Frank LaRose
Ohio Secretary of State

ARE YOU CYBER SAFE?

CYBERSECURITY BASICS FOR SMALL BUSINESSES

by the Office of the Ohio Secretary of State

DEAR ENTREPRENEUR,

I'm pleased to present our **Cybersecurity for Small Businesses booklet.** This informative guide is designed to cover the basics of cybersecurity and provide tools and tips you can use to protect yourself, your business, and the public's trust.

In today's digital world, cyber criminals have increasingly targeted not only major corporations and governments but also individuals and small businesses.

Nearly half of all cyberattacks are now directed at small and medium-sized businesses. The good news is there are several steps any organization can take to secure their digital footprint, even if they don't have the time or resources to invest in designated security experts.

Combating this threat has been one of my office's top priorities – both in my role supporting Ohio's entrepreneurs and as our state's chief elections officer. I hope the information we've gathered will be beneficial as you start and grow your business.

Yours in service,

Frank LaRose
Ohio Secretary of State

TABLE OF CONTENTS

01. INTRODUCTION TO CYBERSECURITY

Cybersecurity includes all measures taken to protect a computer or computer system against unauthorized access or attack. This includes everything from application security that keeps software and devices free of threats, to information security and disaster recovery.

Importantly, establishing good cybersecurity practices doesn't necessarily depend on access to technical experts or IT personnel – it simply involves educating staff about the commonsense steps they can take to protect your organization.

COMMON MISCONCEPTIONS

Employees empowered with the resources and knowledge to protect your organization from cyber threats are one of the best lines of defense you can have. Part of their training should involve dispelling often-quoted cybersecurity misconceptions.

My business doesn't have the time, money, or expertise to prioritize cybersecurity.

Our business is too small to be targeted by cyber criminals. We don't have anything to worry about.

We don't collect any valuable or sensitive information that needs to be protected.

Cyberattacks are rare and unlikely to be a concern in my area.

WHY SHOULD A SMALL BUSINESS WORRY ABOUT CYBERSECURITY?

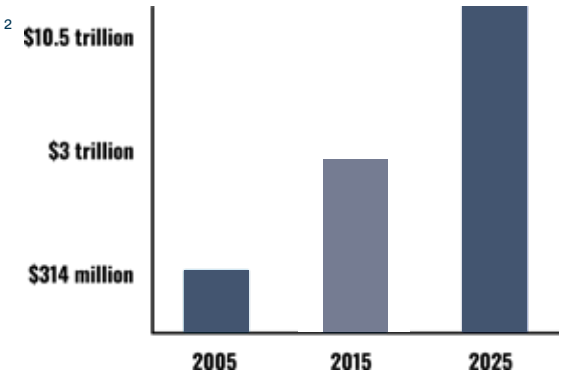
The threats and aftermath of cybersecurity breaches are all around us. Media reports regularly highlight the impacts of the latest data breach, the countless confidential and sensitive records that have been compromised, and the trillions of dollars in damages that occur every year – not to mention the cost of diminished public confidence in our institutions.

While many headlines about cyberattacks involve major corporations or government entities, the truth is they happen at all levels.

CYBERSECURITY IN NUMBERS

[1] **$10.5 TRILLION**

[2]



ESTIMATED GLOBAL COST OF CYBERCRIME BY 2025

[3] **61%**

OF SMALL BUSINESSES REPORT AT LEAST ONE CYBERATTACK IN THE PAST YEAR

43%

OF CYBERATTACKS TARGET SMALL & MEDIUM SIZED BUSINESSES

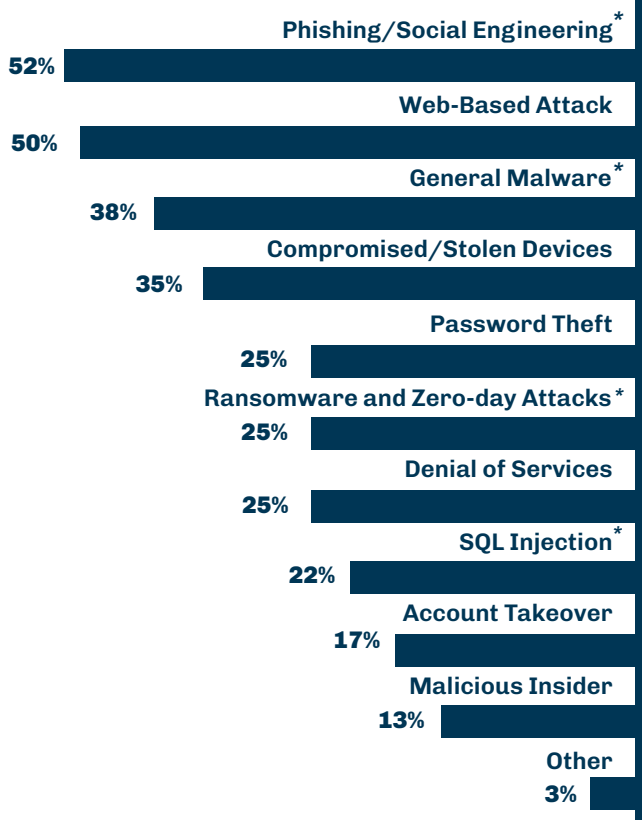
[1] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[2] https://www.blackfog.com/smbs-were-victims-cyberattack/
[3] https://www.sba.gov/blog/2023/2023-09/cyber-safety-tips-small-business-owners#:~:text=In%20fact%2C%20according%20to%20a,employees%20are%20protected%20from%20cyberattacks.

02. HOW ARE BUSINESSES BEING ATTACKED?

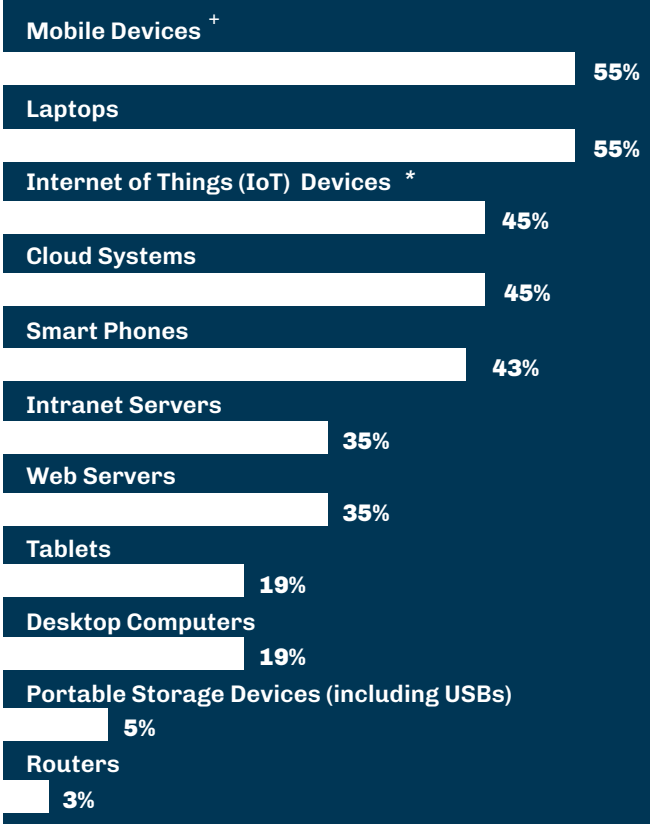
Cyberattacks are a growing threat for small businesses and the U.S. economy. According to the FBI's Internet Crime Report, the cost of cybercrimes in the United States reached $10.3 Billion in 2022.

Small businesses are attractive targets because they have information that cybercriminals want, and they typically lack the security infrastructure of larger businesses. According to a recent SBA survey, 88% of small business owners felt their business was vulnerable to a cyberattack. Yet many businesses can't afford professional IT solutions, have limited time to devote to cybersecurity, or they don't know where to begin.

WHAT TYPE OF ATTACKS HAVE BUSINESSES EXPERIENCED?



WHAT ARE THE MOST VULNERABLE ENDPOINTS OR ENTRYPOINTS TO YOUR BUSINESS NETWORKS AND ENTERPRISE SYSTEMS?

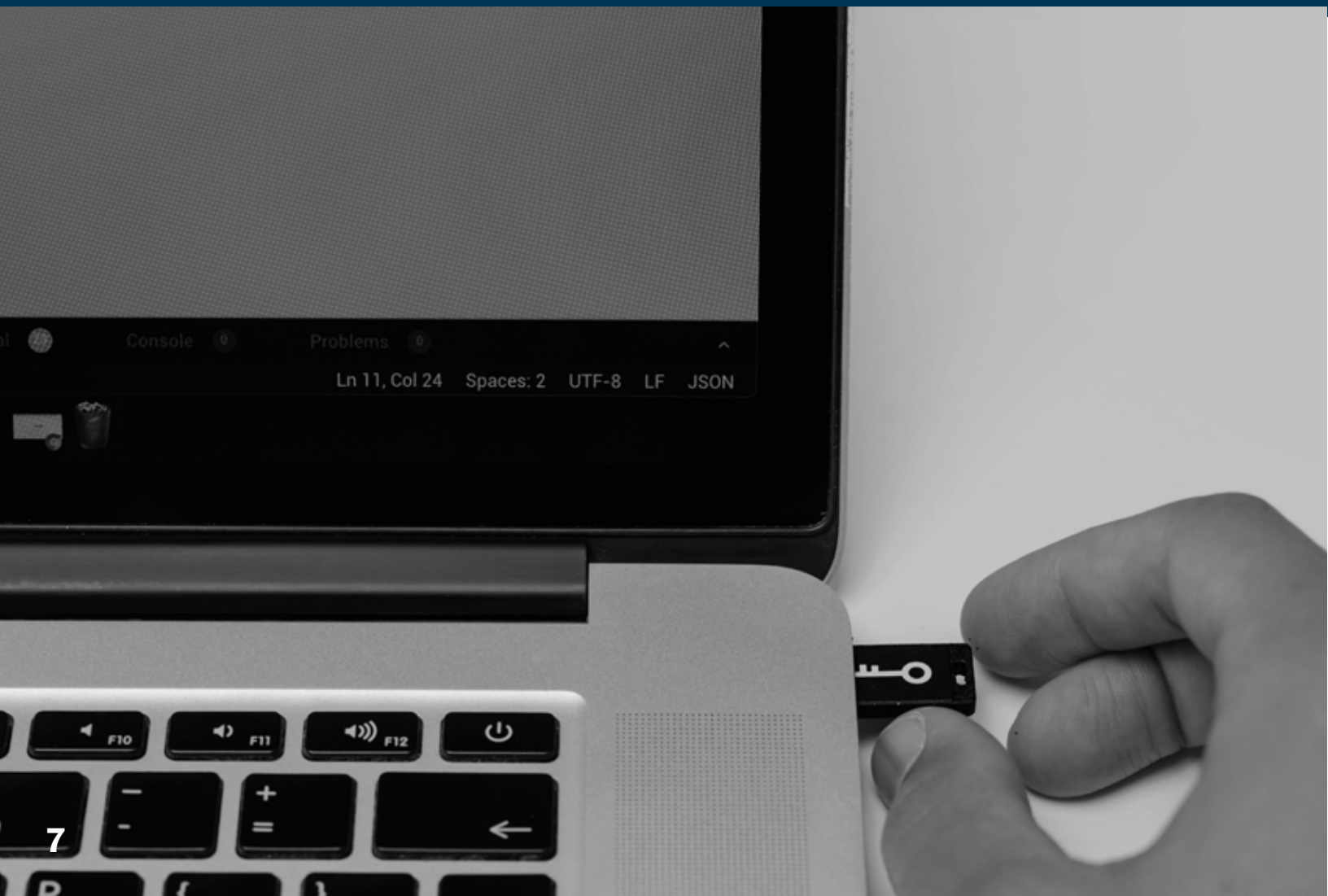


* See page 28 for glossary of terms.

\+ Mobile device includes e-readers, navigation devices, smart watches, digital cameras, Alexa or Echo devices, etc.

03. UNDERSTANDING AND MANAGING RISK

In 2014, Congress tasked the **National Institute of Standards and Technology (NIST)** with developing a cybersecurity risk framework that could be used to help protect our nation's critical infrastructure. This same framework is a useful tool for helping organizations of all sizes think through their risk, improve security, and reduce the likelihood of becoming a victim of cyberattacks.



