SOCIAL ENGINEERING

Social engineering is a method used by cyber-thieves and other criminals to extract information by means of fraud, manipulation or misrepresentation. This type of threat relies on our nature as trusting members of society to believe what we see and hear. It uses our tendencies to respond in predictable ways in order to trick us into divulging secrets that we would not otherwise reveal.

Cyber-thieves have also realized that social engineering can be a lot easier than attempting to hack into a company’s computer network. By using a little fraud and manipulation they can gain access to passwords, account numbers, personal information, and other protected data.

COMMON METHODS OF SOCIAL ENGINEERING:

□ Phishing is a social engineering tactic that uses email messages to trick the recipient into either providing information or downloading some type of malware.

□ Social media messages can contain attachments or links that may ultimately infect a computer with some form of virus or malware.

□ Phone calls can be an effective social engineering tactic. By pretending to be someone in authority or in need of help, a caller can extract valuable information or manipulate a victim into providing access to their computer.

□ Fear is a big factor in social engineering threats. By using a popup message that says a computer is infected, cyber-thieves can get a victim to click on a harmful link or malware program.

□ Social engineering can also take the form of an intruder gaining physical access to a company’s secure data network by pretending to be an authorized individual.

AVOID BECOMING A VICTIM OF SOCIAL ENGINEERING:

□ Be skeptical of urgent emails requesting you to take immediate action by clicking a link or providing information. If in doubt, contact IT support and explain the situation.

□ Question any phone requests for information or requesting computer access. Tell the caller you will look into it and call them back. Remember, there will almost never be a time when you need to immediately supply account or password information.

□ Keep computer software updates and anti-malware up-to-date and active.

□ Don’t be afraid to question someone in your work environment who you don’t recognize. Ask who their contact is and verify it. A little inconvenience is a small price for security.