CYBER SECURITY FUNDAMENTAL (CSF 101)

BEGINNER APPROACH

Compiled by: Godwin Ogazi

INTRODUCTION

Today, internet-connected services are everywhere, and as a result, so are threats from spammers, hackers, and cybercriminals. Understanding the basics of cybersecurity is the first step toward preparing for the fundamentals-level security, compliance, and identity course as well as preventing malicious attacks.

Learning objectives

Upon completion of this training, you'll be able to:

1. **Define cybersecurity and cybercriminals**
2. **Explain how to defend against cyberattacks**
3. **Describe the principles of Zero Trust**
4. **Explain types of attacks, attack vectors, and the threat landscape**
5. **Identify mitigation strategies**
6. **Examine ransomware and extortion-based threats**

Ransomware and extortion-based attacks are a high-reward, low-cost business that has escalated from extorting money from individuals to targeting businesses and organizations. The modules in this learning path will provide you with insights and information to help you better understand this threat, including a broad look at ransomware and extortion-based threats, how cybercriminals exploit security weaknesses to gain access to your computers and devices, some of the steps you can take prevent ransomware threats, and finally, how to recover from an attack.

What is cybersecurity?

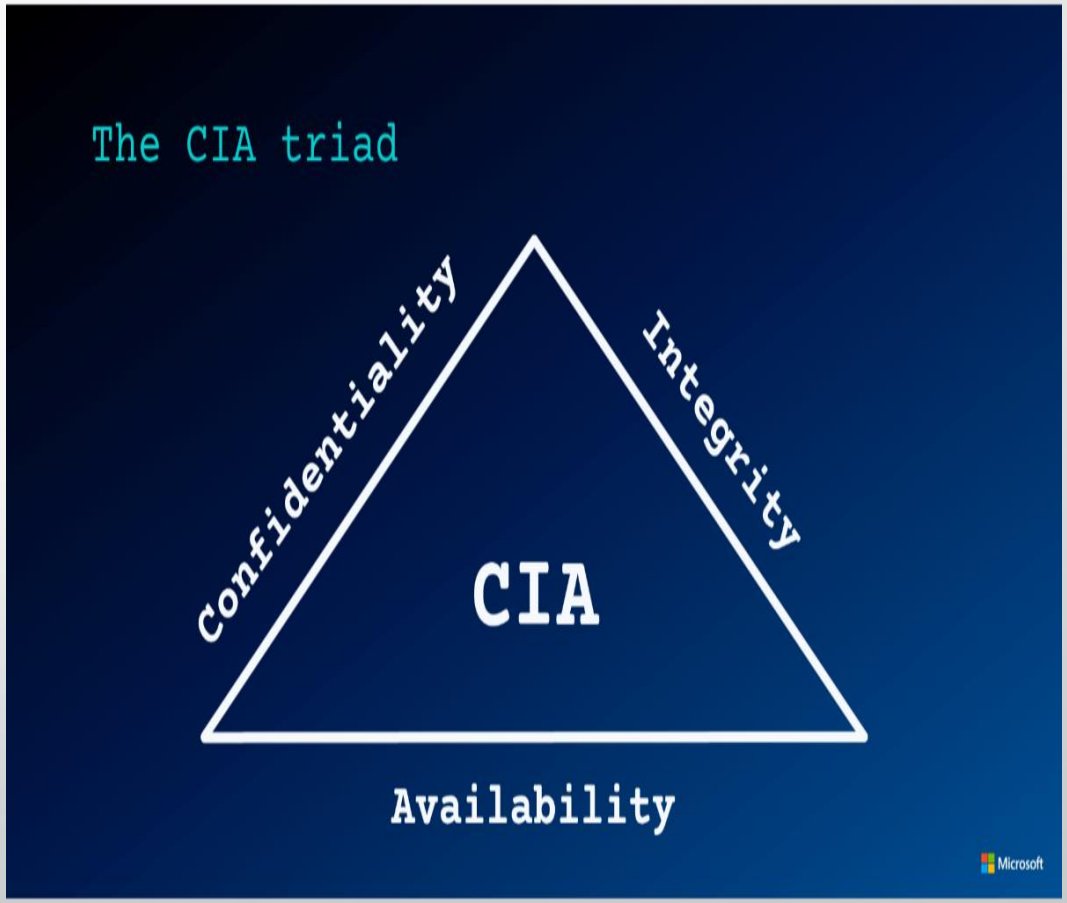
In simple terms, **cybersecurity** is the act of protecting sensitive information stored online or on a server. Formed from two words—cyber meaning "computers" and security meaning "free from danger"—cybersecurity is *any preventative measure that protects information or processes from being stolen or compromised*.

Understanding the importance of cybersecurity is essential in today's digital world. Everyone's work and personal lives include electronic data that may be vulnerable to malicious attacks and invasions of privacy by individuals wishing to do harm.

The three most crucial components of security make up what is known as the CIA Triad:

- **Confidentiality** – The right people have access to sensitive information and the wrong people don't.
- **Integrity** – Only the right people or processes can change sensitive information.
- **Availability** – Information is visible and accessible whenever needed.
- Understanding the CIA Triad and how each part contributes to cybersecurity increases awareness and importance of remaining vigilant in today's digital world.

https://youtu.be/AAytysafa70



Cyberattacks and cybercriminals

Any attempt to gain illegal access to a computer system to cause harm is considered a **cyberattack**. Cyberattacks can happen on any digital device—not just computers. Any device connected to a network or the internet can be attacked, whether or not that device holds valuable data worth attacking. And, cyberattacks can originate from either outside or inside an organization.

People who perform cyberattacks are known as **cybercriminals**. Cybercriminals can be found anywhere—including inside an organization— and can be:

A single person or a group of people.

An organization for hire.
A government entity.

