- australianantiscamalliance.org/
- Some notes on Passwords

Use Strong Passwords:

Create passwords that are at least 12-16 characters long.

Include a mix of uppercase letters, lowercase letters, numbers, and special characters (e.g., !, @, #, $, %, ^, *).

Avoid easily guessable information like birthdays, common words, or phrases.

Unique Passwords for Each Account:

Never reuse passwords across multiple accounts.

Use a password manager to generate and store complex, unique passwords for each account.

Enable Two-Factor Authentication (2FA):

Whenever possible, enable 2FA for your accounts.

2FA adds an extra layer of security by requiring a second verification method, such as a one-time code from an app or a text message.

Regularly Update Passwords:

Change your passwords periodically, especially for critical accounts like email and banking.

Aim to update passwords every 3-6 months.

Beware of Phishing Scams:

Be cautious of emails, messages, or websites that request your login credentials.

Verify the legitimacy of the source before entering your password.

Use Passphrases:

Consider using passphrases, which are longer, easier to remember, and harder to crack.

Create a passphrase by stringing together random words or a sentence.

Avoid Sharing or Saving Passwords:

Do not share your passwords with anyone, even if they claim to be from a trusted organization.

Avoid saving passwords in web browsers, as they may not be as secure.

Secure Your Password Manager:

If you use a password manager, set a strong master password and enable additional security features like biometric authentication if available.

Educate Yourself:

Stay informed about current cybersecurity threats and best practices.

Be aware of common social engineering tactics used by scammers.

Check for Data Breaches:

Use online tools and services to check if your email or passwords have been compromised in data breaches.

Change passwords for affected accounts immediately.

Lock Devices and Accounts:

Use screen locks or passwords on your devices, including smartphones and laptops.

Lock your accounts and log out when not in use, especially on shared or public computers.

Backup and Recovery:

Ensure you have a backup method or recovery process in case you forget your password.

Many services offer account recovery options through email or mobile numbers.

Use Secure Wi-Fi:

Avoid logging into sensitive accounts on public Wi-Fi networks.

Use a virtual private network (VPN) for added security when using public networks.

Regularly Monitor Your Accounts:

Periodically review your account activity for any unauthorized access or suspicious transactions.

Set up account notifications for unusual activity.

Teach Password Security to Others:

Educate friends and family about password security practices to help protect their accounts as well.

By following these best practices, you can significantly enhance the security of your online accounts and reduce the risk of falling victim to cyberattacks and identity theft.