

# Mankato Computer Technology University

Protecting yourself from computer Scams



# Introduction (Why This Matters)

- What are computer Scams
- Common Scams
  - phishing, tech support scams, email fraud, and identity theft.

# Types of Computer Scams

- Phishing Scams
  - How scammers trick people into sharing personal information via fake emails or messages.
  - Example: "Your bank account is compromised" emails.
  - What it is: Scammers impersonate legitimate organizations (e.g., banks, tech companies) via email, text messages, or websites to steal personal information such as passwords, credit card numbers, and social security numbers.
  - How it works: They send emails or messages that look real and usually contain a link that leads to a fake website where you're prompted to enter your information.

# Tech Support Scams

- Scammers posing as tech support agents, often calling or popping up messages on the screen.
- What it is: Scammers pose as tech support agents from companies like Microsoft or Apple and claim there's a problem with your computer.
- How it works: They typically contact you via phone or pop-up message and may request remote access to your computer or payment for fake software fixes.

# Ransomware Attacks

- What it is: A type of malicious software (malware) that locks you out of your computer or encrypts your files, demanding a ransom to regain access.
- How it works: Victims usually get infected by clicking on malicious links or downloading unsafe files. The scammer demands payment (often in cryptocurrency) in exchange for unlocking the computer or files.

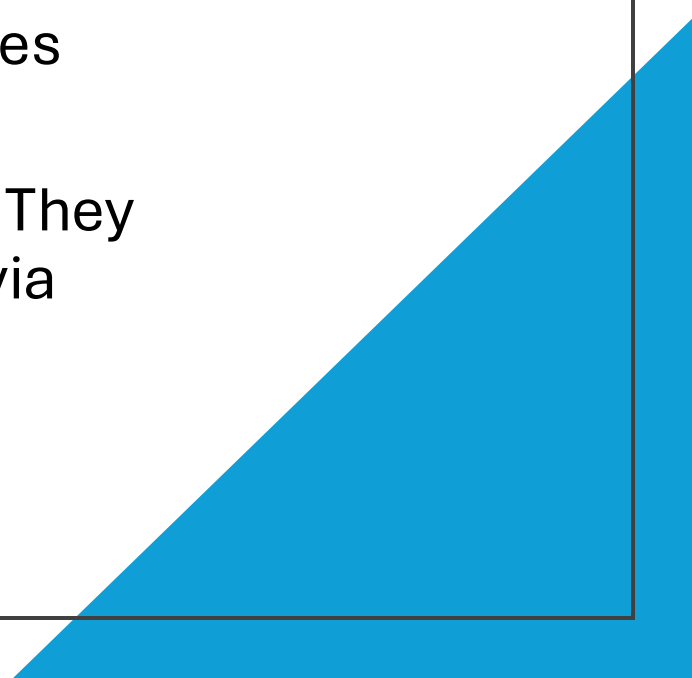
## Fake Antivirus/Software Updates

- What it is: Scammers trick users into believing their computer is infected with malware and convince them to download fake antivirus software.
- How it works: Often appears as a pop-up warning or fake scan results, urging immediate action. The "software" may steal your data or install actual malware.

# Online Shopping Scams

- What it is: Fraudulent online stores or ads offer products at deep discounts, but you never receive the goods.
- How it works: Scammers lure you to fake websites or social media pages offering too-good-to-be-true deals. Once you make a purchase, the product never arrives, and your payment information is compromised.

