BE CYBER SMART
#CyberMonth

CYBERSECURITY AWARENESS
DO YOUR PART. #BECYBERSMART

CYBER SECURE AT WORK

Businesses face significant financial loss when a cyber-attack occurs. In 2020, a sharp increase was reported in cyber-attacks that target businesses using stolen logins and passwords.[1] Cybercriminals often rely on human error—employees failing to install software patches or clicking on malicious links—to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of everyone to keep data, customers, and capital safe and secure. #BeCyberSmart to connect with confidence and support a culture of cybersecurity at your organization.

SIMPLE TIPS

- **Treat business information as personal information.** Business information typically includes a mix of personal and proprietary data. While you may think of trade secrets and company credit accounts, it also includes employee personally identifiable information (PII) through tax forms and payroll accounts. Do not share PII with unknown parties or over unsecured networks.
- **Don't make passwords easy to guess.** As "smart" or data-driven technology evolves, it is important to remember that security measures only work if used correctly by employees. Smart technology runs on data, meaning devices such as smartphones, laptop computers, wireless printers, and other devices are constantly exchanging data to complete tasks. Take proper security precautions and ensure correct configuration to wireless devices in order to prevent data breaches. For more information about smart technology see the Internet of Things Tip Card.
- **Stay 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.
- **Social media is part of the fraud tool set.** By searching Google and scanning your organization's social media sites, cybercriminals can gather information about your partners and vendors, as well as human resources and financial departments. Employees should avoid oversharing on social media and should not conduct official business, exchange payment, or share PII on social media platforms. Read the Social Media Cybersecurity Tip Sheet for more information.
- **It only takes one time.** Data breaches do not typically happen when a cybercriminal has hacked into an organization's infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual sources, do not click on unknown links, and delete suspicious messages after reporting or forwarding all phishing attempts to a supervisor, so that any necessary organizational updates, alerts, or changes can be put into place. For more information about email and phishing scams, see the Phishing Tip Sheet.

IF YOU WORK FROM HOME

- **Only use approved tools.** Only use organization-approved software and tools for business, including company provided or approved video conferencing and collaboration tools to initiate and schedule meetings.
- **Secure your meeting.** Tailor security precautions to be appropriate for the intended audience. Plan for what to do if a public meeting is disrupted. Take precautions to ensure your meeting is only attended by intended individuals.
- **Secure your information.** Tailor your security precautions appropriately to the sensitivity of your data. Only share data necessary to accomplish the goals of your meeting.
- **Secure yourself.** Take precautions to avoid unintentionally revealing information. Ensure home networks are secured. For more information, visit Telework Reference Materials For The At-Home Worker.

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. Identity Theft Resource Center. (2021). *2020 Data Breach Report* https://www.idtheftcenter.org/annual-reports/