photos, to work information, addresses, tax information, our studies and sometimes even financial information.

What if your computer was stolen?

If someone stole your computer, what kind of information could they get access to? And how easily could they get it?

What if someone could remotely get in to your computer?

Although it might be quite unlikely that your computer or device is lost or stolen, it is important to think about what would happen to your information if it did.

WHAT CAN I DO?

- Password protect or encrypt personal information.
- Set up a tracking service on your device.
- Always back up your data, and leave the copy of it in a safe and secure place.
- Set up a firewall.

BEWARE!

Beware of free software. If it sounds too good to be true, then it probably is. Sometimes, you get what you pay for. Don't be cheap when it comes to software! Do your research and buy the safest and securest product.

WHAT IS CYBERCRIME, REALLY?

In Australia, cybercrime is defined as criminal acts involving the use of computer/s or other information communication technology systems.

Pure cybercrime are crimes directed at computers or other information communication systems, such as unauthorised access to, modification of or impairment of electronic communications or data. Examples include hacking and denial of service attacks (also known as DDoS).

Technology-enabled crime is where computers or information communication systems are an integral part of the criminal activity. Examples include fraud or online identity theft.

The offenders, the crooks, the baddies, the fraudsters, the criminals

When you think about it, the 'crooks' and the 'fraudsters' are just using technology to do the same thing they've always done. They are looking for information, for money, for something to gain.

There are so many different ways 'cyber criminals' use technology to commit crime. That's why it's important to undertake a variety of steps to secure yourself in a range of ways.

It's easy to think you won't be the target. However, people involved in this type of activity can be opportunists. They may only be after a small gain, rather than part of an organised criminal syndicate.

KNOW THE TERMS

App

Software which allows its user to perform tasks. For example, Microsoft Word. Phones and tablets also have apps, including Facebook and weather apps.

Bot

A bot is a computer that has been compromised by malicious code. This can sometimes happen without people knowing their computer has been infected. 'Bots' can sometimes work together in something called a botnet, a network of compromised computers that send out malicious software. Unfortunately, due to the amount of computers involved it is sometimes hard to trace the culprit.

Brute force attack

The attempt to gain access to a computer resource using repeated guesses at passwords until it gets the right ones.

Catfishing

Catfishing is where someone sets up a fake online identity to lure people into emotional relationships. This can often be used to leverage that person's trust and gain personal information for the purpose of identity fraud or theft.

Cloud computing

A cloud allows people to store and access saved content over the internet, instead of on a hard drive. For example, iCloud. Cloud computing also encompasses the delivery of services and resources over the internet such as access to applications and infrastructure.

Cookie

A piece of code or data created by a web browser (web server), which is stored on a person's computer and can identify the user and customise web pages.

Cyber attack

A cyber-attack is a deliberate attempt to access an information computer system, usually with the goal of theft, disruption, damage or other unlawful actions.

Darknet

A hidden 'neighbourhood' of the internet, which is only accessible using non-standard protocol. It is basically a marketplace for illegal substances, such as software or illegal images or videos.

Distributed Denial of Services attack (DDoS)

A DDoS attack happens when multiple computer hosts send requests to a target website at such a rate that it crashes.

Encryption

Encryption is the process of converting data into an unrecognisable form. This means the data is not easily understood by unauthorised party.

Firewall

A Firewall is a barrier which protects computers and networks from unauthorised access.

Malware (malicious software)

Malware is intrusion software. It includes computer viruses, worms, trojan horses, ransomware, spyware, adware and scareware.

Money mule

A person who receives and transfers illegally acquired money on behalf of others. Unknowing mules can be recruited through online scams.

Phishing

Phishing attacks use fake emails and fake websites designed to fool recipients into divulging personal financial information such as credit card numbers, bank account details, and usernames or passwords.

Ransomware

Ransomware sneaks into your computer, usually via a website or document, and then locks or encrypts your computer and scams you into paying a ransom to unlock it again.

Remote Access Tool (RAT)

A tool that allows someone to access a computer from a remote location.

Scams

Schemes that seek to take advantage of people to gain a benefit, such as money or personal information.

Need more? Visit thinkuknow.org.au and staysmartonline.gov.au

Secure Sockets Layer (SSL, or the 's' in https)

A barrier that allows internet users to send encrypted messages. This is mostly used with online shopping or banking. A web address that has an 's' after http indicates that an SSL connection is in use.

Spam

Unsolicited emails sent, often sent for the purposes of marketing.

Spear phishing

A targeted phishing attack, which usually contains personal information about the person who receives the email.

