crowley care

CYBER SECURITY AWARENESS

Protecting yourself against Cyber Attacks and Scams

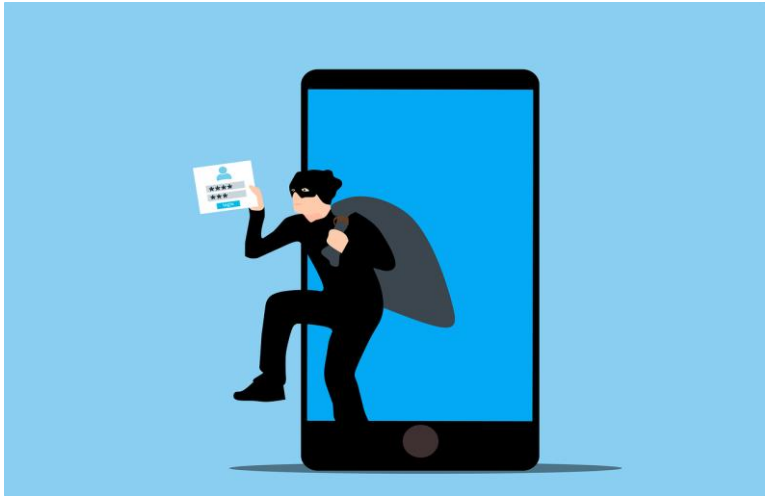
What is Cyber Security?

- Practice of defending
  - Computers
  - Servers
  - Mobile Devices
  - Electronic Systems
  - Networks and Data

- Types of attacks
  - Identity Theft
  - Ransomware
  - Scams
  - Data Breach

Identity Theft

- Financial and emotional consequences can be devastating
- What information do attackers target?
  - Name
  - Date of Birth
  - Drivers Licence Number
  - Medicare Card Number
  - Other personal information
- What is that you can look out for:
  - Check your bank statements
  - You may receive receipts for products you have never purchased
  - You may be going for a loan and have been refused credit



Identity Theft

- So here are some of the ways to protect yourself and your family
  - Limit what you share online **publicly**
  - Set all of your social media accounts to "**Private**"
  - Don't accept "friend" requests from strangers
  - Don't believe that email you received from the bank, have a careful look at it, what is it asking for?
  - For online and social media accounts, use strong passwords and **DON'T** reuse passwords
  - If you are worried your identity information has been compromised, you could use services such as IDCare

Ransomware

- https://player.vimeo.com/video/749391524

Ransomware

- Ask help from a professional.
- Step 1: Record Important Details
- Step 2: Turn off the infected devices
- Step 3: Disconnect your other devices
- Step 4: Change your important passwords

Scams

- Types of Scams
  - Phishing
  - Malware
  - Remote Access
  - Hacking

Scams

Fear/Obligation

Don't fall for common human traits. Think before acting, as kind and courteous human natures are often taken advantage of.

Instant Rapport

Trust no one until you can verify otherwise. Remember trust is built over time and not instantaneous.

Authority

Always verify/validate and don't always assume it is legitimate. Trust your gut instincts.

Urgency/Scarcity

Creates the desired need to perform an action without thinking. Always take your time to analyse and make an informed decision.

Reward/Incentive

Nothing is ever free, somewhere along the line someone is getting something.

Scams

- What to look out for
  - Were you expecting it?
  - Check the following:
    - Senders address
    - Spelling and grammar
    - Contain suspicious attachment

Cues – Triggers to look out for

Errors

Spelling, Grammar and Punctuation

From: Order Confimation [mailto:no-reply@discontcomputers.com]
Sent: Tl 1 lay, December 01, 2016 11:50 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Jane DoeYour order has been processed

2

Click Here To Read Files

Visual Presentation

Low quality images and poor layouts

Language/content

Greetings, signature and formality

Dear Sir,

Please find attached our first order as agreed with my boss.

Waiting for your OC and proforma.

Thank you in advance.

Regards

Data Breaches

- Generally affecting companies
- Often Targeted attacks
- It’s your personal information they are after
- The Privacy Act 1988 makes some companies responsible for communicating breaches to customers affected

Medibank and Optus data breach

- On 22 September 2022, **Optus** became the victim of a cyber-attack that resulted in the disclosure of their customers' personal information.
- Estimates that up to 9.8 million Australians could have their data compromised due to the attack
- 2.8 million severely impacted.

