COURSE CATEGORY: CYBER DEFENCE
COURSE LEVEL: ESSENTIALS
COURSE CODE: IFIS CDE/01
COURSE NAME: INTRODUCTION TO CYBER SECURITY

Institute of Forensics & ICT Security
Forensics. Security. Training

Institute of Forensics & ICT Security
Forensics. Security. Training

With practical skills, You succeed

About this Course

This course is for students with a basic knowledge of computers and technology but no prior cyber security experience so that they can jump-start their security education with insight and instruction from real-world security experts. This five-day course covers a wide range of baseline topics, including terminology, the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles. The hands-on, systematic learning format will enable you to grasp all the information presented even if some of the topics are new to you. You will learn fundamentals of cyber security that will serve as the foundation of your security skills and knowledge for years to come.

Prerequisites

- This course assumes basic knowledge of computers and technology and thus makes no assumptions regarding prior security knowledge.

Learning Outcomes

In this course, you will learn;

(i) Introduction to cyber security, basic terminologies and definitions.
(ii) Understand cyber security concepts, principles, and terms.
(iii) Cryptography
(iv) Cybersecurity technologies to keep you and your company safe.

Course Outline

Topic 1: Cybersecurity foundations

This topic will introduce you to the basics of Cybersecurity. At the end of this class, you will be able to acquire the knowledge and skills to help you in the various fields basing on the topics covered.

- Introduction to cyber security
- Core security terms and principles
- Principle of Least Privilege and Confidentiality, Integrity, Availability (CIA)
- Fundamentals of risk management, security policy, and authentication/ authorization/accountability
- Building better passwords

Topic 2: Computer Functions and Networking

This topic will begin with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using the American Standard Code for Information Interchange (ASCII). Learners will then be introduced to networking.

- Computer Functions and numbering systems
- Using ASCII to encode letters
- Introduction to networks
- How data moves across a network
- Network types and standards
- Open Systems Interconnection (OSI) protocol stack

Topic 3: An Introduction to Cryptograpy

Even though technology changes hastily, the need to assure the confidentiality, integrity, authenticity, and accountability of information does not. Understanding the basics of cryptography is fundamental to keeping your networks, systems, and data secure.

- Introduction
- Network security
- Symmetric and Asymmetric Encryption
- Hash Algorithms, Message Digests and Authentication
- Secure Sockets Layer
- Email Security
- Internet Protocol Security

Topic 4: Cyber security technologies

This topic is intended to give learners the knowledge about how to stay secure by looking at common attacks and how they can best be prevented.

- Wireless network security
- Mobile device security
- Malware and anti-malware technologies
- Data protection protocols
- Secure remote access, secure web access, secure file transfer
- Virtual Private Network (VPN) technologies

Requirements

- A laptop running any version of Microsoft Windows or Apple Mac (Macintosh). A tablet such as an iPad or Android will not be able to complete the labs.
- You need the Google Chrome browser installed on your laptop before you arrive for class. Other browsers *may* be able to complete the labs, but they often cause difficulties.
- The ability to connect to a wireless (Wi-Fi) network.
- A network setting configured to obtain IP address and DNS servers automatically.
- The ability to disable your VPN. (You will access a lab server inside the classroom. You cannot accomplish this while VPN software is running.). Note: this requirement is for students attending the course in a live classroom. Students attending via OnDemand or Simulcast may not need to disable their VPN.

Target Audience

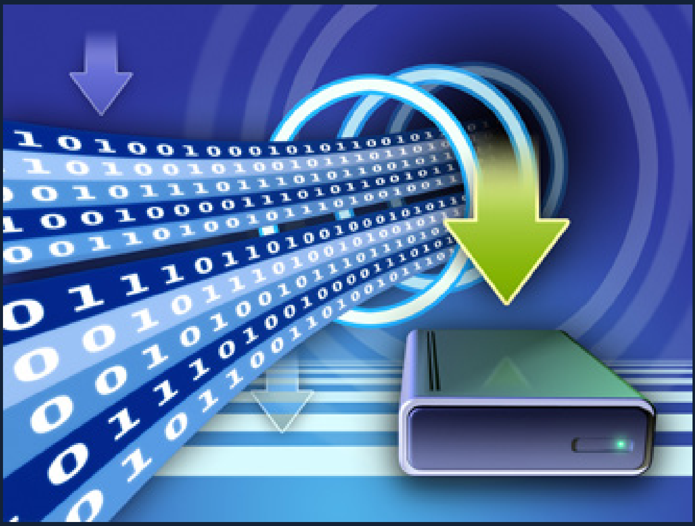
- Anyone new to cyber security and in need of an introduction to the fundamentals of security
- Those who feel bombarded with complex technical security terms they don’t understand, but want to understand
- Non-IT security managers who deal with technical issues and understand them and who worry their company will be the next mega-breach headline story on the 6 o’clock news
- Professionals with basic computer and technical knowledge in all disciplines who need to be conversant in basic security concepts, principles, and terms, but who don’t need “deep in the weeds” detail
- Those who have decided to make a career change to take advantage of the job opportunities in cyber security and need formal training and certification

Application/ Relevance of this course

Communicate with confidence regarding information security topics, terms, and concepts

- Understand and apply the Principles of Least Privilege
- Understand and apply the Confidentiality, Integrity, and Availability (CIA) Triad
- Build better passwords that are more secure while also being easier to remember and type
- Grasp basic cryptographic principles, processes, procedures, and applications
- Understand computer network basics
- Have a fundamental grasp of any number of critical technical networking acronyms, including TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS
- Utilize built-in Windows tools to see your network settings

- Recognize and be able to discuss various security technologies, including anti-malware, firewalls, and intrusion detection systems, content filters, sniffers, etc.
- Build a simple, but fully functional firewall configuration
- Secure your browser using a variety of security plug-ins
- Secure a wireless access point (also known as a wireless router)
- Scan for malware, clean malware from a system, and whitelist legitimate software identified by an anti-malware scanner as “potentially unwanted”.
- Access a number of websites to better understand password security, encryption, phishing, browser security, etc.



Duration and Fees

Duration: 5 days

Pricing: $400

For Inquiries, booking and more information,

Call Admissions on 0393517236/0783517236 or
Email: admissions@forensicsinstitute.org