

Informative Newsletters on Information Security

Social Engineering

WHAT IS SOCIAL ENGINEERING?

- ❶ A collection of techniques used to obtain confidential information through the manipulation of users
- ❷ Relies on weaknesses in people rather than software or hardware.
- ❸ Using the telephone or Internet to deceive people into revealing sensitive information - such as a password or credit card number.
- ❹ Social engineering does not necessarily involve the use of technology.

SOCIAL ENGINEERING TECHNIQUES

- ❶ Offering support to specific problems
- ❷ Sending free software or patch to install
- ❸ Sending a virus/Trojan horse via email to get access to your information
- ❹ Using false pop-up windows that ask for login especially in Internet-Banking applications
- ❺ Capturing victim keystrokes using key loggers
- ❻ Offering prizes for registering through a web site with a username and password.
- ❼ Phishing mails, examples: asking for account validation, warning the users of suspicious activities on their accounts,,offering lottery earnings and asking for monetary aid

PROTECTING YOURSELF FROM SOCIAL ENGINEERING

Do not reveal any personal information in e-mail, online or on the telephone unless you know who you are dealing with and why they need the information. Also make sure you are in a secure environment and using a secure medium of contact:

You can combat Social Engineering by following some simple guidelines:

- ❶ Do not share your passwords with anyone
- ❷ Do not have confidential conversations in public settings
- ❸ Shred sensitive information before throwing it in the trash
- ❹ If you find CD's or Thumb Drives do not place them into your computer to see what is on them as they may have malicious codes
- ❺ Show caution when opening email attachments
- ❻ Do not respond to or forward unsolicited email advertisements asking for personal Information, be sure you have a password-protected email account.
- ❼ If you receive telephone calls requesting company or personal information about you or other employees, be very cautious. Unless you can confirm their identity do not share the information they are asking for.
- ❽ Internet-Banking Applications: **VISIT SITES DIRECTLY**, if you need to enter your account details only enter by typing the site's address directly into the browser. Do not trust any web link you receive
- ❾ Use solid passwords for critical applications such as Internet Banking and change them regularly