



Protecting You and Your Business



ONLINE PRIVACY

The Internet touches almost all aspects of our daily lives. We are able to shop, bank, connect with family and friends, and handle our medical records all online. These activities require you to provide personally identifiable information (PII) such as your name, date of birth, account numbers, passwords, and location information. Stay safe online with these tips:

- ✓ **Shake up your password protocol.** Consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts.
- ✓ **Be up to date.** Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans.
- ✓ **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software.
- ✓ **Play hard to get with strangers.** Cyber criminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate—or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option.
- ✓ **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans.
- ✓ **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use.
- ✓ **Stay protected while connected.** Before you connect to any public wireless hotspot—such as at an airport, hotel, or café, be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. Only use sites that begin with "https://" when online shopping or banking.