CyberSafe: Protecting Your Data from Security Risks

CyberSafe is a three-hour workshop for non-technical users that focuses on using technology without compromising personal or organizational security.

Students will learn the skills they need to protect digital data on computers, networks, mobile devices, and the Internet. They will learn how to identify many of the common risks involved in using technology, such as phishing, spoofing, malware and social engineering, and then learn how to protect themselves and their organizations from those risks.

On completion of the course, students will be prepared for the Certified CyberSafe credential, which they can obtain by completing the credential process on CyberSaftCert.com. The online credential covers 10 questions, and is included as part of the course.

Course Outline

Identifying the Need for Security

- Identify Security Compliance Requirements
  - Consequences of Non-compliance
- Recognize Social Engineering
  - Social Engineering Goals
  - Types of Social Engineering Attacks

Securing Devices

- Maintain Physical Security of Devices
  - Digital Breadcrumbs
- Use Passwords for Security
  - Two-Step Authentication
  - Password Managers
  - Biometrics
- Protect Your Data
  - Data Backup
  - Mobile Device Considerations
- Identify and Mitigate Malware
  - Malware Types
  - Malware Sources and Effects

Securing Devices (continued)

- Use Wireless Devices Securely
  - Wi-Fi Security Techniques
  - Organizational and Personal Devices

Using the Internet Securely

- Browsing the Web Securely
  - URL Structure
  - HTTP vs. HTTPS
  - Suspicious URL's
- Using Email Securely
  - Email Attachments
  - Common Phishing Techniques
- Using Social Networking Securely
  - Common Social Networking Security Risks
- Using Cloud Services Securely
  - Cloud Service Risks
  - IoT (Internet of Things) Device Considerations