Social Engineering

Technologies and methods which hackers use to circumvent information technology users and lead them to voluntarily disclose secret information that allows them the opportunity to penetrate E-Systems.

Methods used:

- Asking questions using the phone or e-mail while impersonating a powerful or influential character.
- Impersonation of close or known character to the user.
- Exploiting the good reputation of certain applications.

Protection methods against social engineering:

- Avoid sharing any personal information or data with anyone, and although this is easy to do, many users overlook this advice.
- Always check who you're talking to by phone, email, instant messaging, etc. For example, if the caller is from an official company, be sure to ask him for his full information and call from a verifiable official phone number.
- Do not open e-mail attachments from unknown people. This method is now widely used to spread malware and access personal information by impersonating major companies and attaching some files to the mail.
- Secure your smartphone or laptop. You can rely on spam filtering using special tools and consider using powerful anti-virus software that includes tools for anti-phishing messages and pages.

What to do when you become a victim of social engineering:

The attack is usually accompanied by social engineering techniques with another attack with malicious software, for example. So when a user becomes a victim to social engineering he has to take steps that vary depending on the type of attack.

In general, however, the following steps can be taken:

- Inform the person responsible for digital security at your organization or colleague who is in charge with digital security.
- Assess the damage and people affected
- Remove traces of attack
- Inform concerned parties (organizations, colleagues, friends, acquaintances, family members) that may have been subject to damage or affected by the user being the victim of an attack.