The reasons cybercriminals attempt cyberattacks vary, but most fall into three main categories:

Criminal

Political

Personal

- **Criminally-motivated** attackers want to steal something for their own gain, such as money or data.
- **Politically-motivated** attackers seek attention and may often make their attacks known to the public. This type of cyberattack is often referred to as "hacktivism."
- **Personally-motivated** cybercriminals often try to disrupt a company's systems for retribution. These attackers are usually current or former employees.

Cyberattacks are either active or passive. Cybercriminals who plan **active attacks** want to alter the targeted system by affecting the integrity, authenticity, and availability of data. Cybercriminals who plan **passive attacks** want to find out as much information as possible about their target in hopes of leading to a breach of privacy.

https://youtu.be/IooFYTLDQEo

Understand basic terminologies

To completely understand the importance of why strong cybersecurity matters, one must first become familiar with basic technological terminology. While not an exhaustive list, the following nine terms are important in gaining a comprehensive understanding of cybersecurity.

- **Network** – A connection between two or more computers that makes communication and exchange of data possible.
- **Internet** – The global computer network made possible by dedicated routers and servers.
- **Internet Protocol** – A set of rules that controls the flow of data over the internet.
- **IP (Internet Protocol) address** – An address assigned to every device that connects to a computer network and uses Internet Protocol for communication. IP addresses are a unique string of numbers and may look something like 192.168.12.5.
- **MAC (Media Access Control) address** – A unique identification number assigned to every device that connects to the internet. Traditional MAC addresses are 12-digit hexadecimal numbers.
- **DNS (Domain Name System) server** – A computer or server that contains a database of IP addresses and the associated domain. A DNS server works like a phone book, transferring text names of internet sites (for example, microsoft.com) to the site's assigned IP address.
- **DHCP (Dynamic Host Configuration Protocol)** – A protocol that quickly and automatically assigns an IP address to a connected device on a network.
- **Router** – A device that routes data to the preferred destination. Routers are often considered the "traffic cops" of the internet.
- **Bot** – Short for "robot," a computer bot is a program that controls computers to simulate a human activity. Bots can be used to automate certain tasks without human intervention. Bots can also be programs that take over a computer without the user's knowledge.

https://youtu.be/SyWRMrXki2M

Principles of Zero Trust

Today's work environment looks different than it did many years ago when all workers performed jobs in similar office spaces. These days, jobs are performed on site, remotely, in the cloud, or hybridly (a combination of on-site and remote work).

Cybercriminals, on the other hand, haven't changed that much. They still look for ways to take advantage of any lapses in security, and they use social engineering to prey on the human weakness of wanting to trust others. Cybercriminals establish trust in their cyberattacks and then use that trust to defraud their victims.

Zero Trust is the best defense against cyberattacks and threats. Zero Trust uses the premise of "never trust, always verify" and requires that all users with access to data authenticate, authorize, and validate before accessing system resources.

Zero Trust is an end-to-end security strategy that monitors and controls the six main pillars of security:

Identity
Endpoints
Applications
Network
Infrastructure
Data

In today's ever-changing digital landscape of cloud applications, data stored in different environments, and devices that connect from various locations, the practice of "trust no one and verify everything" is paramount to avoid a major security breach.

The following three Zero Trust principles provide multiple layers of defense:

- **Verify explicitly** – Strict identity verification for every user and every device trying to access system resources, ensuring constant monitoring, and validating who can access what.
- **Use least privilege access** – Just-in-Time (JIT) and Just-Enough-Access (JEA) ensure that access is minimized, only granting system and application access to authorized users for specific tasks and limited times.
- **Assume breach** – Assumes attackers have already breached the system and embodies a deny-all approach with real-time monitoring to assess every request against known behaviors, creating a mindset of necessary access segregation to minimize damage.

https://youtu.be/_YPlvtQIoVE


Microsoft
Verify explicitly
Apply least privilege access
Assume breach

Understand attack vectors

"Cybercriminals use various means to carry out cyberattacks. Fully understanding concepts like threat landscape and attack vectors helps to build a foundation for developing strong cybersecurity policies.

The cyber **threat landscape** includes all potential cybersecurity threats that might affect an organization's assets. Threat landscapes are ever-evolving. For example, 2020's shift to work-from-home resulted in a heightened threat landscape for many organizations. The threat landscape covers more than just computers and mobile devices. It can include any element owned or managed by an organization—even items not owned or managed by the organization such as:"

Email accounts

Social media accounts

Mobile devices

The organization's technology infrastructure

Cloud services

People

Cybercriminals are aware of an organization's threat landscape and use any means possible to carry out cyberattacks. They look for any entry point to gain access to a system. These entry points are called **attack vectors** and cybercriminals use them to start a security breach. Eight common attack vectors are:


Email
Social media
Removable devices
Browsers
Cloud services
Insiders
Devices
Wireless
Microsoft

- **Email** – Email is perhaps the most common attack vector. Cybercriminals send email messages that look legitimate to entice users to select a link or download a file that will compromise a device or system.
- **Social media** – Monitoring social media accounts is another route cybercriminals use to gain access to information or resources.
- **Removable devices** – Cybercriminals use removable media like USB drives, smart cables, or storage cards to compromise devices. The removable media may hold malicious code that, when plugged into a device, destroys data or records important information like usernames and passwords.
- **Browsers** – As web browsers have become a regular part of everyday life and work, cybercriminals frequently use websites and browser extensions that download malicious software or change a user's browser settings to provide an entry point to a system or network.
- **Cloud services** – As organizations rely more on cloud services for day-to-day activities, cybercriminals look for compromised credentials to gain control of content accessible in the cloud.
- **Insiders** – Whether intentionally or unintentionally, people can serve as attack vectors. Cybercriminals use social engineering practices to exploit a human's reliance on trust by pretending to be a person of authority in an organization. An employee may unintentionally select a link or send important information through email to a fraudster. In some cases, employees with authorized access may intentionally use their credentials to cause harm.
- **Devices** – As the workforce becomes more mobile and employees use multiple devices to do their jobs (phones, laptops, and tablets), the opportunity for these devices to land in the hands of cybercriminals increases, making devices themselves attack vectors.
- **Wireless** – Another common attack vector is an organization's wireless network. Cybercriminals often tap into unsecured wireless networks to look for vulnerabilities.

https://youtu.be/XmfjttuODLA

Understand types of attacks and threat landscape

Cyberattacks, as previously defined, are attacks that try to gain illegal access to a computer system or device to cause harm. Many types of cyberattacks happen in the world today. Each year, cybercriminals find ways to introduce new types of attacks to the threat landscape.

