CyberSecure MISSISSIPPI

Cybersecurity Awareness Fundamentals

CyberSecure MISSISSIPPI

Shelly Hollis
Director
Center for Cyber Education
shelly.hollis@cce.msstate.edu

CyberSecure MISSISSIPPI

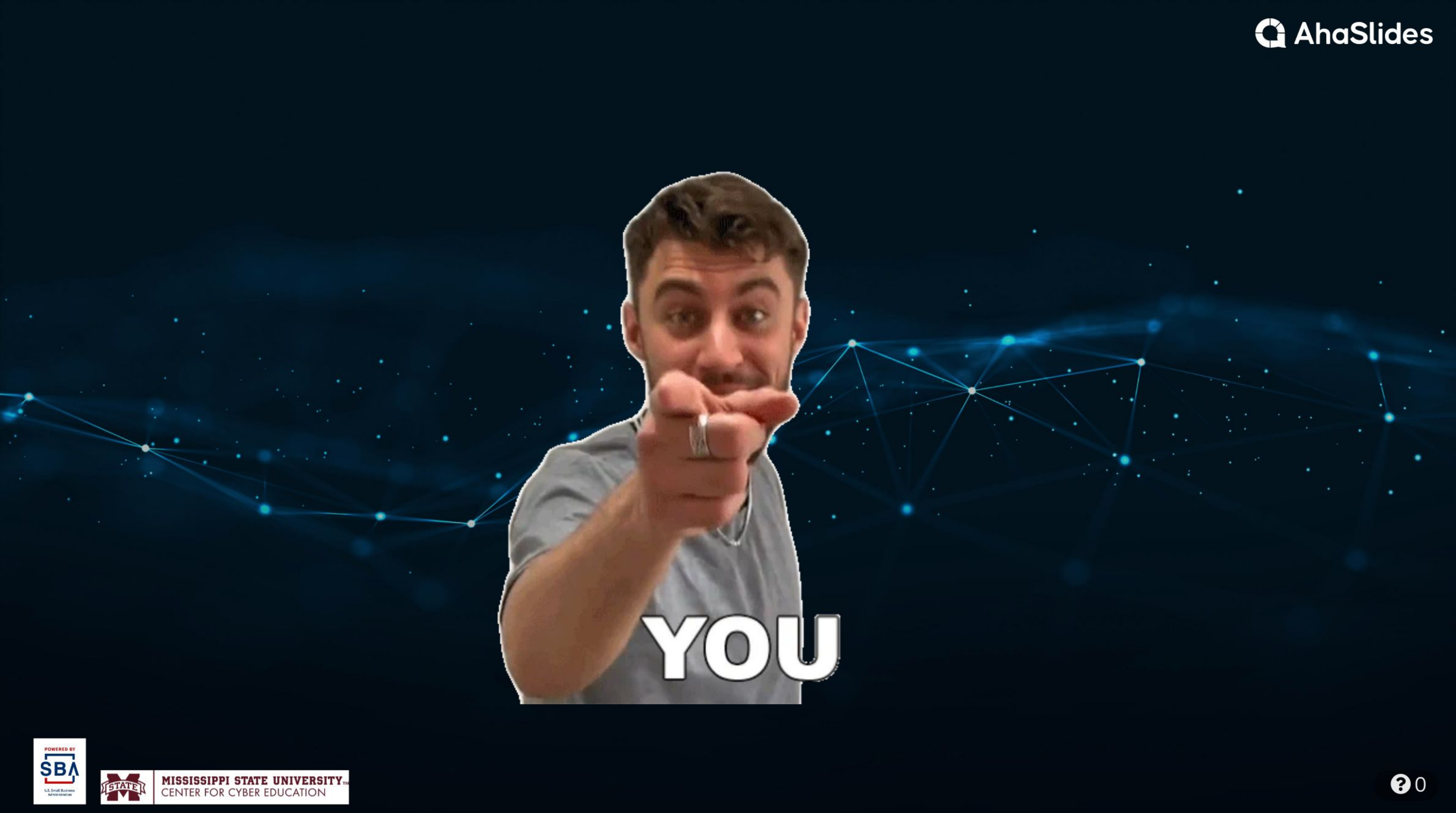
Outline

- Introduction to Cybersecurity
- Foundations of Cybersecurity
- Threats to Cybersecurity
- Protecting Your Company Information
- Cybersecurity & Social Media

Cybersecurity

The protection of networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

What is the weakest link in your organization?



