# Information Security Awareness: An introduction for UK SMEs

## Recognise the main UK SME cyber security breaches and learn how to protect yourself and your company from common attacks

## Overview

### What Will I Learn?

- The value of stolen information and how to recognise UK SME cyber security threats including viruses, spyware, malware, impersonation, denial-of-service, hacking, identity theft and corporate identity fraud
- How social engineering attacks operate and how to protect yourself through cautious behaviour, call verification and by applying email precautions
- Sound practices to safely handle email attachments and follow hyperlinks, identify fake emails, and recognise common business scams
- To recognise and avoid social media dangers including identity theft, social engineering attacks and malware, by adopting sound social media practices
- To securely manage your passwords

### Requirements

- An appreciation of the small business workplace
- A general familiarity with internet browsing and common office applications

## Description

UK SMEs are at risk of cyber-attack.  Security awareness training helps SMEs defend themselves. This introductory, non-technical information security awareness course, avoids (almost all) jargon to outline key SME workplace security threats and give you actionable solutions.

### Develop a security-mindset based on a realistic, evidence-based UK SME threat awareness

- Know *who* the attackers target and *why*
- Minimise your user-enabled security attacks
- Defend yourself and your company against phishing and other lure-based attacks
- Adopt *safe*, and avoid *unsafe* workplace social media practices
- Improve your password management

## Protect yourself and your SME

SMEs with a security-aware culture are less likely to suffer an expensive cyber-attack. Educating yourself about workplace information security threats and adopting secure practices will help protect your company. This course introduces end-user focused, straightforward, non-technical security awareness topics.

The course is particularly suited to *micro* (0-9 employees) and *small* (10-49 employees) SMEs. Some *medium* (50-249 employees) SMEs will benefit from parts of the course. Most examples and many references in the course are UK sourced.

Individuals, families, small businesses and large organisations share many information security threats. How SMEs should prepare for and respond to these threats differs from the other categorise of user. Defensive techniques and tips offered in this course are UK SME oriented.

Key information security awareness topics are presented in a straightforward, accessible and practical manner.

For each topic, you can use the **course workbook** to implement secure practices in your workplace.

## Course content and overview

Actionable end-user security awareness training is structured around *five* key, standalone topics

- You are a target
- Social engineering
- Dangerous email and links
- Social media issues
- Password risks

This course comprises of 33 lectures and ~2 hours of content. Each topic divides into several short lectures. Lectures typically last 4-8 minutes. Following each topic, are **practice activities** and **resources**: e.g. a downloadable lecture pdf, an online quiz providing immediate feedback, a downloadable workbook and a topic bibliography.

A completion certificate is also available.

# Course topics

## You are a target

This topic considers the value of personal or company information and how it is sold on darknet markets. It introduces identity theft, highlighting the type of people deliberately targeted. Corporate identity fraud and basic protection approaches are addressed. Common workplace information security threats, as identified by a UK government survey, are introduced.

## Social engineering

This topic introduces social engineering is and explains its popularity amongst attackers. Three main malicious social engineering techniques are introduced. Mainly UK social engineering examples are given. Defensive techniques against social engineering attacks are outlined.

## Dangerous email and links

This topic considers email attachment dangers. The reasons attackers favour email are given. Email protection steps are provided. Hyperlinks and their dangers are explained. How to distinguish between real and fake email is explored. Scams targeting UK SMEs and protection advice are introduced. A specific attack type – spear phishing – is also considered.

## Social media issues

This topic introduces workplace social media. SME social media concerns are outlined. Key social media dangers including identity theft, social engineering attacks, malware infection, plus employee and employer risks are discussed. Social media advice for UK SME employees and employers is provided.

## Password risks

This topic considers key password issues including the 'worst' passwords, too many passwords, forgotten passwords and main types of password attack. Technical security controls for passwords and their limitations are outlined. The contrast between how users manage passwords and how they *should* manage their passwords is explored. Poor password hygiene practice is demonstrated. Good practice password hygiene is explained. Two-factor authentication is outlined. SME password security – managing multiple logins and passwords plus security tips for passwords are introduced.

## Who is the target audience?

- UK-based SME employers and employees
- UK computing and business students interested in small business

## Contact

If you have any questions about our courses, please get in touch.

**Phone:** +44 (0)1905 821786

**Email:** info@chl.co.uk

**Web:** chl.co.uk


Version: 07/17