CYBERSECURITY AND YOU

The Cybersecurity Threat Landscape

In the digital, highly connected world we live in, it is especially important to ensure online safety at work, at school and at home. Every online interaction, including email, instant messaging, shopping, banking, and social media is an avenue and opportunity for a bad actor to attack, and quite possibly, steal personal information. This fact sheet provides simple information on the most common types of cyber-attacks, and includes straightforward helpful tips to help keep you and your family safe at home, work, school or on the go. And you don't have to be an IT professional to use these tips and put these good cyber hygiene tips into practice.

You are a target

Cybercrime is a big business, and bad guys know that targeting you or your organizations can be as simple as a phishing email designed to get you to share sensitive information or download malware. The days of the clumsy, badly worded, easy-to-spot phishing emails are gone. Today's threats are sleek, sophisticated and very slippery. They can slide right through your organization's software and spam filters and go straight to your inbox.

Let's take a tour of the threat landscape and show you some common ways bad guys try to trick you. Two of the most popular avenues you are likely to be targeted are:

Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you in order to get you to take some action that isn't in your own best interest. Phishing and spear phishing are forms of social engineering. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and/or credit card details by disguising as a trustworthy entity in an electronic communication. Hackers might use the phone, email, post service, or direct contact to try to trick you. Rule #1: Don't open emails from people you don't know and don't click on links you weren't expecting. Simply delete the message.

Web Browsing and Malware

The sad fact of web browsing is that dangers lurk around every virtual corner. From imposter websites to bogus pop-up windows to malware-laden ads and downloads, browsing sessions can be hazardous to you and your organization. Once your computer becomes infected, some malicious apps can swipe your password, other apps can take over your computer and allow a hacker to turn on your webcam to spy on you or listen to your conversations. One type of malware that's in the news a lot is called "ransomware." This malicious software can hold the files on your computer or your smartphone hostage until you pay a ransom!

NORTH Dakota | Information Technology
Be Legendary.™

HELPFUL TIPS TO BE #CyberAware

Top Ten Cyber Security Tips:

1. You Are A Target

Realize that you are an attractive target to hackers. Don't ever say "It won't happen to me."

2. Eight Characters is Not Enough

Practice good password management. Use a strong mix of characters, and don't use the same password for multiple sites. Don't share your password with others, don't write it down, and definitely don't write it on a post-it note attached to your monitor.

3. Lock It Up

Never leave your devices unattended. If you need to leave your computer, phone, or tablet for any length of time—no matter how short—lock it up so no one can use it while you're gone. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.

4. Practice Safe Clicking

Always be careful when clicking on attachments or links in email. If it's unexpected or suspicious for any reason, don't click on it. Double check the URL of the website the link takes you to: bad actors will often take advantage of spelling mistakes to direct you to a harmful domain.

5. Beware Of Browsing

Sensitive browsing, such as banking or shopping, should only be done on a device that belongs to you, on a network that you trust. Whether it's a friend's phone, a public computer, or a cafe's free WiFi—your data could be copied or stolen.

6. Back It Up

Back up your data regularly, and make sure your anti-virus software is always up to date.

7. Physical Cyber Safety

Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.

8. Share Less Sensitive Information

Watch what you're sharing on social networks. Criminals can befriend you and easily gain access to a shocking amount of information—where you go to school, where you work, when you're on vacation—that could help them gain access to more valuable data.

9. Cut Out The "Middle Man"

Offline, be wary of social engineering, where someone attempts to gain information from you through manipulation. If someone calls or emails you asking for sensitive information, it's okay to say no. You can always call the company directly to verify credentials before giving out any information.

10. Stay On Top Of Your Accounts

Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, it could be a sign that you've been compromised.

Source:
cybintsolutions.com/10-important-cyber-security-tips-users/

Remember:

According to the latest threat report from NetIQ, every minute, more than $1.1 million is lost to cyber-crime and 1,861 people fall victim to a cyber-attack. Important things to remember include:

- Don't open emails from people you don't know and don't click on links you weren't expecting. Simply delete the message.
- Social Media
  - Do not post confidential information on public websites, forums, blogs, or social media sites.
  - Posting personal information on these sites gives cyber criminals information to use against you.
- WiFi Security
  - Connect to trusted wireless networks only.
  - If connecting to a guest or public network, do not access confidential information (work, banking info, etc.) unless you are using a VPN connection.

Stay vigilant, remember these important precautions, and help protect yourself, our state and our citizens!