Cybersecurity

All New in 2021!

Cybersecurity is arguably the largest enterprise risk today and experts say cyber attacks have increased over 400% in the last year. One significant cybersecurity breach can put your entire operation at risk, and your security program is only as strong as each employees' understanding of the risks and their safe practices.

Your employees will be trained to identify phishing scams, avoid web based attacks and ransomware, and spot social engineers attacks. We also instruct employees on some best practices for creating strong passwords.

This course teaches:

- A quick introduction to and practical guidance on common cyber security threats to your organization.
- Employees how to identify situations that leave personal or corporate information vulnerable to hacking.
- Non-IT employees best practices for creating strong passwords, avoiding web scams, and safeguarding your organization's devices and information assets.
- About password strength and security, social engineering, phishing attacks, malware and spyware prevention, web-based attacks, personal devices, and ransomware.

Interactive polling questions in the course give employers real insight into how learners feel about the concepts and culture skills presented. And Emtrain's innovative Ask the Expert feature gives learners direct access to course experts.

Course Version
- 30 minutes (Manager and Employee)

Languages
- English and translatable

Required Program Elements
- A PDF of, or link to, your written cybersecurity policy for acknowledgment

See more course details or request a free demo >>

Lesson	Description
Seeing the Risks and Meeting the Challenges	Learning objectives for this program and highlighting that cyber risks are the greatest enterprise risk today.
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 is the most common way to breach cyber security. These 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	Newer cyber attacks include showing ads that lead to websites that are fraudulent and designed to inject malware into your system. 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.

Lesson	Description
Ransomware	Ransomware attacks are on the rise. Ransomware locks critical information and systems unless the organization pays cybercriminals to undo the harm. Learn about this rising risk and how to combat it.
Policies	Our policies, guidance and resources on cybersecurity.
Post-Program Survey	Your thoughts on the program.