Social Engineering Attacks

Recently, The Ministry of Home Affairs (MHA) issued warning to government officials against 'social engineering' attacks

- The MHA asked officials to avoid unsolicited phone calls, visits or email messages from unknown persons claiming to represent some organisation, to prevent the leak of sensitive information.

What is Social Engineering Attack?

- Social engineering attack involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain. It relies heavily on human interaction.
- Social engineering attack manipulates government officials to obtain sensitive information without letting them realise that a security breach is occurring.
- The MHA held that hackers often ask for information by sending an email or text message.
- **Phishing:** The email or text message carrying a link appears to come from a trusted source like a bank.
    - The link takes you to a fake website and once details like login name and passwords are entered, the login credentials reach to the hacker.
- **Quid pro quo attack:** In this case, a hacker comes posing as a technician and uploads malware with the intention to steal information from the system.

Source: TOI