Table of Contents

Fundamentals of cybersecurity and ransomware

Duration: 1 Days

About This Course

This one-day instructor-led course is designed for IT professionals who want to gain a fundamental understanding of cybersecurity with a focus on ransomware. In this course, students learn about cybersecurity threats, encryption, authentication and authorization. They will also learn about ransomware attacks, and how to protect against ransomware.

Audience Profile

This course is intended for both novice and experienced IT professionals. Students typically could have some experience or exposure to other IT-related areas, but have minimal or no exposure to cybersecurity or ransomware. Audience can include, but is not limited to, administrators, developers,testers, analysts, and students.

At Course Completion

- Understand the cybersecurity landscape
- Describe how encryption works
- Understand the difference between authorization and authentication
- Discuss device-based threats
- Understand networks and network-based threats
- Discuss how applications can be exploited by cybercriminals
- Discuss ransomware, the types of ransomware attacks, and ransomware families
- Describe different ways to prevent ransomware
- Understand common signs of ransomware attacks
- Describe how to recover from ransomware attacks

Course Details

Module1: Fundamentals of Cybersecurity

This module explains the fundamentals of cybersecurity. It will give the student an awareness of the cybersecurity landscape, how encryption, authentication and authorization work, and draws attention to different attack vectors that cybercriminals can exploit to carry out attacks and gain unauthorized access.

Lessons

• An overview of cybersecurity

• Basic introduction to encryption

• How to verify your users and control their access

• Network threats

• Devices as threat vectors

• Application vulnerabilities

Lab 1: Fundamentals of Cybersecurity

• Paper-based exercise, break out session with scenario and discussion with the group on the outcome.

After completing this module, students will be able to:

• Describe the cybersecurity landscape.

• Discuss how encryption works.

• Describe the differences between authentication and authorisation.

• Describe different network types, the network threat landscape and how to protect them from cyberattack.

• Describe what a device is, how much a device knows about you, and device-based threats.

• Discuss how applications can be exploited to gain access

Module2: The Basics of Ransomware

This module explains the basics of ransomware. Students will get a basic introduction to ransomware, how to protect against ransomware, and what can be done to effectively recover from a ransomware attack.

Lessons

• Introduction to ransomware

• How to protect against ransomware attacks

• How to recover from a ramsomware attack

Lab 1: The Basics of Ransomware

• Paper-based exercise, break out session with scenario and discussion with the group on the outcome

After completing this module, students will be able to:

- Understand ransomware
- Describe different types of ransomware attacks
- Discuss the ransomware families
- Discuss how ransomware has become a business
- Understand defense mechanisms against ransomware attacks
- Describe ways to prevent ransomware
- Describe antivirus and antimalware tools
- Describe common signs of a ransomware attack
- Understand how to respond to a ransomware attack