ISSUE: 8-14 YEAR: 2014

University Information Security Office Newsletter

The real problem is not whether machines think but whether men do

-B.F. Skinner

From the ISO's Desk

There are many common ways that credentials, personal information and even your whereabouts can be stolen by criminals. Many of these criminal elements use social engineering techniques to get company information, travel habits, or to gain access to your personal accounts. One common way is to get information from people who put personal information on social media sites like Facebook. Often this information can be used to get, for example, answers to password challenge questions like your dog's name or your mother's maiden name. Even in one's daily life, people post their whereabouts on these sites making it easy for thieves to break into their homes, knowing that they are on vacation or out for the evening.

This month's newsletter will help you to understand what social engineering is and to help you identify ways to protect yourself and to prevent it from affecting you.

Thank you,

Jim Pardonek
Information Security Officer

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM

5 Common Social Engineering Attacks

Created by Joseph LaMagna-Reiter

Social engineering, in the context of information security, refers to the psychological manipulation of people into performing actions or divulging confidential information. There are many ways to accomplish social engineering that may be hard to detect. Here are some of the most common social engineering techniques.

#1 Phishing

By far the most common and widespread social engineering attack is email phishing. An attacker can spoof an email address and send mass emails that ask for personal information such as names, addresses, social security numbers, credit card numbers, and more. Any piece of information that an attacker can learn about can be useful to them. Additionally, these emails looks like they come from legitimate sources such as bank corporations, helpdesk emails, or more.

It is also not uncommon for attackers to also use vishing attacks. Vishing is essentially a phishing attempt that is executed through an automated phone call or text. A common message is that your bank account is locked and that you need to confirm your credit card and pin number.

#2 Tailgating

Many buildings are secured with locks requiring keys, access cards, pin numbers, or some other form of physical item or passcode. Tailgating is an attack that preys on a person's politeness of holding a door open in order to bypass the aforementioned security provisions. An attacker may be carrying a big box or just standing by the door saying they forgot their key in order for someone to let them in. Especially in a larger business or social setting, employees will probably not know every single person that works in a building and grant the attacker access.

#3 Technical Talk

Advanced technical talk may be able to allow an attacker to gain access to a computer or even a user account. An attacker can make calls to employees at a company claiming to be their own helpdesk support. Employees may not even know it's a deception because human trust makes us believe the person on the other side of the phone is exactly who they say they are. While engaged in conversation, the attack may convince the employee to give them their password, install malicious software, gain remote access to their computer, or other malicious actions.

#4 Networking

Social networking sites such as Facebook, Google +, and Twitter provide a large amount of free data on potential targets. Many people post information about their work, hobbies, favorite TV shows or books, music interests, and much more. All of this information can be used by an attacker in order to portray themselves as a friend or person who share common interests. The attacker may then try to ask about personal information that they can use even though, to you, it may seem like common knowledge. Birth dates, school, previous and current addresses, and more are all valuable pieces of information.

#5 Drinking

After a long hard week at work, many employees might bond over a drink at a local bar. This is a perfect social place for an attacker to seek out confidential information. There are many ways for different people to start talking at a bar, and an attacker will be on the lookout for an opportunity to connect with a potential target. Once connected, the attacker may offer to buy drinks and seem like a true friend. After a few drinks, the attacker may try taking advantage of his position and ask for confidential information about the workplace, building access, passwords, or more.

The Personal Information Search Engine

Created by Brett Weston

With the constant digitization of public records and storage moving to an ever-scaling and flexible network (a.k.a. the cloud), the everyday person has had more information than ever available to him. But there comes a problem, how do you find what you are looking for? And, to counter, how do you protect what you don't want the world to see?

An outcome of this massive amount of data and a need to search it is what we now call a search engine, an application that scours the web and indexes information to be returned when keywords are entered. The common first step in finding what the Internet knows about you is to simply type your name into one of these search engines such as Google or Bing. For some, like myself, who share a name with someone much more famous than I ever will be, the results do not contain any person information. For others, Facebook and Twitter profiles are among the top hits. But what many people don't know is there are some search engines that exist solely to index personal information and offer more finely tuned searches.

One such engine is Spokeo. Spokeo claims to search a multitude of online and offline data sources. But what makes Spokeo unique, and a little creepy, is just how accurate it can be. A search for myself yielded few results, which is probably because I don't own real estate and have social media profiles locked down with privacy settings. But a search for relatives and friends returned maps of their home, home valuation, spouse, email address, and so much more. Now, Spokeo is a business, so some of this information is only available if you buy the full report of your search but it is a good starting point to see what is potentially available publicly on the web.

How Cyber Criminals Trick People and Get Their Information

Created by Cai Wang

It's almost inevitable that at some point you will get an email from your bank or a credit card company asking you to verify personal information. Reformed computer criminal and security consultant Kevin Mitnick points out in *The CSEPS Course Workbook* that it is much easier to trick someone into giving you a password for a system than to spend the effort to use hacking techniques to crack into it.[1] You should be wary of the authenticity of the email because it is most likely phishing. You need to be aware of any links when getting an email from an unfamiliar email address. A more Recent tactic is for phishers to play the family card. You may get an email that says "I uploaded the pictures from our last weekend's family party to an online album. Here is the link." It is not uncommon for people to have family parties, so many people would not think twice when clicking on a link. That link might be to a malware or virus download site. Once you click on the link, the virus will start to attack your computer.

Even information that you get in your home mailbox can be used to get information that can be used to trick you into thinking a caller is authentic. You might wonder how sales people know which bank you are using or how they know your name. When you throw away your bank statement, it's easy for others to know which bank that you are using. To prevent this fully shred the paper with a cross-cut shredder.

[1]Mitnick, Kevin, Kasperavičius, Alexis. (2004). CSEPS Course Workbook. Mitnick Security Publishing.

Shoulder Surfing

Created by Yuan Liu

We never give a second thought to someone standing behind us in line. Shoulder surfing is the use of direct observation techniques, such as looking over your shoulder, to get sensitive information. It is particularly effective especially in crowded public place.

It is easy to observe someone when they are doing following things:

- filling out a form
- entering a PIN at an ATM or sale terminal
- giving credit card information when paying via telephone
- Entering a password at a public café, library or airport

Example: When you go to public swimming pool, you rent a locker. If you use the same four-digit PIN number that is the same as your credit card. A thief may use shoulder surfing to peek at your locker code, break in, and take away your wallet with your debit card. Now the thief will be able to use your card.

Avoid using your bank PIN or password for other important information. Even though it's easier to remember only one PIN or password, it makes it harder to break into your accounts if you have a different PIN or password for each account. Also, when using your PIN it is a good practice to shield the keypad from others to reduce the shoulder surfing risk.