Online Safety Basics

Online Safety Basics - With a little prep, you can shield your information online and secure your digital systems and devices.

With a little knowledge, a dash of effort, and a few minutes of time, you can keep your sensitive data and computer systems locked down tight. Cybersecurity does not have to be intimidating! It does not require a large investment of time or money! In fact, you can secure your digital life with trusted free tools, and now many cybersecurity best practices can be automated.

Literally a few minutes of preparation can keep you safe. The benefits of a few moments of research, preparation, and action far outweigh the potential costs of losing your unprotected data in a breach or having your identity stolen. And even if some of your data is compromised, if you follow some simple guidelines, you can ensure that the damage will be minimal.

Here are our 10 top tips to stay safe online:

1. **Keep a Clean Machine**: Keep all software on internet connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware. If you want to "set it and forget it," configure your devices to automatically update or to notify you when an update is available. Learn more about software updates.

2. **Create Long, Unique Passwords:** Length trumps complexity. Strong passwords are at least 12 characters long and include letters, numbers and symbols. Ideally, your password is not recognizable as a word or phrase. And, yes, you should have a unique password for each online account. Sounds hard to remember? Using a password manager has never been easier (we'll say more in a second) – many smartphones and web browsers include password managers and even suggest strong passwords. Otherwise, we recommend coming up with a password that is actually a "passphrase," that is, a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember, such as ILov3StayingSafeOnl1ne! (but don't use that one).

3. **Use a Password Manager**: It's time to ditch the notebook if that's where you keep your passwords – use it for doodles. Ditto for that Notes app or word processing doc – save the hard drive space. Instead, the simplest, most secure way to manage unique passwords is through a password manager application. A password manager is software created to manage all your online credentials like usernames and passwords. Many are free. Often, browsers and device operating systems include password management programs. Password managers store your passwords in an encrypted database (think of it as your personal data vault). These programs also generate new

passwords when you need them. Really, it has never been easier to safely generate, store and access your passwords.

4. **Enable Multi-Factor Authentication:** Multi-factor authentication (MFA), sometimes called 2-factor authentication, adds a whole other level of security to your key accounts. MFA includes biometrics (think face ID scans or fingerprint access), security keys or apps that send you unique, one-time codes when you want to log on to a sensitive account. We recommend you use MFA whenever offered. Read more about the different types of MFA.

5. **Think Before You Click**: What's the most common way for cybercriminals to get your sensitive information? It's when you click on something you shouldn't have. Malicious links in email, tweets, texts, posts, social media messages and malicious online advertising (known as malvertising) are a direct way for hackers to get your sensitive information. Don't make it easy for them. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Whenever you get an email or message, count to five – usually that's all the time you need to determine if the missive seems authentic or not.

6. **Report Phishing:** One of the best ways to take down cybercriminals is by reporting phishing attempts, and nowadays its easier than ever. If the email came to your work email address, report it to the IT Help Desk or security team as quickly as possible. If you're at home and the email came to your personal email address, do not click on any links (even the unsubscribe link) or reply back to the email. Most email programs and social media platforms allow you to report phishing attempts. But 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.

7. **Use Secure Wifi:** Public wireless networks and hotspots are unsecured, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Limit what you do on public WiFi. Especially avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.

8. **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 will be able to 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 to backing up your data. The rule is: keep at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) of them located offsite. One of these storage possibilities can be backing up to the cloud, which are secure computer servers you can access through an account.

9. **Check Your Settings:** Every time you sign up for a new account, download a new app or get a new device, immediately configure the privacy and security settings to your comfort level for information sharing. Regularly check these settings to make sure they are still configured to your comfort. Audit your apps, platforms and games every few months and delete ones you no longer use – then you don't need to check their settings!

10. **Share with Care:** Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

Learn More

- **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.
- **Back it Up:** Protect yourself against data loss by making backups – electronic copies – of important files.

- **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.
- **Spring Clean Your Online Life:** A messy digital life leaves your money, identity and personal information vulnerable to bad actors. Keep yourself and your family safe online with these quick tips for a spotless digital space.
- **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.

Additional Resources

- Cybersecurity & Infrastructure Security Agency: Cybersecurity Tips
- Federal Trade Commission: Cybersecurity Basics
