KEY TELECOM
MOBILE / INTERNET / PHONE LINES / BUSINESS IT

Defend Yourself Against a Cyber Attack

8 ways you can protect you and your family online:

- **Be sceptical.** no matter if it appears to be from a company you use and trust, and regardless of whether it is an email, text message, or phone call. Always double-check by reaching out to a company using contact details from their official website.
- **Use strong passwords.** Make your passwords a phrase that is unique to you. Typing a few words is easier and can be more secure than most traditional passwords. Use a password manager to generate passwords and help keep them secure.
- **Use multi-factor authentication** whenever it is available. Many online services offer multi-factor authentication, it's an extra level of security that needs multiple pieces of proof to log you in - so when a website asks you to enable multi-factor authentication, you should seriously consider it.
- **Apply the latest updates.** Protect your devices by making sure the latest iOS or Android updates are applied. Modern phones will automatically check for updates and apply them and do the same for apps downloaded from official app stores.
- **Add an extra layer of security** to your devices for stronger protection against scams, hackers and online viruses.
- **Limit what you share online.** Set your social media accounts to private and limit the amount of personal information you share online like your birthday, address, or photos that identify your children's school.
- **Backup your data** to the cloud or external hard drive regularly. This can protect you from data loss related to hardware failures, theft, or malware.
- **Use secure Wi-Fi.** Be careful about sending and receiving confidential information across a public wi-fi network - it's easier for hackers to intercept it.
- **Clean Out History.** Routinely clean out your browsing history.
- **Delete Unwanted Applications.** If you are not going to use an application again, delete it.
- **Review ACCC Little Black Book.** At https://www.accc.gov.au/publications/the-little-black-book-of-scams, The Little Black Book of Scams is recognised internationally as an important tool for consumers and small businesses to learn about scams including: • the most common scams to watch out for • the different ways scammers can contact you • the tools scammers use to trick you • the warning signs • how to protect yourself, and • where you can find help

KEY TELECOM
MOBILE / INTERNET / PHONE LINES / BUSINESS IT

SCAM EMAILS AND MESSAGES

Phishing

Phishing is the name given to emails or messages that persuade you to provide personal or sensitive information. They can lure you in by pretending to be from large organisations or brands you trust.
These emails are often a bid to obtain your username and password or to get you to open an attachment that could harm your computer.
The poorly written, unofficial-looking phishing scams that first appeared in Australia in 2003 are a thing of the past. Today, these scams are far more sophisticated. They come in the form of emails, text messages and even social media direct messages that masquerade as correspondence from legitimate organisations or institutions, like banks or government departments, and request personal information or prompt you to click on a pernicious link.

- **Spear phishing:** individualised messages from a seemingly trustworthy sender, such as a bank or employer, and usually targeted at employees in an organisation
- **Whaling:** targeted spear phishing, where a senior person in an organisation is phished by a cybercriminal masquerading as someone trusted, like a colleague
- **Pop-up phishing:** deceptive pop-up ads that contain malware
- **Clone phishing:** messages that closely resemble previously received legitimate ones – for instance, a phisher might send a fake promotional email from a brand to a known customer of that brand
- **Voice fishing:** also known as 'vishing', where a phisher will attempt to solicit sensitive information over the phone

Fortunately, while phishing scams can be well disguised, there are red flags you can watch out for. Grammar errors, misspelt names and incorrect facts are common giveaways. You might receive an email from '@combank.com'; a strange 'competition winner' alert SMS from JB Hi-Fi, when you haven't entered a competition; or a cold call from a foreign or private number.

An organisation or institution will generally never ask a customer to share sensitive information through unsolicited correspondence. So as a rule, never give out personal details unless you are 100 per cent sure you know who you're dealing with – in other words, you called them or have verified their identity. Likewise, never click on a link or open an attachment from an unsolicited

message unless you are confident it's legitimate – for example, you know you've safely received correspondence from this brand or person in the past.

VIRUSES, WORMS AND TROJANS

Malware

Malware is a general term for the malicious software that hackers use to get unauthorised access to your computer. They can steal credit card details and bank logins or generate illegal revenue from ads or popups that display in your web browser.

Malware is often delivered via a link or file in an email and is activated when you click the link or open the file.

