TIP SHEET

WHY CYBER SECURITY IS IMPORTANT

AND HOW TO APPROACH IT

WHY CYBERSECURITY IS IMPORTANT AND HOW TO APPROACH IT

Cybersecurity is the art of protecting networks, devices, and data from unlawful access or criminal use. Today, much of your personal information is stored either on your computer, smartphone, tablet, other smart devices or apps like Alexa, smart watches, etc. Knowing how to protect your digital devices is important not just for individuals, but for organizations, as well.

The purpose of cybersecurity is to maintain confidentiality, integrity, and availability of data.

- **Confidentiality**. Ensures the data is accessible by only those who need it—once you post information on the internet, it is there forever.
- **Integrity.** Ensures the data is accurate—corrupt data is of no value to those who need it.
- **Availability**. Ensures the data can be accessed by all those who need it, whenever they need it—fast and reliable connectivity makes computer systems operate more effectively.

Attackers exploit vulnerabilities by using a variety of phishing attacks to compromise the security of networks and devices. To protect your networks, it is vital to become familiar with cyber basics:

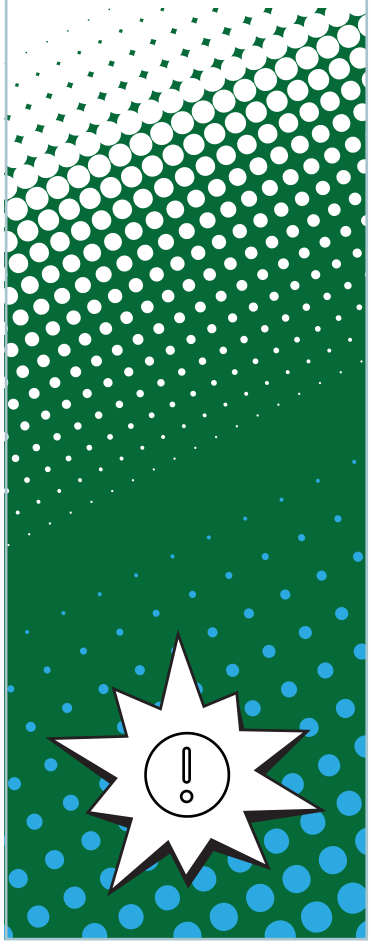
- Attackers can obtain victim identity information by stealing compromised credentials.
- Criminals create new email accounts and hack existing ones to conduct social engineering attacks. A social engineering attack is when an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- Phishing emails contain malware and malicious attachments.
- Malware exploits various common vulnerabilities in software and other applications.

KNOW YOUR CYBER BASICS

- **Protect your personal information.** If people have key details from your life, your job title, birth date, and full name, which you may have shared online, they can attempt a phishing attack on you. Cybercriminals can also try to manipulate you into skipping normal security protocols.
- **Be wary of hyperlinks or attachments from suspicious or unknown/ untrusted sources.** Inspect hyperlinks in emails. Hover over links to verify their source. When making a transaction, ensure that URLs begin with “https.” The added “s” indicates encryption is enabled to protect users’ information.

FOLLOW-ON RESOURCES

- Phishing Tip Sheet
- Ransomware Fact Sheet
- Password and Password Managers Tip Sheet
- Multi-Factor Authentication Guide
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

- **Use anti-virus software and keep it up to date.** This is an important protective measure against cybercriminals and malicious threats. It can automatically detect, quarantine, and remove malware. Enable automatic virus updates to ensure maximum protection against the latest threats.
- **Use long, random and unique passwords.** Creating strong passwords is vital to cybersecurity. Use different passwords for different programs and devices. Use long passwords or passphrases to protect your accounts. Always use strong passwords of 12 or more characters.
- **Use a password manager to store your personal passwords for each account.** This tool is commonly used to generate long, random and unique passwords for web applications. Once generated, they are put in a centralized vault, and encrypted with one master password.
- **Strengthen your login protection.** Enable multi-factor authentication (MFA) to ensure that you are the only person who has access to your account. Use it for email, banking, social media, and any other password-protected services. 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.
- **Backup your data.** Routinely backup data on all computers, and make sure that the backup is stored offline. Backup all data including documents, databases, spreadsheets, financial files, human resources files, accounts receivable/payable files, and more.
- **Control physical access.** Prevent access to your backup data by unauthorized individuals. Make sure to use separate user accounts for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

WHAT TO LOOK FOR

- **Watch for phishing.** Phishing enables cybercriminals to collect your information to make unauthorized purchases or gain access to a secure system. Always check the sender's email address to make sure that it is authentic. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account is in jeopardy. If you suspect an email is fraudulent, reach out to the company or person directly on a separate, secure platform.
- **Be aware of risk.** In addition to malware and phishing viruses, the number one security threat is ransomware. Ransomware is a form of malware designed to encrypt files on any device, rendering any file, and the systems that rely on them, unusable.
- **Train your employees regularly on cyber basics.** Employees and emails are the foremost cause of data breaches for small businesses because they are a direct path into your system. Visit the National Initiative for Cybersecurity Careers and Studies (NICCS).

LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

FOLLOW-ON RESOURCES

- Phishing Tip Sheet
- Ransomware Fact Sheet
- Password and Password Managers Tip Sheet
- Multi-Factor Authentication Guide
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime