Digital Defense - Cybersecurity Basics for Everyone 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

In the modern digital landscape, personal and professional data face unprecedented risk from evolving threats. The rise of AI-driven cyberattacks, sophisticated ransomware, and prevalent phishing campaigns means that basic perimeter defenses are no longer sufficient. Every individual, from the remote worker to the senior executive, is a critical endpoint and the first line of defense. Digital Defense - Cybersecurity Basics for Everyone Training Course offers an essential and non-technical deep dive into foundational security principles. We shift the focus from complex network security architecture to practical, human-centric cybersecurity habits, ensuring all participants can confidently implement robust strategies for digital hygiene, safeguard against social engineering, and maintain data privacy in an increasingly connected world.

This comprehensive training empowers participants to become proactive digital citizens, significantly reducing their personal and organizational cyber risk. By mastering key concepts like strong authentication, securing IoT devices, understanding cloud security basics, and developing an incident response mindset, attendees will transform from potential vulnerabilities into active security contributors. The curriculum is built around real-world scenarios and practical defense mechanisms, making the complex topic of cyber threat intelligence accessible. Upon completion, you won't just know about security; you'll practice it, fostering a culture of continuous security awareness that future-proofs your digital life against the top cybersecurity trends and persistent advanced persistent threats (APTs).

Programme Curriculum

Digital Defense - Cybersecurity Basics for Everyone Training Course

Introduction

In the modern digital landscape, personal and professional data face unprecedented risk from evolving threats. The rise of AI-driven cyberattacks, sophisticated ransomware, and prevalent phishing campaigns means that basic perimeter defenses are no longer sufficient. Every individual, from the remote worker to the senior executive, is a critical endpoint and the first line of defense. Digital Defense - Cybersecurity Basics for Everyone Training Course offers an essential and non-technical deep dive into foundational security principles. We shift the focus from complex network security architecture to practical, human-centric cybersecurity habits, ensuring all participants can confidently implement robust strategies for digital hygiene, safeguard against social engineering, and maintain data privacy in an increasingly connected world.

This comprehensive training empowers participants to become proactive digital citizens, significantly reducing their personal and organizational cyber risk. By mastering key concepts like strong authentication, securing IoT devices, understanding cloud security basics, and developing an incident response mindset, attendees will transform from potential vulnerabilities into active security contributors. The curriculum is built around real-world scenarios and practical defense mechanisms, making the complex topic of cyber threat intelligence accessible. Upon completion, you won't just know about security; you'll practice it, fostering a culture of continuous security awareness that future-proofs your digital life against the top cybersecurity trends and persistent advanced persistent threats (APTs).

Course Duration

5 days

Course Objectives

1. Master Strong Authentication methods, including Multi-Factor Authentication (MFA), to counter credential theft.
2. Identify and mitigate prevalent Social Engineering tactics, such as Phishing and Pretexting.
3. Implement effective data backup and recovery strategies to ensure Ransomware Defense and maintain Business Continuity.
4. Apply the principle of Least Privilege to manage access permissions on personal and work devices, improving Endpoint Security.
5. Understand fundamental concepts of Data Privacy and the regulations like GDPR or HIPAA that govern sensitive information.
6. Secure Remote Work environments by utilizing Virtual Private Networks (VPNs) and adhering to Zero Trust concepts.
7. Recognize the risks associated with unsecured IoT Devices and implement basic protective measures for a smart home/office.
8. Practice safe browsing and transaction habits to avoid Malware and maintain Digital Hygiene.
9. Develop a personal Incident Response plan for immediate action following a suspected breach or security event.
10. Differentiate between encryption methods and their role in Data Security.
11. Secure Cloud Storage accounts by configuring robust access controls and understanding shared responsibility models.
12. Conduct basic Vulnerability Assessment on personal computing assets.
13. Integrate continuous Security Awareness into daily routines to actively reduce the likelihood of human error, the weakest link.

