COURSE

Cyber Security

5th 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
- Built-in employee sentiment surveys

- 50+ Machine Translation Options
- Optional program timer
- Policy acknowledgement tool
- Extensive customization options

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

Lessons

Seeing the Risks and Meeting the Challenges

Learning objectives for this program.

Password Strength and Security

Choosing and maintaining the right password is a simple but key way to keep out cybercriminals. Some information and simple guidelines on how everyone can do their part to safeguard our organization's information and systems.

Social Engineering

Social engineering attacks take advantage of human nature and our own behaviors to access our information and systems. How to recognize and defend against these dangerous attacks.

Phishing Attacks

Phishing attacks are a kind of social engineering attack that targets you. Learn what they are and how to defend against them.

Malware and Spyware Prevention

Malware and spyware attacks turn our own equipment into tools for cybercriminals. Learn what they are and how they compromise our systems.

Web-Based Attacks

Learn how visiting a website can initiate a cyberattack and what to do if something just doesn't seem right on a website.

Personal Devices

Personal devices have become a common and valuable tool in many organizations. That makes it critically important to keep them secure and understand how they fit in our organization's cybersecurity.

Ransomware

Ransomware attacks can lock critical information and systems unless our organization pays cybercriminals to undo the harm. Learn about this rising risk and how to combat it.

Policies

Our policies, guidance, and resources on cyber security.

Provide Your Feedback

Your thoughts.