Some of the most common types of cyberattacks are:

Distributed Denial-of-Service (DDoS) – Attackers target systems, servers, or networks and flood them with traffic that exhausts a network's resources or bandwidth. DDoS attacks often result in system-wide crashes so legitimate end users can't access normal systems or network resources. Examples of DDoS attacks are files that take too long to open and websites that take too long to load or don't load at all.

Man-in-the-Middle (MITM) – A MITM attack is sometimes referred to as an eavesdropping attack. In this type of attack, the cybercriminal hijacks or comes between a client and host in the network to steal and manipulate data.

Ransomware – Ransomware attacks are serious because company or user data or resources are held hostage by cybercriminals who demand money with the promise of regaining access. Paying the ransom doesn't ensure full return or restoration of data or resources.

End users can take precautions to avoid cyberattacks. Some of the best ways to prevent cyberattacks include:

1. Changing passwords regularly and using passwords that are difficult to crack.

2. Updating operating systems and applications regularly.

3. Using a firewall or other security tools.

4. Avoiding emails from unknown senders and reviewing emails closely to avoid being scammed.

5. Backing up data regularly.

6. Using multi-factor authentication or other mitigation strategies.

https://youtu.be/A3UD7b2uVyA

- **Phishing** – Phishing is a type of attack that uses email or websites to ask for personal information from individuals. Phishing email messages and websites can look legitimate and often pretend to come from legitimate sources. Cybercriminals prey on human weaknesses to obtain private information that is then exploited to steal information or resources.
- **Vishing** – Vishing is similar to phishing but is an attack that uses voice communications to deceive victims. Cybercriminals pretend to be from legitimate organizations encouraging victims to verify account or security information. This method is unlikely to lead to a ransomware attack but is commonly used to trick people into revealing bank account information to steal funds.
- **Smishing** – Similar to phishing and vishing, smishing uses SMS (text messages) to exploit victims. The messages contain links to fraudulent sites imitating legitimate sites.
- **Password attacks** – Password attacks occur when a cybercriminal uses a password cracking tool to hack a password. The cybercriminal then uses the password to sign into systems to steal information.
- **Malware attacks** – Malware attacks are some of the most common types of cyberattacks. Malware is malicious software used to breach a network through some type of vulnerability. Spyware falls into this category.

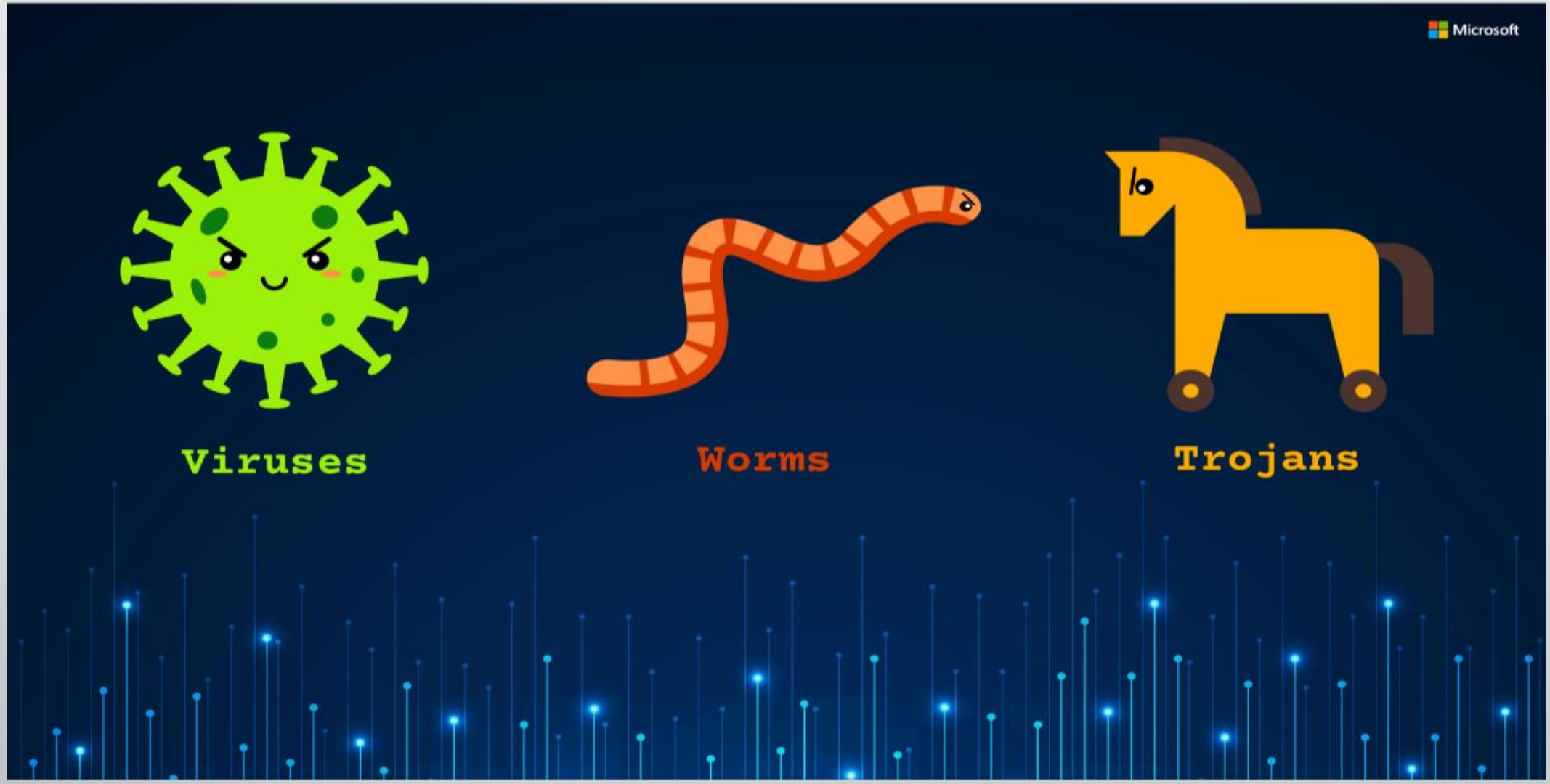
What is malware?

