

# PAYMENT CARD INDUSTRY (PCI) AWARENESS



## Introduction

Payment Card Industry Data Security Standard, also known as PCI DSS, are the technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. These standards apply to all organisations that store, process or transmit cardholder data, with guidance for software developers and manufacturers of applications and devices used in those transactions.

## Course Overview

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

- Understand what the Payment Card Industry Data Security Standards (PCI DSS) is,
- Recognise the PCI Security Standards and requirements,
- Appreciate the benefits for the organisation and its customers,
- Take appropriate action to prevent common fraudulent practices,
- Take appropriate action to protect cardholder data,
- Identify why it's important to create secure passwords,
- Understand how you report issues.

## Course chapters

### 1. PCI Requirements

In this section, we'll cover what PCI DSS is, why you need to be compliant and the benefits for your organisation and its customers.

### 2. Security controls and processes

In this section, we'll cover common fraudulent practices, payments card security features and the key features of PCI DSS compliance systems.

### 3. How to comply with PCI DSS

In this section, we'll cover protecting cardholder data, creating and maintain secure passwords and management reports issues.

## Who will it benefit?

Ideal for workers who work in any type of organisation where cardholder data is stored, processed or transmitted. This course will allow employees to understand what PCI DSS is and why it's important to follow these requirements in protecting cardholder data.

### How it works?

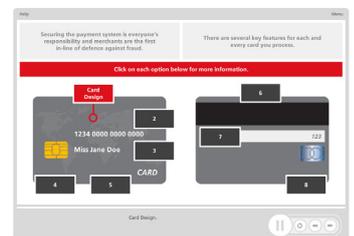
Payment Card Industry is delivered online as an interactive course to each trainee on their computers, or portable device at any internet enabled location. The interactive course is engaging, informative and exciting to use.

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: 25-30 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: 2Mbs

### Software:

One of the following web-browsers:

- Google Chrome
- Safari (Versions as maintained and supported by the manufacturer)
- Internet Explorer (Versions as maintained and supported by the manufacturer)

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

### Plug-ins

- Flash player: Version as recommended by Adobe

### Settings

- 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