



484-P25-CE



In-Class



16 hours

Course Description:

In this course participants will learn how to investigate, detect, and prevent fraud in different fields of electronic payments such as cards, ATM's, e-commerce, none face to face transactions and mobile payment, in addition knowing the latest fraud techniques with practical cases in Egyptian market.

Target Audience:

This program targets customer service employees, tellers, ATM supervisors, card operations center, merchant departments, legal departments, and operation risk departments.

Course Objectives:

- List the Types of Transactions and Electronic Payments Fraud.
- Describe the Latest Fraud trends in ATMs.
- Identify the Latest Fraud Trends against Merchants.
- Identify the Virtual Market as a Future Market.
- Describe Mobile Wallet Payments Potential Threats and Vulnerabilities.
- Explain Security and Vulnerabilities of Online Banking System.

Course Outline

Module 1: Types of Transactions and Electronic Payments Fraud

- Introduction to electronic payment.
- Payment system parties and type of transactions.
- Fraud concept.
- Who presents fraud?
- Fraud in cards and its types.
- Chip transaction and transaction flow.
- Near-term solutions to address the growing threat of card-not-present fraud.
- Case studies.

Module 2: Latest Fraud trends in ATMs

- ATM anatomy, life cycle and the electronic payment /application which included.
- EMV chip technology as a defense from skimming.
- ATM fraud control parameters for Issuers.
- ATM fraud investigation and how to protect your bank against ATM fraud attack.

Module 3: Latest Fraud Trends against Merchants

- Different types of merchant's fraud.
- Fraud in P.O.S. & Fraudulent Activity: recognizing common fraudulent schemes.
- Understanding E-Commerce Risk Exposures.
- Minimizing merchant fraud.

Module 4: Virtual Market as a Future Market

- Social engineering fraud and digital banking fraud.
- The most important regulation from CBE for dealing with aggregators in mobile wallet.
- Applicable policies to mitigate electronic payment fraud.

Module 5: Mobile Wallet Payments Potential Threats and Vulnerabilities

- Mobile Wallet Application Users Threats.
- Mobile Devices Threats.
- Mobile Wallet Applications Threats.
- Merchants Threats.
- Payment Service Providers Threats.
- Acquirers Threats.
- Payment Network Providers Threats.
- Card Issuers Threats.
- Tokenization fraud scenarios and solutions:
 - Understanding payment tokens and provisioning cards.
 - Threats in tokenization and fraud scenarios.
 - Token processing mechanisms and vulnerabilities.



484-P25-CE



In-Class



16 hours

Module 6: Security and Vulnerabilities of Online Banking System

- Online banking system mechanism.
- The Security Models and Measures.
- Biometric authentication technology.
- The nature of the attack techniques.
- Types of Online Attacks:
 - Trojan attacks.
 - Phishing attacks.
 - Brute force.
 - Back doors or trap doors.

Assessment Strategy:

Participants will be informally assessed on their interaction during sessions and their participation in group exercises.

Upon Successful Completion of this Course, participants will obtain:

1.3 CEUs.

Course Language:

English.

Prerequisites:

Intermediate level of English Language.