THE NIST FRAMEWORK HAS FIVE CORE PARTS

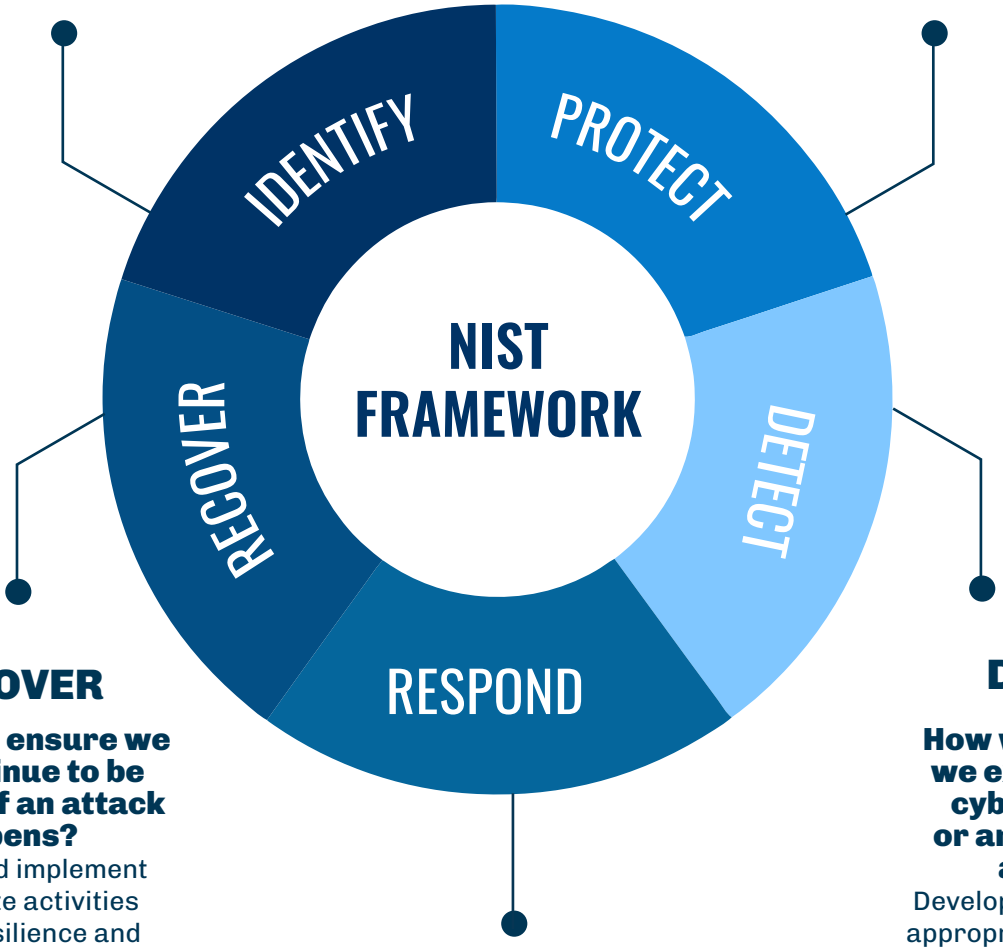
Identify, Protect, Detect, Respond, Recover. These five components, when considered together, provide a comprehensive view of the lifecycle for managing cybersecurity risk over time. Here's a summary of the framework and how it applies to your business:

IDENTIFY

What does my small business need to secure?
Develop an organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities.

PROTECT

What steps can I take to secure our digital space?
Develop and implement appropriate safeguards to ensure delivery of critical services.



RECOVER

How do we ensure we can continue to be effective if an attack happens?
Develop and implement appropriate activities to build resilience and restore any capabilities or services impaired due to a cybersecurity event.

DETECT

How will I know if we experience a cyberattack – or an attempted attack?
Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

RESPOND

How will we respond if a cyberattack happens?
Develop and implement appropriate actions when a cybersecurity event is detected.

CYBERSECURITY TIPS FOR SMALL BUSINESSES

1. Regularly update or enable auto updates on both the operating system and applications that are installed on your computers and other devices to protect them from attack.
2. Know and understand all devices connected to your networks. This includes your Wi-Fi networks, cloud-based storage such as Dropbox or Google Drive, and local networks.
3. Ensure all accounts are configured with multifactor authentication, where possible, including social media accounts.
4. Deploy a border firewall* and endpoint firewalls* to protect your internal network from the internet and your endpoints from each other.
5. Regularly back up critical systems and data.
6. Document information flows. It's important to not only understand what type of information your enterprise collects and uses but also to understand where the data is located and how it is used.
7. Deploy malicious code detection and prevention solutions such as antivirus or anti-malware software.
8. Develop an incident response and business continuity plan.
9. Use strong, unique passwords for every account. Don't share passwords. Require individual accounts for employees using computers and business applications.

   For administrative functions, require a separate account that is not the person's everyday user account.
10. Conduct cybersecurity awareness training for employees.
11. Limit access to sensitive systems and data to only those personnel who absolutely need that access.
12. Use caution with email attachments and untrusted links and watch for suspicious activity on your accounts.

* See page 28 for glossary of terms.

TECHNOLOGY INVENTORY

What kinds of technology do you utilize in your business?

Each of these items comes with a security risk because they are connected to the internet and interact with other devices. Assessing each technology item in your business will allow you to identify best practices to reduce the risk of a security breach.

* See page 28 for glossary of terms.

04. SECURITY TRAINING AND AWARENESS

Your staff is the first line of defense in protecting your information. Make sure all employees understand the importance of good cyber hygiene. As a best practice you should train individuals on the items listed on the next page.

Once employees are trained and understand the security protocols of your business, you may want to require that they sign an acknowledgment stating that they understand and agree to follow all business policies. You should also make sure that they understand the consequences of not following those policies.

AS A BEST PRACTICE YOU SHOULD TRAIN INDIVIDUALS ON THE ITEMS BELOW.

1. Specific security policies for the business
2. Proper use of computers, networks, and internet connections.
3. Limitations on the personal use of business resources such as phone, computers, and printers.
4. Restrictions on working from home and processing business data offsite.

