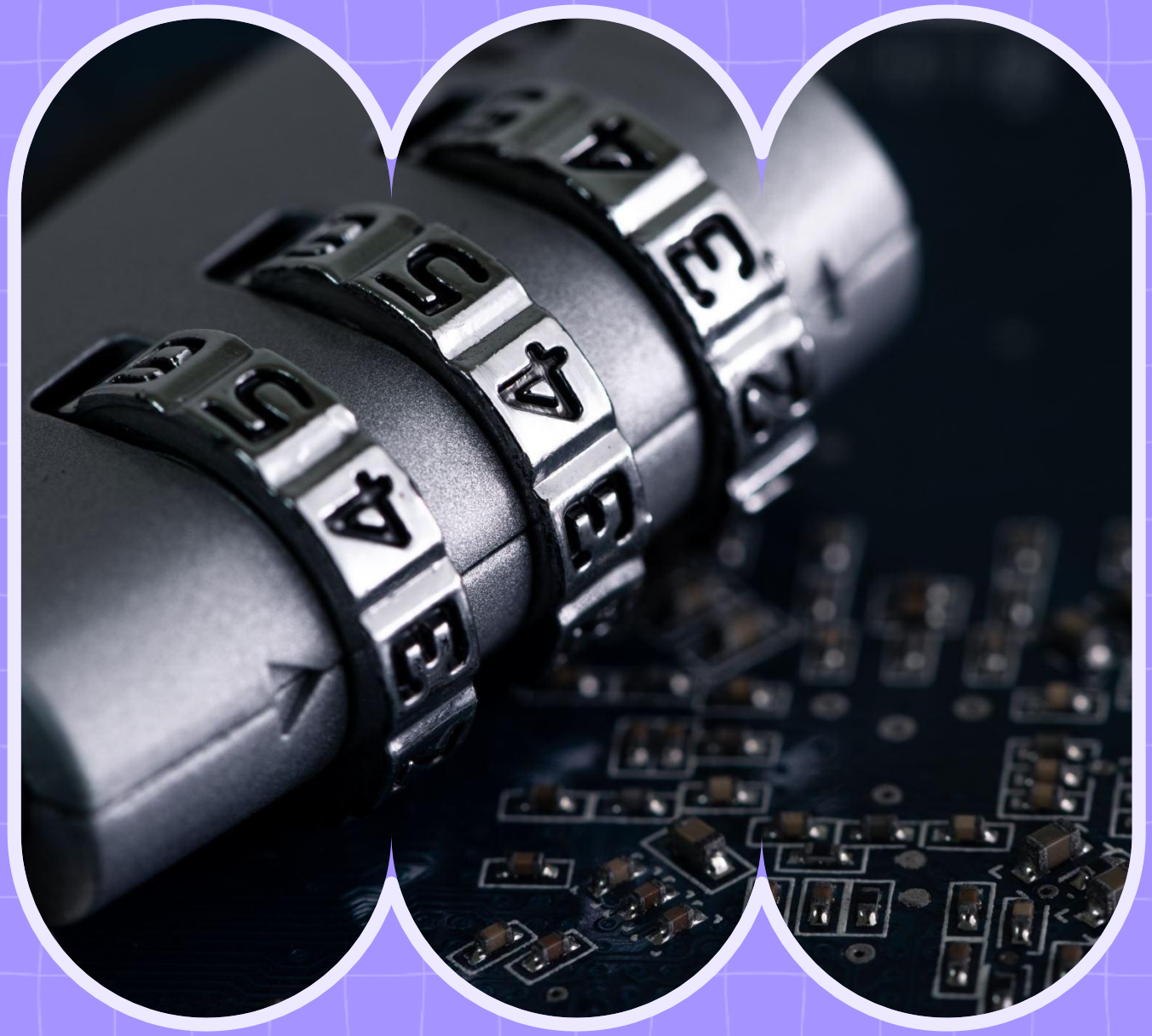
MANKATO
COMPUTER TECHNOLOGY

COMPUTER SCAMS & ONLINE SAFETY - YMCA CLASS

Protecting yourself from online threats and fraud



MANKATO
COMPUTER TECHNOLOGY

Understanding Computer Scams and Online Safety

Overview of Computer Scams and Online Threats

Common Scam Techniques

Scammers use fear and urgency to trick victims into sharing personal data or payments.

Phishing and Impersonation

Phishing emails and impersonation scams mimic trusted companies and government agencies to steal information.

Online Shopping Frauds

Fraudulent websites offer counterfeit or no products after taking payments from buyers.

Recognizing Red Flags

Check for spelling errors, suspicious URLs, unexpected attachments, and high-pressure language to avoid fraud.

MANKATO
COMPUTER TECHNOLOGY

Class Goals

By the end of this session, participants will:Recognize the most common online scams.

1. Identify red flags that signal a scam.
2. Learn how to protect their devices, accounts, and personal information.
3. Know what to do if they think they've been scammed.
4. Practice safe online habits.

Common Types of Online Scams

Phishing Scams

Phishing scams impersonate trusted organizations through emails or texts to steal personal information.

Tech Support Scams

Fraudsters claim computer infections, using fake pop-ups to pressure users into calling for fake help.

Online Shopping Scams

Fake retail sites or ads offer discounts but deliver counterfeit or no products to buyers.

Romance and Social Media Scams

Scammers build trust emotionally online or through social media, then request money or personal data.

MANKATO
COMPUTER TECHNOLOGY

Protecting Yourself from Scams

Strong Password Practices

Use passwords with at least twelve characters combining letters, numbers, and symbols. Use unique passwords for each account.

Multi-Factor Authentication

Enable MFA to add a second verification step, preventing unauthorized access even if passwords are compromised.

System Updates and Security

Keep operating systems, browsers, and antivirus software updated to patch security vulnerabilities scammers exploit.

Safe Browsing and Red Flags

Avoid suspicious links, verify URLs, and be cautious of urgent or unexpected requests in messages or emails.

MANKATO
COMPUTER TECHNOLOGY

Responding to a Suspected Scam

Immediate Actions After Suspicion

Disconnect from internet and run antivirus scans to stop malware and identify threats quickly.

Securing Accounts

Change passwords immediately for banking, email, and social media accounts to prevent unauthorized access.

Financial and Incident Reporting

Contact banks to stop transactions and report scams to official authorities to aid investigations.

Preventing Identity Theft

Place fraud alerts with credit bureaus and inform trusted contacts to reduce further risks.

MANKATO
COMPUTER TECHNOLOGY

Final Online Safety Tips

Practice Cautious Behavior

Slowing down and thinking critically helps avoid falling for scams driven by urgency and fear.

Verify Identities

Always double-check identities by contacting official sources instead of replying directly to unsolicited messages.

Secure Devices and Passwords

Keep devices updated, use antivirus tools, and protect passwords with a reliable password manager.

Shop Safely Online

Research websites, read customer reviews, and ensure URLs use secure HTTPS encryption.

MANKATO
COMPUTER TECHNOLOGY

James Vietch

This Is What Happens When You Reply to Spam Email | TED

MANKATO
COMPUTER TECHNOLOGY