Information Security:
Social Engineering via Social Media

Social engineering is a type of cybercrime that involves manipulating someone into taking a specific action or divulging confidential or personal information, rather than technical hacking techniques, to gain access to data or systems.

Social Media is a very effective tool for cybercriminals to glean personal information about you. Such information may include the people you socialise with, your personal interests, where you've been on holiday, the services you use, and where you live. They can also peruse websites like LinkedIn to find your job information, educational background, as well as your working relationships. This information can be used to create convincing phishing emails or SMS messages that align with your interests. It could also be used by a social engineer to approach a colleague or friend via these avenues and very convincingly claim to be you.

Social media quizzes are an easy way for attackers to compel you to "over share" useful information - perhaps it was a dozen fun facts people might not know about you. Common questions may ask for; your first pet, mother's maiden name, first car and the month you were born. Sound familiar? That's because these are also common security questions for website logins. While it may seem harmless, sharing such information publicly may leave you vulnerable to account take-over attacks, identity theft or fraud.

Taking proactive measures can make it harder for cybercriminals to target you:

- Think twice before posting anything. Even if you delete it, posts can live forever in screen captures
- When away from home for extended periods, don't reveal your location. Watch out for the information you share in photos
- Customise your social media privacy settings to be as restrictive as possible regarding who can read and see posts. Consider an account for people you trust and another for public use
- Use multi-factor authentication