The word **malware** comes from combining two words—"malicious" and "software." Malware is a piece of software cybercriminals use to infect systems and cause harm by stealing data or disrupting normal processes.

Malware has two main components: **propagation mechanism** and **payload**. Let's look more closely at each part.

Propagation mechanism

Propagation is how the malware spreads itself across systems. The most common types of propagation mechanisms are viruses, worms, and trojans.


Microsoft
Viruses
Worms
Trojans

Just as biological viruses do, technology-based **viruses** depend on an entry point to begin causing harm. Viruses need an end user to perform some type of action so the virus can infect the system. Examples of these types of actions are downloading an infected file or plugging in a removable device like a USB device that contains the virus.

Worms, however, don't need an end user to perform an action to spread across a system. Worms find system vulnerabilities and exploit them to cause damage. Worms may sit on top of legitimate applications that have access to a system. Once the application is launched, the worm begins to spread across devices in the same network or in connected networks.

A **trojan** is much more difficult to recognize than the other two propagation mechanisms. A trojan pretends to be a genuine piece of software. When the software is installed, the trojan pretends to be working as expected when in actuality it's secretly performing malicious acts in the background like stealing information.

Payload

Payload is the action that malware performs on an infected system or device. Some common types of payload include:

- **Ransomware** which locks systems or data until the victim has paid a ransom.
- **Spyware** which spies on a device or system to collect protected information like usernames and passwords.
- **Backdoors** which allow a cybercriminal to exploit a system's vulnerability and bypass existing security measures.
- **Botnets** which join a computer, server, or other device to a network of similarly infected devices that can be controlled remotely to carry out harmful actions.
- Understanding propagation mechanisms and payload helps make end users more aware of malware and its potential damage.

https://youtu.be/rrxJpzpqbZg

What is a mitigation strategy?

Another important word to learn in the quest to understand cybersecurity is the word **mitigation**.

Defined as "an action that reduces severity, seriousness, or painfulness of something," mitigation in the technology world is the *set of steps an organization takes to prevent a cyberattack*.

Organizations, including Microsoft, use different mitigation strategies. Some of the most well-known include:

- Multifactor authentication (also known as MFA)
- Browser security
- User education
- Threat intelligence and detection

Multifactor authentication

works by requiring an end user to provide more than one form of identification to verify their identity. Cybercriminals use compromised usernames and passwords to steal information. Multifactor authentication helps reduce this type of threat by requiring a second layer of authentication using fingerprints, retinal scans, or authentication software.

Browser security

Cybercriminals know that modern workers access the internet via browsers as a regular part of their job. Cybercriminals therefore rely on the use of browsers to find vulnerabilities. Implementing **browser security** policies helps protect organizations against this type of cyberattack by:

- Preventing the installation of unauthorized browser extensions or add-ons.
- Only allowing permitted browsers to be installed on devices.
- Blocking certain sites using web content filters.

  Keeping browsers up to date.

USER EDUCATION

As discussed in an earlier unit, cybercriminals rely on the vulnerabilities of humans to cause harm through social engineering. Organizations can defend against social engineering through **user education**. Educating the end user to recognize malicious content and know what to do when they spot something suspicious is a critical mitigation strategy. Some examples of user education include teaching them to:

- Spot suspicious elements in an email message.
- Never respond to external requests for personal information.
- Lock devices when not in use.
- Abide by policies on how to store, share, and remove company data.

Threat intelligence and detection

Threat intelligence and **threat detection** allow an organization to collect systems information, details about vulnerabilities, and information on attacks to develop and implement policies that defend against cyberattacks. This collection of information can be a technological solution that automatically collects information and hunts for and responds to attacks and vulnerabilities.

Implementing and enforcing mitigation strategies is crucial to an organization's cybersecurity.

https://youtu.be/D6xPo2z7thM

What is prevention software?

Part of the Zero Trust strategy includes implementing a network defense plan that protects data and applications to make them more secure. Using prevention devices and software helps organizations reach this goal.

Prevention devices or software well known for securing networks are:

- Firewalls
- Virtual private networks (VPN)
- Antivirus software
- Routine device updates
- **Firewalls**

A **firewall** is a network security device that filters incoming and outgoing network traffic. Firewalls prevent unwanted network traffic and malicious software from reaching the network. Networks that don't use a firewall accept all connection requests from any device anywhere, which is a huge security risk.

VPNs

A **virtual private network** (VPN) is a secure connection from one network to another. A VPN extends a private network across a public network by creating an encrypted tunnel. Data transferred within this tunnel is hidden from third parties. For example, organizations can provide a VPN connection to end users who need to sign into the company's network from locations that don't have secure connections, like coffee shops or airports. A VPN increases security by making sure that:

- The user's location stays private.
- Data is encrypted.
- Identity is anonymous.

