Cyber Security Awareness Training

Course Outline

sonic PERFORMANCE SUPPORT

Course Description

Cybersecurity has never been more prominent in the news than these days. Colossal breaches made headlines across the globe. In nearly all cases it was a human who clicked on an attachment that installed malware or unveiled sensitive information. Becoming aware of cyber-attack tactics and techniques will reduce the chances of a data breach dramatically.

In a modern world, everyone will soon be connected in some way via computers, smartphones, and other devices, leaving a wide range of opportunities for those who act unlawfully.

Who should attend?

Our video training program is focused on increasing cyber security awareness and the use of best practices by individuals and organizations of all sizes.

Course Objectives

In this course you learn

- how to PREVENT an attack, DETECT an attack and REACT to an attack
- how to convey effective defense techniques without getting overly suspicious and being unhelpful to legitimate customers
- to balance trust with verification

Benefits

According to Reuters.com, end-user awareness and training reduces security-related risks for organizations by 45% to 70%.

18
Training Videos

70
Minutes*

2
Simulations

17
Handouts

6
Quizzes

** Add time for reading the handouts and taking the quiz.*

Cyber Security Awareness Training

Course Outline

1 Course Overview

Become a security aware citizen, protecting yourself and making others aware of security risks. Learn how to convey effective defense techniques without being overly suspicious and being unhelpful to legitimate customers.

Course Overview (4 min.)

Most attacks do not start as a technically sophisticated attack. The most successful data breaches and cyber incidents can ultimately be traced back to human error or carelessness. You need to educate yourself to enjoy the benefits of modern life, be part of the modern workforce, and protect yourself and your employer from serious loss.

Handout: Course Outline

Here you can find the Table of Contents to download and print. This way you always have an overview of the contents covered in this course.

Handout: Why do Hackers hack?

The motives and goals of hackers in cyberattacks vary widely.

2 Why should you care about Cybersecurity?

The modern life we are living is unthinkable without being connected to the internet. The potential financial costs of a data breach are immense, and the company's reputation is at risk.

Why should you care about Cybersecurity? (4 min.)

Being connected and using the internet so extensively puts us at risk of being hacked. Risks range from financial costs, to loss of intellectual property and career damage.

Handout: Why should you care about Cybersecurity?

Learn more of the many reasons why you should protect yourself.

Quiz - Why care? (4 Questions)

It’s easy to validate your knowledge with our end of chapter quizzes. You can also skip a module and use the quiz to verify that you already know the content.

Cyber Security Awareness Training

Course Outline

3 What is “Social Engineering” and why does it matter to me?

Social Engineering refers to the psychological manipulation of people into performing actions or divulging confidential information.

What is Phishing and how does it work? (8 min.)

Nearly all users get at least one phishing email a day trying to trick them into installing malicious software or leaving a username and password on a suspicious site. You can protect yourself, and your company's data, when you know how to identify phishing emails.

Handout: Phishing

Learn more about the indicators of phishing attacks.

What is Spear Phishing? (3 min.)

There are two tactics of phishing – sending emails to hundreds or thousands of users and waiting to see who responds, or a very targeted approach to a specific person, called spear phishing. A spear fishing attack built around a single person is much harder to spot.

Handout: Spear Phishing

Spear phishing attacks are well crafted and hard to identify.

What is Vishing and how does it work? (4 min.)

Vishing is an attack performed by phone (voice) rather than by email. This involves impersonation, pretending to be a friend or colleague on a social networking site in order to obtain additional personal information, possibly in preparation for a spear phishing attack.

Handout: Vishing

A more in-depth analysis on why Vishing works and the indicators to look for.

Handout: First Aid

What do you do if you think you are a victim?

Simulation - Identify legitimate emails (6 Questions)

Test if you can spot those phishing emails.

Quiz - Social Engineering (8 Questions)

It’s easy to validate your knowledge with our end of chapter quizzes. You can also skip a module and use the quiz to verify that you already know the content.

Course Outline

4 Malware

Malware is short for “malicious software".

Malware – what is it and what can it do? (3 min.)

Malware includes viruses and spyware that get installed on your computer, phone, or mobile device without your consent. These programs can cause your device to crash, can be used to monitor and control your online activity, encrypt your data until you pay a ransom and much more.

