Cyber Security Essentials: Training course

Description/Overview

The purpose behind cybersecurity training for employees is always to alter their habits and behaviours, and create a sense of shared accountability, so that the company is safe from attacks.

This cybersecurity module was developed to raise awareness on how to avoid online threats that might target you or your organization. By identifying common online threats, understanding risk factors for each type of threat, and learning how to minimize the risk of an attack.

This course consists of six modules outlining security fundamentals and provides a wide overview of tangible cyber-security concepts and practices. It provides fundamental practical knowledge about working habits and safely operating in an increasingly technology-driven world. Providing a base about what employees need to know to keep your company data and devices safe.

The course modules are:

- Spear phishing
- Malicious links
- Passwords
- Outside the office threats
- Malware
- Data protection

The course is structured:

- Fully automated, online and secure
- Secure login allows individual online users to resume the course at any point any time• Introduction video with built-in test questions and interactive sections designed to reinforce good habits.
- Full course material in PDF format that is downloadable to study.
- Module test questions with scoring required to pass each module• Certification of completion when individuals have passed the assessment.

The below is an overview of the course material:

Phishing and Advanced Spear Phishing (module1)

Most cyber-intrusion attempts begin with spear phishing emails. These targeted attacks are delivered via malicious links, file attachments, and login forms. This lesson helps to identify the warning signs and what to do in the event of a spear phishing attack. Individual learners follow different paths through the instruction based on their responses. As they progress, they build their awareness of phishing tactics. They also test their ability to identify threats and hone their competencies in how to avoid phishing.

The spear phishing and advanced course achieves the following objectives:

- Builds user awareness of key types of phishing attacks.
- Teaches learners how to identify each type of attack and what course of action to take in each instance.
- Enables learners to define phishing and its risk to the individual and the organization.
- Promotes understanding of delivery methods for phishing attacks, including email, phone and mobile.
- Instils best practices on how to avoid phishing.
- Enhances the ability to identify web links and suspicious URLs.
- Social engineering

Malicious Links (Module 2)

On the Web and in email, hyperlinks are the easiest tool that cyber criminals can use to deliver malware—all it takes is the click of a link. In this lesson, we break down the parts of a link and the structure of a URL to reveal the warning signs of a malicious link.

- Why links can be dangerous.
- Upon completing this lesson, you should be able to:
    - why links can be dangerous.
    - Identify the components of a link.
    - Break down the parts of a URL.
    - Understand what to do if you are targeted with a malicious link.

Passwords (Module 3)

Passwords are the keys to your sensitive data when using websites, email accounts and your computer itself (via User Accounts). This module is designed to provide users with an understanding of the importance of strong passwords along with the best techniques and tool to assist users in choosing and managing their passwords.

- The different cyber-attacks that put your password at risk
- What constitutes a strong password?
- How to manage your passwords
- How multi-factor authentication keeps your account safer.

Security outside the Office (Module 4)

When working outside of the office, employees must be on their guard against an array of threats. The email and browsing habits of employees can leave a company wide open to malicious software, which attacks company applications and social accounts, steals information, and possibly even money. So, it is crucial that cybersecurity training for employees in your company includes policies and guidelines for using email, internet, and social media. Use this lesson to educate your users about threats that linger in public places, and what they can do to protect sensitive information.

- Attack methods that put your information at risk.
- The risks of using a portable storage device.
- The difference between a public and a secure network.
- What to do if your device is lost or stolen.

Malware (Module 5)

Malware has been a threat for decades, and it has grown more sophisticated over the years. Various forms of malware might spy on your activity, allow attackers remote access to your drives, or take control of your device. This lesson teaches what the different types of malware do, and how to avoid falling victim to them.

- What malware is, common varieties of malware.
- How malware is used
- The value and limitations of anti-virus software

Data Protection (Module 6)

Every company has its own policies on the protection of data, but don't assume that all employees are aware of these policies, or that they understand them.
First, use this training to help employees become aware of unexplained errors, spam content, and legitimate antivirus warnings. Then, educate them on the process they should follow to report these red flags, as well as the right people to talk to about suspicions of a cyber-attack.

- Your responsibilities toward data privacy
- Data destruction standards
- Dangers of leaving private/confidential information out in the open