Target Audience

1. General Employees/End Users.

2. Remote/Hybrid Workers.
3. Small Business Owners.
4. Seniors and Family Members.
5. Recent Graduates/Career Changers.
6. IT/HR Administrators.
7. Digital/Online Shoppers & Banking Users.
8. Parents and Educators.

Course Modules

Module 1: The Human Firewall: Phishing & Social Engineering

- Identifying the four primary types of Social Engineering.
- Spotting the red flags in a phishing email.
- Understanding the danger of Business Email Compromise and how it exploits trust.
- Defense Mechanism.
- Case Study: The Target Data Breach (2013) traced back to credentials stolen from an HVAC vendor via a simple phishing email, highlighting supply chain risk.

Module 2: Fortifying the Gates: Passwords & Authentication

- Creating a truly Strong Password using passphrases and avoiding common dictionary words.
- The essential role of a dedicated Password Manager for generating and storing unique credentials.
- Implementing Multi-Factor Authentication and differentiating between SMS, app-based, and hardware token methods.
- Avoiding password reuse and understanding the risks of storing passwords in plain text.
- Case Study: The Yahoo! Data Breach (2013-2014) involving over 3 billion user accounts due to compromised, unhashed passwords, emphasizing the need for MFA.

Module 3: Malware Mayhem: Viruses, Ransomware, and Spyware

- Defining and differentiating key types of malicious software.
- The escalating threat of Ransomware and the importance of offline backups.
- Securing your Endpoint using Antivirus/Antimalware software and ensuring automatic updates are enabled.
- Understanding common infection vectors: malicious email attachments and drive-by downloads.
- Case Study: The WannaCry Ransomware (2017) attack that spread globally, exploiting a known vulnerability and crippling major institutions like the UK's NHS, stressing the need for immediate patching.

Module 4: Your Digital Fortress: Device & Software Security

- The criticality of continuous Patch Management to eliminate software vulnerabilities.
- Configuring and understanding your device's Firewall and its role in network traffic filtering.
- The importance of physical security.
- Securing your Wi-Fi router.
- Case Study: The Equifax Data Breach (2017) caused by the failure to patch a known vulnerability in the Apache Struts software, illustrating a failure of patch management.

Module 5: The Cloud and Remote Frontier

- Securing Cloud Storage accounts through MFA and strong file permissions.

- The Zero Trust philosophy.
- Best practices for using public Wi-Fi.
- Understanding the limitations of the Cloud Shared Responsibility Model.
- Case Study: The Capital One Data Breach (2019) where a misconfigured Web Application Firewall in a cloud environment led to a massive data exposure, stressing configuration over just platform security.

Module 6: Data Privacy, Identity Theft, and the Dark Web

- Defining Personally Identifiable Information and understanding how to minimize its exposure.
- Practical steps to protect against Identity Theft online and what to do if you suspect a compromise.
- Understanding the basic function of the Dark Web and how stolen credentials are traded.
- The concept of Data Minimization.
- Case Study: The Marriott/Starwood Data Breach (2014-2018) where customer PII was stolen over a period of years, highlighting the massive scope of identity theft risk.

Module 7: Securing Your Smart World (IoT)

- The unique Security Risks associated with IoT Devices
- Best practices for securing new IoT devices: immediate password change and network segmentation.
- Configuring separate Guest Wi-Fi or a dedicated IoT network for smart devices to limit attack surface.
- Understanding device permissions and disabling unnecessary features for better Data Privacy.
- Case Study: The Mirai Botnet Attack (2016) which exploited weak default passwords on thousands of IoT devices to launch massive Distributed Denial of Service attacks.

Module 8: Incident Response & Digital Future

- Steps for immediate Incident Response.
- The importance of continuous Security Awareness Training and self-auditing your online presence.
- Preparing for the future
- Reviewing the concept of Data Encryption
- Case Study: The Colonial Pipeline Ransomware Attack (2021) which caused massive physical disruption, demonstrating that a cyber incident can have severe real-world, operational consequences.

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.org 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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now