Security Best Practices When Using Public Wi-Fi:

1. Avoid accessing sensitive information, like banking or logging into accounts that hold private data.
2. Stay away from networks with suspicious names like “free Wi-Fi.”
3. Turn off airdrop and file sharing.
4. Turn on any firewalls you have installed.
5. Turn off Wi-Fi when not in use.
6. Tether your phone’s internet connection to your laptop, allowing you to use your phone’s data on your laptop. Also known as your phone’s hotspot.
7. Invest in an unlimited data plan so you don’t need to use public Wi-Fi.
8. Change your device settings so that your device doesn’t automatically connect to available Wi-Fi networks.
9. Don’t use the same password for all sites. LastPass can help you keep track of passwords.
10. Enable two-factor authentication whenever possible.
11. Log out of sites when you leave them.

Tips for a Strong Password

1. Make your password eight characters or longer
2. Use a passphrase, then add in some punctuation and capitalization
3. Don’t make passwords easy to guess
4. Do not include personal information such as your name or pets’ names easily to find on social media
5. Avoid using common words in your password
6. Substitute letters with numbers and punctuation marks or symbols
7. Never share your password
8. Watch for attackers trying to trick you into revealing your passwords through email or calls
9. Unique account, unique password. Use different passwords for different accounts

First National Bank

OF ST. IGNACE

Clearing Browsing Data (Cookies, Cache, Saved Passwords etc.)

When you visit a website, your browser will save information about the sites you visit to your computer. Stored information includes cache, cookies, browsing history, passwords, and other browsing data. This is done to help the browser load pages faster when you visit the same site again. However, over time your computer might save thousands of files, and this process can actually slow down your computer.

Additionally, this stored information poses a security risk. Cache and browsing history files disclose which websites you have visited in the past. Cookies and saved password files can disclose your passwords or other private information you have typed into web forms.

To ensure this information is protected, and to help your browser function more efficiently, it is a good idea to delete your cache, cookies, history, saved passwords, saved web form information, and other saved browser files, periodically. This way, if your computer ends up in the wrong hands, your private information will not be as easily available.

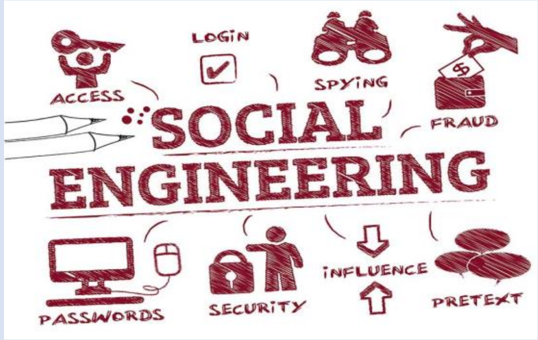
What is Social Engineering?

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Security is all about knowing who and what to trust. It is important to know when and when not to take a person at their word and when the person you are communicating with is who they say they are. The same is true of online interactions and website usage: when do you trust that the website you are using is legitimate or is safe to provide your information?

Example: Let’s say you received an email, naming you as the beneficiary of a will. The email requests your personal information to prove you’re the actual beneficiary and to speed the transfer of your inheritance. Instead, you’re at risk of giving a con artist the ability not to add to your bank account, but to access and withdraw your funds.



6 Types of Social Engineering Attacks

1. Baiting

This type of social engineering depends upon a victim taking the bait, not unlike a fish reacting to a worm on a hook. The person dangling the bait wants to entice the target into taking action.

Example: A cybercriminal might leave a USB stick, loaded with malware, in a place where the target will see it. In addition, the criminal might label the device in a compelling way — “Confidential” or “Bonuses.” A target who takes the bait will pick up the device and plug it into a computer to see what’s on it. The malware will then automatically inject itself into the computer.

2. Phishing

Phishing is a well-known way to grab information from an unwitting victim. Despite its notoriety, it remains quite successful. The perpetrator typically sends an email or text to the target, seeking information that might help with a more significant crime.

