

Social Engineering

The art of deception

Social Engineering

Social engineering is a collection of techniques intended to trick people into divulging private information, which the social engineer can then use to gain unauthorized access to an information system or to commit fraud.

Social engineering may result in identity theft and financial loss, and it may jeopardize the security of information and information systems.

To avoid or minimize these losses, you must be able to recognize social engineering techniques to avoid being scammed by them.

- Email Bank Fraud
- Impersonation
- Phishing
- Spear phishing



Social Engineering - Plays on Human Nature

Social engineering plays on human nature. It may take advantage of our desire to be friendly and helpful, or of our conditioned response to people of authority, or of our interest in opportunities for personal gain. Social engineering is not a new phenomenon.

In addition to personal contact and telephone solicitation, technologies such as email and the Internet provide new ways for criminals to obtain private information. Having your private information stolen through the act of social engineering places you great risk.



Social Engineering through Email Bank Fraud

Also known as the Nigerian scam or foreign lottery emails.

To protect yourself from this type of social engineering, delete emails from senders that you don't know. If you do accidentally open an email of this type, do not respond to it. Just delete it. Responding validates that the sender has a valid email address and puts you at risk for additional social engineering attempts. Never provide your personal financial information to anyone in an email. Do not forward these types of emails to anyone. In addition to being social engineering, they might contain a virus.



Social Engineering through Impersonation

Impersonation is when a person plays the role of someone you are likely to trust or obey, to get access to your office, to information, or to your information systems.

This type of social engineering plays on our natural tendencies to believe people are who they say they are, and to follow instructions when asked by an authority figure.

Remember that technical support personnel do not ever need your password or other information related to accessing your system. Never disclose this type of information to anyone. Ask for identification.



Social Engineering through Phishing

Phishing is a high-tech scam that uses email or websites to deceive you into disclosing your credit card numbers, bank account information, Social Security Number, passwords, or other sensitive information. By sending an email or pop-up message claiming to be from a business or organization that you deal with, phishers play on the credibility of the legitimate company.



Social Engineering through Spear Phishing

Like phishing, spear phishing uses an email or web site to trick you into providing information.

Spear phishing differs from phishing in that the email comes from someone who appears to be from inside your organization. It may even appear to be from someone in a position of authority to make it more likely that you will comply with the email's request.

Spear phishing also differs from phishing in that it's usually an attempt to obtain information that can be used to hack into information systems.



Spear Phishing - Example

For example, a spear phishing attempt may ask you for your password or how to get remote access to the network. It could also ask you to click on a link to download a software program. Spear phishing is usually performed by very sophisticated hackers. Don't click on the links provided in an email. Those links might download spyware. If you believe that you may have fallen for a spear phishing attempt, report the incident to your technical support staff.



Knowledge Check

1. You receive an email asking you to verify personal information and there is a link to a website

- A. click on the link to investigate but do not enter anything
- B. do not click the link. Delete the email
- C. leave the email open and call the tech support staff.
- D. All of the above
- E. None of the above

2. In social engineering , a legitimate person may be impersonated by an attacker to gain useful information.

True or False



Knowledge Check

3. Social engineering is the scientific discipline that studies how people interact with computers, including how to make computers easier to use and how to prevent some of the human failures that hackers exploit to break into computer networks.

TRUE or FALSE

4. Social engineering" is what hackers call conning legitimate computer users into providing useful information that helps the hacker gain unauthorized access to their computer system.

TRUE OR FALSE



Knowledge Check

5. Phishing is

- A. A bogus but official looking email
- B. A request for you to provide personal or confidential information
- C. links to websites that expose you to malware
- D. All of the above
- E. None of the above

