COURSE

Cyber Security

6th Edition   Ethics   🌐

Prevent Data Breaches and Phishing Attacks

In our modern world, cyber attacks have unfortunately become an inevitable reality that shows no signs of fading away. Beyond causing disruptions to business operations, these malicious incidents can result in staggering financial losses of up to $9.5 million per attack in the United States. Given the high stakes involved, a pragmatic solution to mitigate vulnerabilities is to invest in cybersecurity training programs for your staff. By doing so, you can equip your team with the necessary skills and knowledge needed to combat these ever-present threats effectively.

A robust cybersecurity awareness training plan brings additional protection to your organization at a level even beginners can understand. Emtrain's cybersecurity Course teaches the fundamentals of keeping sensitive information protected at all organizational levels. This invaluable learning experience could prevent a costly attack by hackers or scammers that can drain profits and damage customer confidence.

Key Concepts

- Introduction to information security and the common threats to your organization
- Identifying scenarios that leave corporate and personal data at risk
- Practical steps for non-IT professionals to create strong login credentials
- Avoiding online scams, social engineering cons, phishing attacks, malware, spyware, and ransomware
- Engaging in network security, mobile device protection, and safeguarding organizational assets

Course Features

- Access to our Anonymous Ask the Expert tool
- Rich video scenarios based on real-world events
- 50+ Machine Translation Options
- Optional program timer

- Built-in employee sentiment surveys
- Policy acknowledgement tool
- Extensive customization options

Lessons

Understanding Today's Cyber Threat Landscape

This lesson explores the modern cyber threat landscape, emphasizing that security is a collective responsibility in an era of AI-driven attacks and evolving actor motivations.

Modern Authentication and Access Control

Passwords alone are no longer enough — learn how modern authentication methods, MFA, and access control principles work together to keep accounts and organizational data secure.

Social Engineering and Phishing

Explore how social engineering and phishing attacks exploit human psychology, and learn to recognize manipulation tactics and verify suspicious requests before acting.

AI-Powered Attacks and Deepfakes

AI has made cyberattacks more convincing and harder to detect than ever — learn how AI-powered attacks and deepfakes work, and what to do when you can't trust what you see or hear.

Malware, Ransomware, and Supply Chain Attacks

Malware, ransomware, and supply chain attacks can cripple organizations — learn how these threats work, how they spread, and what you can do to prevent, detect, and respond to an infection.

Securing Remote Work and Personal Devices

Working outside the office creates real security risks — learn how to protect your devices, secure your home network, and maintain safe practices wherever work takes you.

Understanding PII and Why Cyber Security Matters

Personal data is one of the most valuable targets for cybercriminals — learn what counts as PII, why protecting it matters, and the role every employee plays in keeping it secure.

Incident Response, Reporting, and Our Policies

When something goes wrong, every second matters — learn how to recognize a security incident, report it quickly and correctly, and understand your role in keeping the organization protected.

PILLAR

Ethics (https://emtrain.com/products/ethics/)

VERSIONS

All Employees (30 min)

WHAT'S COVERED

- Malware & Spyware
- Passwords
- Personal Devices
- Phishing Attacks
- Ransomware
- Social Engineering
- Web-Based Attacks

COURSE EXPERTS

David Brezinski
Cybersecurity Expert