Virus

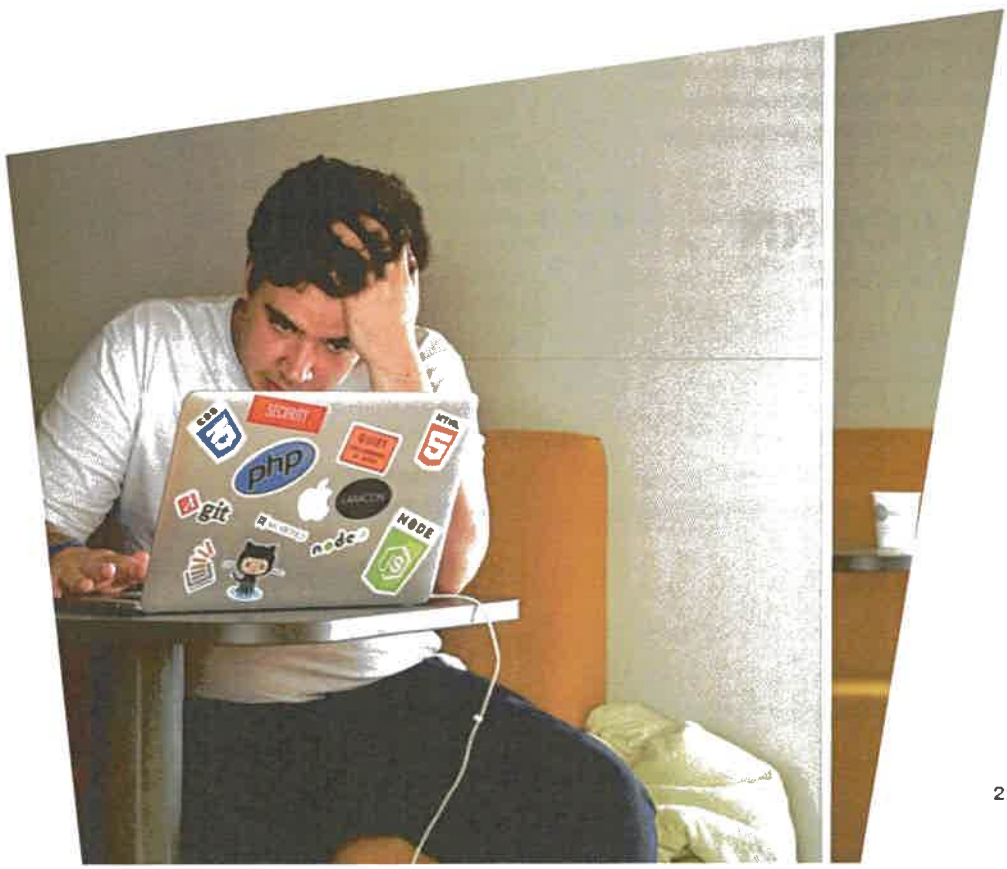
A virus is a piece of programming code which is contained within another program. It causes damage by infecting the computer or device with the virus. Viruses can erase data or damage content on your computer or device.

Watering—hole

A compromised website which contains malware that is intended to compromise visiting users.

Whaling

A targeted phishing attack, targeted at senior executives of companies.



TAKING ACTION

Where can I report?

You can report hacking and identity crimes to the Australian Cybercrime Online Reporting Network (ACORN) at **acorn.gov.au**.

After submitting your report, you will not receive any further correspondence on behalf of ACORN. If further information is required, the police agency investigating your report will contact you.

If you have lost money as a result of cybercrime or you suspect that someone has gained access to your banking details, contact your financial institution as soon as possible. Be aware that it is not always possible to recover money lost to scammers online, particularly when the scammer is overseas.

ACORN
Australian Cybercrime Online Reporting Network

Where can I get emotional and financial support?

iDcare 1300 432 273
A national identity theft support service for Australia and New Zealand.
idcare.org

Lifeline 13 11 14
A 24-hour crisis support and suicide prevention service.
lifeline.org.au

BeyondBlue 1300 224 636
A service for connecting people with mental health professionals.
beyondblue.org.au

Kids Helpline 1800 55 1800
A free, confidential telephone and online counselling service for young people between 5 and 25 years.
kidshelp.com.au

Reach Out
Whatever's going on, ReachOut.com's info, stories, apps, online tools and forums can help.
au.reachout.com

National Debt Helpline
1800 007 007
A not-for-profit service that helps people tackle their debt problems.
ndh.org.au

ThinkUKnow TOP TIPS

- Ensure you have the most up to date software and apps on every device you use.
- Use a passphrase that has more than 16 characters and includes numbers, letters and symbols.
- Always use secure websites when shopping, banking or sharing personal information online. This is usually shown by the 's' on https.
- Be careful about the information you share on social media.
- Be careful not to click on links in suspicious emails, and don't open emails from people you do not know.

CYBER SECURITY CHECKLIST

- [ ] My operating system is up to date.
- [ ] I have installed anti—virus software and security software, such as a firewall. And, it is up to date!
- [ ] My passphrase has more than 16 characters and includes a mix of numbers, letters and symbols.
- [ ] I never open emails from people I don't know, and I never click on suspicious links.
- [ ] I've backed up all my files and have kept them in a safe and secure place.
- [ ] I know what a scam and malware is, and I know how to spot one.
- [ ] I turn off the location services (GPS) in my phone when it does not require a current location.
- [ ] I am careful with what sites I visit and what I log into when I am using public Wi-Fi.
- [ ] I've considered whether I should encrypt my personal data, and have taken the necessary action.

USEFUL WEBSITES AND CONTACTS

Stay Smart Online
staysmartonline.gov.au

Australian Cybercrime Online Reporting Network
acorn.gov.au

Scamwatch
scamwatch.gov.au

Australian Federal Police
afp.gov.au

IDCARE
idcare.org

Commonwealth Bank
commbank.com.au/security

WANT MORE INFORMATION AND RESOURCES?

Visit **thinkuknow.org.au** to view and download our SOS Guide to Cyber Safety.

STAY SMART ONLINE

ThinkUKnow is a free cyber safety program, delivered by volunteers from:

AFP bankwest CommonwealthBank DATACOM Microsoft

In collaboration with: