Protecting your clients from cyberattack

Simple steps your clients can take

Recent high profile cyberattacks of some of Australia's largest companies have highlighted the importance of keeping your data and personal information safe. We've outlined some of the steps you can take to help protect yourself from a cyberattack.

Password Hygiene

- Use longer and complex passwords
- Never share or send your passwords or multi-factor authentication codes with anybody, even if you trust them.
- Do not use consecutive letters or number or personal references e.g. abc, 123, your birthday.
- If credentials have been compromised reset passwords as soon as possible.
- Periodically reset passwords to reduce the ongoing risk of credential compromises.
- Use a password manager to help manager your passwords e.g. Lastpass, Google Password Manager, Keepass, NordPass

Password support sites

- **Has your password been compromised?**
  Visit https://haveibeenpwned.com
- **How strong is your password?**
  Visit https://www.security.org/how-secure-is-my-password

Email management

- Verify and authenticate every sender before taking any action such as downloading attachments or replying.
- Keep your work and personal emails on separate devices
- When relying on auto-complete to select the email recipient check and recheck the email before sending it.
- Never share personal or sensitive information via email.

How to spot a phishing scam

- Don't trust display names - Check the sender's email address before opening a message
- Check for typos - Spelling mistakes and poor grammar are typical in phishing emails.
- Look before clicking - Hover over hyperlinks in genuine-sounding content to inspect the link address.
- Read the salutation - If the email is addressed to "Valued Customer" instead of to you, be wary. It's likely fraudulent.
- Review the signature - Check for contact information in the email footer. Legitimate senders always include them.
- Beware of threats/urgencies - Fear-based phrases like "Your account has been suspended" or "send information immediately" are prevalent in phishing emails.

praemium