Handout: Malware

Interesting facts on Malware

How can you get infected? (3 min.)

A staggering 66% of all infections happen via email attachments or links in emails that direct you to websites trying to trick you into installing malware. But USB sticks and downloading software from the internet are other common ways to get infected.

How to protect against Malware (3 min.)

Instead of learning to precisely distinguish between different types of malware, e.g. viruses, adware, spyware, worms or trojans, it is more important for you to master some simple actions that can prevent you from becoming a victim.

How can you tell if your PC is infected? (4 min.)

Unfortunately, most of the time you won't immediately know when you get infected. Learn how to identify the warning signals.

First Steps if you realize you have been infected (2 min.)

Maybe you just realized that someone tricked you and you opened a harmful attachment. Now what? What should you do if you have evidence that you are infected?

How to remove Malware from your PC (2 min.)

Removing malware requires an IT specialist – if you don’t have an IT department, consider allowing an IT consultant to help you with these steps.

Quiz - Malware (7 Questions)

It’s easy to validate your knowledge with our end of chapter quizzes. You can also skip a module and use the quiz to verify that you already know the content.

Course Outline

5 Password Management

Despite hacks and data breaches becoming commonplace, it seems most people are still picking a password based on convenience rather than security.

What is wrong with your P@ssw0rd? (5 min.)

Nearly all of us are guilty of not using strong passwords, and no wonder – how to remember them all without writing them down?

Handout: Strong Passwords

Do's and don'ts

Password Management Tools (4 min.)

In the past, people wrote their passwords on a notepad and "hid" them below their keyboard. This is not a good idea – you don't do that, right? Why not let the computer create and remember strong passwords – there are tools for that.

Handout: Password Management Tools

List of vendors and what to look for

Two-Factor Authentication (5 min.)

Two-factor authentication is an authentication mechanism to double check that your identity is legitimate. Two-factor authentication is strongly recommended.

Handout: Two-Factor Authentication

How it works and a list of vendors

Quiz - Password Management (8 Questions)

It's easy to validate your knowledge with our end of chapter quizzes. You can also skip a module and use the quiz to verify that you already know the content. (8 Questions)

Course Outline

6 Secure Internet Usage

Browsers are the main gateway for Internet traffic. This is why many malware programs and cybercriminals in general target browsers first.

Use Wireless Devices securely (4 min.)

It's so easy to work while traveling or while outside the office. Public Wi-Fi access is practically everywhere, but it also causes serious security challenges you'll need to be able to handle.

Handout: Secure Websites

Learn how to investigate if a link to a website is legitimate or not. What is a URL? What is secure URL? HTTP vs. HTTPS. Understand SSL and digital certificates.

Browse the Internet securely (5 min.)

You need to know how safe and secure browsing limits potential threats and how to minimize some of the risks associated with the Internet.

Handout: Secure Websites

How to secure your Web Browser

Handout: Virtual Private Networks

Virtual Private Networks - An overview

Simulation - Is this Website legitimate? (7 Questions)

Test if you can spot insecure websites.

Quiz - Secure Internet Usage (6 Questions)

It’s easy to validate your knowledge with our end of chapter quizzes. You can also skip a module and use the quiz to verify that you already know the content.

Course Outline

7 Maintain Physical Security

Learn how to protect yourself and your organization's data from threats that arise from loss, theft and espionage.

Maintain Physical Security (4 min.)

Some techniques allow you to protect sensitive data from being exposed even if your laptop, PC or mobile device gets lost or stolen.

Handout: Maintain Physical Security

How to maintain physical security

Quiz Chapter 07 - Maintain Physical Security (2 Questions)

It's easy to validate your knowledge with our end of chapter quizzes. You can also skip a module and use the quiz to verify that you already know the content.

8 Moving Forward

Security technology is a race between the good guys and the bad guys. Even after finishing this training and applying what's learned, don't think your work is done and your responsibility ends!

Review and suggestions to stay cyber safe (2 min.)

Now you know motives, tactics and some important technologies used by cybercriminals. You are also able to understand important terminology related to cybersecurity in order to follow the cybersecurity news and to be able to talk to IT professionals.

Handout: Glossary

Glossary

Handout: Suggestions for continuous learning

Websites, blogs and other worthwhile things to read