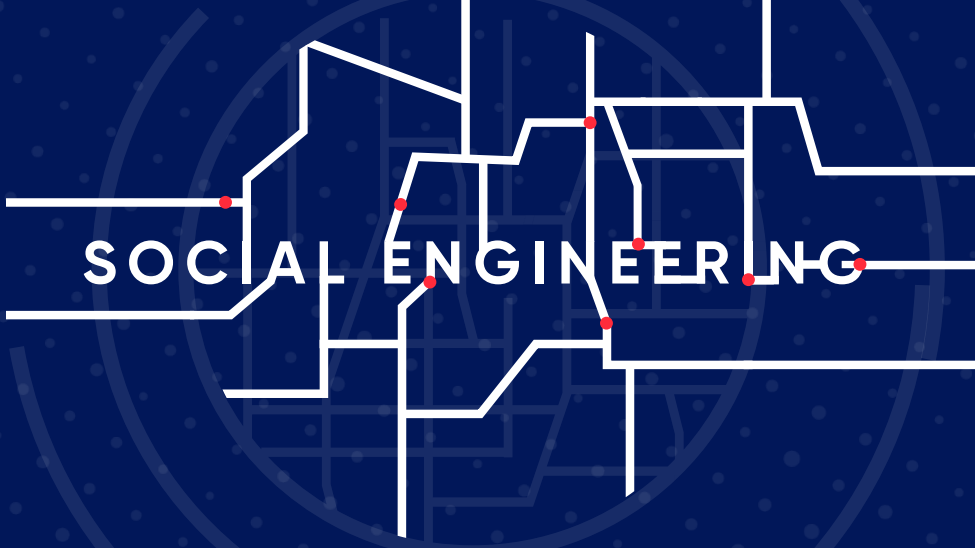
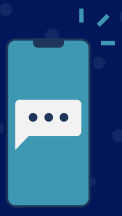
Government Security





Social Engineering

Social Engineering involves deliberately deceiving people into disclosing private information or granting system access — through emails, calls, messages, or even in person.

As civil servants we have access to a host of information which anyone seeking political or economic gain could benefit from.

Your organisation might well have sophisticated firewalls, good password protection and robust entry procedures, but the threat from Social Engineering remains.

Approaches may be made

- In person
- Via phone or IT devices
- Via Social Media

There are some easy ways you can help to minimise this threat:

- Never reply to messages, click on links or open attachments immediately, even if there is a sense of urgency, unless you are certain of its authenticity.
- Attackers may know your daily habits or places you go, both physically and electronically, so be aware that this knowledge might be used in a message to convince you it is genuine.
- Before posting information in the public domain consider whether it would be helpful to a hostile, such as the department you work for or information relating to sensitive projects.

For more information visit the **National Protective Security Authority**

Always report suspicious approaches to obtain information or access by following your department's security protocols.