INTELLECT
INTELLIGENCE SERVICES

Critical Incident Advice Line

t: 0843 289 8627
e: critical@intellect-intelligence.com

BASIC CYBER AWARENESS – ONLINE LEARNING

A course for organisations wishing to improve awareness and safeguarding of their employees and vital assets.

Course Duration
TBA

Dates and Venues
Please contact us for details

t: 0843 289 8627
e: info@intellect-intelligence.com

BASIC CYBER AWARENESS – ONLINE LEARNING

Who Is The Course For?

Providing employees with the awareness and training to safeguard against common cyber threats can be hugely beneficial to your organisation's information security. Cyber awareness training teaches employees to understand vulnerabilities and threats, empowering them and the organisation to better protect and prevent against common cybercrime and information security risks, including social engineering, online fraud, phishing, whaling and web-browsing risks.

Course Overview

Are You Effectively Training Employees in The Battle Against Ransomware?

Basic cyber awareness can help train your employees to avoid emailed or online links that are suspicious or from unknown

sources. Such links can release malicious software or a variant of ransomware infecting and encrypting organisational data.

Many ransomware attacks could be avoided through professional employee education and training.

However, most training in this area amounts to little more than a newsletter or leaflet provided to employees or a information security presentation.

Intellect's cyber security specialists have trained organisations (private/public) and government personnel all over the world.

Along with our successful training courses we also provide organisations and governments alike with unique methods of building awareness in the workplace.

Aims and Objectives

Online learning is highly successful for large organisations wanting to create a level of awareness within their organisation. It uses blended learning techniques with the use of media and video and tests, building a level of awareness to a large audience in a very short space of time.

Our basic online courses can be tailored to your organisations needs but typically last between 15-60min.

Introduction – The Web Mindset

To enable people to recognise what data leakage on the Internet is and how it can be minimised to protect what they do online.

What do you want to use the Internet for and what does the Internet want to use you for?!

Advertising, malware, phishing, etc. Your web footprint (Signing into Gmail, how does this affect your searches and collected data about you?) Google Analytics and data captures Tabbed Browsing and handshaking Cleaning your cookies - Why? What benefits?

e: info@intellect-intelligence.com
t: 0843 289 8627

Safeguarding Yourself Online

Enable employees to understand security online and data leakage through social media examining personal, family and work accounts Social Networks (safe use of social media) - Simple to complex ie Security Settings, what you post, who can see? Being Tagged by others - Family, Friends (Their settings can affect yours) Your footprint - Your families

footprint (what personal details exist for you all and those associated with you ie directories, eBay, email, phone numbers) - Search for yourself exercise Location posts - checking in, (4Square etc) showing patterns (social, work, family...all make you vulnerable)

Work Networks (Linked In) - Why do you use it? - Looking at other individuals/companies? What do you give away by searching? What do you put on it? Self-Assessment Phase 1. Search Online 2. Search Social Networks (individual, close family) 3. Search Work Networks.

Safeguarding Your Devices

Enable staff to understand what vulnerabilities exist around mobile devices and risk to the corporation Personal & Work - Do you carry them both all the time? What security do you have on them? Pin lock? 10 attempts and then the phone is wiped enabled? Find my iPhone etc (Android alternatives) What does your device give away about you? Siri" (Expand Data Leakage) calendars etc "Ok Google" BACK UPS Cloud Microsoft 365 iTunes (what syncs with what?) Corporate vs Home sharing - Best of Both Worlds?

Internet Security

Enable staff to understand what risk exists around unsolicited emails and sources Of malware and subsequent risk to the individual and/or corporation Common Sense vs Targeted Commercial Malware Common Sense - Emails (Spam, Spoofing, Phishing, Spear Phishing) Email attachments (authenticity & verification) - Know your audience, if in doubt, don't open it!

Targeted Malware or Non Targeted Malware Types of Malware (examples including commercial and private file targeted Cryptolockers) Sources of compromise- Pornography, children using your devices! Not having antivirus or malware installed - computer and phone (android) Common sense still applies

Due Diligence

Enable staff to conduct a limited check of companies, organisations and individuals with whom they engage with to enable a determination of risk to the corporation

Overview of Due Diligence - What checks can be done against: companies organisations individuals