Weekly Safety Briefings

Week 42: October 14 – October 20, 2019

Cyber Security

Every 14 seconds, a business falls victim to a computer network cyber-attack. These attacks access sensitive information, lead to money extortion, and interrupt normal business processes. A strong cyber security defense can help prevent damage from these attacks.

What is cyber security? Cyber security is the practice of protecting systems, networks, and programs from cyber-attacks. At an individual level, a cyber-security attack can result in anything from identity theft to the loss of important data, like government documents or family photos. On the business side, everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Think about what happens when their computer networks are compromised by cyber-attacks. In 2018, Erie County Medical Center became a victim of a cyber-attack. Essential medical systems shut down, making patient treatment very difficult until the attack was resolved.

Today, organizations spend around $500 million on cyber security each year because proper security is essential in keeping our society functioning. As individuals, cyber security is necessary for protecting our data and privacy. This week, we will identify the different types of cyber-security threats, explain the email phishing scams that are on the rise, talk about the benefits of using two-factor authentication, and discuss best practices for internet security.

Monday - Types of Cyber Security Threats

Cyber security reports show that at least 30% of organizations have at some point encountered cyber-attacks on their operations technology. Such attacks include hacking, data breaches, and abuse of cloud services. The common attacks you should watch out for are ransomware, malware, and phishing.

- **Ransomware** is a form of software that is designed to extort money from users by blocking access to files or the computer system until the ransom is paid. This is known as Distributed Denial of Service and is typically the driving motivation behind a majority of cyber-attacks. With this form of cyber-attack, paying the ransom does not guarantee file recovery or system restoration.
- **Malware** is a type of software that is designed to gain unauthorized access or cause damage to a computer or network system. A computer virus is one of the many types of malware.
- **Phishing** is a malicious form of social engineering where fraudulent data that looks reputable is sent out to users in order to gain access to sensitive data, such as credit card numbers or login information. Phishing is the most common type of cyber-attack. You can help protect yourself through education or a technology solution that flags and filters malicious activity.

Tuesday – Business Email Compromise (BEC)

A BEC phish is a malicious email which attempts to get the receiver to send or do something of value against their own organization’s interests by appearing or claiming to be from a boss, co-worker, or vendor with who the receiver has an existing relationship.

A multitude of businesses have lost thousands to millions of dollars due to BEC phishing scams.

Signs of a BEC

- If the email’s display “From” and “Reply To” email addresses are different.
- If the email is unexpected, has a strange, unexpected subject, or contains unusual grammar and typos.

Stressor events

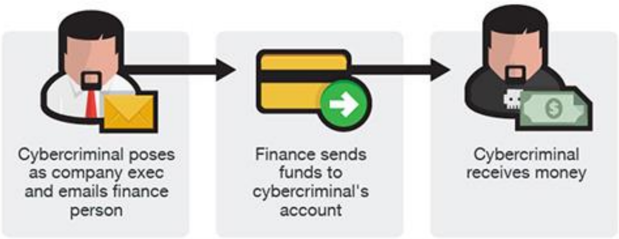
BECs almost always include one or more “stressor events” to help push the receiver past any little concerns they may have. A stressor event is anything that is intended to override the receiver’s logic with emotions. Common stressors include text similar to the following:

- “I need you to do this ASAP! There is a huge business deal depending on this.”
- “If this bill is not paid immediately it will be turned over to collections!”
- “I need the gift cards by the time my flight sets down!”
- “Don’t let me down, this is what I pay you for.”
- “If we do not get the W-2 list today payroll will be late!”
- “If you have not made your escrow payment at least 10 days before the closing meeting, you will not be able to close on your house.”

Wednesday – Common BEC Scams

The most common forms of BEC scams are fake invoices, tax scams, fraudulent wire transfers, online gift card requests, and executive or attorney fraud. Here are some common types of BEC scams to look out for:

- **Fake Invoices** are common in the business world. Many people receive fake invoices requesting payment for things like new computers or printing supplies arriving out of nowhere.
- **Tax Scams** are very common and can affect you in your personal life. In tax scams, scammers request confidential information about you or your company and file fraudulent tax returns. The IRS will not contact you through email to collect payment. These are always scams.
- **Fraudulent Wire Transfers** are one of the most common forms of BEC scams. These are where the scammers try to trick the receiver into wiring money electronically using specific instructions. The sender typically claims that an existing invoice is overdue and sends “updated instructions” from the email account of someone the victim frequently does business with.
- **Executive or Attorney Fraud** happens when scammers pretend to be lawyers or executives dealing with confidential and time-sensitive matters.


Cybercriminal poses as company exec and emails finance person
Finance sends funds to cybercriminal's account
Cybercriminal receives money

- **Online Gift Cards** are another common scam that affects businesses and individuals alike. Scammers pose as someone the victim knows, to encourage the victim to send them money because they had a car accident, unexpected bills, home loan payments called by the bank, etc. The scammer asks the victim to buy thousands of dollars in online gift cards, and forward the serial numbers and activation codes to the scammer. If your boss, relative, or friend has not spoken to you in person about purchasing gift cards, these emails are most likely a scam.

Thursday – Two-Factor Authentication

Two-Factor Authentication (also called 2FA) is a fantastic technology to protect your personal and professional information. 2FA adds another layer of security to online accounts beyond just a password. Instead of a password being your only form of data protection, 2FA requires the user to provide a second form of proof, usually a phone number, to allow access.

Once you have 2FA setup, your data is much more protected. Some websites even notify you of failed login attempts. If this happens, there are some additional precautions you can take such as logging out of that account, changing your password immediately, confirming the email address associated with that account, and changing other passwords that are tied to that email.

Many of the social media sites you use in your free time offer 2FA. A few are Facebook, Gmail, Twitter, Instagram, and Yahoo. To set up 2FA, navigate to settings and privacy and sign up.

Friday – Best Practices for Internet Security

Despite firewalls, antivirus software, security services, and identity protection, cyber-attacks are not 100% preventable. There are still many vulnerabilities to keep in mind.

In businesses or large organizations, security precautions such as 2FA are encouraged, but at home, it's easy to ignore the dangers because a mistake probably won't cost you your job. However, unsecure personal data can lead to identity theft, fraudulent transactions, and a headache! Follow these best internet security practices to help maintain your security on the web.

- **Use secure passwords!** Even today, the most common passwords are "123456" and "password". These passwords are not secure! Mix up your passwords with a combination of letters, numbers, and special characters. Remember to change your password every 3 months.
- **Don't reuse passwords!** Using the same password for every site give a hacker easy access to *all* your information if they gain access to one site. Make each password unique and secure!
- **Go with your gut.** If an external download or link looks funny or feels off, it probably is. Phishing emails are designed to imitate legitimate communication from a real person or company in order to obtain your information.

- **Backup your data.** Do this on a regular basis. You can use a cloud based tool to allow you to securely store and access your data from anywhere. However, consider storing sensitive information, such as government documents, on an external hard drive with a secure password.
- **Keep your software, programs, and applications up to date.** Never disable your firewall and always keep software up to date. Many times, updates come with patches for previous security issues and help protect your data.
- **Install, register, and renew a total antivirus, antispyware, and firewall package on every computer.** New computers may only come with trial software. When this trial runs out, your computer is left unprotected. Make sure to purchase, renew, or register a security package and install it on all your devices.

Has anyone here fallen victim to ransomware or malware? How about a computer virus? What do you think caused it and what did you do to fix it? Do you take security seriously now as you surf the web?