Antivirus software

Antivirus software is also an essential component of network security. Antivirus software protects the device against malicious software coming from the internet. Antivirus software works by using the main actions of detection, identification, and removal of threats.

Routine updates

Regularly updating software and firmware on all devices is one of the easiest ways to protect against cyberattacks. Operating systems are continually being updated to protect devices against newly discovered vulnerabilities and exploits. Because cyberattacks are constantly evolving, **routine updates** are paramount in keeping information protected.

https://youtu.be/6NdPmXyvnfU

How to defend against attackers

Defending against cybercriminals and hackers is a major part of cybersecurity. Cyberdefense includes gauging the risk, anticipating the attack, and then deciding how to defend against and outsmart the attackers or "hackers."

Three types of defenses against hackers are:

- Cryptography
- Encryption
- Hashing

Cryptography

Foundational to protecting the CIA Triad of confidentiality, integrity, and availability of information, **cryptography** is an essential element in defending against cyberattacks.

The word cryptography means "hidden language." The prefix "crypt-" means "hidden", and the suffix "-graphy" means "language." In the technology world, cryptography is defined as *the use of codes to convert data so only specific recipients can read it*.

This concept isn't a new one. The Egyptian practice of hieroglyphics—using complex pictograms only known to an elite few—was probably the first use of cryptography.

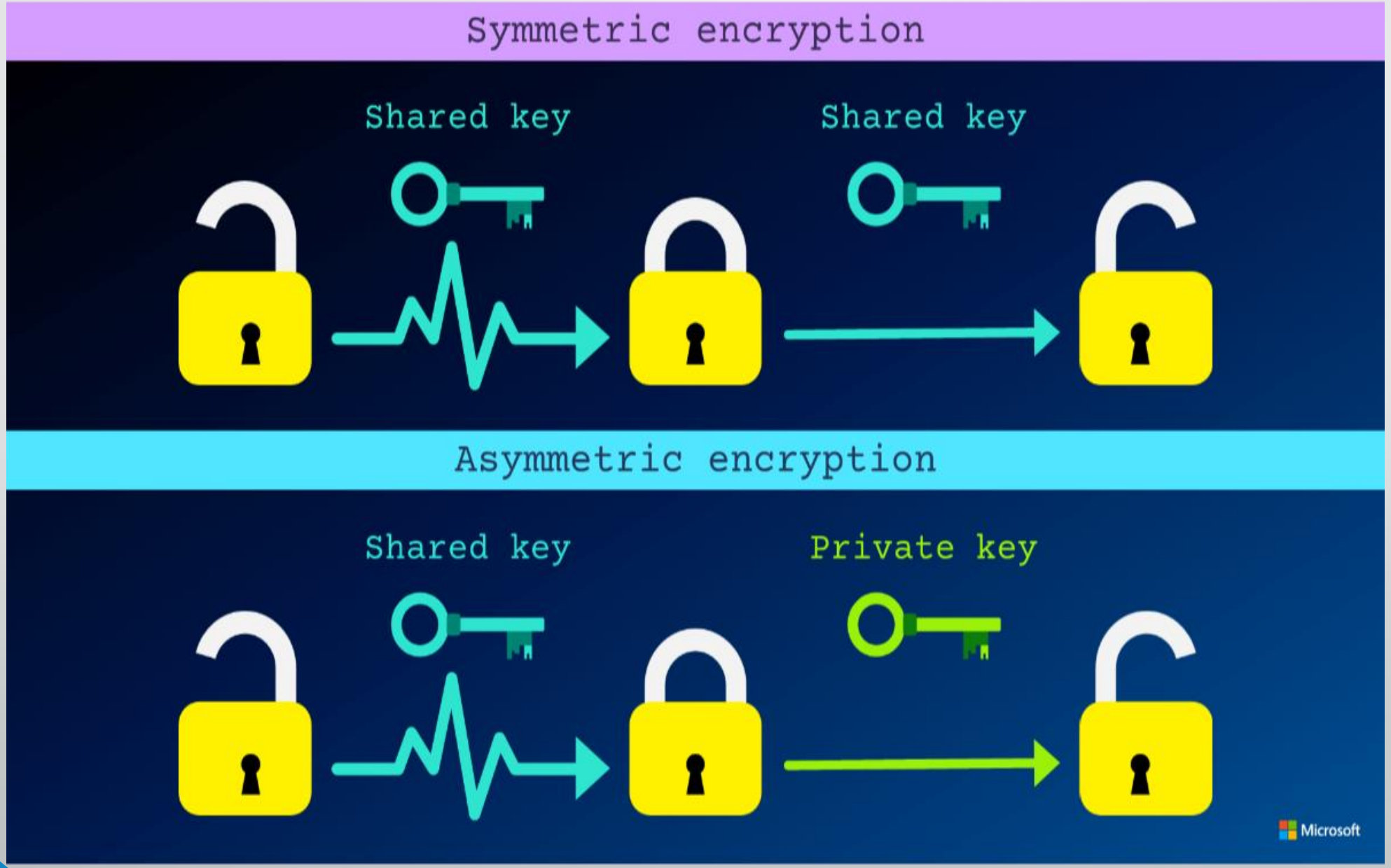
Cryptography has its own language of terms and phrases. Two of the most important are:

- **Plaintext** – any message (documents, music, pictures, movies, data) waiting to be cryptographically transformed.
- **Ciphertext** – represents the encrypted/secured data.

Encryption

Encryption is the process of making data unreadable and unusable to unauthorized viewers. Using or reading encrypted data requires a **secret key** to decrypt the information. A secret key is a *variable* in cryptography that is used with an algorithm to encrypt and decrypt data.