Everything is online and connected

- Email
- File storage
- Pictures
- Video conferencing
- Shopping/Ordering
- Shipping
- Banking/Payroll
- Point-of-Sale

What is at risk?

- Loss of Access
- Loss of Personal Information
- Loss of Money
- Loss of Business Information
- Loss of Reputation/Business
- Loss of Critical Services

Did you know?

"50% of small to medium-sized businesses (SMB) have been the victims of cyber attack and over 60% of those attacked go out of business."

Dr. Jane LeClair, Chief Operating Officer
National Cybersecurity Institute

Local Government Attacks

Atlanta: Ransomware

Demand: $51,000 in Bitcoin

Cost: $2.7 Million

Baltimore: Ransomware

Demand: $80,000 in Bitcoin

Cost: $6 Million

Pensacola

Demand: $1Million

Cost: $140,000

Small Business Cybersecurity Stats

Incidence Rates:

- 43% of cyber attacks target small businesses.
- 60% of small businesses go out of business within six months of a cyber attack.

Cost of Cyber Attacks:

- The average cost of a cyber attack on a small business is $200,000.
- 52% of small businesses experienced a cyber attack in the last year.

Common Types of Cyber Attacks:

- Phishing attacks: 76%
- Malware: 60%
- Ransomware: 34%

Security Measures:

- 30% of small businesses have an active cybersecurity policy.
- 47% of small businesses have no understanding of how to protect themselves against cyber attacks.

Employee Training:

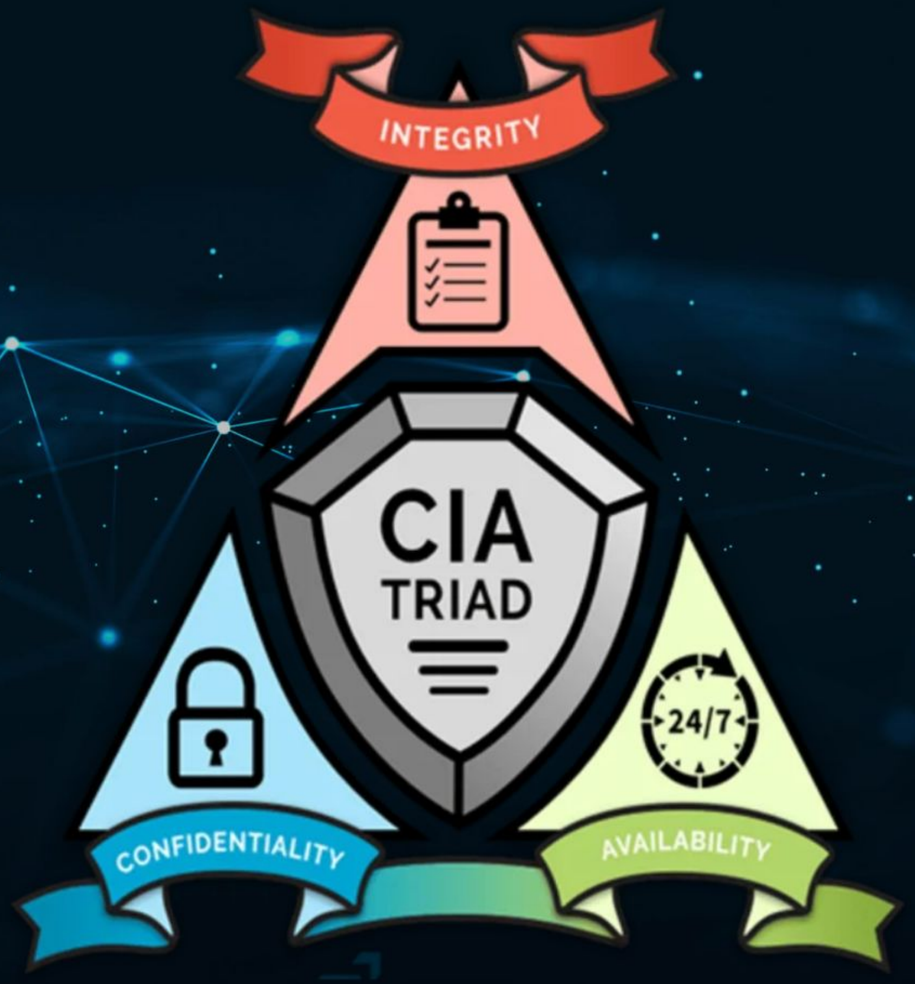
- 48% of data breaches are caused by acts of malicious intent, human error, or system glitches.
- 21% of small businesses conduct annual security training.

