BE CYBER SMART
#CyberMonth

CYBERSECURITY AWARENESS
DO YOUR PART. #BECYBERSMART

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. #BeCyberSmart when sharing personal information online to reduce the risk of becoming a cybercrimes victim.

DID YOU KNOW?

- 72% of Americans believe that most of what they're doing while online is being tracked by advertisers, technology firms and other companies.[1]
- Over half of Americans (52%) say they have decided not to use a product or service because they were worried about how much personal information was being collected about them.[1]
- Data breach costs rose from USD 3.86 million to USD 4.24 million in 2021.[2]
- Compromised credentials, like passwords, were responsible for 20% of breaches at an average breach cost of USD 4.37 million.[2]

SIMPLE TIPS

- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.
- **Shake up your password protocol.** Use 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. Read the Creating a Password Tip Sheet for more information.
- **Keep up to date.** Keep your software updated to the latest version available. Maintain your security settings to keep 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 IT, Protect IT.** 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. Read the Phishing Tip Sheet for more information.
- **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 to no longer receive messages from a particular sender.

- **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. Disable location services that allow anyone to see where you are—and where you aren't—at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.
- **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. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **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.

CONTACT THE CISA CYBERSECURITY AWARENESS MONTH TEAM

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please email our team at CyberAwareness@cisa.dhs.gov or visit www.cisa.gov/cybersecurity-awareness-month or staysafeonline.org/cybersecurity-awareness-month/ to learn more.

RESOURCES

1. Auxier, Brooke, "How Americans see digital privacy issues amid the COVID-19 outbreak." Pew Research Center: Fact Tank. May 4, 2020. https://www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/
2. IMB, "Cost of a Data Breach Report 2021." IMB Security. July 2021. https://www.ibm.com/security/data-breach