



# Cybersecurity Awareness For End Users

**Course Description:** This course will provide practical knowledge of IT and cybersecurity and security methods for computer, network, and electronic communication. The course will cover fundamentals, such as terminology, threats and their sources, authentication, computer access control, data protection concepts. The student will receive a comprehensive view on security in cyber space.

**Duration:** Instructor-led, group-paced, classroom-delivery learning model – 2.5 hours.

**Target Audience** The course is designed to be of great value for anyone working with computers, mobile devices, or anything where electronic access can be gained to obtain sensitive and/or valuable information. Government organizations, private companies, academia, and anyone who wishes to further their career in the cybersecurity area or need to extend their expertise with cybersecurity related topics.

**Upon successful completion of this course, students will be able to:**

- Comprehend a wide variety of cybersecurity terms.
- Recognize common cybersecurity threats.
- Protect themselves from falling victim to a phishing, malware, or social engineering attack.
- Create secure passwords that are easy to remember yet difficult to determine through illicit means.
- Create a more secure computing environment both at work and abroad.

**Prerequisites:** No prerequisites needed

## Course Outline

- **Key Cybersecurity Terminology**
- **Common Threats**
- **Dangerous Threats**
- **Understanding and Detecting Phishing Attacks**
- **Understanding and Preventing Malware Attacks**
- **Understanding Social Engineering**
- **Password Security**
- **Security Concerns When Working Remotely**
- **Wi-Fi Security Strategies for Home and in Public**
- **Text Message-based Threats**
- **Social Media Attacks**
- **How to Become a Human Firewall**