Scarborough IT Department

Security Awareness Basics

Let's have a brief introduction to the topic of Security Awareness. The information below can apply to both your home and business. As you may be aware, a growing number of organizations have been struck by hackers that have managed to infiltrate and lock public (*and private*) data networks. Once locked, these hackers then demand a sum of money (*ransom*) prior to allowing staff further access to those systems. To increase our ability to prepare for such an attack, Scarborough IT has been conducting a system-wide Security Awareness training series for staff over the past several months.

The "90/10 Rule" can often be used to describe a good security awareness program. 90% of security safeguards rely on the computer user ("*You*") to adhere to good computing practices. 10% of security safeguards are technical. The same principles that you use to secure your home apply in technology security. Checking to see if your door is closed, ensuring others do not prop your door open, keeping control of your keys, and remembering to lock your lock is 90% of your security practice. The actual lock on the door is the final 10%. You need *both* parts for effective security.

This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, device and data secure. Take steps to ensure that your computer is protected by using the latest operating system and software updates. An unprotected computer can become infected or compromised within a few seconds after it is connected to a network. It is important to understand that a compromised computer is a hazard to everyone else, too – not just to you. Technology security is everyone's responsibility, and these practices work at both work and home!

Key Skill Upgrades

Many cyber security threats are largely avoidable, and involve more common sense than any amount of technology skills.

- Try using phrases instead of words and insert both special characters and numbers (ex. *Thequickbrownfox@Jumped83times*).
- Try using a password manager application on your device to keep track of your many passwords in a secure manner (ie. *LastPass, OnePass, etc.*).
- Avoid reusing passwords for multiple accounts or websites, keep your passwords secret, and resist the urge to simply write them down in easily located places.
- Avoid clicking on unknown or unsolicited links or attachments, and don't download unknown files or programs onto your computer.

- Finally, to help reduce risk, look for “https” in the URL before you enter any sensitive information or a password. (The “*s*” stands for “*secure*”.)

Types of vulnerabilities and attacks

There are many types of technology vulnerabilities and attacks that can occur, but the four major types to watch for as a general user are noted below. Keep in mind what has been stated previously. Many cyber security threats are largely avoidable. It is your efforts to adhere to good computing practices that will keep you safe.

- ***Phishing*** *is a form of identity theft in which a scammer uses an authentic-looking email from a legitimate business to trick recipients into giving out sensitive personal information.*
- ***Social Engineering*** *utilizes various methods to engage in deceptive practices that are used to manipulate individuals into divulging confidential or personal information that can be used for fraudulent purposes. This includes popular social media platforms such as Facebook, Instagram, Twitter, Pinterest, and others.*
- ***Ransomware*** *is a type of malicious software designed to block access to a computer system until a sum of money is paid.*
- ***Theft*** *is the action or crime of stealing. In relation to technology, this might include the loss of a laptop or desktop computers, tablet, smartphone, or storage device (hard drive, flash drive, etc.) that contains sensitive, confidential or protected information.*

We hope that you have found this article to be helpful and informative. Information technology is often portrayed as ever-changing, but there are also many aspects of it that remain steady. Common sense, patience and a thoughtful engagement with the tools and information available are the key to good computing practices Remember, technology security is everyone’s responsibility!