CYBER SECURITY Newsletter

SOCIAL ENGINEERING – HACKING YOUR MIND

The Attack

Today, 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 via instant messaging, send SMS messages on your smartphone, and/or communicate with email. These technologies have made it much easier to communicate and work with people around the world. However, these 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 which exploits your vulnerabilities. Cyber criminals build up your trust, pretending to be a person or organization you know. They then exploit this trust by obtaining access to your computer and/or your passwords. These attacks are launched using the same tools you use every day, such as email, the phone, and the web.

Protecting Yourself

Social engineering attacks are the hardest attacks to protect against because technology alone cannot solve the problem. The best defense is you. Understand that you are a target and that cyber criminals will try any way to gain your trust to exploit you.

The key to protecting yourself is to only trust communications that you initiate or you expect to receive. For example, only open attachments when you are expecting one. Only click on a website link if you were expecting someone to send you the link. If you receive a phone call asking for your information or for you to visit a website, it is most likely an attack. First, validate the person calling or call the organization directly. Because you know or trust an organization who contacts you does not mean it really is that organization. It is very simple for cyber criminals to pretend to be others over the phone and on the Internet. If something seems 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.

Idaho State University

This newsletter is published by Idaho State University, for more information please contact us at:

help@isu.edu

The Hotel Room

A non-technical example of a social engineering attack is one that does not involve computers or any advanced technology. Take, for example, this situation that uses a phone and a hotel room.

You have been traveling and just checked into your hotel room. As you walk into your room and set your bag down, your phone rings. A nice girl introduces herself as Rebecca from the front desk. She explains there has been an issue during check-in and she needs to re-confirm your credit card information. Assuming she is calling from the hotel front desk, you provide your credit card information. She then informs you everything has been resolved and to enjoy your stay.

Unfortunately, you have been socially engineered. That was not Rebecca from the front desk, but a criminal from another country. She has been 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 call the front desk to confirm you are talking to someone from the hotel.

Hacking Your Mind

Below are several common social engineering attacks. Often the cyber criminal's goal with these attacks is to take control of your computer or steal your log in and password information. Cyber criminals have learned that 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 are aware of this fact and often use this to their advantage. Cyber criminals create thousands of websites pretending to sell legitimate anti-virus software. When connected to these websites, they pretend to scan your computer and inform you your computer is infected. They then recommend you buy and download their software to fix your infected computer.

These websites are often very professional looking, including replicated logos that appear to be real, customer reviews, and even customer ratings. However, all of this is a scam, and the anti-virus software is phony. When you download and install the program the software will infect your computer, giving the 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

Email is one of the most common methods used for attacks because it is so widely used around the world. Email also makes it 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 scams, usually including infected attachments or links directing 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 trust the sender.

Scams

Criminals are not only after your computer, but your money, and often the easiest way to steal something is to ask for it. One way criminals achieve this is with various scams, such as lottery scams. These email scams explain you've won the lottery, and to collect your lottery winnings you must contact a person and provide them your banking information. The criminals then require you to pay a transaction fee or taxes to receive your winnings. Once you provide your information and pay the fees or taxes, the cyber criminals disappear with your money and banking information. The best way to protect yourself is to delete these emails. If it sounds too good to be true, it most likely is.