

COMPUTER SECURITY IN THE WORKPLACE



Introduction

Computer crime is a very real threat that needs to be addressed, which is why computer security is increasingly important to ensure the best protection. Simple human error and a lack of security awareness are often the root causes of computer security breaches in the workplace. This module provides guidance for employees to maintain security when using the computers in the workplace.

Course Overview

At the end of the course, trainees will be able to:

- Identify the common threats, distinguish between authentic and suspicious emails and links
- Understand the risks of removable media
- Know how to download files safely
- Understand the value of good password practice
- Recognise the risks of mobile working
- Know what to do in the event of a computer security incident.

Course chapters

1. Introduction to computer security.

In this section, you'll cover what is Cyber-Crime? What is Computer Security? Policies and procedures, common threats and spam and phishing.

2. Policies and Processes

In this section, you'll cover identifying suspicious emails, the importance of keeping a clean machine, the risks of removable media, safe downloading, good password practice and the risks of mobile working.

3. Maintaining Computer Security

In this section, you'll cover staying alert and speaking up, the warning signs that your Computer may be infected and what to do in the event of a computer security incident.

Who will it benefit?

Employees have a critical role to play in their organisation's security. Protecting your organisation begins with ensuring you are prepared to assist in keeping your computers and networks safe. This course will benefit anyone who works on a computer.

How it works?

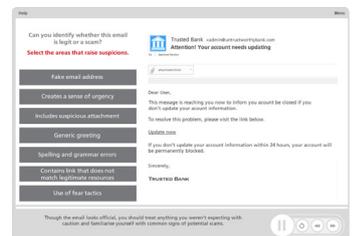
Computer Security in the Workplace is delivered online as an interactive course to each trainee on their computers, or portable device at any internet enabled location. The interactive course is engaging, informative and exciting to use.

Using up-to-date, modern graphical images, users will be faced with a selection of interactive elements and mini quizzes to test their knowledge.

Users will receive informative advice and guidance and will be tested on their understanding of the subject at the end of the course by completing the compulsory self-test.

This course also features a risk checklist which asks the user a series of questions relating to their current working environment.

Course Format: Interactive
Running Time: 20-25 minutes



Technical Information

Internet Access: Users will need a computer or apple device with a web browser and an internet connection to access Safety Media e-Learning Solutions.

Minimum Recommended Bandwidth: 2Mbps

Software:

One of the following web-browsers:

Windows: Internet Explorer
» Latest versions as maintained and supported by the manufacturer
» Google Chrome

OS X: » Latest versions as maintained and supported by the manufacturer
» Google Chrome

iOS: » Latest versions as maintained and supported by the manufacturer
» Google Chrome

Android: » Latest versions as maintained and supported by the manufacturer
» Google Chrome

Adobe Reader or Reader DC (for viewing of PDF documents downloadable from the solution where applicable)

Plug-ins Settings
» Flash player: Version as recommended by Adobe
» Enable JavaScript
» Allow cookies

Hardware

Processor: 600MHz
Minimum Hard Disk Space Required: 1GB
RAM: OS Dependent

Audio

The courses contain audio, system requirements for running the courses are browser dependent. Where no enabled audio device is detected and the browser defines that this is required the user will be informed via an error message window upon launching the course.

For more information, please visit our website.

Safety Media

+44 (0)1745 535000
sales@safetymedia.co.uk
www.safetymedia.co.uk