National Cybersecurity Awareness Month

Cybersecurity Awareness Month is an international initiative that educates everyone about online safety and empowers individuals and businesses to protect their data from cybercrime.

Even amidst large-scale data breaches and cyberattacks, Cybersecurity Awareness Month reminds everyone that there are simple, effective ways to keep yourself safe online and protect your personal data.

The 2025 theme of Cybersecurity Awareness Month is simply ***Stay Safe Online*****,** here to remind us that there are simple ways to protect yourself, your family and your business from online threats. Protecting yourself online doesn't have to be complicated or expensive. A few simple habits can dramatically reduce your risk of falling victim to cybercrime. While you can never be "hackproof," you can become resilient in the online world.

At the heart of online safety there are four essential behaviors that the National Cybersecurity Alliance call the "**Core 4**." These simple steps will help shield your personal information, protect your accounts, and keep your devices secure.

Meet the Core 4: Cybersecurity basics

1. Use long, unique, and complex passwords (and a password manager!)

Your passwords are the first line of defense between a criminal and your sensitive information.

Here's how to have amazing passwords:

- **Every password must be long, unique, and complex.** Nowadays, every password should be at least 16 characters long, which significantly overwhelms password-cracking programs. Use a random mix of letters, numbers, and symbols. And every account needs a unique password.
- **Don't reuse passwords!** Every account needs a unique password. Unfortunately, making little changes, like adding numbers or switching out an S with a $, doesn't count as a unique password.
- **Use a password manager to store and generate strong passwords.** If you're wondering how to manage so many unique, long passwords, the answer is a password manager! There are many free, secure options. Password managers are the safest way to store your passwords. If you prefer to keep a password notebook, treat it like cash.

2. Enable multifactor authentication (MFA)

Multifactor authentication (sometimes called 2FA) adds an extra security layer by requiring something more than just your password to log in. Think of it as using two locks on your digital door instead of only one. This could be:

- A one-time code sent to your phone
- A biometric scan like a fingerprint scan or FaceID
- A physical security key

Enable MFA on your accounts – especially email, banking, and social media. It's a simple way to supercharge the security on your accounts. Also, never share MFA codes with anyone – this includes not sharing them over the phone, through texts, or via email. Only scammers will ask for MFA codes.

3. Keep software updated

Software updates don't just bring new features. They often fix security flaws that criminals exploit. It usually takes a few minutes, but updates are worth it. Here are some tips:

- Turn on automatic updates when possible for your devices and apps – you can usually find these options in your Settings menu.
- Install updates promptly for your operating systems, browsers, antivirus tools, and apps.
- Don't click Remind Me Later – the security is worth it.
- Remember your phones, smartwatches, and tablets are computers – keep these devices updated as well!

4. Watch out for phishing and scams

Phishing remains the most common online threat. Criminals send fake emails, texts, or social media messages to trick you into revealing sensitive information or clicking malicious links. These messages aim to get you to click before you think by playing your emotions. Scammers will even call you! Here's how to look out for phishing and scams:

- Be highly skeptical of unexpected messages, especially those urging immediate action or asking for personal details.
- Phishing emails can light up positive emotions ("You've won our sweepstakes!") or negative ones ("You've been hacked!").
- Don't click suspicious links or download unexpected attachments.
- Report phishing attempts to your email provider, social media platform, or IT department.
- If you're unsure if a message is legit, ask a friend, coworker, or family member. A second set of eyes can be invaluable in spotting scams.

More simple tips to stay safe online!

5. Back it up

The best way to protect your valuable work, music, photos, data, and other digital information is to make copies and store them safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you can restore the data from a backup. If you break your computer or it crashes, you won't lose the data along with the device. Use the **3-2-1 rule** as a guide:

- Keep at least three (3) copies of your data.
- Store two (2) backup copies on different storage media, like on the cloud or on an external hard drive.
- One (1) of copy should be located offsite – this includes the cloud!

Today, one of the easiest backup storage options is backing up to the cloud – the cloud is a network of secure computer servers that you can access through an online account.

6. Check your privacy settings

Every time you sign up for a new account, download a new app, or get a new device, configure the privacy and security settings to your comfort level for information sharing.

- Think about what information an app is asking for and if it's necessary for the app to function.
- Think about who can see your profile.
- Audit your apps, platforms, and games every couple of months and delete the ones you don't use.

7. Share with care

When you're having fun on social media, think before posting about yourself and others. Consider what a post reveals, who might see it, and how it might affect you or others. With every post, think about:

- Who will see it?
- Could it reveal personal information?
- How might it affect your digital reputation?

8. Report phishing

One of the best ways to take down criminals is by reporting phishing attempts, and nowadays its easier than ever.

- If the email came to your work email address, report it to the Metro ITS Help Desk.
- If you're at home and the email came to your personal email address, most email programs and social media platforms allow you to report phishing.

Do not click on any links (even the unsubscribe link) or reply back to the email. Also, don't keep that phishing message around – delete it ASAP. You can further protect yourself by blocking the sender from your email program, social media platform or phone.

9. Don't reply to mistaken texts or messages

A common scam nowadays starts with a seemingly "mistaken" text, where an unknown number contacts you, and it seems like a mistake.

- The text can be simple ("How are you") or elaborate ("Do you have a dentist recommendation?")
- If you respond, the other person will strike up a conversation and "friendship"
- These mistaken text scams, which are also called pig butchering scams, can last for weeks or months before the criminal requests money or tells you about an exciting investment opportunity.

Not responding to a text or call from a number you don't know isn't rude. It's safe!

10. Use secure wi-fi

With your home router, remember to change the default password. When you're out and about, public wi-fi is convenient, but its security might be questionable:

- Avoid accessing sensitive accounts like banking or email.
- Use a VPN or your phone's hotspot for a more secure connection.
- Turn off auto-connect for wi-fi and Bluetooth. These settings can make your device connect to unknown or malicious networks automatically.
- On public computers in hotels, libraries, or cafes, avoid accessing personal accounts. If you must, always click "log out" – closing the browser isn't enough.

Links to Additional Cybersecurity Topics

Spam and Phishing: Cybercriminals spend each day polishing their skills in luring people to click on malicious links or open bad attachments.

Online Shopping**:** Just like you would watch your wallet when at the store, it's crucial to protect yourself when shopping online.

Malware, Botnets and Ransomware**:** The internet is a powerful, useful tool, but in the same way that you shouldn't drive without buckling your seat belt or ride a bike without a helmet, you shouldn't venture online without taking some basic precautions.

Romance Scams: We all know that people online aren't always as they appear. However, tens of thousands of internet users fall victim to online romance scams each year, and it can happen to anyone.

Tax Time Safety**:** Tax season can be a stressful time for many Americans, and while scams are prevalent year-round, there is often a greater proliferation during tax time. Stay safe online while filing your taxes with these best practices, tips and resources.

Vacation and Travel Tips**:** Stay cyber safe while away from home by following some simple practices to help keep your devices safe and your vacation plans from going awry.

Online Safety Tips for Older Adults: Being online today is now a daily routine for most of us, no matter your age.

How to Spot and Avoid Phone Scams: Cybercriminals are calling, but you don't have to pick up!