
Cybersecurity
Awareness Month
MARIST

What is Cybersecurity? Why is it Important?

Cybersecurity is the process of:

- Protecting systems, networks, and data from unauthorized access or attacks
- It utilizes a varied set of technologies, processes, and practices designed to safeguard information

Cybersecurity is important because:

- It's crucial for protecting personal information
- Individuals and companies can lose up to millions from cyberattacks
- Important industries such as healthcare need to remain running at all times
- Users need to trust in Cybersecurity if they wish to feel safe on the Internet

General Best Practices & Tips

Use strong, unique passwords

- Use hard-to-guess passwords
- Don't use the same password for multiple accounts
- Utilize multi-factor authentication (MFA) when available

Keep your devices up-to-date

- Always update your computers, phones, and apps to the latest version
- Updates fix issues and protect your devices from new threats

Protect your internet connection

- Use security programs like antivirus software and firewalls to secure your network and devices
- Use VPN when working remotely or on a public network

Stay informed and be cautious

- Learn how to spot suspicious emails/messages
- Do not click unknown links or download unknown files
- Share safety tips with others and encourage cyber awareness.

Password Safety Tips

Passwords are sometimes the only line of defense to protect our accounts from unwanted access

It is important to have secure and unique passwords that bad actors cannot easily guess or reuse across websites/services

- Use a password longer than the default minimum
- Use a mix of lowercase, uppercase, numbers, and symbols
- Reset your password at least once a year
- Use a password manager to save and safely store your passwords, that way you only need to remember one password

Social Engineering: What is it?

Attackers are always attempting to trick people into giving away sensitive information or access by pretending to be someone trustworthy. (e.g. a colleague, IT support, high ranking official)

Types of Social Engineering

- Phishing
- Vishing (Voice Phishing)
- Pretexting
- Baiting
- Tailgating

How do you spot it?

- Urgency or pressure to respond
- Unusual requests for information
- Unfamiliar contacts
- Emotional manipulation
- Physically following

How do you protect yourself?

- Phishing
- Vishing (Voice Phishing)
- Pretexting
- Baiting
- Tailgating

Email Security: Phishing, Quishing, and More!

What is Phishing?

- It is when bad actors send fake emails pretending to be someone trustworthy to trick you into giving away sensitive information
- **How do you spot it?** Look for poor grammar and spelling errors, urgent requests or threats, and hover over links before clicking to see where they lead.

What is Quishing?

- It is when bad actors use QR codes to lead unsuspecting users to a fake website designed to steal information.
- **How do you spot it?** Do not scan QR codes from unknown/suspicious sources. Be cautious of emails with QR codes asking you to log in or verify information.

General Tips

- Always verify links before visiting
- Contact person or organization directly via phone call if something feels off
- Do not open attachments from unknown senders.

Mobile Security

People use their phones everyday, be it for work, social media, or even ordering food. So it's important to keep them secure.

Here are some easy ways to keep your phone safe:

- Download an Antivirus
- Don't click random links
- Don't scan random QR codes
- Use a safe password (The last 4 digits of your phone number is not secure)

Cyber Physical Security

While not typically thought of, physical security is still a part of cybersecurity, as devices still need to be physically secure

Here are some tips on maintaining physical security:

- Don't leave your device unattended
- Lock public computers if you need to step away from them for some time
- Restart public computers when you are done using them

Malware: What is it?

Malware is any software designed to disrupt, damage, or otherwise compromise a computer system, network, or other device

Some types of Malware include:

- Viruses – Attached to legitimate files and spread when infected files are shared
- Worms – Self-replicating malware that spreads without human interaction
- Trojan Horses – Disguised as legitimate software but contains hidden malicious code

How Malware Spreads:

- Phishing
- Infected Website/Downloads/USB Drives
- Software Vulnerabilities

Prevention:

- Keep software up-to-date
- Use Antivirus
- Avoid suspicious downloads and emails

Impact of Malware:

- Data Theft – Stolen personal, financial, or corporate information to be sold for money
- System Damage – Corrupts or deletes data in order to disrupt operations
- Financial Loss – Costs associated with recovery efforts, legal fines, and potentially ransom payments

Ransomware: What is it?

Ransomware is a type of malware that focuses on encrypting files on a computer system and demanding money for the decryption or retrieval of them.

In the event of a ransomware attack:

- Isolate your device from the network – The Ransomware may try to infect more devices on the network so it can do more damage
- Keep Calm – Ransomware tries to make use of a sense of urgency to get you to pay exorbitant amounts of money
- Do NOT Pay the Ransom – There is no guarantee that paying money will result in file recovery and it encourages further attacks.
- Report to Authorities/Response Teams – Report the attack to potentially recover your data and help law enforcement track ransomware gangs
- Restore from Backups – If backups exist, verify they are uninfected before restoring. Then ensure systems are clean before reconnecting to the network
- Strengthen Security Measures – Identify how the attack occurred and take measures to prevent it from re-occuring.

Questions?

For any questions or cybersecurity related concerns, contact Cybersecurity@marist.edu

To report phishing emails, contact, Phishing@marist.edu

Visit https://www.marist.edu/information-security for more cybersecurity related content.

Visit https://www.marist.edu/gonephishing for examples of phishing observed in our environment.

www.marist.edu


Thank You!
MARIST