Cyber Safety and Scam Protection

Cyber Safety is about developing safe practices when using the Internet and technology to prevent personal attacks or criminal activity.

Types of cyber attacks and scams

- Malware (Malicious software) is an umbrella term for all programmes and software that can be downloaded to your computer. There are different categories like viruses, trojans, worms, spyware and ransomware. They can be downloaded onto your computer through email attachments, links on dodgy websites etc.

- Spyware is a type of malware that once installed on a computer, collects information without you knowing. It can be difficult to detect, so it can be almost impossible to know you've been the victim of a spyware scam.

- Virus is a specific type of malware that spreads by inserting its code into other programs. Viruses can be spread through email attachments, file-sharing networks, and infected websites.

- Phishing - A type of attack that tricks people into revealing personal or financial information. Phishing attacks can be delivered through emails, SMS, voice, and QR scam codes.

Remember: Keep your software up to date and ensure your anti-virus and malware is turned on.

Your identity

Remember: You are more than just your driving licence or physical ID. Information you fill out online, on forms, competition entries, Facebook and many other places have personal information about you.

How they get you:

Phone calls - pretending to be a company or organisation. They may already have some personal information on you, but will try to get you to share more, either personal or financial.
They'll sound convincing and will try to get you to believe it's urgent. They might send you emails with bogus links or ask you to install software on your computer.

In some cases they might threaten you by saying you are being prosecuted for fraud or be given large fines.

Don't give out passwords, don't give any personal information, don't install any software they ask you to and hang up. If you've given them any information, contact your bank or organisation directly and check with them.

Email and text: Don't open any links from suspicious emails or texts. If in doubt, delete it. It's rare that banks and organisations send emails and texts with links (unless you've requested them, or clicked 'forgot password' etc)
Companies like 'My Gov' will email or text you and tell you to check your messages, forcing you to go to the website directly without sending you the links.

Remember: Doesn't matter how 'Urgent' a message claims to be, it's not urgent enough that you can't take 5 mins and follow it up through legitimate sources yourself.

Cyber Safety and Scam Protection

Protect Yourself

Passwords

- Never give out your passwords
- It is ok to write passwords down as long as they are safe away from obvious places. It's nearly impossible to memorise all the passwords we seem to need in today's society
- Make sure you have a strong password
- Use two factor identification when it is available
- Make sure your phone, iPads and computers etc have passcodes or passwords to access

Software:

- Keep all your technology software up to date.
- If you have an iPhone or iPad, check for updates regularly for both the operating system and the apps
- On computers check for updates to Windows or Mac
- Make sure you have firewall and virus protection on. Make sure it is updated and run a scan every week.
- Windows 11 and Mac iOS have very good protection built in. It isn't necessary to purchase additional antivirus software as it used to be a few years ago. If you do wish to use additional software, there is plenty of free stuff out there. You certainly don't need to buy or get subscriptions to packages like Norton or McAfee etc. Just google 'Free antivirus software to find alternatives like 'Avast' and 'Malwarebytes' etc

Paying online:

- Only shop on reputable websites and try to use PayPal as it offers end to end encryption and two factor identification
- Paying in shops use 'tap and go', which is safer that using your physical credit card.

If you've been scammed:

- Don't send any more money. Block all contact from the scammer.
- Contact your bank or financial institution immediately to report the scam. Ask them to stop any transactions.

The best place for full details of what to do if you've been scammed is to got to the governments 'Moneysmart website', but also check out the other websites below for more information on a range of cyber safety topics.

*Links on next page

- scamwatch.gov.au

- moneysmart.gov.au
- https://www.cyber.gov.au/report-and-recover/report
- https://www.youtube.com/watch?v=iCs3aJYXLwo
- https://www.esafety.gov.au/media/cybersmart-forever-video
- https://www.youtube.com/watch?v=aO858HyFbKI
- https://www.youtube.com/watch?v=Xn51DSTCcO4
- https://www.esafety.gov.au/parents/issues-and-advice/online-porn
- https://www.internetmatters.org/resources/protecting-children-from-online-pornography/
- https://www.esafety.gov.au/parents/issues-and-advice/online-safety-basics