HUMAN RED TEAM
A DIVISION OF SYNOVUM CYBER SECURITY

ETHICAL SOCIAL ENGINEERING FOUNDATION

Master the Fundamentals of Understanding Human-Centric Cyber Threats

In the world of cyber security, technology is only part of the battle. **Social Engineering**, the manipulation of individuals into revealing sensitive information or performing actions that compromise security, has become a key method for attackers to bypass even the most sophisticated technical defences.

Human vulnerabilities are often regarded as the weakest link in any security system, making social engineering one of the most important areas to address in modern cyber security strategies.

Why Social Engineering is a Critical Area of Cyber Security

- **Exploiting Human Weaknesses**: No matter how secure your organisation's firewalls or software might be, attackers know that **humans are often the easiest target**. By exploiting trust, fear, or curiosity, cybercriminals can manipulate employees into giving up sensitive data or access, completely bypassing complex technological barriers.
- **Growing Attack Vector**: **Phishing, vishing, pretexting, baiting**, and other forms of social engineering attacks have surged, affecting organisations of all sizes. These tactics are often the entry point for more complex technical attacks.
- **Difficult to Defend Against**: Unlike traditional cyber security threats that often rely on technical vulnerabilities, social engineering targets **human behaviour**. This makes it harder to detect, prevent, and mitigate without proper training and education.
- **High-Profile Breaches**: Some of the most devastating security breaches and attacks in recent years have been traced back to social engineering attacks, proving that even the most well-defended organisations are vulnerable when the human element is exploited.

Course Overview

This foundation-level training course introduces delegates to the psychological and behavioural tactics used by malicious threat actors to manipulate individuals and gain unauthorised access to systems, data, or facilities. Designed for beginners, the course breaks down the core concepts of social engineering, including phishing, pretexting, baiting, and impersonation, while exploring the real-world consequences of these attacks in personal, corporate, and public sector environments. Participants will learn how these techniques exploit human vulnerabilities and why technical controls alone are not enough to defend against them.

Delivered by an experienced instructor, this interactive course highlights the role of ethical social engineering in testing and strengthening organisational resilience, making it ideal for professionals looking to enhance their level of knowledge in this area, build a career in cyber security, or contribute to a more security-conscious workplace. No prior technical background is required — just curiosity and a commitment to learning how people can become the strongest link in security.

Course Benefits

By attending this course, delegates will gain the knowledge to understand, recognise, and prevent/mitigate social engineering attacks, strengthening both personal and organisational security posture.

Predict, Prevent, Protect: Master Ethical Social Engineering

training@synovum.co.uk
www.synovum.co.uk
www.humanredteam.com
@syncybersec
@humanredteam

Key Learning Objectives

- **Describe** the fundamental principles and concepts in social engineering.
- **Understand** the main social engineering attack categories and vectors.
- **Recognise** the different ways in which people can become victims of social engineering.
- **Describe** ways in which individuals can protect themselves from social engineering-based attacks.
- **Demonstrate** understanding of foundation-level ethical social engineering by passing an end-course online assessment, achieving a minimum score of 60%.

Why Attend?

- **Protect Yourself & Your Organisation** – Understand how social engineers exploit human behaviour to bypass technical security systems and learn how to stop them.
- **Build Awareness of Human Hacking Tactics** – Get insight into real-world phishing, pretexting, baiting, and impersonation attacks .
- **Recognise Red Flags Early** – Gain the skills to spot manipulation techniques before they lead to data breaches or reputational damage .
- **Be Empowered as the First Line of Defence** – Be equipped with practical knowledge to respond confidently and appropriately to suspicious activity .
- **No Prior Knowledge Required** – Designed for beginners, this course builds foundational understanding in an accessible, engaging format.

Who Should Attend?

- **Security/IT Professionals** who want to comprehend social engineering tactics that bypass technical controls .
- **HR, Compliance, and Risk Officers** wanting to appreciate human-based threats and help shape better security policies and education/training programmes.
- **Frontline Staff, Security & Customer Service Teams** who need to recognise coercion/manipulation attempts using phone, emails, messaging, or in-person interactions .
- **Students or Career Starters in Cyber security** who want to gain foundational knowledge to support further study or certifications.
- **Managers and Business Leaders** who need to appreciate how social engineering attacks can impact operations, reputation, and data protection.

Course Duration

- 1 Day.

Assessment

Delegates will be required to pass the following assessment:

- 45-question (1 hour) multiple-choice exam.

Successful candidates will receive a certificate and separate certification badge.

Delegate Pack

- Electronic version of the *Ethical Social Engineering-Foundation* delegate manual.
- Exam.

Gain essential knowledge in a high-impact area of cyber security by attending this training course.
Get in touch with us to find out more.

Predict, Prevent, Protect: Master Ethical Social Engineering

training@synovum.co.uk
www.synovum.co.uk
www.humanredteam.com
@syncybersec
@humanredteam