LEAST PRIVILEGE ACCESS*

Even after agreeing to data use and security policies, employees should only be given the network access necessary for their assigned roles. This is a cybersecurity best practice known as “least privilege access.”

* See page 28 for glossary of terms.

CYBERATTACK PLANNING WORKSHEETS

UNDERSTANDING DATA

ESSENTIAL DATA INFORMATION

Where is your data stored? _____

How does your data flow in your business? _____

Who has access to your data? _____

Is your data encrypted? _____

Is your data considered sensitive or only some parts? _____

DATA MONITORING

Is there a log or record of who has accessed your data? _____

Where is your data backup located? _____

DATA VALUE

What is valuable? _____

Do you keep data on your customers? _____

Do you need to? _____

Who would want to steal your data? _____

After assessing your risk of cyberattack and learning basic security best practices, it's time to develop a plan for what to do if a breach does occur. It's always better to be proactive and think through potential responses before an attack happens.

Think through your answers to the questions in the following worksheets.

CYBER TASK FORCES

Cleveland Office:
(216) 522-1400

Cincinnati Office:
(513) 421-4310

FBI.gov/contact-us/field-offices

BUILDING YOUR RESPONSE TEAM

WHO TO CALL FOR HELP

Internet Service Provider (ISP)* _____

Attorney _____

Insurance Agent _____

Additional Software as a Service (SaaS)* _____

Providers _____

Other _____

KEY STAFF

Business Owner _____

Accountant/Finance Professional _____

Manager _____

IT professional _____

OUTSIDE EXPERTS

Cybersecurity _____

Advisor _____

Other _____

* See page 28 for glossary of terms.

05. PASSWORDS AND NETWORK SECURITY

You probably use personal identification numbers (PINs), passwords, or passphrases every day from getting money at the ATM or using your debit card in a store to logging in to your email or into an online retailer.

Tracking all of the number, letter, and word combinations may be frustrating, but these protections are important because hackers represent a real threat to your information. Often, an attack is not specifically about your account but about using the access to your information to launch a larger attack.

WHAT CAN BE DONE TO MAKE PASSWORDS AS EFFECTIVE AS POSSIBLE?

Passwords are the most common defense against unauthorized access to computers and systems, but they're often ineffective due to poor user habits.

DO:

- Include a mix of upper and lowercase letters, numbers, and special characters such as **$** or **!.**
- Use a passphrase instead of a password. An example could be **OH!O$maIIBusinessIsGr8!**
- Use a different password for each of your accounts.
- Use a password manager to keep track of multiple passwords.
- Use **Multifactor Authentication (MFA)** when possible. Factor one is something you **KNOW,** such as your password. Additional factors will be something you **HAVE,** such as a text message sent to your phone, or something you **ARE**, such as your fingerprint.

DON'T:

- Use personal information as part of your password.
- Store your passwords on a piece of paper near your computer.
- Use the same password for multiple accounts or use an easily guessed variation of the same password.
- Share your password with anyone.

QUICK TIPS FOR SETTING UP A WIRELESS NETWORK

1. When setting up a wireless network, be sure to change the network name to something that's unique and doesn't give away any personal information.
2. Enable wireless encryption and use a long, complex password.
3. Create a guest network that is separate from your business network.
4. Be sure to change the network's admin password often, especially when individuals with that information leave your business.
5. Regularly check with the manufacturer of your wireless router for updates.

SECURE NETWORKS

Connecting to public wireless networks can leave you open to a cyberattack. Public wireless networks allow anyone to connect and make it easy for hackers to intercept information transmitted over that network. Be sure you only connect to secure, private wireless networks you know and trust.

Step 1: Check for a lock.
Depending on your operating system, when a network is secure, you'll see a padlock displayed next to the network.

Step 2: Check the network.
Make sure the network is one you know and trust. The most secure networks use WPA3 and are password protected.

How to Check Your Wi-Fi Security

For the Wi-Fi network you're connected to, select "Properties" next to the Wi-Fi network name. On the Wi-Fi network screen, look at the value next to "Security Type." It'll include WPA3 if you're connected to a network using WPA3 encryption for security.

You might also consider buying a mobile hotspot from your wireless internet provider to use when you're away from your secure home or office network.

BE WARY OF FREE WI-FI.

MULTIFACTOR AUTHENTICATION (MFA)

MFA, previously known as two-factor authentication, 2MA, or two-step verification is an account login process that requires multiple methods of authentication to verify your identity. Using MFA makes it harder for criminals to access an online account. When it's available, always turn it on because it's easy to do and greatly increases your security.

How does MFA work?

You'll provide two or more identifying factors from different identity categories. There are three categories:

1. what you **KNOW**, such as a password;
2. what you **HAVE**, such as an authenticator app on your phone; and
3. what you **ARE**, which uses biometric verification methods.

The first identifying factor is normally entering your password or personal identification number (PIN) or possibly answering a security question. Then you'll be required to supply one or more forms of identity from different categories.

What type of accounts offer MFA?

Not every account offers MFA, but it's becoming more popular every day. It's seen on many accounts that usually hold either valuable financial or personal information like banks, financial institutions, online stores, or social media platforms. Any place online that is storing your personal information (especially financial information), or any account that can be compromised and used to trick or defraud someone else should be protected with MFA. **Simply put, use MFA wherever it's offered.**

MFA can include:

