# FAKE PROFILES

Nowadays, most online users have at least one social media profile or account. However, is the person in the photograph you see on the profile the same person that is on the other side? Individual users may use fake profile in online dating or social media sites. On the other hand, using their software, cyber criminals can also produce tons of fake profiles to commit crimes such as identity theft, romance scam, cyber bullying, phishing, sexual exploitation, and other online crimes.

While some fake profiles are easy to spot, some might not be so. Here are some ways you can protect yourself from falling victim to fake profiles.

- Familiarize yourself with the privacy and security settings on the social media sites you are using.
- Only share information with the people you want to share. NEVER share sensitive information i.e. login details, online banking, and personal details with anyone.
- Protect your accounts with strong passwords and two-factor authentication. A string of complex and hard-to-remember alphanumeric does not necessarily make a strong password. A password should be characters that represent an information that only you know what it is and easy to recall.
- It is better to approve a friend request from someone you have met in person.
- Look for highlighted words such as “Prince”, “Widowed”, “Royalty”, “Engineer/Architect”, “PhD”, or cities in developed countries, etc. There is a chance they are fake profiles.
- The friend requester only has one photo and the person in the photo is extremely attractive or sexy. Chances are the profile could also be empty or no to little social connections. However, it is getting harder to detect fake profiles as some criminals filled up their profiles with stolen photo, and fake bios and followers.
- They are too forward or flirty e.g. sending messages and photos of sexual nature.
- They ask for your personal information