Social Engineering Attack

Social Engineering Attack

From the information security perspective, social engineering attack refers to an attack exploiting human weaknesses or cheating people into disclosing personal or sensitive information, such as bank account number, personal password, etc.

Examples of Social Engineering Attack

The following are some typical examples of social engineering attack:

- The attacker impersonates the senior executive of an organisation to call the staff of internal IT support team. The attacker will request the staff to reset the password for the senior executive and give the new password to the attacker. With the new password, the attacker can use the senior executive's identity to log in the organisation's computer system and launch an attack.
- Some negligent staff may dispose of documents or storage media containing sensitive information in the bin. This gives a chance for the attacker to retrieve useful information easily from the bin and further attack the organisation's internal computer network.
- Some attackers will send out fraudulent emails. Recipients who trust the content of these messages will follow the instructions to enter fraudulent websites and key in sensitive information. Then the attackers can easily obtain these information for illicit purposes.
- Attackers can also steal information simply by peeping. For example, the attacker may stand near a user and peep at the password he enters. If the user is not vigilant, the password will be leaked.
- Attackers will also try to make a guess according to the tendency and habit for choosing passwords. Information such as user name, address, date of birth, etc. are too predictable and should not be used as passwords.

Security Measures

Following are the security measures against social engineering attack:

- Do not disclose personal or sensitive information to strangers or unreliable organisations.
- Do not click on the hyperlinks in dubious emails.
- Do not send personal or sensitive information to any website before verifying its credibility and security.
- Use a stronger password such as “1+Tw0Eq3” and change regularly.
- Install privacy protection filter on computer monitors so that attackers cannot peep and read sensitive information displayed on the monitors.
- The most important is to enhance one’s knowledge and awareness of information security.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk