**CYBERSECURITY BEST PRACTICES**

The continued development of the internet has put the world at anyone's fingertips, which has made protecting personal information much more critical. With the constant development of new technology, comes massive innovation, and nonetheless, massive vulnerabilities. Due to these vulnerabilities, breaches and security implications by digital attacks are becoming far too common in today's fast-paced, technology-ruled world. As a result, innocent people are frequently becoming the victims of identity theft, phishing scams, and many other digital crimes. To help reduce cybersecurity-related threats at your business or organization, follow these essential cybersecurity best practices and share them with your employees and members for a well-educated front line of security.

**LOCK BEFORE YOU LEAVE** - Always lock your computer before leaving your desk. While this best practice seems trivial, one would be surprised at how often this is not done in the workplace or at home. Our computers house sensitive information and business processes and when a workstation is left unlocked there is a possibility an attacker could have unrestricted access to the system.

**THINK BEFORE YOU CLICK** - Once a link has been clicked it is possible that malicious software can install itself on the user's computer. Don't click on any link unless you know you can trust the source it is being sent from and you are certain of where the link will send you. If you are unsure about a link, the best thing to do is call the individual prior to clicking on the link. Double-checking the address where the link came from can aid in determining if the link is actually valid or not. You can hover the mouse over the link and check at the bottom of the browser to see if the actual URL link matches the link in the message.

**ALWAYS BE ON ALERT** - Social engineering is the attempt to gain unauthorized information or access to facilities through manipulation. The social engineer will research the organization to find information that could aid them. They typically call the victim with a made-up story designed to steal or access information. To help combat this, employees must be trained to be helpful, but stern when it comes to giving out information, as well as how to identify a potential social engineering attack. The employee should ask questions that would be difficult for the social engineer to answer. If incorrect information is provided, the employee should politely decline the individual, and alert management on the attempt to gain access to sensitive information.

**WATCH FOR THE "S"** - One of the most common methods of secure communication online is https. "Http" stands for hypertext transfer protocol, while the "s" at the end stands for security. It is important to make sure that "https" is displayed as part of a URL you visit, as it shows the authenticity of the security certificate on the webpage you are visiting. If you are surfing the web and attempt to access a webpage with a certificate that is expired or no longer secure; there is a chance you are accessing a website that could be loaded with malware, viruses, trojans, or even eavesdroppers.

> **TIP** - The best way to ensure you are on a website with a trusted certificate is by looking to the left of the URL and making sure there is a lock icon displayed. This means you are on a website with a trusted security certificate.

**USE STRONG PASSWORDS** – It is important to create strong, complex passwords for your systems. Here are some best practices for stronger passwords:

- Create passphrases instead of passwords. Individual words, even with slight variations, are easy to guess, but a series of words in a passphrase makes them more secure.
- For a non-privileged account, your complex password should be at least 12 characters long and should be updated every 90 days. Privileged account, the password should be at least 14 characters and should be updated every 45 days.
- User accounts should be temporarily disabled if more than 5 failed attempts are detected.

- Do not use the same password for multiple systems, websites, or accounts.
- Do not use single words that can be found in the dictionary of any language. Password-cracking tools often come with dictionary lists that can try thousands of common words.
- Do not use passwords that include personal information that could be easily accessed or guessed. This includes your birth date, SSN, phone number, or family member names.
- Do not store your list of passwords in a plain text file on your computer. Instead, there are several third-party password management programs that can help you stay secure.

**PROTECT YOUR MACHINE -** It is imperative to properly install and continually update software firewalls on every machine that contains digital information. A firewall helps to prevent unauthorized access to or from a network. It is the first line of defense when it comes to guarding digital information not intended for the public eye. Patching your operating systems and applications is a vital security practice as well. Patches are often released on a scheduled basis, however, there are times when patches are sent out "off schedule" in order to defend against newfound threats. When these patches come out, it is important to immediately install them. Keep in mind, as time passes new threats will be found, so system patching will be a constant security measure.

**MFA -** Implement multi-factor authentication (MFA) wherever possible - on all web applications that allow the feature, on your enterprise password manager, on your email, on Active Directory, etc. MFA is the hand sanitizer to account takeover attacks and can prevent 99.9% of account compromises. Yes, this extra layer of security adds a bit of inconvenience and another speed bump in the login process, but the risk it mitigates is well worth the additional step

**BE A CAUTIOUS "SURFER" -** Surfing the web can be risky if you aren't careful, so use caution. This is due to the fact that it is possible for users to pick up malicious code that can infect a computer with viruses and other unwanted malware with just one link click. It is also imperative you do not surf the web if you are on an account that has administrator privileges. If you pick up malware using a computer with administrator privileges, you have successfully just given the malware the same administrator rights that you have on your user account.

> **TIP** - Create a guest account that has access to the internet but has limited access to everything else to avoid this issue.

**MIND YOUR MOBILE MANNERS** - Today's mobile devices have made it far more convenient for people to surf the web, check emails, or update social media statuses from anywhere. However, when connected to the company network there is the potential to cause a lot of damage if one clicks on a bad link or visits the wrong page. If employees are allowed to use the company network, then proper security measures should be taken such as phone encryption, strong passwords, or even using the guest Wi-Fi network instead.

**EDUCATE, EDUCATE, EDUCATE -** If all users and employees have a basic understanding of security or know how to identify a potential incident, you are less likely to fall victim to an attack. Security awareness training should cover basic information security principles and response steps to social engineering and phishing - the two most common causes of data loss and breaches. If you are well-trained in the basics of network, system, and information security, it is a huge step in today's cyber world and is one of the best investments that can be made.