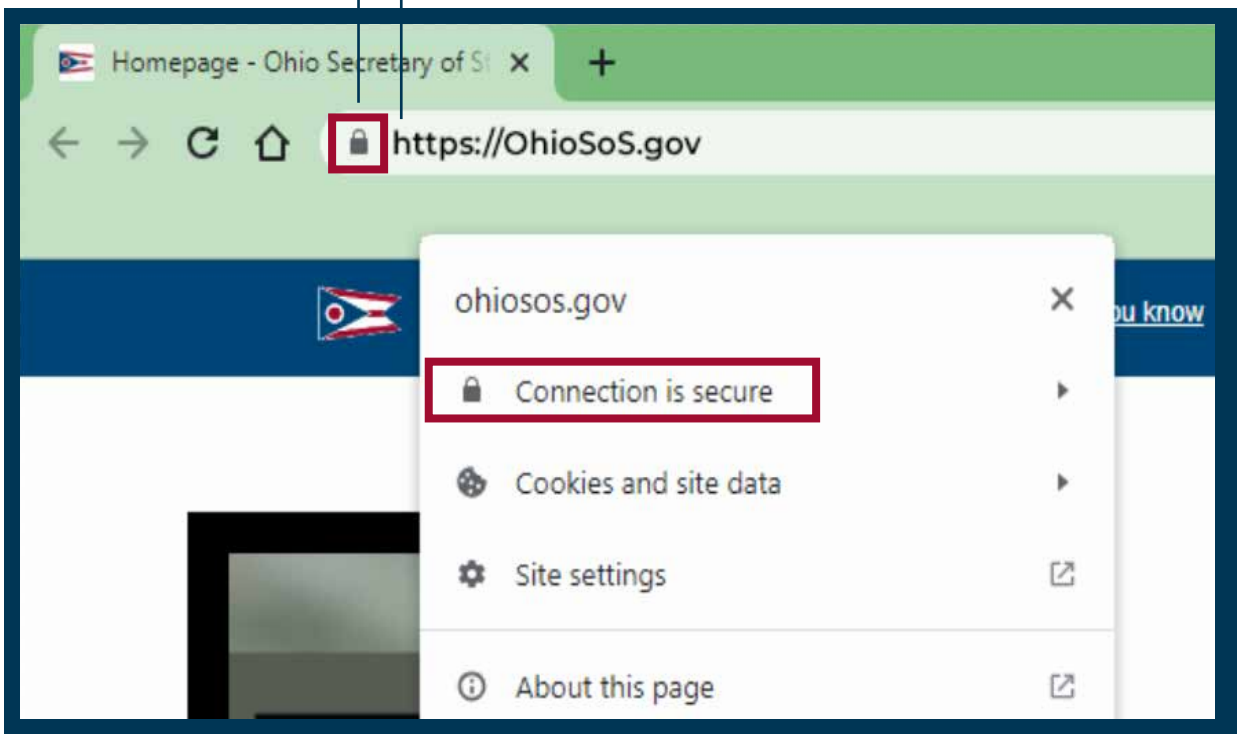
- An additional PIN.
- The answer to a security question such as, "What's your favorite pet's name?"
- A code either emailed and/or texted to a mobile number.
- A biometric identifier such as facial recognition, retinal scan, or a fingerprint.
- A unique number generated by the system to be verified on an authenticator app.
- A secure token, which is a separate piece of hardware (such as a key fob that holds information, an ID badge) that verifies a person's identity with a database or system.

SECURE CONNECTIONS

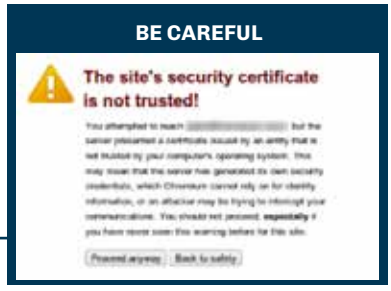
Cybercriminals will utilize fraudulent or unsecured websites to try to steal your data and infiltrate your network. Always check that your internet traffic is encrypted by examining the security certificate of websites you visit.

Step 1: Check the URL.
Standard websites use the prefix **"http://"**, but secure websites will use **"https://"** - that extra **'s'** means your connection to the website is encrypted.

Step 2: Check for a lock.
Depending on your browser, when a site is secure, you'll see a padlock displayed either in the address box or bottom right corner of your browser window.



Step 3: If you get an SSL warning, don't click through.
If your browser (i.e. Chrome or Firefox) believes that the site you're connecting to isn't what it should be, a warning will be displayed about the site's security certificate being untrusted. To be safe, you shouldn't proceed unless you know and understand the technical reason why you've received the warning.



06. DATA MANAGEMENT

Backing up data is the practice of copying data from a primary to a secondary location to protect it in case of a disaster, accident, or malicious action. Data can be the most important asset in a modern organization, and losing data can cause massive damage and disrupt business operations. Backing up your data is critical for all businesses, large and small.

When backing up data, it should include all necessary data for the workloads a server is running. This can include documents, media files, configuration files, machine images, operating systems, and registry files. Essentially, any data that you want to preserve can be stored as backup data.

Regular backups of your data are important. Equipment can fail, be stolen, lost, or become inaccessible due to a security incident such as a ransomware attack. Regular scheduled backups are important to ensure the availability of your information. Make sure the backup is stored in a secure offsite location and tested to ensure it will work in case of an emergency. Cloud-based storage can offer a secure way to store data. An external hard drive can also be used if direct access to the information is available.

IDENTIFY IMPORTANT INFORMATION

- What types of customer, financial, and human resource data do you store electronically?
- Which pieces of information would be valuable if they fell into the wrong hands?
- How is this information stored?
- Are you collecting any of the following types of information?

IS THERE ANY INFORMATION THAT YOU ONCE COLLECTED BUT NO LONGER UTILIZE OR FIND NECESSARY TO KEEP?

CYBERSECURITY DOESN'T HAVE TO BE EXPENSIVE.

The cyber community is helping every day to ensure money does not stand in the way of improving your cybersecurity posture. Open-source tools and resources are a great FREE way to increase your cyber defense with limited investment.

