Human-Centric Cybersecurity Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The contemporary threat landscape has irrevocably shifted: human error remains the single greatest vulnerability, accounting for over 90% of successful cyberattacks. While organizations invest heavily in next-generation firewalls and AI-driven defense systems, the most potent attack vector the person behind the screen is often neglected. Traditional, compliance-driven "check-the-box" training is failing, leading to persistent security lapses like successful phishing, social engineering, and insider threats. A new paradigm is essential. Human-Centric Cybersecurity Training Course moves beyond basic awareness to fostering a robust, data-driven Security Culture. By integrating behavioral science, cognitive psychology, and personalized, gamified microlearning, we transform every employee from a potential weak link into the organization's first line of defense, dramatically reducing the enterprise's overall cyber risk score.

The Human-Centric Cybersecurity model recognizes that security behaviors are driven by motivation, ability, and psychological context not just technical knowledge. Modern threats are increasingly sophisticated, with threat actors leveraging Generative AI to craft highly convincing deepfake and spear-phishing campaigns. This curriculum is engineered to address these emerging threats, focusing on critical thinking, incident reporting procedures, and security hygiene in a constantly evolving remote and hybrid work environment. Participants will gain practical, role-based security awareness skills and a deep understanding of their personal accountability in maintaining data protection, regulatory compliance, and overall organizational resilience.

Programme Curriculum

Human-Centric Cybersecurity Training Course

Introduction

The contemporary threat landscape has irrevocably shifted: human error remains the single greatest vulnerability, accounting for over 90% of successful cyberattacks. While organizations invest heavily in next-

generation firewalls and AI-driven defense systems, the most potent attack vector the person behind the screen is often neglected. Traditional, compliance-driven "check-the-box" training is failing, leading to persistent security lapses like successful phishing, social engineering, and insider threats. A new paradigm is essential. Human-Centric Cybersecurity Training Course moves beyond basic awareness to fostering a robust, data-driven Security Culture. By integrating behavioral science, cognitive psychology, and personalized, gamified microlearning, we transform every employee from a potential weak link into the organization's first line of defense, dramatically reducing the enterprise's overall cyber risk score.

The Human-Centric Cybersecurity model recognizes that security behaviors are driven by motivation, ability, and psychological context not just technical knowledge. Modern threats are increasingly sophisticated, with threat actors leveraging Generative AI to craft highly convincing deepfake and spear-phishing campaigns. This curriculum is engineered to address these emerging threats, focusing on critical thinking, incident reporting procedures, and security hygiene in a constantly evolving remote and hybrid work environment. Participants will gain practical, role-based security awareness skills and a deep understanding of their personal accountability in maintaining data protection, regulatory compliance, and overall organizational resilience.

Course Duration

5 days

Course Objectives

1. Master the principles of Human Risk Management (HRM) to shift from compliance-only to a data-driven security strategy.
2. Analyze and mitigate the top five human-centric attack vectors, including spear-phishing, vishing, and pretexting.
3. Implement effective Multi-Factor Authentication (MFA) and password hygiene across diverse platforms and devices.
4. Develop critical thinking and suspicion-level skills to preempt and detect advanced social engineering campaigns.
5. Understand the unique security risks posed by Generative AI tools and establish safe usage protocols.
6. Identify and manage the insider threat through behavioral indicators and policy adherence.
7. Apply Zero Trust principles to daily operations, reinforcing the "never trust, always verify" mindset.
8. Navigate and ensure compliance with major data privacy regulations in data handling and sharing.
9. Secure the remote and hybrid workspace, addressing risks associated with BYOD and public Wi-Fi.
10. Execute proper incident reporting procedures and understand the chain of custody in a security event.
11. Cultivate a positive, blame-free Security Culture led by management and reinforced by peer behavior.
12. Use behavioral science nudges and gamification to ensure continuous security awareness and knowledge retention.
13. Analyze real-world data breach case studies to internalize the cost and impact of human error.

Target Audience

1. All Employees.
2. Remote and Hybrid Workers.
3. New Hires undergoing onboarding.
4. Sales and Customer-Facing Teams
5. Executive Leadership.
6. IT and Security Teams
7. HR and Legal/Compliance Personnel.

8. Third-Party Vendors/Contractors with network access.

Course Modules

Module 1: The Human Element & Cyber Risk Foundation

- Understanding why human error is the leading cause of data breaches
- Cognitive Biases in Security.
- Identifying and classifying the Insider Threat
- Defining your personal Cyber Risk Score and key behavioral indicators.
- Case Study: The Maersk/NotPetya Attack

Module 2: Advanced Social Engineering Defense

- Deconstructing the Phishing Kill Chain.
- Spear-Phishing and Whaling
- Defending against non-email threats
- The psychology of Pretexting and the "helpful" security violation.
- Case Study: The RSA SecurID Breach

Module 3: Authentication and Identity Management

- Creating Strong Password Hygiene.
- Multi-Factor Authentication.
- The dangers of password reuse and the safe use of Password Managers.
- Securing credentials against Keyloggers and Brute-Force Attacks.
- Case Study: The Colonial Pipeline Ransomware Attack

Module 4: Secure Data Handling and Privacy

- Understanding the difference between PII, PHI, and Intellectual Property.
- Adherence to GDPR and CCPA.
- Securely sharing sensitive files.
- Safe disposal of physical and digital records to prevent dumpster diving.
- Case Study: Equifax Data Breach

Module 5: Mobile, Remote, and Hybrid Work Security

- Securing the Home Network.
- Bring Your Own Device Policy adherence and separating work/personal data.
- The risks of using Public Wi-Fi and best practices for secure VPN usage.
- Securing physical devices.
- Case Study: Target Data Breach

Module 6: Emerging Threats and Technology Security

- Generative AI Protocol.
- Ransomware Defense.
- Understanding and minimizing risks from Supply Chain Attacks and third-party software.
- The importance of Software Updates and Patch Management.
- Case Study: The UAE Deepfake Voice Fraud.

Module 7: Incident Response and Accountability

- What to do when you click.
- Identifying and reporting suspicious activity or uninvited people in the physical office
- Understanding the Incident Reporting Procedure and the role of the security team.
- Legal and financial consequences of a major Data Breach.
- Case Study: MGM Resorts Incident

Module 8: Building a Security Culture

- Moving from Awareness to Culture.
- The role of leadership in championing security from the top down.
- Implementing Behavioral Nudges and Gamification for long-term retention.
- Encouraging peer-to-peer security reinforcement and celebrating positive security behavior.
- Case Study: The Netflix Culture Deck

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com