Social Engineering – Hacking Your Mind

The Attack
Nowadays much of your interaction with other people is done virtually, you no longer need to be in physical contact to communicate. You talk to people on the phone, chat with them over instant messaging, send SMS messages on your smartphone, or communicate with email. These technologies have made it much easier to communicate and work with people around the world. However, these same technologies also make it easier for cyber criminals to launch one of their most effective attacks against you, social engineering.

Social engineering is not a technical attack, it does not exploit a vulnerability in a program. Instead, it is a psychological attack that exploits vulnerabilities in you. Cyber criminals build trust with you, pretending to be a person or organization you know. They then exploit this trust to get what they want, such as access to your computer or your passwords. These attacks are launched via the same tools you use every day, such as email and instant messaging.

Protecting Yourself
Social engineering attacks are the hardest attacks to protect against because technology alone can not solve the problem. The best defense is understanding that you are a target and that cyber criminals will try to fool you. On the second page of this newsletter we give you examples of some of the most common social engineering attacks.

The key to protecting yourself is to only trust communications that you began yourself or that you expected to receive. For example, only open an attachment in email when you were expecting to receive an attachment. Only click on a link to a website if you were expecting someone to send you the link. Just because you know or trust an organization that contacts you does not mean that it is really that organization. It is very simple for cyber criminals to pretend to be others when on the Internet. If something seems to be suspicious or too good to be true, it most likely is.

Hacking Your Mind
Cyber criminals have learned that the easiest way to take control of your computer or steal your passwords is to simply ask you for them.
Hacking Your Mind

Below are several common social engineering attacks. Often the cyber criminal’s goal in these attacks is to take control of your computer or steal your information, such as your login and password. Cyber criminals have learned that often the simplest way to gain control of your computer, or to steal your passwords, is to simply ask for them.

Fake Anti-Virus

Everyone tells you that to protect your computer you need to download and install anti-virus software. Cyber criminals know this and take advantage of the fact. Cyber criminals have created thousands of websites that pretend to sell legitimate anti-virus software. When you connect to these websites they pretend to scan your computer, informing you that your computer is infected. They then recommend you buy and download their software, which will fix your infected computer.

These websites are very professional looking, with what appear to be real logos, customer reviews, and even ratings. However, all of these are a lie. The anti-virus software is fake; if you download and install the program the software will infect your computer, giving cyber criminals total control of your computer. Only download and install anti-virus software (or any software) from websites you know and trust.

Malicious Email

Another common attack is through email. Email is one of the most common methods used for attacks because so many people around the world use it. Also, with email it is very easy for cyber criminals to pretend to come from real organizations. For example, cyber criminals will create official looking emails that look like they come from popular sites such as Facebook, well known banks, or trusted government organizations. These emails are lies, usually any attachments are infected or any links take you to malicious websites that will attack your computer. The best defense is to not click on a link or open an attachment unless you were expecting it.

Scams

Finally, criminals are not only after your computer but your money. Once again, often the easiest way to steal something is to simply ask for it. One way criminals do this is with scams, such as lottery scams. These emails explain that you’ve won the lottery. To collect your money you are requested to contact a person and give them your banking information. The criminals then require you to pay a transaction fee or taxes to get your lottery winnings. Once again this is all a lie; once you give up your information and pay the fee or taxes, the cyber criminals disappear, never to return. Your banking information and money have just been stolen. The best way to protect yourself is simply to delete such emails. If it sounds too good to be true, it most likely is.

The Hotel Room

Here is a non-technical example of a social engineering attack. It does not involve computers or any advanced technology, only the phone and your hotel room.

Let’s say you have been traveling and you just checked into your hotel room. As you walk into your room and set your bag down your hotel room phone rings, so you answer it. A nice girl on the other end introduces herself as Rebecca from the hotel front desk. She explains there has been a problem with your check-in. She needs to confirm your information and asks you for your credit card number. Since you think she is calling from the hotel front desk, you give her your credit card information. She then tells you that everything checks out and asks you to enjoy your stay.

Unfortunately, you have just been socially engineered. That was not really Rebecca from the front desk but a criminal from another country. She is calling every hotel room attempting the same attack. She built trust with you pretending to be the front desk and used that trust to steal your credit card number. If you ever receive a phone call like this, hang up and then call the hotel front desk back, that way you know you are really talking to someone at the front desk.