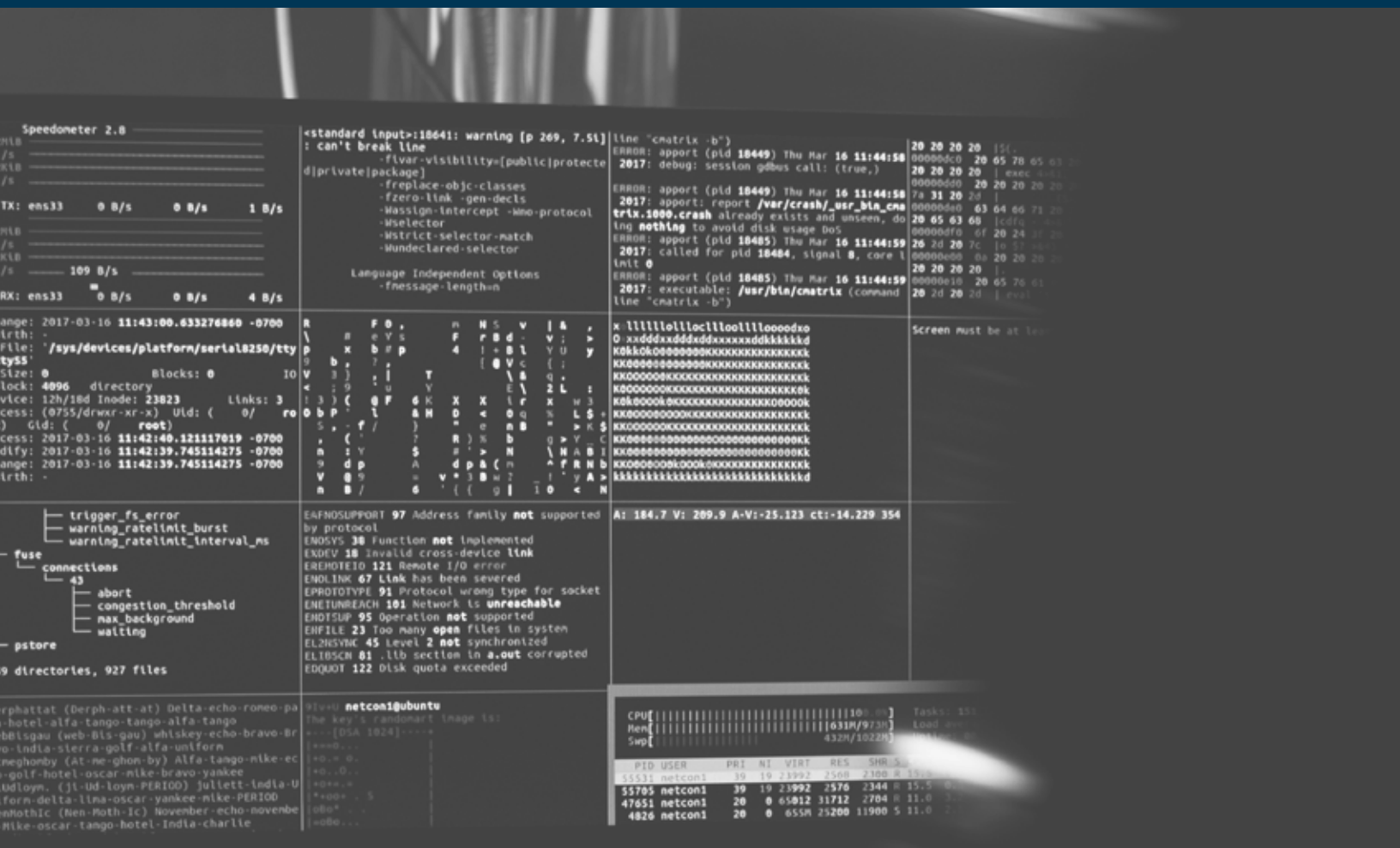
The Cybersecurity and Infrastructure Security Agency (CISA) maintains a list of free tools to get you started.

To learn more, visit CISA.gov/cyber-essentials.

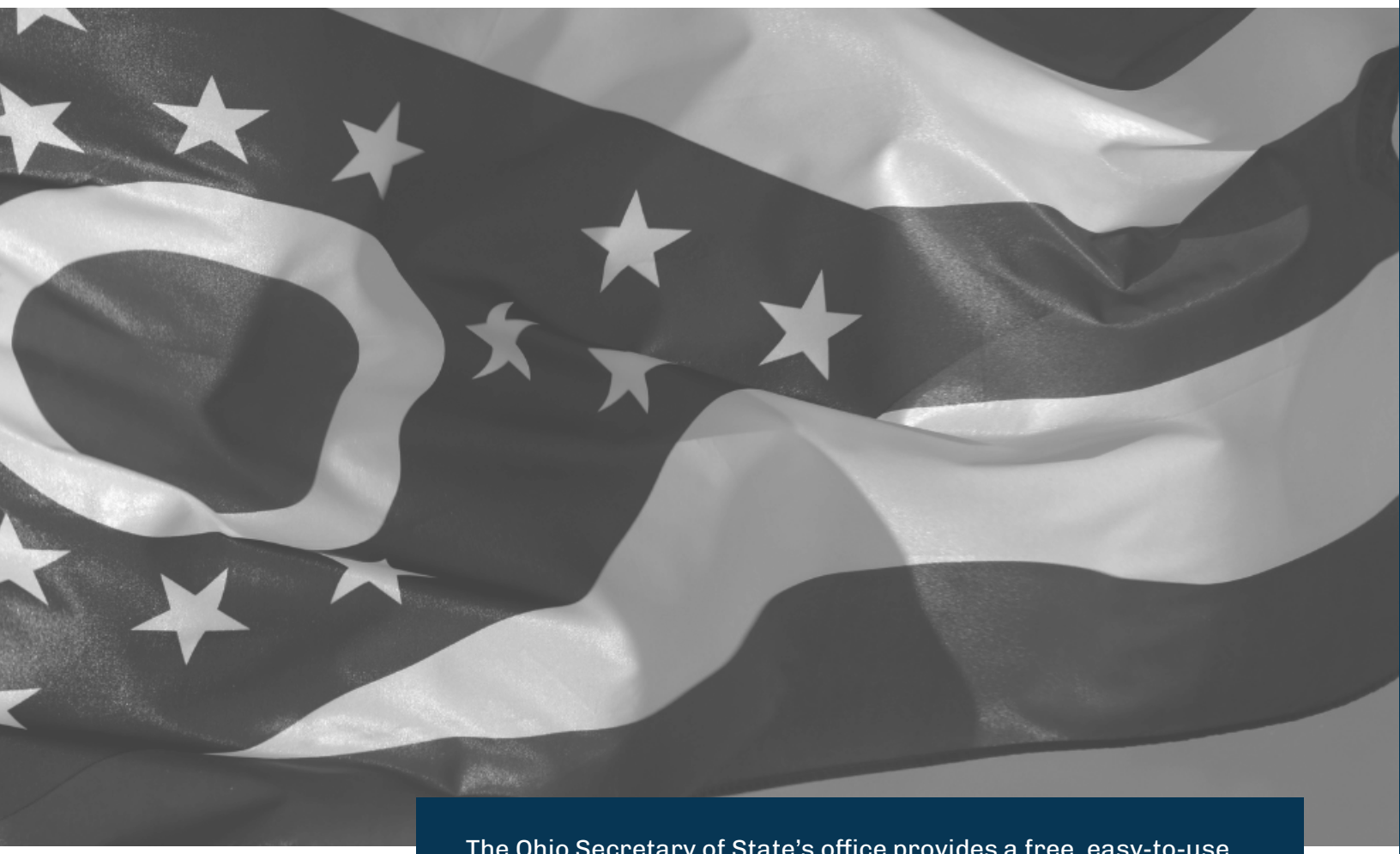
07. BUSINESS ID THEFT AND HOW TO PROTECT YOURSELF