PERSONAL INFORMATION

Identity theft

When a hacker has access to your personal information, they can use it to create fake identity documents or apply for real ones - they may take loans out in your name or make expensive purchases online.
Though it's a relatively uncommon crime, it can take a long time to recover from identity theft and the emotional and financial cost can be high.

Scam Phone Calls

Telephone based scam callers will frequently claim to be from well-known organisations such as Telstra, the Government, or other brands or organisations you are likely to be familiar with.

These scam callers will often try to convince you of the urgent need to follow their instructions. Sometimes they will try to convince you to give them access to your computer remotely, such as by pretending to be a Telstra service representative. Often, they will apply inappropriate pressure, including threats and potentially inappropriate language, as part of their scam.

What to look out for:

- Calls from people impersonating representatives from well-known organisations, such as the Government, or familiar brands and companies.
- Calls seeking financial details (such as your credit card or banking details) to process a refund or other "overpayment".
- Call quality may be poor, and the caller may be difficult to understand.
- Callers who attempt to apply a lot of pressure, urging you to take immediate action to address a problem.
- Calls offering to place a number on the Do Not Call Register for a fee. This is a free service, for more information visit: https://www.donotcall.gov.au
- Callers advising that your computer has a virus or is attacking others.
- Note: We won't call you for a service or technical matter unless you contact us first.

- To learn about what Key Telecom will contact you for, refer to our verification page

Example of live phone scams:

- Calls imitating the Australian Federal Police that require your assistance to help them track down criminals and partake in criminal investigations. In these calls you're often asked to transfer money abroad using international wire transfer services.
- Calls asking for bills to be paid via pre-paid gift cards – such as iTunes and Westfield – on behalf of a credit agency representing Telstra or the ATO (Australian Taxation Office).
- Calls imitating "support desk" staff looking to access your computer by pretending to know your "CLSID". This is a non-unique identifier that scammers try to trick you into thinking is something only a legitimate support person would know.

What to do next:

- If you're not sure that the person on the other end of the phone actually is who they say they are, hang up and call the organisation by using their official published contact details.
- If the caller is claiming to represent Key Telecom, do not share your personal information, credit card or online account details over the phone unless you made the call and the phone number you called came from a trusted source, such as contact details obtained from your physical bill .
- Don't respond to missed calls that come from numbers you don't recognise. Calling back may result in instant charges in excess of $30.00.
- Be careful of phone numbers beginning with "190". These are charged at a premium rate and can be expensive.
- Be careful of being tricked into calling expensive international phone numbers.
- If you think something's not quite right, just hang up. If it's an SMS, delete it and don't reply.
- Report it. Submit a Report Misuse of Service form and include as much detail about the call and caller as you can remember. Our Cyber Security team will investigate the report and may be in touch if they have additional questions.

SMS Scams

SMS or MMS scams are a popular way for criminals try to get you to click on a link that could compromise your mobile phone, trick you into making an expensive phone call, or send a message which could cost you a significant amount of money to send.

What to look out for:

- Unexpected SMS messages asking for your personal details, advertising promotional material, or asking you to click a link.
- SMS and MMS numbers that start with 19xx. These are charged at a premium rate and can be expensive. Also look out for numbers that start with an international country code other than +61, which is Australia's country code.

- Texts promising unexpected prizes that require you to send money to claim them, and mysterious text messages that can cost you a lot of money if you reply to them.
- Texts that encourage you to click a link, which may then ask you to install a piece of software on your mobile phone or tablet. Just like computers, malicious software can put your phone and personal information at risk.
- Mobile providers are rolling out anti-scam software that allows you to block most potential scam SMS's, if it is available on your mobile service, turn this on.
- There are a number of third-party number blocker applications available, research these on the application store appropriate to your phone.

For example:

"Congratulations! You were lucky. You have been chosen among 100 thousand people. You won a new iPad from us. http://ti7.in/Jnk7Mw"

What to do next:

- Do not call telephone numbers contained in suspicious SMS message.
- Do not reply to an SMS from a number or person you can't identify – even to unsubscribe.
- Report it. Submit a Report Misuse of Service form and include as many details as possible. Our Cyber Security team will investigate the report and may be in touch if they have additional questions, or possibly to a
- Ask for a screenshot of the unwanted message.