The two top-level types of encryption are symmetric and asymmetric. **Symmetric encryption** uses the same key to encrypt and decrypt the data. **Asymmetric encryption** uses a public key and private key pair. Either key can encrypt data, but a single key can't be used to decrypt encrypted data. To decrypt, a paired key is required.

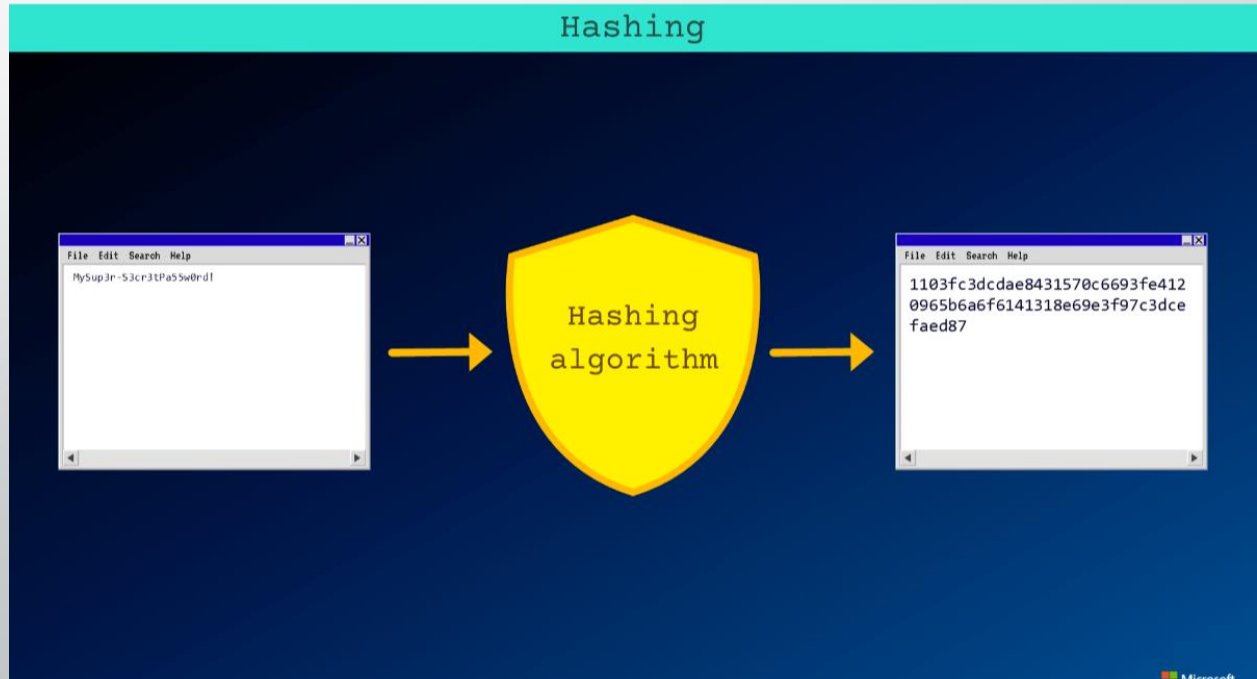

Symmetric encryption
Shared key
Shared key
Asymmetric encryption
Shared key
Private key
Microsoft

Hashing

Hashing is different from encryption in that it doesn't use keys, and the hashed value isn't decrypted to the original. The process of hashing uses an algorithm that converts text to a unique fixed-length value called a "hash." Whenever text is hashed using the same algorithm, the same value is produced.

Hashing is often used to store passwords, which is more secure than storing passwords in plain text.

https://youtu.be/KDeFrpzoL5w



Protect your passwords

This unit focuses on cybersecurity measures designed to safeguard personally identifiable information (PII) and maintain online privacy on classroom devices.

Effective password use

Creating a strong, unique password that is difficult to crack is a frontline defense for your personally identifiable information (PII) and sensitive data. For example, if you fall for a social engineering trick that reveals your computer username, it only takes 5 minutes for a cybercriminal to figure out a complex, 8-character password like Tx5!rp9? using a computer and artificial intelligence. Although this password is complex and unmemorable, it presents a security vulnerability. You can dramatically reduce the chance of a social engineer figuring out a password by making it more complex and lengthier.

One way is to choose a phrase, sentence, quote, or lyric that is meaningful to you but unknown to someone else, then change the characters. Follow these steps to create a strong password:

- **Find a memorable phrase:** A fan of the band Bon Jovi might love the song, *Livin' on a Prayer*, which includes the line: Tommy used to work on the docks. This can be the starting point for a password, but it isn't secure in its current form. Notice that the lyric is long–about 31 characters including spaces.
- **Remove spaces:** Take out the spaces in the phrase. For example: Tommyusedtoworkonthedocks. You can also replace spaces with hyphens (-) or underscores (_) between the words. For example: Tommy_used_to_work_on_the_docks
- **Add uppercase letter(s):** Replace at least one of the characters with an uppercase letter. For example: TommyusedtoworkontheDocks.
- **Add number(s):** An easy way to add numbers to a password is to replace letters with numbers that are visually similar. For example: Tommyu5edtoworkontheDock5. Other potential substitutions include:
  - O/o to 0
  - L/l to 1
  - E/e to 3
  - S/s to 5
- **Add special character(s):** Using a phrase like a lyric makes it easy to add a special character like a punctuation mark or use special characters to replace letters (like the @ sign instead of a). For example: Tommyu5edtoworkontheDock5!

Ensure that your password remains strong and secure by also following these guidelines:

- Avoid using publicly available information in your passwords like family names, pets, birthdays, and addresses.
- Never share your password with another person, including colleagues, friends, and even school technology personnel.
- Use a unique password for every website or application. Try a password manager to save and generate unique passwords.
- Don't write your password on sticky notes, notebooks, or other places that are easily discovered. Make it memorable or use a password manager.
- Don't save passwords in browsers that are used by other people. If the device is shared, never allow a browser to remember your credentials.

