BE CYBER SMART
#CyberMonth

CYBERSECURITY AWARENESS MONTH 2021: DO YOUR PART. #BECYBERSMART

CYBERSECURITY 101

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 elses 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?

- There is a cyber attack every 39 seconds[1]
- 43% of Cyber Attacks target small business[2]

HOW CRIMINALS LURE YOU IN

The following messages from the Federal Trade Commission's OnGuardOnline are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."
- To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit https://www.irs.gov/privacy-disclosure/report-phishing.

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

include add firewall. Make sure your device is currently using a firewall and that it is configured properly.

- **Utilize strong passwords.** Selecting creating passwords that will be difficult or as cybercriminals to guess is of much importance. 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 Strong 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.
- **Phishing.** The goal is to gain information about you and steal your information to make unauthorized purchases. So be suspicious of unexpected emails and always check your sources email address.

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. Talalaev, A. (2021, June 30). *Website Hacking Statistics You Should Know in 2021*. Patchstack. https://patchstack.com/website-hacking-statistics/
2. 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