- On 13 October 2022, one of Australia's largest medical insurers, **Medibank**, announced it had suffered a cyberattack
- Personal details of 9.7 million customers in Australia.

Good Password Practices

Secure

Create a passphrase using:

- A combination of different words
- Capitals and lowercase letters
- Numbers
- A symbol

For example: ILikeChocolate2022!
A password like this would take approximately 5 quadrillion years to crack. Check my password

Change

When it is time to change your password:

- Randomise it as much as possible
- Don't just simply change a number at the end.
- It needs to be unique and different from all your other passwords

Store

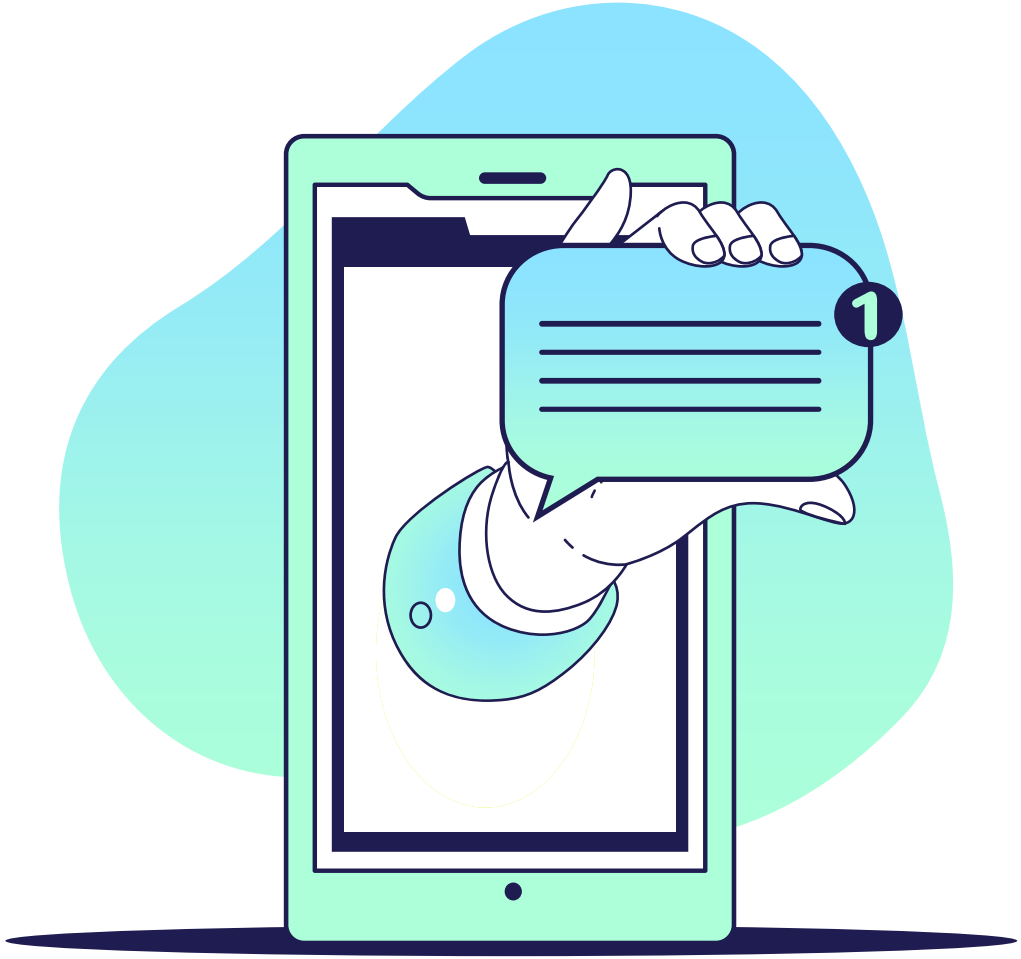
- Don't use a Word Document or a sticky note to remember all your passwords.
- Use a password manager
- Don't share your password with anyone (this includes other staff members)

Key Takeaways

- Be aware and vigilant before opening emails or clicking on links.
- Look for the phishing cues/triggers
- Limit what you share online **publicly**
- Keep regular backups of your devices
- Stop, Think, Act
- Have good password practices

THANK YOU!

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories



Resources

- https://www.cyber.gov.au
- https://www.idcare.org
- https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/Identity-fraud
- https://www.ncoa.org/article/how-older-adults-can-improve-their-personal-cyber-security
- https://bitwarden.com/
- https://www.esafety.gov.au/