

LAPT

LONDON ACADEMY OF PROFESSIONAL TRAINING

CERTIFICATE

Personal Digital Security & Phishing Awareness

Workshop Level



LAPT — London Academy of Professional Training

Address 85 Great Portland Street, W1W 7LT, London, United Kingdom

Email info@lapt.org

Telephone +44 7513 283044

Web lapt.org

Reference IT-CSI-W • IT Centres

UKPRN 10067351 • Registered in England and Wales, company 4984798

AT A GLANCE

REFERENCE	IT-CSI-W
AWARD	Certificate
ASSESSMENT	440 marks — 264 to pass (60%)
PREREQUISITES	None
VALIDITY	Lifetime
AWARDING BODY	LAPT — London Academy of Professional Training

CURRICULUM

1 Basic Security Measures 3 chapters · 12 classes65 marks • 1 Understanding the Basics of Personal Digital Security — 4 classes › 1.1 Recognizing Personal Digital Security Threats › 1.2 Exploring Common Phishing Tactics › 1.3 Implementing Basic Security Tools and Practices › 1.4 Developing a Personal Digital Security Plan • 2 Identifying and Mitigating Common Phishing Attacks — 4 classes › 2.1 Understanding Phishing: Recognizing Common Tactics › 2.2 Analyzing Phishing Emails: Spotting Red Flags › 2.3 Practicing Safe Responses: Steps to Take When Threatened › 2.4 Implementing Protective Measures: Strengthening Your Personal Security • 3 Implementing Advanced Security Measures for Enhanced Protection — 4 classes › 3.1 Understanding Multi-Factor Authentication for Enhanced Login Security › 3.2 Implementing Strong Password Practices and Management Tools › 3.3 Recognizing and Mitigating Advanced Phishing Tactics › 3.4 Updating Software and Systems for Optimal Cyber Security	2 Case Studies in Cyber Security 3 chapters · 12 classes90 marks • 1 Understanding Real-World Cyber Security Breaches — 4 classes › 1.1 Analyzing the Anatomy of a Cyber Security Breach › 1.2 Exploring Case Studies: Famous Cyber Attacks and Their Impact › 1.3 Recognizing Patterns: Common Vulnerabilities and Risks › 1.4 Learning from the Past: Implementing Effective Anti-Phishing Strategies • 2 Analyzing Successful Phishing Attacks and Defense Strategies — 4 classes › 2.1 Understanding the Mechanics of Phishing Attacks › 2.2 Identifying Common Phishing Tactics and Techniques › 2.3 Exploring Case Studies of Real-World Phishing Incidents › 2.4 Developing Effective Defense Strategies Against Phishing • 3 Evaluating Response and Recovery Post-Cyber Attack — 4 classes › 3.1 Analyzing Cyber Attack Aftermaths: Key Indicators and Impacts › 3.2 Formulating Strategic Response Plans: Best Practices and Frameworks › 3.3 Implementing Recovery Tactics: Tools and Techniques › 3.4 Evaluating Recovery Success: Metrics and Continuous Improvement
--	--

3

Introduction to Cyber Security

3 chapters · 12 classes

65 marks

• 1 Understanding Cyber Threats and Vulnerabilities — 4 classes

- › 1.1 Identifying Common Cyber Threats
- › 1.2 Exploring Vulnerabilities in Digital Systems
- › 1.3 Recognizing Phishing Attempts
- › 1.4 Applying Strategies to Mitigate Cyber Threats

• 2 Implementing Personal Security Practices — 4 classes

- › 2.1 Understanding Basic Personal Security Concepts
- › 2.2 Identifying and Mitigating Common Digital Threats
- › 2.3 Creating Strong, Secure Passwords
- › 2.4 Safe Practices for Online Communication

• 3 Recognizing and Responding to Phishing Attacks — 4 classes

- › 3.1 Understanding Phishing: Common Tactics and Techniques
- › 3.2 Identifying Phishing Emails: Key Signs and Red Flags
- › 3.3 Analyzing Real-Life Phishing Scenarios: What Went Wrong?
- › 3.4 Responding to Phishing Attempts: Best Practices and Tools

4

Phishing Awareness and Prevention

3 chapters · 12 classes

65 marks

• 1 Understanding Phishing: Types and Techniques — 4 classes

- › 1.1 Exploring the Basics: What is Phishing?
- › 1.2 Identifying Common Phishing Techniques
- › 1.3 Analyzing Real-World Phishing Examples
- › 1.4 Practicing Prevention: How to Protect Yourself

• 2 Recognizing Phishing Attempts: Indicators and Red Flags — 4 classes

- › 2.1 Identifying Common Phishing Techniques
- › 2.2 Analyzing Email Content for Red Flags
- › 2.3 Exploring Websites for Phishing Indicators
- › 2.4 Applying Knowledge to Prevent Phishing Breaches

• 3 Preventive Measures and Response Strategies — 4 classes

- › 3.1 Understanding Phishing Threats and Their Impact
- › 3.2 Identifying Common Phishing Techniques
- › 3.3 Implementing Preventive Measures Against Phishing
- › 3.4 Responding Effectively to Phishing Incidents

5

Practical Security Application

3 chapters · 12 classes

90 marks

• 1 Understanding Personal Digital Security Threats — 4 classes

- › 1.1 Identifying Common Digital Security Threats
- › 1.2 Recognizing Characteristics of Phishing Attacks
- › 1.3 Evaluating Risk Levels of Digital Interactions
- › 1.4 Implementing Basic Personal Security Measures

• 2 Identifying and Mitigating Phishing Attacks — 4 classes

- › 2.1 Understanding the Anatomy of a Phishing Attack
- › 2.2 Recognizing Common Phishing Tactics
- › 2.3 Analyzing Real-World Phishing Examples
- › 2.4 Applying Techniques to Safeguard Personal Information

• 3 Applying Practical Security Tools and Best Practices — 4 classes

- › 3.1 Understanding Digital Security Essentials
- › 3.2 Identifying and Avoiding Phishing Attacks
- › 3.3 Implementing Password Protection Strategies
- › 3.4 Utilizing Security Tools in Everyday Situations

6

Understanding Digital Threats

3 chapters · 12 classes

65 marks

• 1 Identifying Common Digital Threats and Vulnerabilities — 4 classes

- › 1.1 Recognizing Common Digital Threats
- › 1.2 Identifying Vulnerabilities in Digital Systems
- › 1.3 Understanding Phishing Techniques
- › 1.4 Analyzing Real-life Threat Scenarios

• 2 Techniques and Tools Used by Cybercriminals — 4 classes

- › 2.1 Unmasking Phishing: Recognize Deceptive Emails and Websites
- › 2.2 Decoding Malware: Identify Malicious Software Threats
- › 2.3 Protecting Your Data: Understand the Methods of Data Breach
- › 2.4 Counteracting Cyber Threats: Employ Tools for Digital Protection

• 3 Strategies for Mitigating Digital Threats — 4 classes

- › 3.1 Identifying Common Digital Threats
- › 3.2 Evaluating Risks in Digital Environments
- › 3.3 Implementing Security Measures Against Threats
- › 3.4 Practicing Safe Digital Behaviors