Foundations of Cybersecurity

CIA Triad

Three principles make up the foundation for everything associated with cybersecurity.

Everything that needs t obe protected will depend on at least one of these principles.



Threats to CIA Triad

Confidentiality Threats

- Data Breaches
- Weak Passwords
- Phishing Emails
- Spyware
- Ransomware

Integrity Threats

- Not Backing Up Data
- Unathorized Access to Data
- Malware
- Ransomware

Availability

- System Crashes
- Network Errors
- Power Outages
- DoS Attacks
- Ransomware

Phishing

Attacks structured to get victims to perform some type of action.

Phishing attempts often play on the emotion of the receiver:

- Fear
- Joy
- Pain
- Urgency

Identifying Phishing Threats

Check Email For

- Misspelling
- Close but not the same
- Never respond to requests for credentials from within email

Check URLs

- Hover over URL to see path
- On a phone, this is a long press
- Verify the URL is accurate

Check Links & Attachments

- Avoid clicking on links without verifying them
- Do not open attachments without verifying
- If it seems odd or unlikely, it probably isn't valid

Social Engineering

Social Engineering is the art of manipulating people into performing tasks.

- These tasks tend to provide the attacker with valuable data or money.
- Technical background not always required.

Malware

Malware is any software that has malicious intent.

There are many different types of malware such as:

- Ransomware
- Viruses
- Spyware
- Worms

Ransomware

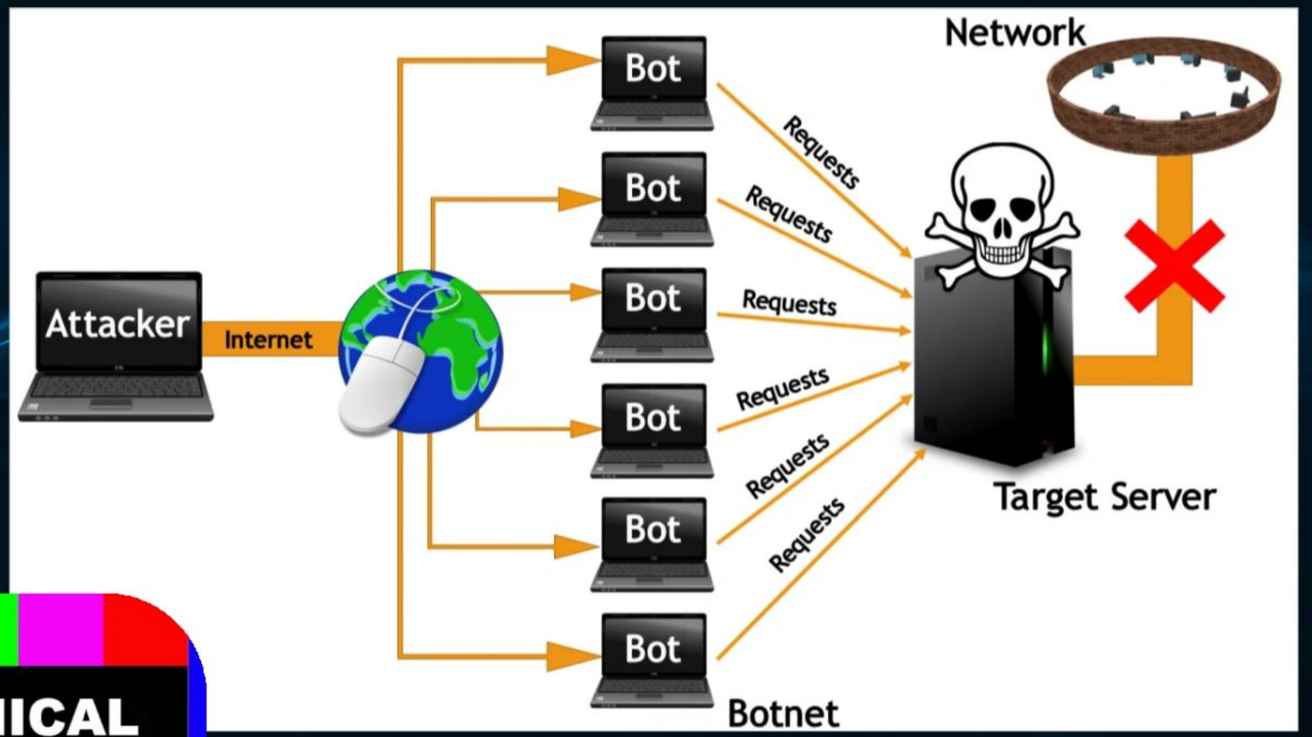
Ransomware is malicious software designed to block access to data until money is paid.

