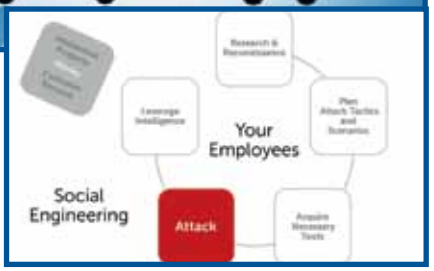
Social Engineering and Countermeasures

Ahmed Saleh*
CISM, CRISC, PMP, ITIL, COBIT5, CEH
Information Security & Business Continuity Manager



When it comes to hacking, it is a common assumption to imagine attackers who utilize their technical expertise to infiltrate protected computer systems and compromise sensitive data. We hear about this breed of hackers in the news all the time, and we are urged to counter their exploits by investing in new technologies that will harden our network defenses.

However, there are other types of attackers who can use their tactics to avoid our tools and solutions. They are the social engineers, people who exploit the one weakness that is found in each and every organization: Human Psychology.

Using a variety of techniques, including phone calls, email sand social media, these attackers trick people into offering them access to sensitive information.

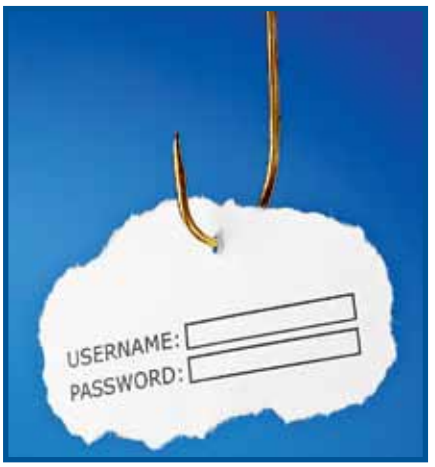
What is Social Engineering?

Social engineering is the attempt to manipulate or trick a person into providing confidential information to an individual that is not authorized to receive such information. In definition: It is a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Some major social engineering techniques include:

Phishing scams

Phishing scams are without a doubt the most common type of social engineering attacks used today. Most phishing scams are characterized by their effort to obtain personal information,



E.mail: ahmed.n.saleh@hotmail.com

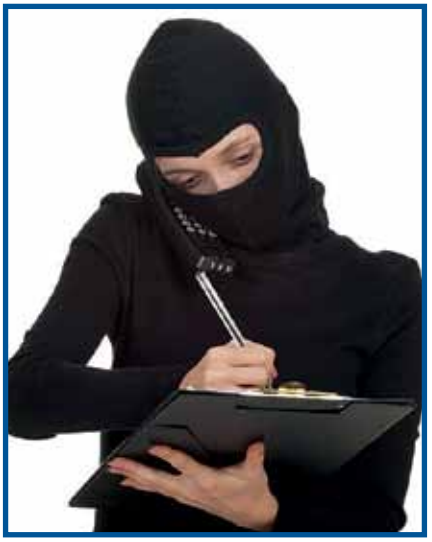
such as names, addresses, habits, social media profiles and if lucky: bank account numbers. These scams can be performed by the usage of the email system along with link shortners or embedded links that redirect users to suspicious websites in URLs that appear legitimate.

In their communication messages (emails), social engineers convey the sense of fear, urgency, reward and even threats in an attempt to manipulate the user into acting quickly.

Some phishing emails are more poorly crafted than others to the extent that their messages often shows generic receivers along with incorrect spelling and grammatical errors, but these emails are focused on directing victims to fake websites where hackers are able to steal user login credentials and other personal information.

To protect yourself against phishing scams, you need to:

- Exercise little bit awareness when you receive unknown email messages;
- Show some common sense: come on, you can't win a lottery that you haven't even participated in!
- If the message looks suspicious, do some research, Google the parties sending these messages along with some part of the messages;
- You should realize that there is nothing as "Get Rich Quickly"
- You should know that: if the deal is too good, then it is too good to be true.



Pretext Calling

Pretext calling is a fraudulent mean of obtaining an individual's personal information. Armed with limited information, such as a name, an address, job position etc... Pretext caller may pose as a client, an employee, a service provider "depending on the situation". During this call the pretext caller attempts to convince you into giving him confidential information.

For example: A caller claiming that he is from the Internet Service provider tries to distract you by being over friendly in a effort to change and diverse your focus from the fact that he is seeking information about your work description, work habits, what time do you usually use your computer, what operating system do you have, what is your antivirus etc.....

Protection against Pretext calling:

A healthy dose of paranoia is certainly a good way to fight pretext calling, you shouldn't answer any question regarding issues that expose your private information and especially to unknown people.

Dumpster Diving

Dumpster diving simply involves searching through trash to collect sensitive information; the objective is to gather information that has been carelessly thrown away. (Awful yet very effective)

Dumpster diving, also known as trashing, a huge amount of information can be collected through company dumpsters for example: "company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware."

