NCSC Certified Training - Cyber Security and Social Media

Maritemex
Holistic Cyber Security Resilience

1. COURSE

This seminar is dedicated to:

- The value of information and you and your organisation's role in protecting, valuing and safely exploiting information including via Social Media
- Cyber Security threats including, social engineering threats including the Insider Threat, phishing techniques and scams
- Social Media best practice at home, at work and in a hybrid environment
- An overview of key legislation, policies and processes in relation to your responsibilities
- Best practice leadership, governance and policies and processes
- Cyber hygiene - using social media, video conferencing, shopping and apps etc.
- Exercises and real-world scenarios
- Further information and support.

2. COURSE CONTENT

Social media is an everyday engagement for most people and businesses. Sadly, social media can be a source of vulnerability for businesses and organisations. A clear understanding of the threats associated with personal and business use of social media is vital if you need to protect a business or organisation from attack.

This one-day course will help protect organisations from financial, operational and reputational harm, which could be caused wittingly or unwittingly, by an Insider attack. Delegates will be equipped with the context and knowledge to understand best practice and to mitigate the risks associated with the Insider Threat. The course will explore potential motivators and indicators, including social engineering; and look at how to create an environment where employees understand the value of protecting information both at work and at home..

3. COURSE FORMAT

Learners will engage in an interactive workshop which will allow them to develop theoretical knowledge and apply it to their own situations. Delivery will be through a blended approach that will allow learners to fully engage in the session and gain practical examples of how to turn theory into practice.

4. DETAILED COURSE PROGRAM (unrolled training sequences)

Session	Delivery
1	***Inrodaction***
2	***Cyber Threats and Risks – The Insider*** Consider the motivations and indicators of potential insider threats (both malicious and non-malicious), including social engineering, phishing and ransomware
3	***Responsibilities and Accountability*** A review of current legislation and regulations in relation to your responsibilities as both as home and at work
4	***Organisational Leadership and Governance,*** Reviewing the key roles of leaders in the management of information assets and governance – including policies and processes
5	***Social Media Scenarios and Course Application*** Engaging in a number of scenarios and working together to practice skills and learning theory including best practice policy ('Dos and Don't's')
6	***Implementation*** Examine ways in which organisations can learn from real life examples and scenarios and how these could be implemented across an organisation

5. COURSE PREPARATION

This course is open to anyone responsible for leading, managing or assisting in the response to Cyber Security and Information management.

6. COURCE EVALUATION

Participant engagement and contribution is essential in this course. It is expected that all learners fully interact with the learning and the group activities.

7. BIOGRAPHY

All course tutors will have the following professional credentials.

- UK National Cyber Security Centre Certified Trainers
- Higher level professional and teaching qualifications, gained over a career in Cyber Security practice.
- Contribution to the profession, giving back to the community at large, through voluntary engagement and seats on esteemed industry panels, working groups and special interest groups.
- Wide experience of professional roles in Cyber Security, leading to national and in many cases international reputations in domain.
- A complete and extended understanding of Cyber Security, Information Governance across a number of sectors
- A wide-ranging understanding of Finance and Procurement in relation to Cyber Security related practices

Our experienced, expert and engaging NCSC and Executive Trainer pool includes the following profiles:

NCSC Certified and Executive Trainer: Experienced strategy adviser and solution implementer, with international leadership experience in both government and commercial organisations. Over 22 years' experience in the fields of Cyber Security, Information Assurance and Information and Communications Technology after a background in Computer Science and Computing Information Systems. A Visiting Teacher of Cyber Security at the Oxford Martin School of Oxford University. Leads on audits and compliance-related activities with a focus on Critical National Infrastructure, including Central Government and Law Enforcement.

NCSC Certified Executive Trainer: Extensive financial services sector, developing Cyber Security and Information Assurance strategies, delivering Board briefings, leading audits and training and mentoring Senior Executives. Clients include G7 banks, central banks, retail banks and private equity firms. A thought leader in the area of Cyber Security and Information Assurance, speaking at conferences with articles regularly published. A visiting Professor at Oxford University.

NCSC Certified and Executive Trainer: Extensive experience includes mentoring Senior Executives in both the private and public sector. An established and highly effective leader with operational and commercial experience spanning private and defence sectors in the UK, Europe and the Middle East. Led Cyber Health Checks and Audits for multi-national clients, identifying key Cyber risks and threats and advising on improving Cyber resilience.

NCSC Certified and Executive Trainer: Expertise and experience in delivering training and workshops to Board and senior audiences across government and the commercial sector. Background includes geopolitical risk and global threats, information risk and security, as well as risk mitigation, crisis management and prevention. Fostered networks for sharing best practice with Cyber Security organisations in the US, the EU and across the Commonwealth and was a member of the Cyber Assessment Advisory Panel at the UK National Cyber Security Centre (NCSC).

NCSC Certified and Executive Trainer: coaches and trains leadership on Cyber and Risk across sectors and in the Critical National Infrastructure. Brings significant operational and field experience to his practitioner and academic work and specialises in the human dimension of cyber security. Previously, he was Chief Executive of a UK national body and author of a number of Cyber Security books sold internationally.

NCSC Certified and Executive Trainer: Experience of wide ranging oganisational support. Advises on information governance policy development and Cyber Security leadership and strategy. Background in education, academia and the not-for-profit sector has seen him advise government on national skills strategies and develop skills programmes in Cyber Security across the UK. Vice Chairman of the Information Assurance and Advisory Council. Working with national and regional bodies, and private sector parties, he focuses on developing regional cyber resilience strategy. Recipient of a National Cyber Security Award for his work with young people and cyber security.