- Can pose as a legitimate software installation
- Can encrypt your whole computer
- Unlocked only with an encryption key
- Attackers usually ask for you to pay a ransom to gain access to your data again

"Statistics demonstrate that 82% of ransomware attacks are upon small to midsize businesses."

Denial Of Service

A Denial of Service or DoS attack is where an attacker attempts to make a computer or network resource unavailable by overwhelming it with a flood of traffic.



3 Critical Steps to Protecting Company Data

Insist on strong passwords and train employees.

1

Recognize the threats and vulnerabilities around you.

2

Know what data you have and make sure it is backed up regularly.

3

Good Password Hygiene

- Never use the same password across multiple accounts.
- Do not use a similar password as one that you have used in the past.
- Change your passwords at least once a year.

Password Managers

- What is a Password Manager?
  - Password managers like LastPass keep up with all your passwords in one secure location.

- A password manager can also provide you with randomized passwords that can not be guessed or easily brute forced.

What is Two-Factor Authentication

Authentication

The ability to verify the identity of someone or something before allowing access.

Checks multiple things to confirm an identity

Something you know

Something you have

Something you are

Often uses password and mobile devices to confirm an identity

Antivirus Software

- Antivirus software such as Windows Defender, Avast or Malwarebytes are free products available to protect your computer.

- Updating your antivirus software will help to keep your computer protected from the latest threats.

Updating Software

- Keeping your applications updated will help prevent your computer and phone from being exploited by software vulnerability

- Malware usually exploits vulnerabilities in outdated software

Public Wi-Fi: Guide for Users and Providers

For Users:

- Use a VPN.
- Avoid Sensitive Activities like accessing bank.
- Ensure you connect to a legitimate Wi-Fi network.

For Businesses:

- Implement Strong Encryption: Use WPA3.
- Monitor for Threats: Deploy intrusion detection.
- Change default passwords on wireless access points.

Virtual Private Networks (VPN)s

- What is a VPN?
  - VPNs encrypt your data crossing the network so that an attacker cannot see it.

- Can use a VPN to prevent attackers from viewing and making changes to the data exchanged over a public network.

BACKUP, BACKUP, & BACKUP AGAIN!

- Backup your data regularly and follow the 3-2-1 rule.
- Backups are the best defense against ransomware!

3-2-1 Rule

Cybersecurity and Social Media

According to the Better Business Bureau, *"Small businesses [social media accounts] are three times more likely to be targeted by cybercriminals than larger companies."*

Cybersecurity & Social Media

If not careful, social media can be leveraged by attackers as a source of information.

Potential attacks include:

- Malicious Adds
- Might Target your Followers
- Might Capture Sensitive Personal or Business Information

c.

Protecting Information on Social Media

Check for unfamiliar Posts to ensure no one has gained access to your business account

Never repeat password across accounts

Enable two-factor authentication for ALL accounts that are available

Contact Us!

MISSISSIPPI STATE UNIVERSITY™
CENTER FOR CYBER EDUCATION

- Shelly Hollis
  - Center for Cyber Education
  - shelly.hollis@cce.msstate.edu
  - 662-325-0585