Cyber Security Awareness Workshop

#CyberAwareness101

> Read_Me

Our Cyber Awareness Workshop will provide employees with the essential knowledge to practice good cyber hygiene. Delegates will understand their responsibility for protecting company data and how to implement practical cyber security processes into their everyday working lives.

We use a blended approach that makes use of digital interactive scenarios and games combined with discussions, videos and case studies. The approach is both engaging and informative. 8 sessions cover 'how-to' and cyber security best practice in the following areas: Passwords, Encryption, Phishing, Email Security, Online Security, Offline Security, Data Classification, Remote Working, Social Engineering and Risky Behaviours.

Our cyber security and behavioural experts work within business throughout the year. In the workshop, they will deliver practical demonstrations and presentations. They will explain the day to day threats companies and employees experience and how these threats are evolving. Delegates will be able to ask questions and work with our experts so they can become more cyber secure and safe.

Aimed at: All Employees
Numbers: 25 delegates per course
Session objectives:

- Understand the threats that directly affect you as an employee
- Learn how to be secure at work and online
- Grasp essential cyber security processes.

Delivery style: Presentations, demonstrations and interactive exercises/discussions.
Resources/interactions:

- Breakout sessions
- Videos
- Demonstrations
- Interactive scenarios and exercises
- Certificate of attendance - level up by doing a post workshop online refresher test.

< WORKSHOP GAMIFICATION >

Sessions 4, 6 & 8 are linked into an overall cyber security game to increase engagement and understanding. Four teams compete during the day to win a prize.

Timings: 10.00 to 16.30

METRIX CLOUD

LUKE RAPHAEL | 020 3876 3644 | info@metrixcloud.co.uk | www.metrixcloud.co.uk

> COURSE OUTLINE

Sessions 1 – 5
Cyber Security Awareness
Past, Present & Future
Human Risk
Typical Scenarios

Sessions 6 - 7
People
Processes / Physical
Information Technology

Session 8
Cyber Security Strategy
(Develop, Deter and Defend)

> SESSIONS

> Session 1: Introduction and Awareness

- Welcome | Ground Rules
- Why do we need cyber security training?
- How cyber breaches happen?
- Why do hackers target the human?
- What are your personal experiences of cyber-crime? **< DISCUSSION >**

> Session 2: Cyber-Security - Past, Present and Future

Jamie Woodruff, a leading cybersecurity expert, will make a 30-minute presentation. Jamie will give delegates an understanding of what motivates a hacker and why you or your company might be compromised. The full focus of this presentation will be:

- **Evolution of Hacking -** How cybercrime has evolved from 10 years ago to the current day.
- **Perception of a Hacker -** How people stereotype, what the modern-day hacker looks like and what are their motivations.
- **Organised Business (Cybercrime) -** Businesses have been set up around the world to hack other companies and extract data to sell. Organised crime, with target based hackers, try to steal corporate data.
- **Safest methods of communication -** How to stay safe when using smart devices to communicate sensitive data.
- **IOT – Internet of Things**
  - With smart TV's, smart phones and even smart fridges, our modern lives mean that we are linked to IOT, if we like it or not. Connected devices in homes are currently unregulated. And once on the network they may lead to data and other devices being compromised if not correctly secured.
  - Personal security is key. We need a greater understanding of the technology we use in our day-to-day lives to make it more difficult for hackers to access our data. We need to help younger and older generations to stay cyber safe. And, implementing security into our personal lives has a positive effect on our business lives.

> Session 3: Human Risks

The importance of the human in cyber defence (social engineering and risky behaviours):

- Potential outcomes of a human breach.
- Threat landscape and future predictions.
- Impacts on you and the business. Your duty as an employee. **< DISCUSSION >**

> Session 4 – Scenarios

< SCENARIOS >

Gamification

- Four teams explore scenarios.
- Key learning message: vunerabilities are not just about IT.
- Score for how well they understood the scenario and presented the recovery plan.

