BE CYBER SMART
#CyberMonth

CYBERSECURITY AWARENESS MONTH 2021: DO YOUR PART. #BECYBERSMART.

WHY IS CYBERSECURITY IMPORTANT?

Cybersecurity is the art of protecting networks, devices, and data from unlawful access or criminal use and the practice of guaranteeing confidentiality, integrity, and availability of information. Communication, transportation, shopping, and medicine are just some of the things that rely on computers systems and the Internet now. Much of your personal information is stored either on your computer, smartphone, tablet or possibly on someone else's system. Knowing how to protect the information that you have stored is of high importance not just for an individual but for an organization and those in it.

DID YOU KNOW?

- As of 2021, there is a ransomware attack every 11 seconds, up from 39 seconds in 2019[1,2]
- 43% of cyber-attacks target of small businesses, and they have grown 400 percent since the outbreak began [3,4]

HOW CRIMINALS LURE YOU IN

Companies and organizations in the United States, as well as multiple foreign governments, were harmed by theft of intellectual property, trade secrets, and other highly valuable information by Advanced Persistent Threat (APT). By establishing initial access, the APT exploits user and administrator credentials, enables lateral movement within the network, and locates high value assets to exfiltrate data. To reduce risk, network defense procedures should be implemented and comply with best practices. These guidelines can facilitate managing the risk and mitigating the threat.[5]

- By stealing compromised credentials, an attacker can obtain victim identity information
- Criminals create new email accounts and hack existing ones to conduct social engineering attacks
- Spear phishing emails are sent containing malware and malicious attachments
- Malware is used to exploit various common vulnerabilities and exposures by exploiting software vulnerabilities in applications.

SIMPLE TIPS

- **Use antivirus software.** Antivirus software is very important. It's an important protective measure useful against cyber criminals and malicious threats. It can automatically detect, quarantine, and remove types of malware. Automatic virus updates should always be enabled to ensure maximum protection against the latest threats.
- **Keep software up to date.** Attackers have been known to take advantage of well-known problems and vulnerabilities. Making sure you install software patches and utilizing automatic updates for your operating system will help protect you from attackers.
- **Utilize a firewall.** Firewalls can prevent some attacks by limiting malicious traffic before it can enter a computer

system. It also restricts unnecessary outbound communications. Some devices and operating systems come with a firewall preinstalled. However, make sure your device is currently using a firewall and that it is configured properly.

- **Utilize strong passwords.** Creating passwords that will be difficult for cybercriminals to guess is vital. Use different passwords for different programs and devices. It is also best to use long, strong passphrases or passwords that consist of at least 15 to 16 characters. 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.
- **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.
- **Watch for Phishing.** The goal is to gain information about you and use your information to make unauthorized purchases or gain access to a secure system. Be suspicious of unexpected emails and always check email address sources to make sure the email is not coming from a fake website.

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. Braue, D. (2021, June 3). *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Cybersecurity Ventures. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
2. Talalaev, A. (2021, June 30). *Website Hacking Statistics You Should Know in 2021*. Patchstack. https://patchstack.com/website-hacking-statistics/
3. Small Business Trends LLC. (2020, March 10). *43% of Cyber Attacks Still Target Small Business - Ransomware On Rise*. Small Business Trends. https://smallbiztrends.com/2019/05/2019-small-business-cyber-attack-statistics.html
4. Charlotte Today. (2021, August 30). *Protecting small businesses from cyber attacks*. WCNC-TV. https://www.wcnc.com/article/entertainment/television/charlotte-today/protecting-small-businesses-from-cyber-attacks-malware-ransomware-viruses/275-168d2459-085a-4515-8f4e-6c6f9a59abb3
5. CISA. (2021, July 19). *Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department*. CISA. https://us-cert.cisa.gov/ncas/alerts/aa21-200a