Example: A fraudster might send emails that appear to come from a source trusted by the would-be victims. That source might be a bank, for instance, asking email recipients to click on a link to log in to their accounts. Those who click on the link, though, are taken to a fake website that, like the email, appears to be legitimate. If they log in at that fake site, they’re essentially handing over their login credentials and giving the crook access to their bank accounts.

In another form of phishing, known as spear phishing, the fraudster tries to target — or “spear” — a specific person. The criminal might track down the name and email of, say, a human resources person within a particular company. The criminal then sends that person an email that appears to come from a high-level company executive. Some recent cases involved an email request for employee W-2 data, which includes names, mailing addresses, and Social Security numbers. If the fraudster is successful, the victim will unwittingly hand over information that could be used to steal the identities of dozens or even thousands of people.

3. Email hacking and contact spamming

It’s in our nature to pay attention to messages from people we know. Some criminals try to take advantage of this by commandeering email accounts and spamming account contact lists.

Example: If your friend sent you an email with the subject, “Check out this site I found, it’s totally cool,” you might not think twice before opening it. By taking over someone’s email account, a fraudster can make those on the contact list believe they’re receiving email from someone they know. The primary objectives include spreading malware and tricking people out of their data.

4. Pretexting

Pretexting is the use of an interesting pretext — or ploy — to capture someone’s attention. Once the story hooks the person, the fraudster tries to trick the would-be victim into providing something of value.

5. Quid pro quo

This scam involves an exchange — I give you this, and you give me that. Fraudsters make the victim believe it’s a fair exchange, but that’s far from the case, as the cheat always comes out on top.

Example: A scammer may call a target, pretending to be an IT support technician. The victim might hand over the login credentials to their computer, thinking they’re receiving technical support in return. Instead, the scammer can now take control of the victim’s computer, loading it with malware or, perhaps, stealing personal information from the computer to commit identity theft.

6. Vishing

Vishing is the voice version of phishing. “V” stands for voice, but otherwise, the scam attempt is the same. The criminal uses the phone to trick a victim into handing over valuable information.

Example: A criminal might call an employee, posing as a co-worker. The criminal might prevail upon the victim to provide login credentials or other information that could be used to target the company or its employees.

5 Tips to Help You Avoid Being a Social Engineering Victim

1. Consider the source. A found USB stick isn’t necessarily a good find. It could be loaded with malware, just waiting to infect a computer. And a text or email from your bank isn’t necessarily from your bank. Spoofing a trusted source is relatively easy. Don’t click on links or open attachments from suspicious sources — and in this day and age, you may want to consider all sources suspicious. No matter how legitimate that email appears, it’s safer to type a URL into your browser instead of clicking on a link.

2. Slow down. Social engineers often count on their targets to move quickly, without considering the possibility that a scammer may be behind the email, phone call, or face-to-face request on which they’re acting. If you stop to think about the ask and whether it makes sense or seems a bit fishy, you may be more likely to act in your own best interest — not the scammer’s.

3. If it sounds too odd to be true …. Seriously, how likely is it that a Nigerian prince would reach out to you for your help? Or, on the flip side, that a relative is texting you to post bail while traveling? Investigate any requests for money, personal information, or any item of value before handing it over. There’s a pretty good chance it’s a scam — and even if it’s not, better to be safe than sorry.

4. Install an antivirus software or a security suite and keep that software up to date. Also, make sure your computer and other devices are running the latest versions of their operating software. If possible, set the operating systems to update automatically. Having the latest versions of these software applications on your devices will help ensure they’re prepared for the most recent security threats.

5. Your email software can help you. Most email programs can help filter out junk mail, including scams. If you think yours isn’t doing enough, do a quick online search to find out how to change its settings. The goal is to set your spam filters too high to weed out as much junk mail as possible.