# Lottery, Sweepstakes, and Prize Scams

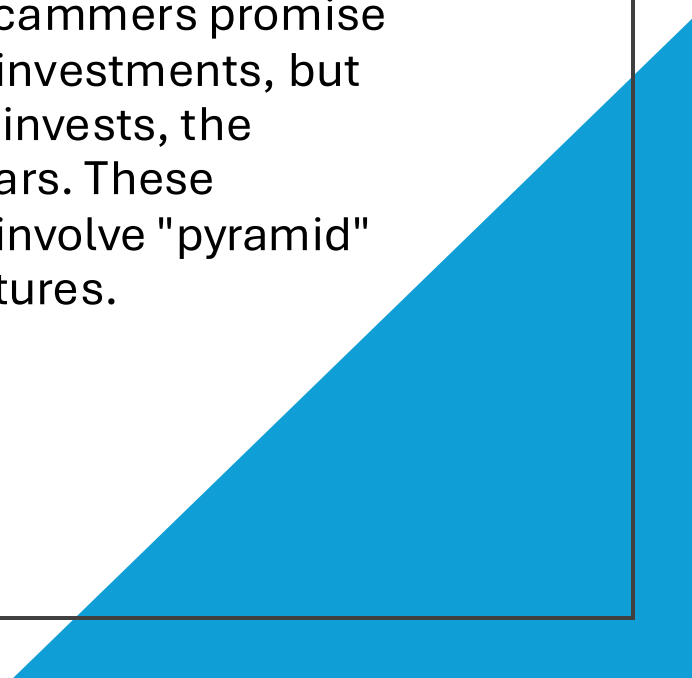
- What it is: Scammers claim you've won a lottery, sweepstakes, or prize, but you need to pay fees or taxes upfront to claim the reward.
  - How it works: These scams come via email or phone. They ask for personal or financial information or payment via wire transfer, gift cards, or cryptocurrency.
- 



# Romance Scams

- What it is: Scammers build fake romantic relationships with victims online, often through dating sites or social media, with the intent to steal money.
- How it works: After gaining the victim's trust, the scammer asks for money due to an "emergency" (e.g., medical bills, travel expenses).

# Investment Scams

- What it is: Fraudulent investment opportunities, often involving cryptocurrency, stocks, or real estate.
  - How it works: Scammers promise high returns on investments, but once the victim invests, the money disappears. These schemes often involve "pyramid" or "Ponzi" structures.
- 


# Work-from-Home Scams

- What it is: Scams offering fake jobs or business opportunities that require you to pay upfront fees.
- How it works: Scammers advertise jobs that promise easy money working from home, but they ask for payment to secure the position, for training materials, or for equipment. After paying, the victim realizes there is no job.

# Bank/IRS Fraud Scams

- What it is: Scammers impersonate banks or government agencies (such as the IRS) and claim there is an issue with your account or taxes.
- How it works: Scammers threaten legal action or financial penalties unless you pay immediately. They may ask for personal information to “verify your identity” and steal sensitive data like social security numbers or bank account details.

# Credential Stuffing and Account Takeovers

- What it is: Scammers use stolen login credentials (from data breaches) to access your online accounts.
  - How it works: Once they access your accounts (e.g., email, bank, or social media), they can steal your personal information, make unauthorized transactions, or use your identity to scam others.
- 
- A blue triangle graphic is located in the bottom right corner of the slide, pointing upwards and to the left.

# Email Attachments/Links with Malware

- What it is: Emails that contain malicious attachments or links that download malware onto your computer.
- How it works: These emails often pretend to be from a trusted source (like a company or friend). Once the attachment is opened or the link is clicked, malware is installed, which could steal your personal information, log keystrokes, or even take over your computer.

# Email Fraud and Fake Links

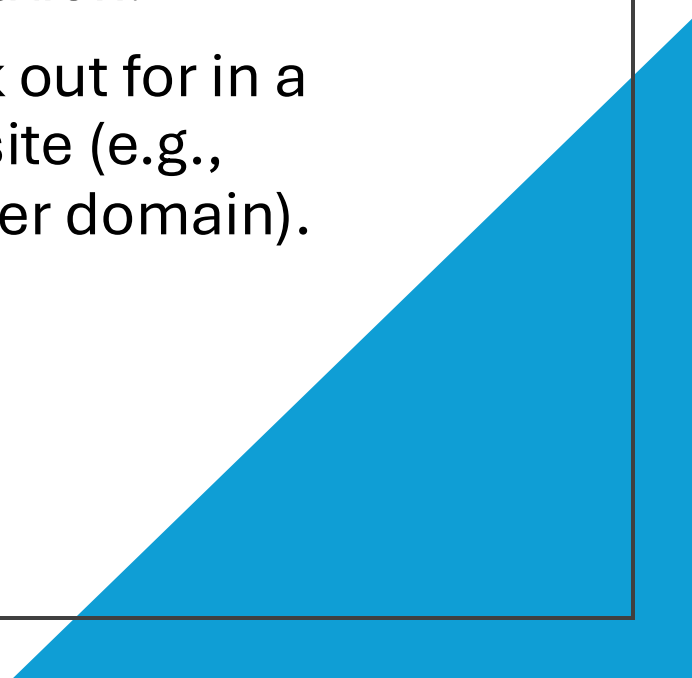
- How to spot fraudulent emails and fake websites.
- Warning signs: poor grammar, unknown sender, suspicious attachments or links.

