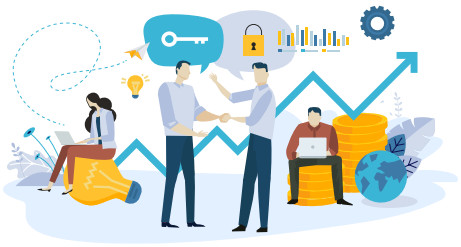
What is Social Engineering?



Social engineering is a manipulation technique used by cybercriminals to trick people into giving up confidential information.

Social engineering relies on the basic human instinct of trust to steal personal and corporate information that can be used to commit further cybercrimes. For example, a cybercriminal might use social engineering to convince an employee to divulge company passwords. The cybercriminal then uses these passwords to access corporate networks to steal data and to install malware on the company network.

All it takes is an email, phone call or text message disguised as coming from a colleague, friend, or known company and the cybercriminal has won. The cybercriminal may use a familiar yet urgent tone to convince the victim to update their banking information or tell the victim that to claim their prize they have to provide their credit card information.

Social engineering is hard to defend against because human beings are unpredictable. There is no way of knowing who will fall for a social engineering attack. Cybercriminals hope to catch the victim off-guard when they forget to remain alert to cyber attacks.

Why Is Social Engineering So Dangerous?

Social engineering is so dangerous because people make mistakes. Although victims know they need to be suspicious of emails that promise refunds or phone calls that tell them they'll be arrested immediately if they don't provide their tax information – people do get caught off-guard.

Social engineering success relies on human nature – being busy, not paying attention, being too trustworthy, complacency and simply forgetting the basics of cyber security awareness. It is not unheard of for people to be repeat victims of social engineering attacks.

It is much easier for cybercriminals to hack a human than it is to hack a company network. This is exactly why it's so important that you focus on people-centric cyber security awareness training. By putting your people first, you can give them the education, resources and tools to stay aware of social engineering.

How Does Social Engineering Happen?

Social engineering attacks happen with 9 common techniques:

1. Phishing

Phishing uses tactics including deceptive emails, websites and text messages to steal confidential personal and corporate information. Criminals who use phishing tactics are successful because they carefully hide behind emails and websites that are familiar to the intended victim.

2. Spear Phishing

Spear phishing is a cybercrime that uses emails to carry out targeted attacks against individuals and businesses. Criminals use savvy tactics to collect personal data about their targets and then send email emails that are familiar and trustworthy.

3. Baiting

Baiting relies on the human desire for reward. Baiting is both an online and physical social engineering attack that promises the victim something in exchange for their action. For example, plugging in a USB key or downloading an attachment in order to receive free movie downloads for life. The computer and potentially the network are then infected by software that can capture login credentials or send fake emails.

4. Water-Holing

Water-holing targets a group of users and the websites they commonly visit. The cybercriminal looks for a security vulnerability in one of these websites and then infects the website with malware. Eventually, a member of the targeted group is infected by the malware. This is a very specific social engineering technique that is hard to detect.

5. Vishing

Vishing uses voice mails to convince victims that they need to act quickly, or they could be in trouble with the law or at risk. For example, a criminal may leave a voice mail that urges the victim to reset their banking information because their account has been hacked.

6. Pretexting

Pretexting is a social engineering technique that uses false identity to trick victims into giving up information. For example, the cybercriminal may know that the victim recently bought an item from Apple, so the cybercriminal sends an email pretending to be an Apple customer service representative who needs to confirm the victim's credit card information.

7. Quid Pro Quo

Quid pro quo scams rely on an exchange of information to convince the victim to act. This social engineering technique offers to provide a service to the victim in exchange for a benefit. A common technique is for the criminal to impersonate an IT support employee who calls victims who have open support tickets. The cybercriminal promises a quick fix if the person disables their antivirus software or confirms their login credentials.

8. Malware

Malware is used to trick victims into paying to remove malware, viruses, or other infected software from their computers. Victims are tricked into believing that there is a virus or malware on their computer and if they pay, they can have it removed. Depending on the scam, the criminal might only steal the victim's credit card information or also install actual malware or ransomware on the computer.

9. Tailgating

Tailgating is a physical social engineering technique which relies on trust to gain access to a building or secure area in a building. The criminal may simply walk closely behind someone and slip through an open door or ask to be "badged in" because they forgot their employee swipe card. This scam underscores the need for employees to pay attention to who is loitering near doors and to never hesitate to ask for identification.