Password resets

It's important to change your passwords in the event you either fall victim to a social engineering attack or suspect your credentials (username and password) might be compromised.

Some common password reset options in schools include:

- Requiring educators to use a different set of credentials for each service that requires an account, each with its own password reset steps.
- Providing self-service tools that allow educators to reset their password on a designated website that then changes the password for other services.
- Using a single sign-on service (SSO) that allows educators to use one set of credentials, like a Microsoft 365 account, with one set of steps for changing passwords.
- Follow these steps on our support page to reset your password on your Windows device.

Identity authentication

Schools now require more than just a username and password to access computers, networks, databases, and systems. Many use additional identity authentication measures to make it more difficult for a social engineer to use stolen credentials that might have been compromised.

There are two common approaches to confirming identities beyond usernames and passwords. Review these approaches then use the video to learn more.

- **Two-factor authentication (2FA):** This authentication approach uses a phone call, text message, mobile app notification, or one-time password along with a username and password to confirm an identity.
- **Multifactor authentication (MFA):** This authentication approach uses more than two methods of authentication to confirm an identity. Sometimes this includes 2FA methods along with a file (token) on your computer, your fingerprint, or a camera with facial recognition.

https://youtu.be/nc7fpGJsE1g

Protect your personally identifiable information

Some cyber threats try to get you to reveal personally identifiable information (PII), or any information that directly identifies you as an individual, in order to gain access to authorized services or steal privileged information.

Examples of PII include:

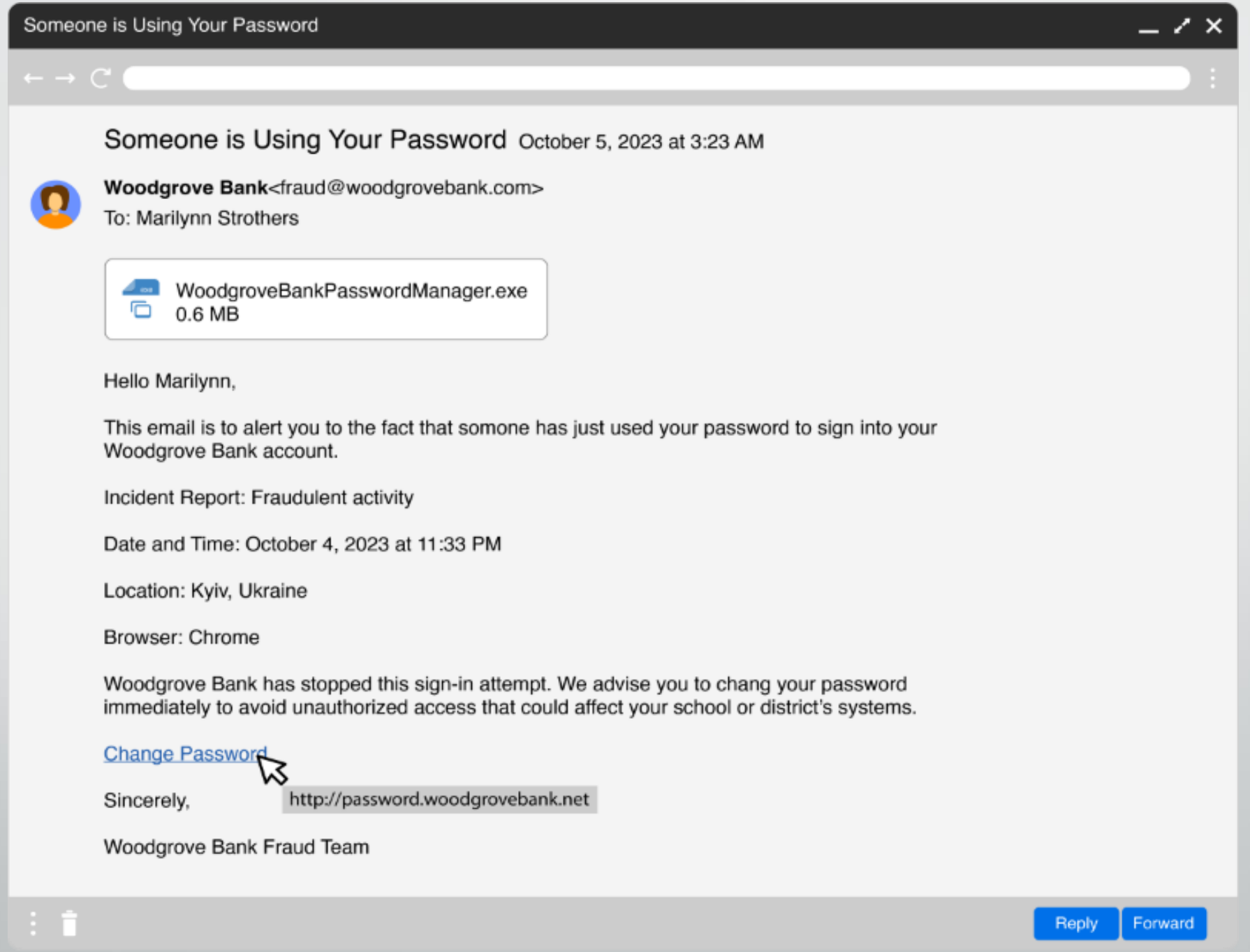
- Full names
- Addresses
- Email addresses
- Telephone numbers
- Social security numbers
- Birthdays
- Account information (such as usernames and passwords)
- Demographic information that identifies a person
- Educational records

