INFOSECTRAIN

Cyber Security Awareness

Training Program

COURSE HIGHLIGHTS

24 Hours of Instructor-led Training

Post Training Support

Access to Recorded Sessions

Scenario-Based Learning

COURSE DESCRIPTION

Unlock the power to defend yourself and your digital world with our Cybersecurity Awareness Program. In an increasingly interconnected and data-driven society, cyber threats are omnipresent. This comprehensive program delves deep into the intricacies of cybersecurity, equipping you with the knowledge and practical skills necessary to navigate the digital landscape safely. Explore the evolving cyber threat landscape, learn vital cyber hygiene practices including password management and secure browsing, discover strategies to safeguard your personal data and digital assets, fortify your devices against cyberattacks,master the art of secure communication and email practices, protect your privacy on social media, develop incident response expertise, and stay ahead of emerging threats.

Whether you're a professional seeking to enhance your cybersecurity acumen, an organization concerned about employee awareness, or an individual simply wanting to fortify your digital defenses, this program is tailored to your needs. Delivered online with engaging video lessons, interactive exercises, expert insights, and real-world scenarios, it empowers you to proactively guard against cyber threats, making the digital world a safer place for yourself and your community.

COURSE OBJECTIVES

01 Understand the importance and extent of cybersecurity in the contemporary digital landscape.

02 Learn to stay safe from common cyber threats, attacks and risks.

03 Comprehend the value of digital identity management and secure access control.

04 Cultivate practices for ensuring online safety during browsing and work activities.

05 Identify the hazards linked to social media and adopt strategies to safeguard personal privacy.

06 Acquire fundamental knowledge on responding effectively to cybersecurity incidents.

07 Discern the common methods through which ransomware is distributed to end-users.

TARGET AUDIENCE

Designed for all – from cybersecurity enthusiasts to employees of all backgrounds, because everyone should be cyber aware, whether in IT or not.

PRE-REQUISITES

No experience required.

COURSE CONTENT

Module 1 Introduction to Cybersecurity

* Objective: Understand the significance and scope of cybersecurity in today's digital age.
* What is cybersecurity?
* Importance of cybersecurity in personal and professional life
* Real-world incidents and their impact on businesses and individuals

Module 2 Digital Identity and Access Management

* Objective: Understand the importance of digital identity and how to manage access securely.
* What is digital identity?
* Password best practices
* Multi-factor authentication (MFA)
* Role-based access control (RBAC)
* Practical: Setting up MFA for a common online service

Module 3 Safe Online Behavior

* Objective: Develop habits to ensure safety while browsing or working online.
* Safe browsing habits and tools
* Recognizing and avoiding suspicious links and websites
* Importance of software updates and patches
* Practical: Evaluating browser security settings

Module 4 Email and Communication Security

* Objective: Learn to communicate securely and recognize potential threats in communication channels.
* Recognizing and reporting suspicious emails
* Secure communication tools and platforms
* Importance of encryption in communication
* Practical: Identifying red flags in sample emails

Module 5 Physical Security and Device Management

* Objective: Understand the importance of securing physical devices and the data they contain.
* Securing physical access to devices
* Device encryption and why it matters
* Safe disposal of old devices and data
* Practical: Encrypting a USB drive or external hard disk

Module 6   Social Media and Personal Privacy

* Objective: Recognize the risks associated with social media and how to protect personal privacy.
* Risks of oversharing on social media
* Privacy settings on popular platforms
* Recognizing and avoiding social engineering attempts
* Practical: Reviewing and adjusting privacy settings on a social media platform

Module 7   Introduction to Incident Response

* Objective: Gain a basic understanding of how to respond when a cybersecurity incident occurs.
* Basics of incident response
* Reporting and escalation procedures
* Importance of timely response and communication
* Practical: Role-playing a basic incident response scenario

Module 8 · Common Ransomware Delivery Methods

* Objective: Recognize the most frequent ways ransomware is delivered to end users.
* Phishing emails
* Malicious downloads and drive-by downloads
* Exploit kits and unpatched software
* Infected USB drives and external devices
* Practical: Analyzing real ransomware phishing emails

Module 9 · Module 9: Social Engineering

* Techniques and tactics
* Defense strategies
* Practical: Role-playing social engineering scenarios

Why Cybersecurity Awareness Program - for Organizations?

1. Cybersecurity Should Be Your TOP Priority
Shield your company from cyber threats by making security your #1 focus.
2. The Human Element is The Weakest Link
Don't let your workforce be THE vulnerability! Learn how to fortify your team against
cyberattacks.
3. Because Your Workforce is Your Best Defense
Train your workforce for resilience with the right knowledge and skills

Why Cybersecurity Awareness Program - for Individuals?

1. Incidents of Cyber Fraud and Cyber Crime are on the Rise
Shield yourself, your loved ones and your organization from being the next target by
being cyber aware and spreading awareness.
2. The Need to Be Cyber Smart is Greater than Just Being Smart
Awareness about the tactics used by cyber criminals can save you from falling for these
scams.
3. Cyber Attacks Don't Just Target Big Organizations
Cyber crime is also targeted towards the common man who is vulnerable and unaware
of the latest cyber threats.

INFOSECTRAIN

www.infosectrain.com I sales@infosectrain.com