Business identity theft, or corporate or commercial identity theft, occurs when a business's identity is used to transact business and establish lines of credit with banks and/or vendors.

Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor.



BUSINESS FILING NOTIFICATION SYSTEM



The Ohio Secretary of State's office provides a free, easy-to-use Business Filing Notification System that allows businesses to track any changes and updates to business filings with our office. Businesses or individuals need only submit an email address and business charter or license number for each filing, which can be found through a simple online business search.

LEARN MORE AT OHIOSOS.GOV/NOTIFY

TAKE THE FOLLOWING INITIAL STEPS TO PROTECT YOUR BUSINESS FROM IDENTITY THEFT:

1. Subscribe to the Secretary of State's Business Filing Notification System.
2. Periodically check your business information on the Secretary of State's website.
3. Obtain a commercial credit report for your business.
4. Sign up for electronic notifications with your bank, other creditors, and service providers.
5. Monitor accounts and bills, and immediately report any suspicious activity to the originating company.
6. Protect your EIN *(employer identification number)*, account numbers, and other personal information.
7. Create and follow a policy for carrying, using, and reporting a lost or stolen business credit card.
8. Inventory documents you maintain.
9. Store only those documents you must keep, and keep them in a safe and secure location.
10. If you plan to discard documents, shred them using a cross cut or "confetti" shredder.
11. Don't share any sensitive information over email or on any web-based service.

To perform a business search, sign up for the Business Filing Notification, or to find more business resources, visit OhioSoS.gov/business.

08. ADDITIONAL RESOURCES

- **Center for Internet Security** (CIS) *CISecurity.org*
- **Federal Bureau of Investigation (FBI)** *FBI.gov/Investigate/Cyber*
- **Federal Trade Commission – Data Security** *FTC.gov/DataSecurity*
- **Homeland Security – Cybersecurity & Infrastructure Security Agency (CISA**) *CISA.gov*
- **Homeland Security – Stop. Think. Connect.** *DHS.gov/StopThinkConnect*
- **National Cybersecurity Alliance** *StaySafeOnline.org*
- **National Institute of Standards and Technology (NIST)** *NIST.gov*
- **Ohio Secretary of State Office of Public Integrity** *OhioSoS.gov/PublicIntegrity*
- **Small Business Administration (SBA)** *SBA.gov/* *(search "Cybersecurity")*

09. GLOSSARY OF TERMS

Adware
Adware refers to any piece of software or application that displays advertisements on your computer.

Antivirus
Antivirus software is a computer program used to prevent, detect, and remove malware.

Artificial Intelligence (AI)
AI refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions.

Authentication
Authentication is a process that ensures and confirms a user's identity.

Backdoor
A backdoor is used to describe a hidden method of bypassing security to gain access to a restricted part of a computer system.

Backup
A backup is to make a copy of data stored on a computer or server to reduce the potential impact of failure or loss.

Bluetooth
Bluetooth is a wireless technology for exchanging data over short distances.

Blackhat
Blackhat refers to a hacker that violates computer security for personal gain or malice.

Border Firewall
A border or perimeter firewall refers to a security application that defends the boundary between a private network and a public network. Its goal is to prevent unwanted or suspicious data from entering the network.

Botnet
A botnet is a collection of internet-connected devices, which may include PCs, servers and mobile devices that are infected and controlled by a common type of malware.

Broadband
Broadband is a high-speed data transmission system where the communications circuit is shared between multiple users.

Browser
A browser is software that's used to access the internet. The most popular web browsers are Chrome, Firefox, Safari, internet Explorer, and Edge.

Brute Force Attack
A brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any password protected system or account.

Bug
A bug refers to an error, fault, or flaw in a computer program that may cause it to unexpectedly quit or behave in an unintended manner.

Cloud Computing
Cloud computing is the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

Cookie
Cookies are small files which are stored on a user's computer. This provides a way for the website to recognize you and keep track of your preferences.

GLOSSARY CONTINUED

Critical Update
A critical update is a fix for a specific problem that addresses a critical, non-security-related bug in computer software.

Cyberattack
A cyberattack is a computer operation carried out over a device or network that causes physical damage or significant and wide-ranging disruption.

Cybercrime
A cybercrime is any criminal activity that involves a computer, networked device, or a network.

Cybercriminal
A cybercriminal is an individual or group of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data and generate profits or cause harm.

Data Breach
A data breach is a confirmed incident where information has been stolen or taken from a system without the knowledge or authorization of the system's owner.

Data Server
Data server is the phrase used to describe computer software and hardware that delivers database services.

Distributed Denial-of-Service (DDoS) Attack
A DDoS attack is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.

Deepfake
Deepfake refers to any video in which faces have been either swapped or digitally altered with the help of AI.

Disaster Recovery
Disaster recovery is an organization's ability to restore access and functionality to IT infrastructure after a disaster event, whether natural or caused by human action (or error).

Domain Name
A domain name is part of a network address which identifies it as belonging to a particular domain.

Domain Name Server (DNS)
A DNS is a server that converts recognizable domain names into their unique IP address.

Encryption
Encryption is coding used to protect your information from hackers. Think of it like the code cipher used to send a top-secret coded spy message.

Endpoint Firewall
An endpoint firewall protects the data on the device itself, enabling the business to monitor the activity and status of all its employees' devices at all times.

Exploit
An exploit occurs when an application or script is used maliciously to take advantage of a computer's vulnerability.

Firewall
A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the internet.