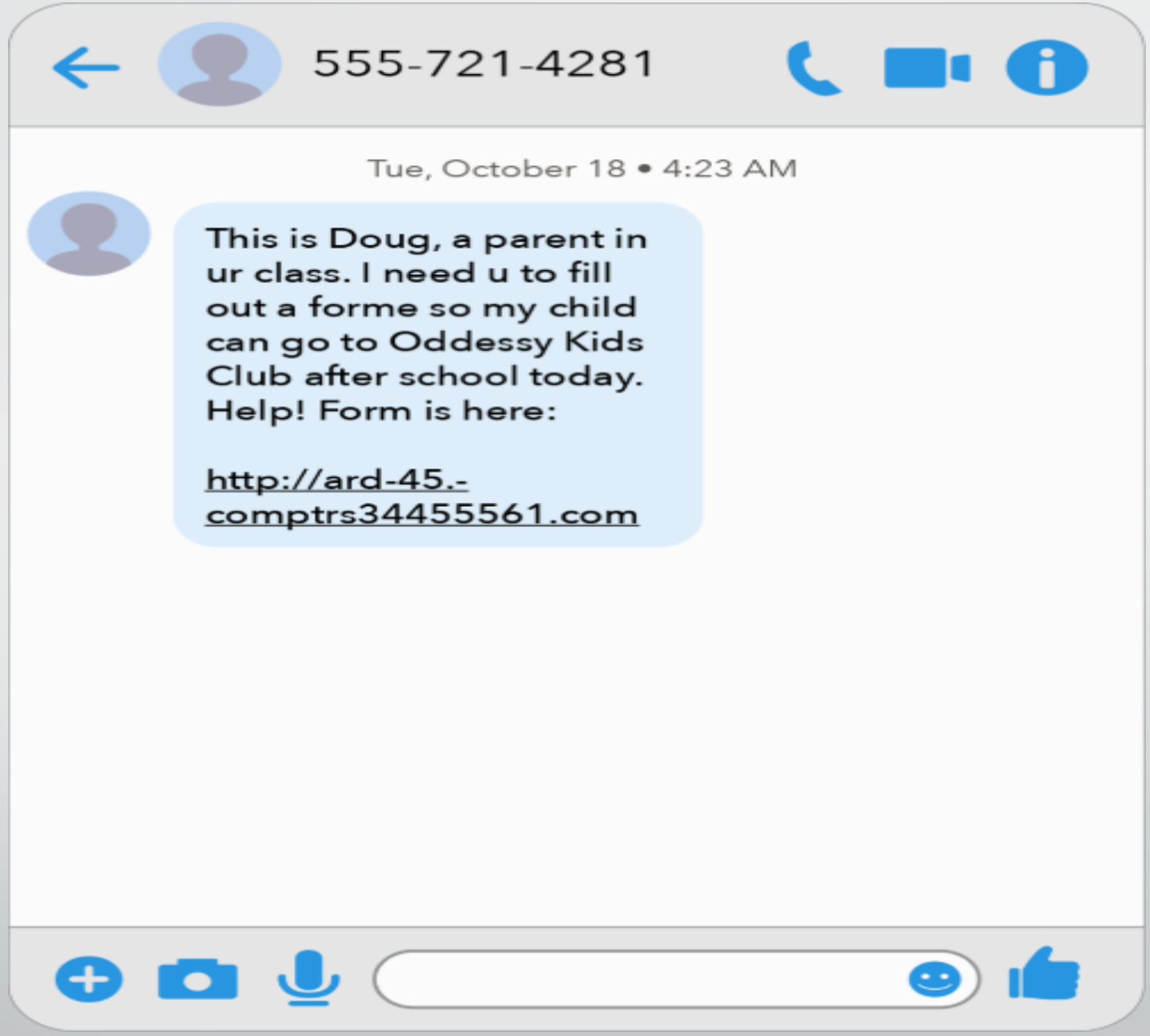
Know the threat: Phishing

Phishing occurs when a cybercriminal pretends to be a trusted institution (like an HR department) or an individual (like your principal or a parent) to persuade you to share personal information. Phishing attempts are often sent through email or text messages, but sometimes appear as browser pop-ups or spoofed websites. In 2022, Microsoft Security blocked over 710 million phishing messages every week. Although robust security tools prevent many phishing attempts from ever reaching educators, messages still arrive in inboxes because social engineers are adept at their craft.

Identify phishing scams

If you're the target of a phishing scam, would you know what to look for? Try to identify the red flags in the screenshots of a phishing email and a text message


Someone is Using Your Password
Someone is Using Your Password October 5, 2023 at 3:23 AM
Woodgrove Bank<fraud@woodgrovebank.com>
To: Marilynn Strothers
WoodgroveBankPasswordManager.exe
0.6 MB
Hello Marilynn,
This email is to alert you to the fact that somone has just used your password to sign into your Woodgrove Bank account.
Incident Report: Fraudulent activity
Date and Time: October 4, 2023 at 11:33 PM
Location: Kyiv, Ukraine
Browser: Chrome
Woodgrove Bank has stopped this sign-in attempt. We advise you to chang your password immediately to avoid unauthorized access that could affect your school or district's systems.
Change Password
Sincerely,
http://password.woodgrovebank.net
Woodgrove Bank Fraud Team
Reply
Forward


555-721-4281
Tue, October 18 • 4:23 AM
This is Doug, a parent in ur class. I need u to fill out a forme so my child can go to Oddessy Kids Club after school today. Help! Form is here:
http://ard-45.-comptrs34455561.com

Resources

- CIA triad diagram (Microsoft Learn)
- Zero trust principles graphic (Microsoft Learn)
- Hashing diagram (Microsoft Learn)
- Symmetric and asymmetric encryption diagram (Microsoft Learn)
- Examine ransomware and extortion-based threats (Microsoft Learn)
- Prepare to teach SC-900 Microsoft Security, Compliance, and Identity Fundamentals in academic programs (Microsoft Learn)
-