# How Scammers Operate

- Social Engineering
  - Explain how scammers use emotional manipulation and urgency to create panic.
  - Examples: "You've won a prize!" or "Your account will be closed."



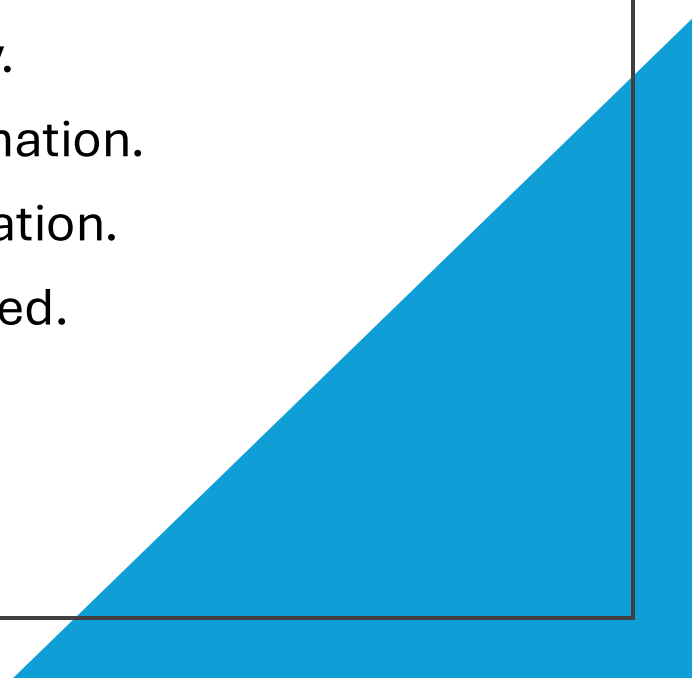
# Fake Websites and Pop-ups

- How scammers mimic legitimate websites to steal information.
  - What to look out for in a secure website (e.g., HTTPS, proper domain).
- 

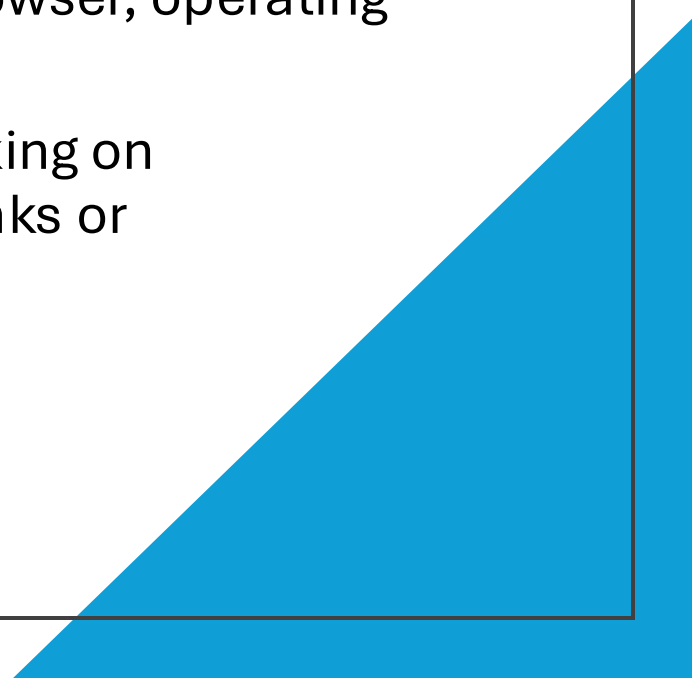
# How to Protect Yourself

- Recognizing Red Flags
- Unsolicited requests for personal information.
- Threats or pressure to act quickly.
- Requests for payments via gift cards, wire transfers, or cryptocurrency.