Protection against dumpster diving:

Awareness: Staff members

of different levels should be educated about the dangers of untracked trash. Accordingly they are mandated to use:

Paper shredders: all documents that contain confidential or customer information must be shredded when no longer required.

Sanitization: all media CDs, floppies, USBs, Hard Disks that contain sensitive information should be destroyed prior to throwing these things in the dumpster.

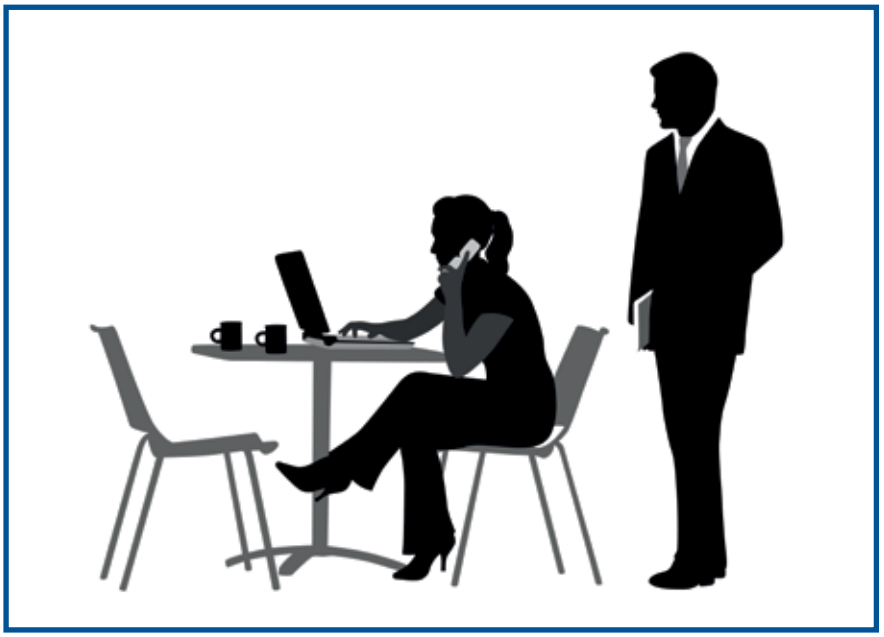
Shoulder Surfing

Shoulder surfing occurs when someone may obtain sensitive information just by standing close to the victim, skimming and scanning across desks where the victim left his PC and Papers. It is quite notable that "well trained people" may stand a little far away facing your keyboard and watch you login to your email or even e-banking webpage.

Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or unlock their PC.

Protection against shoulder surfing:

- Ensure that computer monitors are positioned in a way that prevents individuals from seeing confidential information.
- Educate employees to make sure that no one is watching them typing confidential data, even if they consider themselves fast typists
- Educate employees to refrain from leaving sensitive information spread on their desks.



Baiting

In baiting the attacker leaves a malware infected media device such as a CD ROM, or USB flash drive in a location sure to be found. (Bathrooms, elevators, parking lots), he also spares no effort in giving this media a legitimate look, and simply waits for the victim to use the device. For example, an attacker might create a disk featuring a corporate logo, readily available from the target's web site, and sticks an attractive label to complete his bait on the front.

The attacker would then leave the removable media on the floor of an elevator or somewhere in the lobby of the targeted company.
In case of merely inserting the disk into a computer to see the content, the user would unknowingly install a malware. This malware will most likely giving an attacker unfettered access to the victim's PC and perhaps, the targeted company's internal computer network.

Unless computer controls block the infection, PCs set to "auto-run" inserted media may be compromised as soon as a rogue disk is inserted.

Protection against baiting:
It is hard to protect organizations against baiting, however to be effective, security professionals should train and educate employees by giving them examples, and a "what could happen" scenario.

There are also technical controls that might be required from the security administrators to enforce a strict policy on removable media.

"Quid pro quo" or "Something for Something"

Something for something is an act where an attacker calls random numbers at a company claiming to be calling back from technical support. Eventually they will come across someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will "help "solve the problem and in the process has the user type commands that give the attacker access or launch malware.

In conclusion, humans have proven to be the weakest link when it comes to information security. But with proper awareness and proper diligence staying safe is not that hard to achieve. Hackers who engage in social engineering attacks prey off human psychology and curiosity in order to compromise their targets' information. With this human-centric focus in mind, it is up to users and employees to counter these types of attacks.

Boost Your Productivity by Protecting Your Time
If you want to get more done, take ownership of your time. Our most satisfying work comes about when we're playing offense, working on projects that we ourselves initiate. Look for ways to automate or delegate activities that are not a good use of your time. Say no to projects that aren't a priority and maintain a relentless focus on self-directed goals that only you can achieve. Program your phone to only ring for select people, and resist emails first thing in the morning until you've achieved at least one important task. Recognize and honor your physical limitations by getting plenty of exercise and sleep, cycling between 90-minute bursts of focused work and short restorative breaks. And use your vacation time. Top performers view time off not as stalled productivity but as an investment in their future performance.

www.hbr.org