CYBERSECURITY

INTRODUCTION

Today many business communications and other tasks take place using the internet and connected devices. The ease and convenience of these methods of communication and ways of completing work have turned criminals to cybercrime to collect information and cause damage to a business. This lesson will cover what cybersecurity is, the types of cyberattacks used, the potential consequences, and ways to protect information.

WHAT IS CYBERSECURITY

Cybersecurity, also referred to as information technology security, is the protection of computers, internet-connected devices, and information from attack, theft, or damage. This is achieved through a variety of methods, including:

- Anti-virus and anti-malware software
- Technology security services
- Virtual Private Networks (VPNs)
- Strong passwords
- Firewalls
- Company technology policies and procedures
- Website security

TYPES OF CYBER ATTACKS

There are many ways for cyberattacks to be made. Attacks can include:

Malware

Malicious software that is used by cybercriminals to break into a network. Typical malware includes the use of:

- Spyware
- Ransomware
- Trojans
- Viruses
- Worms

Once the malware has broken into a network, it can do the following:

- Install additional software that could harm the network or device.
- Block access to critical components of the network. This is commonly completed with ransomware.
- Quietly and covertly obtain information from the hard drive through data transmission. This type of activity is typically achieved through spyware.
- Render a system inoperable by disrupting specific components of the infected device or network.

Social Engineering

Social engineering is the psychological manipulation of individuals to trick them into giving away sensitive information or making a security mistake that will allow the attacker to gain information. Common types of social engineering include:

- Phishing, otherwise known as an email or text campaign, aims to create a sense of curiosity, urgency, or fear in the victim. The aim is to have the victim reveal sensitive information, click onto links that will take them to malicious or look-a-like webpages, or install malware on the system by having the person open an attachment. This can include spear phishing, a more targeted version of phishing that focuses more on one individual or company, and whaling, targeting CEOs and other higher-ups in a business.
- Scareware, otherwise known as software, involves false alarms and fictitious threats. This type of attack attempts to trick an individual into thinking that their system has been infected by malware and prompts them to install software (or the actual malware) to correct the issue.
- Pretexting is an attack where the criminal tries to obtain sensitive information from a victim by stating the need for the information to perform a critical task.
- Baiting, when a cybercriminal uses a false promise or another method to pique a person's curiosity or greed. This type of attack usually involves a trap that steals information or infects a system with malware. The most common trap involves an infected flash drive left in an area where a victim will see it. Interested in what could be on the flash drive, the victim inserts it into their computer, where the flash drive installs malware onto the computer.

Man-in-the-Middle Attack

This type of cyber attack is when a cybercriminal intercepts communication between two parties by either looking at or modifying digital traffic between the two. Reasons for such an attack include:

- Stealing login credentials such as usernames and passwords
- Stealing personal information (credit card, bank, social security numbers, etc.)
- Spying on the victim
- To sabotage communications
- To corrupt data

This type of attack is usually made by entering two common points of entry:

- Unsecured public Wi-Fi
- Installed malware on an infected device

CONSEQUENCES OF CYBER ATTACKS

When a business finds itself the victim of a cyberattack, it could experience one or more consequences because of the damage:

- Reputational damage
- Theft of data
- Financial losses in the form of money that has to be spent on recovery efforts
- Fines for failure to comply with local, state, or federal regulations
- Loss of productivity
- Legal liability

WAYS TO PROTECT INFORMATION

Many of the cyberattacks covered can be prevented. You can do your part to protect your company's information by utilizing the following:

Passwords

Create strong passwords. To create a strong password, you should:

- Think of a phrase that is meaningful to you. Once you have a phrase, it is recommended to use a shortcut code or acronyms from the phase to create your password. For example: "To be or not to be, that is the question" could be turned into 2BorNot2B_ThatIsThe?. Please note that it is recommended that you avoid common substitutions, for example, replacing the "O" in House for a "0".
- Have a password that is at least eight characters long. However, many security experts recommend a minimum of 12 characters.
- Include numbers, symbols, capital letters, and lower-case letters in your password.
- Use a recommended password manager. If you are on a company computer, only use password managers that your company has approved.
- Use different passwords for different accounts.

After you have created your password, remember to change it at company-specified intervals.

When creating passwords, you should avoid the following:

- Using common words such as "Password."
- Using information that is easy to identify, such as your last name and birth year or a sequence of numbers such as 1234.
- Short passwords, stick to recommended character lengths.
- Do NOT reuse passwords because multiple accounts can be compromised.
- Do NOT write your passwords down either on paper or electronically.
- Do NOT share your passwords.

Email

Some of the most common attacks are through email. Before you open an email, click on any links, or open attachments, look for the following:

- The email is from the stated sender. Many criminals will try to pose as a legit person or company (Amazon, PayPal, eBay, etc.). Still, the email address may be off by one or more characters or come from a different address and hidden by the contact's name. To see the actual email address, hover your mouse over the name, and the address will appear. If the email does not match the sender, do NOT open. The same trick can apply to links.
- Check the spelling and grammar of the email.
- Do NOT open attachments if they come from an unknown sender.
- If the email does not seem typical for the sender, contact the stated sender to confirm if they sent the email or not.

You should only open emails that:

- Come from people that you know.
- You have received previous emails from them.
- Emails that you were expecting.
- Passes your company's anti-virus program test.

If you receive a suspicious email, contact either your information technology (IT) department or supervisor for direction on what to do with the email.

Wi-Fi

Another way cyberattacks commonly occur is through the use of unsecured or public Wi-Fi. To help minimize the chances of an attack occurring on company devices, you should:

- Do NOT assume that the network name is the actual wireless network for the location. Verify the name of the Wi-Fi network with the business owner.
- Treat all public Wi-Fi as though it were unsafe. Do not use sensitive websites (social networks, banks, etc.) on these Wi-Fi connections. If your company has policies for public Wi-Fi use, make sure to follow them.
- If you must use a sensitive website, use your cell phone.

Software

Additionally, you should NOT download any unauthorized software onto your company computer or devices. If you must have new software installed, either have your IT department do it for you or only download it from company-authorized sites. If you are unsure about a piece of software or the website to download software, please speak with your IT department or supervisor.

Security Updates

You should also make sure that all security updates for your computer and other devices have been performed. For many companies, this means making sure that you have your settings set to automatic updates. If you are unsure about your update settings, please speak with either your IT department or supervisor.

Websites

When going to a website, you should:

- Only go to trusted or company-authorized websites.
- Make sure that websites, where you submit information are legitimate and encrypted. You can check if a site is encrypted by looking at the URL in the browser bar. If the website begins with https, it means that the website has encryption and is secure. If the website begins with http, the site is unsecured and unencrypted.

If you are unsure about a website, please speak with your IT department or supervisor to see if it is a website you should be accessing.

CONCLUSION

To conclude, using the internet and internet-connected devices have become staples in the business world. The ease of accessibility to the web and its interactions with computers and other devices have made it an easy target for cybercriminals. These criminals use a variety of tactics to get information and do further damage. You, as an employee, play an essential role in your company’s cybersecurity system.