# How to Protect Yourself:

- Never share personal information in response to unsolicited requests.
  - Be skeptical of emails, texts, or calls that urge you to act quickly.
  - Verify the legitimacy of websites before entering sensitive information.
  - Use strong, unique passwords and enable two-factor authentication.
  - Install reputable antivirus software and keep your system updated.
- 

# Security Best Practices

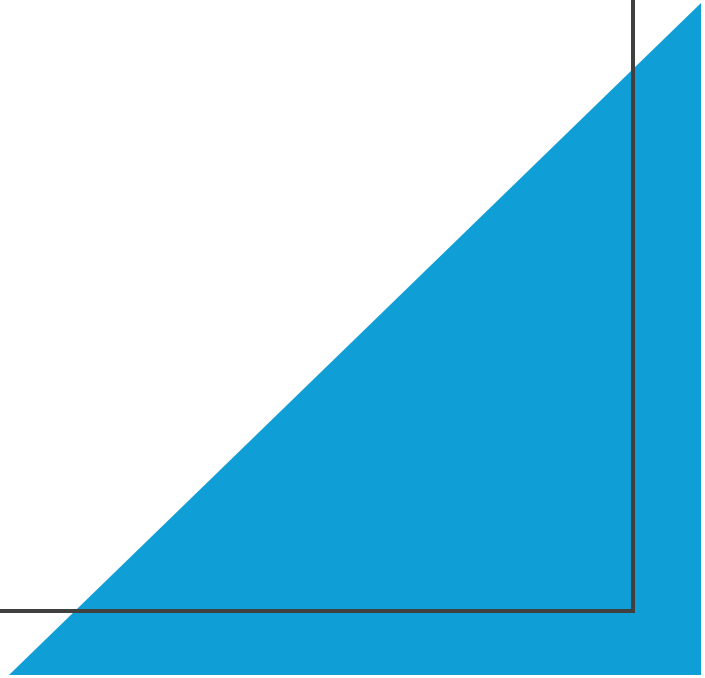
- Using strong, unique passwords.
  - Updating software regularly (antivirus, browser, operating system).
  - Avoiding clicking on suspicious links or attachments.
- 

# *Safe Browsing Tips*

- Only enter personal information on secure, trusted websites.
- Double-check URLs for legitimacy.
- Be cautious with unfamiliar or unsolicited emails.

# What to Do If You've Been Scammed

- Immediate Actions
  - Disconnect from the internet.
  - Run an antivirus scan.
  - Change passwords for important accounts.



# Report the Scam

- How to report scams to authorities (e.g., FTC, FBI, local police).
- Resources available for support (banks, credit bureaus, tech support).

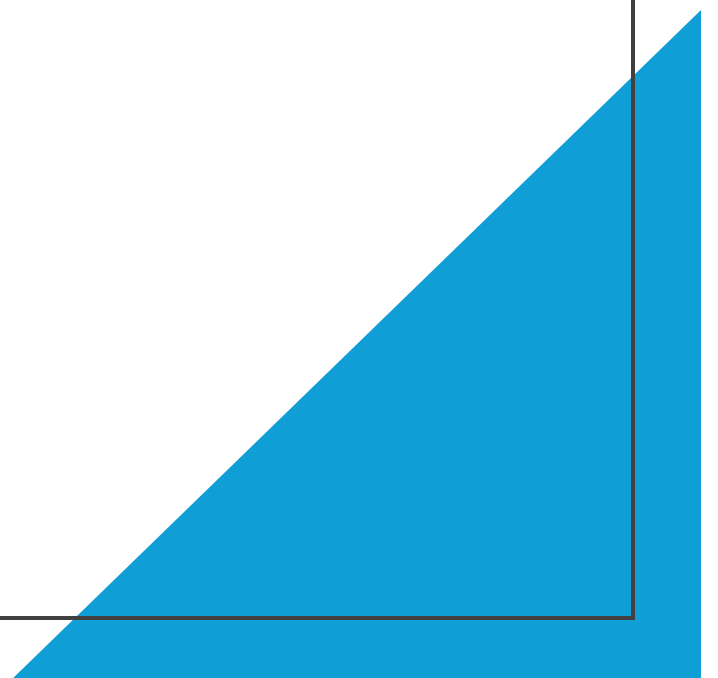
# Resources

- Useful Tools
  - Anti-phishing browser add-ons, antivirus software.
  - Websites and hotlines for scam reporting and information (e.g., AARP Fraud Watch Network).



# Family and Friends

Encourage seniors to talk to a trusted family member or friend before taking action when in doubt.





# How to Spot a Scam

Understanding the Signs

# Scamalot - The Gold