Interactive case studies exploring vulnerabilities:

- What and why did it happen?
- What were the consequences?
- How did you spot it and you handle it?

Four teams look at:

1. CEO Fraud - compromised email accounts of a company and its lawyers allows a sophisticated phishing scam to transfer millions.
2. Ransomware – an eCommerce website is hacked; will the team pay a ransom to get it back online?
3. Social Engineering - a customer services agent is manipulated into giving sensitive information over the phone.
4. Risky Behaviours - while visiting a conference Mike leaves his computer open and it gets mined. Within the week, his company gets attacked.

Feedback - PIP/P Model (Vulnerabilities)

Cyber Security can be categorised into three areas:

- People;
- Information Technology;
- and Processes/Physical.

We term this the PIP/P Model.

People

Social Engineering
Social Media Exploitation
Risky behaviours

Information Technology

Viruses
Malware
Hacking
Denial of Service

Processes / Physical

Physical Security
Housekeeping
Organisational Process Exploits
Insider Threats

> SESSION 5: Phone hacking and Wi-Fi Devices **< DEMONSTRATION >**

Jamie will give a demonstration on how Wi-Fi and mobile devices can be compromised. He will show how mobile devices can be hacked and what devices can be used to pull data from tablets, laptops and mobile phones. Delegates will gain a better understanding of their vulnerabilities and how to protect themselves.

> SESSION 6: People / Processes / Physical Protection

Exercise 1: Housekeeping

- VPNs, data storage and clear desk best practice.
- **< INSTRUCTOR-LED EXERCISE >** Office and process audit plus recommendations.

Exercise 2: Social Engineering

- Much like a computer firewall, we need to defend against people who seek to manipulate and attack us.
- **< INSTRUCTOR-LED EXERCISE >** Case study of a breach (social engineering leading to physical attack).

Exercise 3: Remote Working

- We need to be aware of the risks associated with remote working and Wi-Fi usage.
- **< COMPUTER-BASED EXERCISE >** Protocols, procedures and responsibilities.

Exercise 4: Social Media Exploitation

- In the social media age, we publish a huge amount of information about ourselves and our company that can be used to build up the basis of an attack.
- **< COMPUTER-BASED EXERCISE >** Research and attack.

< INTERACTIVE EXERCISES >

Gamification

- Each team explores 4 exercises.
- Key learning message: protection needs to be well thought out and comprehensive.
- Score for how well they did.
- Feedback using video and discussions.

> SESSION 7: IT Protection **< PRESENTATION & DEMONSTRATIONS >**

Passwords	Emails	Internet Use	Encryption
• How they get hacked • What you should protect • Strong passwords	• Types of phishing • What happens if you click a phishing link • What makes you more likely to click	• How to be aware of a secure website • Checks you can do to make sure it's safe • If in doubt statement	• What is encryption • Usage • Basic guide to encryption

> SESSION 8: Developing a Cyber Security Policy and Final Scores

PIP Model (Protection) = Cyber Security Strategy

Once your organisation has undertaken a cyber security audit, it needs to create a Cyber Security Policy. The Policy will cover:

DEVELOP Cyber Security Resilience	DETER and DEFEND from Attacks
• The business case • Skills and knowledge need • Ongoing communications approach • Roles and responsibilities	• Procedures: people • IT systems and procedures • Procedures: physical and organisational processes • Protocols (in the event of an attack)

The End Game

- Final development of the team's Cyber Policy
- Understand cyber security in terms costs versus risk management.

Feedback

- Conclusions
- Q&A
- Close

< INTERACTIVE EXERCISES >

Gamification

- How much will they take from the overall business budget?
- How much will they commit to the 3 areas of PIP/P?
- Update the game logic.
- Feedback and award prize.

METRIXCLOUD

LUKE RAPHAEL | 020 3876 3644 | info@metrixcloud.co.uk | www.metrixcloud.co.uk