



# Cybersecurity Awareness 2.0

**Enterprise Training**

**Defend & Protect Your Digital Workspace**

## Program Highlights

In our hyper-connected digital world, cyber threats have become a daily reality. InfosecTrain's Cybersecurity Awareness Training 2.0 is designed to equip you with the knowledge and skills to navigate the online landscape securely. Whether you're a professional, a student, or simply someone who wants to safeguard your digital life, this program is your gateway to a safer online experience.



## Course Highlights



**16-Hour**  
of Instructor-led Training



**Scenario-Based**  
Learning



In-depth  
**Case Studies**



Learn from **Industry**  
**Experts**



Highly Interactive and  
**Dynamic Sessions**



Access to  
**Recorded Sessions**



Extended Post  
**Training Support**



**Career Guidance** and  
Mentorship



Comprehensive  
**Cybersecurity Curriculum**

## Target Audience

It is designed for everyone, from cybersecurity enthusiasts to employees of all backgrounds, because everyone should be cyber-aware, whether in IT or not.

## Pre-Requisites

No experience is required.

## Course Objectives

- ✓ Grasp the importance of confidentiality, integrity, and availability.
- ✓ Learn key terms such as threats, vulnerabilities, risks, and impacts.
- ✓ Identify different types of cyber attacks: phishing, social engineering, malware, and insider threats.
- ✓ Adopt safe browsing habits and recognize suspicious websites.
- ✓ Understand physical security measures like device locking and application whitelisting.
- ✓ Monitor credit reports and use security measures like credit freezing
- ✓ Perform immediate steps to minimize damage from security breaches
- ✓ Engage in hands-on simulations to contain data breaches and malware infections.
- ✓ Recognize AI-driven threats and deepfake technology risks

# Course Curriculum

## Introduction to Information Security

- ✓ What is Information Security?
  - ✓ Definition and Importance
  - ✓ Key Concepts: Confidentiality, Integrity, Availability
  - ✓ Definition of key terms: Threats, Vulnerability, Risk, and Impact
  - ✓ Cost of cybercrime examples

## Understanding Cyber Attacks

- ✓ Types of Cyber Attacks
  - ✓ Phishing
  - ✓ Social Engineering
  - ✓ Insider Threats
  - ✓ Malware
- ✓ Motivations behind cyberattacks
  - ✓ Service disruption
  - ✓ Data exfiltration
  - ✓ Case Study

## Basic Security Best Practices

- ✓ Multi-Factor Authentication
  - ✓ How to set up 2FA on common platforms
- ✓ Biometric Authentication
- ✓ Password Authentication
  - ✓ Importance of strong passwords
  - ✓ How to create and manage strong passwords
- ✓ Employee Training and Awareness

## Safe Browsing Habits

- ✓ Identifying suspicious websites
- ✓ Using reputable web browsers with built-in security

## Securing Devices and Endpoints

- ✓ Endpoint Security Measures
  - ✓ Install Antivirus/Antimalware Software
  - ✓ Awareness of Endpoints
  - ✓ Conducting a Security Checkup on Personal Devices
- ✓ Patch Management
  - ✓ Regular Updates
  - ✓ Automated Patching

- ✓ User Training and Awareness
  - ✓ Security Awareness Training
  - ✓ Policies and Procedures
- ✓ Physical Security
  - ✓ Device Locking (Password, PIN, Smart Card locks)
- ✓ Application Whitelisting in organizations
  - ✓ Approved Applications
  - ✓ Block Untrusted Software

## Symptoms of Network and Endpoint Attacks

- ✓ Network Attack Symptoms
  - ✓ Increases bandwidth usage
  - ✓ Performs degradation
  - ✓ Unusual Log-In Attempts and Account Lockouts
- ✓ Endpoint Attack Symptoms
  - ✓ Unexpected Device Behavior
    - Performance issues
    - Unauthorized changes
    - Strange pop-ups and messages
  - ✓ Disabled Security Software
    - Firewall disabled
    - Error messages/Failed updates

## Taking Action to Minimize Damage

- ✓ Immediate Steps
  - ✓ Changing passwords on compromised accounts
  - ✓ Placing a fraud alert on your credit report
- ✓ Protecting Yourself from Identity Theft
  - ✓ Monitoring your credit report for suspicious activity
  - ✓ Freezing your credit if necessary
  - ✓ Enabling two-factor authentication (MFA) on all accounts

## Advanced Security Concepts

- ✓ Securing Home and Office Networks
  - ✓ Securing Home and Office Networks
  - ✓ VPN and its benefits
- ✓ Navigating the Digital World Safely
  - ✓ Email Security Essentials
  - ✓ Mobile Security Measures
- ✓ Responding to Image Misuse
  - ✓ Identifying Image Misuse
  - ✓ Taking Action Against Misuse



## Social Engineering and Phishing Attacks

- ✓ Phishing Attacks
  - ✓ Types of Phishing attacks

## Social Engineering

- ✓ Types of Social Engineering Attacks
  - ✓ UPI Scams
  - ✓ Fake KYC (Know Your Customer) Updates
  - ✓ WhatsApp Scams
  - ✓ LinkedIn Awareness ( Fake job posting )
  - ✓ Securing Your Gmail Account

## Recognizing and Avoiding Phishing Attacks

- ✓ Identifying Phishing Emails and Messages
- ✓ Phishing Simulation Exercise

## Symptoms of Malware and Ransomware Infections

- ✓ Malware Infection Symptoms
- ✓ Ransomware Attack Symptoms

## Social Media Security

- ✓ Privacy settings on social media platforms
- ✓ Avoid oversharing personal information online

## Cloud Security

- ✓ Understanding Cloud Storage Services
  - ✓ Benefits and risks of cloud storage
  - ✓ Popular cloud storage providers
- ✓ Securing Your Cloud Accounts
  - ✓ Securing file-sharing permissions
  - ✓ Strong password creation and using MFA
  - ✓ Data encryption options in cloud storage

## AI and Deep Fake Awareness

- ✓ Understanding AI in Cybersecurity
  - ✓ AI-Driven Threats
  - ✓ Highly Personalized Phishing Attempts
  - ✓ Automated Attack Patterns
- ✓ Deepfake Technology
  - ✓ What are Deepfakes?
  - ✓ Risks Associated with Deepfakes (Identity Theft, Misinformation)
  - ✓ Unrealistic Audio/Video Quality
  - ✓ Inconsistencies in Background or Timing

## Incident Response and Recovery

- ✓ Understanding Incident Response
  - ✓ What is an Incident Response Plan?
  - ✓ Key Steps in Incident Response
- ✓ Creating an Incident Response Plan
  - ✓ Developing a Basic Incident Response Plan
  - ✓ Responding to Common Attacks
- ✓ Responding to Malware Infections
  - ✓ Steps to Take if Infected by Malware
  - ✓ Using Malware Removal Tools
- ✓ Responding to Phishing Attacks
  - ✓ Identifying and Reporting Phishing Attempts
  - ✓ Reporting Phishing Emails

## Data Breach Response

- ✓ Immediate Steps to Take During a Data Breach
  - ✓ Identifying and Containing the Breach
  - ✓ Notifying Internal Teams and Stakeholders
- ✓ Data Breach Containment Exercise
  - ✓ Hands-On Simulation: Containing a Data Breach
- ✓ Legal and Regulatory Requirements
  - ✓ Reporting Obligations
  - ✓ Communicating with Affected Parties



[www.infosectrain.com](http://www.infosectrain.com) | [sales@infosectrain.com](mailto:sales@infosectrain.com)