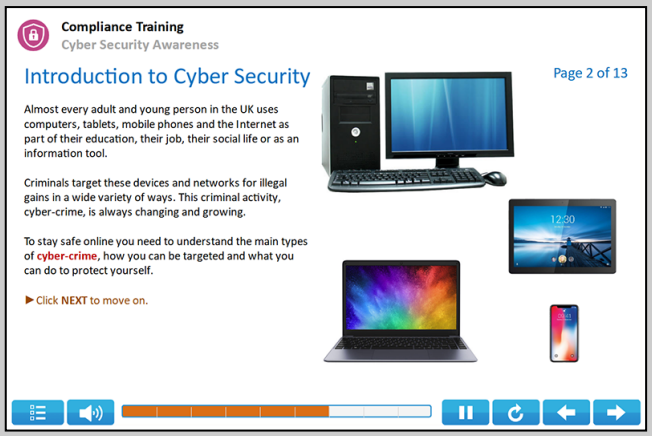
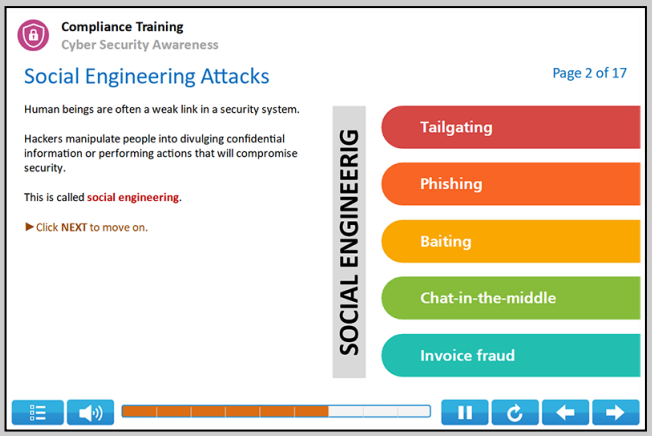
ENGAGING, RELEVANT, COST EFFECTIVE TRAINING

Cyber Security Awareness

£17.50 + VAT





- **IIRSM approved training**
- **Certified by CPD**
- **Audio voiceover**
- **Downloadable certificate on completion**
- **100% online training**
- **No time limits**

This online Cyber Security Awareness training will help you to understand the potential impact of common cyber threats. It outlines safe behaviour on the Internet and identifies what steps you can take to protect yourself and your organisation from cyber-attacks.

The training is suitable for anyone who uses the Internet at work and applies to all devices that have internet access, including desktop and laptop computers, tablets and smartphones.

The approximate duration of this training is 1.5 hours.

PURCHASING FOR YOUR ORGANISATION

If you are buying for your organisation rather than for yourself, it is simple for you to add learners, assign training and print certificates. You will have a dashboard to monitor learner progress.

Our training licences **don't expire** and are only assigned to a learner when they launch the training. Substantial discounts are available for bulk purchases.

Learners are able to download their certificate on successful completion of the online assessment.

0333 577 5016

info@i2comply.com

i2Comply

ENGAGING, RELEVANT, COST EFFECTIVE TRAINING

Cyber Security Awareness

This training course contains the following 7 topics:

1. INTRODUCTION TO CYBER SECURITY
- Who is a potential target for cyber-attacks.
- Who commits cyber-crime.
- How human behaviour creates risks.
- The risks associated with the Internet of Things.
- How data protection regulations affect you with respect to cyber-crime.

2. BRUTE FORCE ATTACKS
- What a brute force attack is.
- How social media is targeted by hackers to help them guess passwords.
- What makes for a secure password.

3. INTERNET COOKIES
- The Why cookies are important and what they do.
- The risks associated with them.
- What you can do to minimise these risks.

4. SOCIAL ENGINEERING ATTACKS
- Four kinds of social engineering - tailgating, phishing, baiting and chat-in-the-middle.
- Ways to protect yourself from phishing attacks.

5. MALWARE
- Types of malware - viruses, worms, Trojans, logic bombs and ransomware.
- Ways to defend against malware attacks.

6. GRAYWARE
- How a variety of different grayware works - adware, keyloggers, bots and botnets.
- Ways to reduce grayware on your device.

7. IDENTITY THEFT
- How criminals steal identities and what they do with them.
- Signs that indicate you may be a victim of identity theft.
- What to do if your identity is stolen.

0333 577 5016
info@i2comply.com

i2Comply