Protecting What Matters: Human-Centric Cybersecurity Course

Introduction

Cybersecurity is no longer solely a technical problem, it is a human one. The majority of successful cyber attacks exploit human behaviour rather than technical vulnerabilities, targeting how individuals think, feel, and make decisions.

This course provides a powerful and engaging insight into the psychological and behavioural drivers behind cyber risk. It explores how individuals are influenced by social engineering, online environments, and cognitive biases, both inside and outside the workplace.

Delivered through a combination of real-world examples, interactive discussion, and scenario-based learning, this course moves beyond traditional "tick-box" training and explicitly links personal digital behaviour with organisation risk, reflecting modern working practices such as remote and hybrid working. It equips participants with the awareness and practical understanding required to recognise manipulation, challenge assumptions, and make more secure decisions in both their professional and personal lives.

What you will learn:

- How cyber attacks exploit human behaviour rather than technology
- Networking fundamentals for everyone
- The psychology behind phishing, social engineering, and manipulation techniques
- The role of cognitive biases (e.g. optimism bias, normalcy bias, authority bias) in decision-making
- How social media, online activity, and "echo chambers" influence perception and behaviour
- Real-world examples of insider threat development and behavioural exploitation
- How to recognise suspicious activity and respond appropriately
- The link between personal digital habits and organisational risk
- Practical steps individuals can take to protect themselves and their organisation
- How small behavioural changes can significantly reduce cyber risk

Who should attend?

This course is designed for personnel at all levels within an organisation, from frontline staff to senior leadership. It is particularly relevant for individuals who interact with digital systems, handle sensitive information, or are responsible for maintaining organisational security in day-to-day operations.

No prior technical cyber security knowledge is required, making it suitable for both technical and non-technical audiences.

Key Organisations

Ministry of Defence

Government Departments and Agencies

Critical National Infrastructure (CNI) Organisations

Financial Services, Healthcare and Legal Sectors

Defence Industry and Commercial Organisations

Any organisation seeking to reduce human cyber risk and strengthen security culture

Course Duration
1 Day

Location
Mercury EW Ltd – Training Facility or Customer Site