# Cybersecurity Awareness & Building Human Firewalls Training Course

## Ref: #CYB6953

## Course Introduction / Overview:

This comprehensive training course is designed to empower trainers and security professionals with the essential knowledge and skills needed to transform employees into an organization's strongest defense. While technology-based security solutions are crucial, the human element remains the most vulnerable link in the chain. This program goes beyond a simple list of dos and don'ts, teaching you how to design, implement, and measure a cybersecurity awareness program that truly changes behavior. Participants will learn how to create engaging content, use storytelling to explain complex threats, and simulate real-world attacks like phishing to test employee resilience. We will cover key topics like social engineering, data privacy, and the psychological principles that make humans susceptible to manipulation. Drawing from the academic research of renowned authors like Steven M. Furnell and his work on security culture, this program provides a strategic and practical framework for cultivating a security-conscious workforce. His research highlights that an effective security culture is about more than just compliance; it is about making security a part of an organization's DNA. This course at BIG BEN Training Center will empower you to build a human firewall that can resist the most sophisticated attacks.

## Target Audience / This training course is suitable for:

- Cybersecurity awareness trainers.
- Human resources professionals.
- IT and security managers.
- Chief Information Security Officers (CISOs).
- Internal communications specialists.
- Compliance and risk officers.
- Training and development professionals.

## Target Sectors and Industries:

- Corporate and enterprise.
- Financial services.
- Healthcare.
- Technology and software.
- Manufacturing.
- Government agencies and equivalents.
- Education.

## Target Organizations Departments:

- Information Security.
- Human Resources.
- Compliance.
- Training and Development.
- Internal Communications.
- IT.
- Risk Management.

## Course Offerings:

By the end of this course, the participants will have able to:

- Design and implement a dynamic cybersecurity awareness program.
- Educate employees on the latest cyber threats and trends.
- Create engaging and effective training materials.
- Conduct simulated phishing and social engineering exercises.
- Measure the effectiveness of a training program.
- Foster a culture of security within an organization.
- Influence employee behavior to reduce human-related risks.

## Course Methodology:

This training course at BIG BEN Training Center uses a highly interactive and practical methodology. The program includes a series of workshops where participants will design and present their own awareness campaigns. You will learn to use storytelling, humor, and real-world case studies to make security concepts memorable and relatable. The course emphasizes a train-the-trainer approach, giving you the tools to become an effective educator and to coach others on how to deliver impactful security training. You will practice conducting simulated phishing campaigns and analyzing the results. The instructor will provide personalized feedback on your communication style and content. This approach ensures you will leave with the confidence and skills to turn passive learners into active defenders.

## Course Agenda (Course Units):

### Unit One: The Human Element in Cybersecurity

- The role of humans in the security chain.
- Psychology of social engineering.
- Phishing, fishing, and smishing attacks.
- The cost of human error.
- Building a business case for security awareness.
- Measuring human risk.
- Case study: a real-world social engineering incident.

## Unit Two: Designing a Comprehensive Program

- Defining a security awareness program’s goal.
- Audience segmentation and content tailoring.
- Creating engaging and memorable training materials.
- Developing a communication plan.
- Selecting the right delivery methods (e.g., e-learning, workshops).
- Best practices for program rollout.
- Practical lab: a security awareness campaign design.

## Unit Three: Content and Delivery

- Storytelling for security awareness.
- Creating anti-phishing training.
- Password security and multi-factor authentication.
- Safe browsing and mobile security.
- Data privacy and confidentiality.
- Securing remote work.
- Case study: a successful awareness program.

## Unit Four: Measuring and Reporting

- Key performance indicators (KPIs) for security awareness.
- Measuring behavioral change.
- Using simulated phishing results for reporting.
- Reporting to leadership and stakeholders.
- Benchmarking against industry standards.
- Continuous improvement models.
- Practical lab: data analysis of a simulated phishing campaign.

### Unit Five: Building a Security Culture

- What is a security culture?
- Leadership's role in security culture.
- Making security a habit.
- Gamification and incentives.
- Rewarding good security behavior.
- The future of security awareness.
- Final project: a long-term security culture plan.
- Frequently Asked Questions:

## FAQ:

### Qualifications required for registering to this course?

There are no requirements.

### How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

### Something to think about:

In an era where employees are constantly bombarded with information and alerts, how can organizations ensure that cybersecurity awareness training is not only effective but also avoids causing "alert fatigue" and apathy?

## What unique qualities does this course offer compared to other courses?

This course stands out by providing a unique and vital focus on the human side of cybersecurity. Unlike technical security training, this program is designed for trainers and managers who must communicate complex topics to a non-technical audience. The curriculum is built around a practical, behavior-focused approach. It teaches you how to design programs that not only inform but also influence and change employee actions. The emphasis on real-world case studies, psychological principles, and hands-on exercises ensures you gain an actionable understanding of how to build a security-conscious workforce. It is for professionals who recognize that the best defense is not just technology, but a well-informed and vigilant team.