INTRODUCTION TO CYBERSECURITY AND CYBER ATTACKS HANDS-ON TRAINING

Course Description

This course provides an introduction to the fundamental concepts of cybersecurity, including the principles of confidentiality, integrity, and availability (CIA), common cyber threats and attacks, and best practices for securing digital assets. Participants will gain an understanding of the evolving cyber threat landscape, the motivations behind cyber attacks, and the strategies used by attackers. Through a combination of theoretical instruction, case studies, and real-world examples, participants will develop the knowledge and awareness necessary to recognize, prevent, and respond to cyber threats effectively.

A Comprehensive two (2) day hands-on training for Network Administrators and Network Security Specialist!

—

Conducted by one of best Cybersecurity Expert in the Philippines!

—

Full packed with real-world case studies, malware analysis, network traffic analysis, and cyber attack simulation!

—

Guaranteed learning as we always do hands-on!

—

ITLLECTUAL MANILA

Suite 210 FMSG Bldg.
1823 E. Rodriguez Sr. Ave.
Brgy. Immaculate Conception
Cubao, Quezon City
Philippines 1111

www.itelleqq.com
0915-4885708 | 0919-5618888

I.T.LLECTUAL MANILA

ITELLEQQ TRAINING AND CONSULTANCY

Course Objectives:

Upon completion of this training, participants will be able to:

- ✓ Define the basic principles of cybersecurity, including confidentiality, integrity, and availability (CIA).
- ✓ Identify common cyber threats and attack vectors, including malware, phishing, ransomware, and social engineering.
- ✓ Understand the motivations behind cyber attacks, including financial gain, espionage, activism, and sabotage.
- ✓ Recognize the importance of cybersecurity in protecting personal and organizational digital assets.
- ✓ Describe the impact of cyber attacks on individuals, businesses, and society as a whole.
- ✓ Explain the concept of risk management in cybersecurity and its role in mitigating cyber threats.
- ✓ Identify best practices for securing digital devices, networks, and data against cyber attacks.
- ✓ Understand the importance of user awareness and training in preventing cyber incidents.
- ✓ Analyze case studies of real-world cyber attacks to understand their methods and consequences.
- ✓ Develop basic incident response skills to effectively respond to and mitigate cyber incidents.

Course outline:

Module 1: Introduction to Cybersecurity

- ✓ Definition of cybersecurity
- ✓ CIA Triad: Confidentiality, Integrity, Availability
- ✓ Evolution of cybersecurity threats

Module 2: Common Cyber Threats and Attack Vectors

- ✓ Malware: Types and characteristics
- ✓ Phishing: Techniques and prevention
- ✓ Ransomware: Impact and mitigation
- ✓ Social Engineering: Tactics and red flags

Module 3: Motivations Behind Cyber Attacks

- ✓ Financial gain
- ✓ Espionage
- ✓ Hacktivism
- ✓ Cyber warfare

Module 4: Cybersecurity Best Practices

- ✓ Securing digital devices: Endpoints, servers, mobile devices
- ✓ Network security: Firewalls, intrusion detection/prevention systems
- ✓ Data protection: Encryption, backups, access controls

Module 5: Risk Management in Cybersecurity

- ✓ Identifying and assessing cybersecurity risks
- ✓ Risk mitigation strategies
- ✓ Incident response planning

Module 6: User Awareness and Training

- ✓ Importance of cybersecurity awareness
- ✓ Best practices for end-user training
- ✓ Creating a culture of cybersecurity

Course outline, continued:

Module 7: Case Studies of Cyber Attacks

- ✓ Analysis of real-world cyber incidents
- ✓ Methods used by attackers
- ✓ Consequences for individuals and organizations

Module 8: Incident Response Basics

- ✓ Recognizing a cyber incident
- ✓ Incident containment and mitigation
- ✓ Reporting and documentation

Target Audience:

This course is suitable for individuals with limited or no prior experience in cybersecurity, including students, professionals from non-technical backgrounds, small business owners, and anyone interested in understanding the basics of cybersecurity and cyber attacks.

Prerequisites:

Basic understanding of telecommunications and networking concepts

is recommended but not required.

Duration:

2-Days | 14-hours (Customizable based on specific training needs)

Delivery Method:

Instructor-led training with a combination of lectures, case studies, group discussions, actual demonstration, and hands-on exercises.

Certification:

Upon successful completion of the training program and assessment, participants will receive a Certificate of Completion in Introduction to Cybersecurity and Cyber Attacks Training.

Training Investment:

Per head Investment – **Php17,920.00 (VAT-Inc)**

Exclusive/Group Training – **Php 179,200.00 (VAT-Inc),** maximum of 10 participants

Outside Manila or Provincial Training – Subject to verification and customized costing.

Securing the training slot:

Upon settling the training investment, send the proof of payment, full name, mobile number, and email address to itllectualmanila@gmail.com.

Where to pay:

Bank Name: LANDBANK OF THE PHILIPPINES

Account Name: ITELLEQQ TRAINING AND CONSULTANCY

Account Number: 5462-0024-42

Bank Name: BANCO DE ORO

Account Name: VANESA CEZAR

Account Number: 001100-205134

GCASH

Account Name: VANESA CEZAR

Gcash Number: 09154655700

Other concerns? Contact our Hotline:

0915-4885708 | 0919-5168888 | itllectualmanila@gmail.com

"Anyone who stops learning is old, whether 20 or 80, anyone who keeps learning stays young. The greatest thing in life is to keep your mind young."

– Henry Ford -