Social Engineering Training

8o% of Cyber Security Attacks can be Mitigated by Cyber Training of ALL your Staff

BACKGROUND

Social engineering attackers are very effective at breaking into your organisation. In fact, 80% of all successful cyber-attacks have a social engineering element to them. Many businesses focus on protecting systems with complex and expensive technological solutions but fail to protect the weakest element - human nature.

Social engineers take advantage of the human tendency to trust and use this to gain information and access to our most confidential and secure systems. The damage caused by social engineering attacks can be devastating, expensive and result in huge litigation costs as well as severe reputational damage.

The good news is that social engineering training when done effectively will greatly bolster your organizations' cyber security posture and can significantly reduce your risks in a very economical manner.

The Workshop

Duration: 2 Days **Presentations and Workgroups**

Oxford Systems Social Engineering training is unique in the fact that instead of just reeling off a series of disturbing statistics and creating a climate of fear, we offer a long-term solution to social engineering attacks that also trains your staff in the safe use of technology both in and out of the workplace.

The program has been developed by world renowned authority on Cyber Security Dr John McCarthy Ph.D. B.Sc. (hons) MBCS. This is achieved by training your staff in 2 key Social Engineering attack counter measures. Understanding good cyber hygiene practices and creating a cyber security culture in your organization. The practices are simple to understand and adopt. They have been proven suitable for employees at any level in your organization.

Contact: cyber@oxfordsystems.eu Tel: +442081235477 Website: www.oxfordsystems.eu

Social Engineering Training

8o% of Cyber Security Attacks can be Mitigated by Cyber Training of ALL your Staff

Topics Covered

- Social Engineering concepts
- Understand the nature of Social Engineering attacks
- The business impacts of Cyber Security breaches
- In business terms, how hackers choose and attack their targets
- Understand Cyber Security terminology
- The types and motives of attackers
- The cyber threat landscape
- How to reduce business risk exposure and reduce costs while increasing overall security posture
- OSNIT – Open Source Intelligence and how this is used against us
- Cyber Security regulations and standards
- Hacking demonstration

Cyber Hygiene

- What is Cyber Hygiene?
- How can it protect us from cyber-attack?
- Delivering great service with Cyber Hygiene and saving money

Creating a Cyber Security Culture

- Creating a Cyber Culture where to begin?
- Ensuring you are operating best cyber practice
- How to reduce business risk exposure and reduce costs while increasing overall security posture
- Generate money and business opportunities from good information security practices.

Contact: cyber@oxfordsystems.eu Tel: +442081235477 Website: www.oxfordsystems.eu