Hacking
Hacking refers to an unauthorized intrusion into a computer or a network.

Hypertext Markup Language (HTML)
HTML is the standard markup language for creating web pages and web applications.

Identity Theft
Identity theft is a crime in which someone uses personally identifiable information to impersonate someone else.

Incident Response Policy
An incident response policy is a plan outlining an organization's response to an information security incident.

Internet of Things (IoT)
The IoT refers to the billions of physical devices around the world that are now connected to the internet, collecting, and sharing data.

Internet Protocol (IP) Address
An IP address is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network such as the internet.

Internet Service Provider (ISP)
An ISP is a company that provides subscribers with access to the internet.

Keystroke Logger
A keystroke logger is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you are unaware actions are being monitored.

Least Privilege
Least privilege is the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Malware
Malware is shorthand for malicious software and is designed to infiltrate, damage, or obtain information from a computer system without the owner's consent.

Man in the Middle Attack
A man in the middle attack is an attack on the "middleman," in this case, defined as the Wi-Fi system that connects users to the internet. Hackers who commit man in the middle attacks can break a Wi-Fi's encryption and use this as a means of stealing your personal data.

Multifactor Authentication (MFA)
MFA provides a method to verify a user's identity by requiring them to provide more than one piece of identifying information.

Network
A network is two or more computers connected together to share resources, exchange files, or enable electronic communications. A network's connections to its computers can be made by cables, phone lines, radio waves, satellites, or infrared laser beams.

Packet Sniffer
Packet sniffer is software designed to monitor and record network traffic.

Patch
A patch is a piece of software code that can be applied after the software program has been installed to correct an issue with that program.

Penetration Testing
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit.

Phishing
Phishing is a method of trying to gather personal information using deceptive emails and websites.

Policy Management
Policy management is the process of creating, communicating, and maintaining policies and procedures within an organization.

Proxy Server
A proxy server is another computer system which serves as a hub through which internet requests are processed.

Pre-texting
Pre-texting is the act of creating a fictional narrative or pretext to manipulate a victim into disclosing sensitive information.

GLOSSARY CONTINUED

Ransomware
Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

Redundant
To be redundant is to include extra components which are not strictly necessary to functioning, in case of failure in other components.

Router
A router is a piece of network hardware that allows communication between your local home network and the internet.

Scareware
Scareware is a type of malware designed to trick victims into purchasing and downloading potentially dangerous software.

Secure Socket Layer (SSL)
SSL and its successor, TLS, are protocols for establishing authenticated and encrypted links between networked computers.

Security Awareness Training
Security awareness training is a training program aimed at heightening security awareness within an organization.

Server
A server is a computer program that provides a service to another computer program and its user.

Smishing
Smishing is any kind of phishing that involves a text message.

Social Engineering
Social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Software
Software is the name given to the programs you will use to perform tasks with your computer.

Software as a Service (SaaS) Provider
A SaaS provider is a software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet. In this model, an independent software vendor (ISV) may contract a third-party cloud provider to host the application.

Spam
Spam is slang commonly used to describe junk email on the internet.

Spear Phishing
Spear phishing is an email-spoofing attack that targets a specific organization or individual seeking unauthorized access to sensitive information.

Spoofing
Spoofing is when a hacker changes the IP address of an email so that it seems to come from a trusted source.

Spyware
Spyware is a type of software that installs itself on a device and secretly monitors a victim's online activity.

SQL Injection (SQLI)
SQL injection is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

Tablet
A tablet is a wireless, portable personal computer with a touchscreen interface.

Traffic
Web traffic is the amount of data sent and received by visitors to a website.

Trojan
A Trojan, also known as a Trojan horse, is a type of malicious software developed by hackers to disguise as legitimate software to gain access to a target users' systems.

Two-Factor Authentication (2FA)
2FA, often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are.

Universal Serial Bus (USB)
USB is a popular connection used to connect a computer to devices such as digital cameras, printers, scanners, and external hard drives.

Uniform Resource Locator (URL)
A URL, commonly known as a web address, is a unique location of reference to a resource that specifies its location on a computer network and a mechanism for retrieving it.

User Authentication
User authentication is a technique to prevent unauthorized users from accessing sensitive data. For instance, User A can only see data that is relevant and cannot view User B's sensitive information.

Username
A username is a name that uniquely identifies someone on a computer system.

Virus
A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

Virtual Private Network (VPN)
A VPN gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your IP address so your online actions are virtually untraceable.

Vulnerability
Vulnerability refers to a flaw in a system that can leave it open to attack.

Vishing
Vishing is the telephone equivalent of phishing. It is an attempt to scam someone over the phone into surrendering private information that will be used for identity theft.

Whitehat
Whitehat hackers perform penetration testing, test in-place security systems, and perform vulnerability assessments for companies knowingly and legally without malice.

World Wide Web (the web, WWW, W3)
The web refers to all the public websites or pages that users can access on their local computers and other devices through the internet. These pages and documents are interconnected by means of hyperlinks that users click on for information.

Worm
A computer worm is a malware computer program that replicates itself to spread to other computers.

Wi-Fi
Wi-Fi allows computers, smartphones, or other devices to connect to the internet or communicate with one another wirelessly within a particular area.

Wi-Fi Protected Access 3 (WPA3)
WPA3 is the most secure of three security certification programs developed after 2000 by the Wi-Fi Alliance to secure wireless computer networks. All Wi-Fi certified devices must have a certification from the Wi-Fi Alliance.

Zero-day or Zero-day vulnerability
Zero-day is a security flaw or vulnerability that does not have a fix or patch yet provided by a vendor.

Zero-day Attack
A zero-day attack is a vulnerability that is exploited before the software creator/vendor is even aware of its existence.

CYBER PARTNERS

CIS Center for Internet Security®

FBI

CISA CYBER+INFRASTRUCTURE

Ohio Homeland Security

NATIONAL CYBERSECURITY ALLIANCE

PUBLIC INTEGRITY DIVISION
Honest. Secure. Accountable.

Visit us online at **OhioSoS.gov.**

Or contact our office by:
Email: **info@OhioSoS.gov**
Telephone: **614.466.3613**
Toll free: **877.767.6446**

SOS 0322 (01/2024)

printed in-house