BE CYBER SMART
#CyberMonth

CYBERSECURITY AWARENESS MONTH 2021: DO YOUR PART. #BECYBERSMART

DID YOU KNOW?

- Human error accounts for 95% of all cybersecurity breaches[1]
- 77% of organizations do not have a cybersecurity plan[2]

HOW DO I APPROACH CYBERSECURITY AS A BUSINESS, SCHOOL, OR INDIVIDUAL?

As cyber-attacks and their consequences grow, the imperative for cybersecurity and resilience is becoming increasingly important, not just to homeland security, but businesses, schools, and individuals. Attackers use a variety of vulnerabilities and phishing attacks to compromise the security of networks and devices. To approach this threat effectively and protect your networks, it is even more necessary to become familiar with cyber essentials.

SIMPLE TIPS

- **Be aware of risk.** Be aware of possible risk such as malware viruses, ransomware, and phishing. It's also important for everyone in your organization to be aware of the possible risk and threats that could occur should your systems become affected by any of these threats.
- **Train your employees.** Employees and emails are the foremost cause of data breaches for small businesses because they are a direct path into your system. Train and inform your employees and even students on basic Internet practices. This will go a long way in preventing cyber-attacks.
- **Keep antivirus software updated.** Make sure all your computers, Internet-connected devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.
- **Secure your networks.** Secure your network by using a firewall and encrypting information. This is also useful for the individual. If you have a Wi-Fi network, secure it by hiding the network, by setting up a wireless access point or router so it doesn't broadcast the SSID service set identifier and network name. Protect the router and put the password on.
- **Use strong passwords.** Creating strong passwords is an easy way to improve your cyber security. Try to use different passwords for different accounts. For businesses and schools make it a requirement that strong passwords include one uppercase letter, one lowercase letter, at least one number and 10 or more characters. 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.
- **Backup your data.** Routinely back up data on all computers. After backing up your systems make sure the device that the backup is stored on is offline. Backup data could include word processing documents databases, electronic spreadsheets, financial files, human resources files, accounts receivable/payable files and student information.

- **Control physical access.** Control access to backup data as well as school or business computers by unauthorized individuals. Make sure to use separate user accounts for each employee or student and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.
- **Play hard to get with strangers.** Links in emails and online posts are often the way cybercriminals compromise your computer. If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments found in that email. Be cautious of generic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.
- **Think before you act.** Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization but still looks "phishy," reach out to them via customer service to verify the communication.
- **Protect your personal information.** If people contacting you have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.
- **Be wary of hyperlinks.** Avoid clicking on hyperlinks in emails and hover over links to verify authenticity. Also ensure that URLs begin with "https." The "s" indicates encryption is enabled to protect users' information.
- **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 How-To-Guide for more information.
- **Install and update anti-virus software.** Make sure all your computers, Internet-connected devices, phones, and tablets are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.

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 cisa.gov/cybersecurity-awareness-month or staysafeonline.org/cybersecurity-awareness-month/ to learn more.

RESOURCES

1. Why Human Error is #1 Cyber Security Threat to Businesses in 2021. (2021, February 4). The Hacker News. https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html
2. Majority of Organizations Lack a Cybersecurity Incident Response Plan. (n.d.). Www.meritalk.com. Retrieved September 2, 2021, from https://www.meritalk.com/articles/majority-of-organizations-lack-a-cybersecurity-incident-response-plan/#:%7E:text=Despite%20the%20near%20constant%20threat%20of%20a%20cyberattack%2Cc