SECURITY AWARENESS: PROTECTING ATM OPERATIONS AND FINANCIAL DATA FROM MODERN SECURITY THREATS



GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats Training Course prepares banking and ATM operations staff to recognise, resist and report the threats that target cash machines and financial data. Participants learn how criminals attack terminals physically and digitally, and how staff behaviour determines whether an attack succeeds. The programme covers social engineering, skimming and shimming, jackpotting, malware and ransomware, payment card fraud, phishing and insider risk. Furthermore, it addresses data protection duties, incident reporting and everyday security habits. As a result, delegates act as a working layer of defence around ATM estates and customer data. Gentex Training Center delivers the programme through scenario workshops and applied case work.

Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats Course Objectives

- Identify the main physical and digital threats to ATM operations.
- Recognise social engineering and pretexting attempts in daily work.
- Detect skimming, shimming and terminal tampering indicators.
- Explain jackpotting, malware and ransomware attack methods.
- Apply card fraud prevention and data handling rules at the terminal.
- Recognise phishing, smishing and business email compromise attempts.
- Apply data protection and confidentiality duties to customer information.
- Follow incident reporting, escalation and evidence preservation procedures.
- Apply password, device and remote access security practices.
- Apply insider risk awareness and third-party access controls.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Course Methodology

The course combines awareness briefings with scenario workshops, walkthrough exercises and applied case studies. Participants review real attack patterns, inspect a terminal tamper checklist and work through an incident escalation scenario. In addition, group discussion and peer review reinforce habits, and each day closes with a practical security exercise.

Who Should Take This Course

- ATM operations, cash replenishment and field service staff.
- Branch, teller and customer service employees.
- Bank security, fraud prevention and risk officers.
- IT support and helpdesk staff serving banking operations.
- Cash-in-transit and third-party service provider personnel.
- Team leaders and supervisors responsible for site security.

Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats Course Outlines

Day 1: Understanding the Modern Threat Landscape

- Who targets financial institutions and why.
- Physical attack types facing ATM estates.
- Digital attack types: malware, ransomware and network intrusion.
- Organised crime, fraud rings and insider threat patterns.
- Regulatory expectations for security awareness and training.

- The cost of an incident: cash loss, data loss and reputation damage.
- Workshop: mapping threats against a sample ATM estate.

Day 2: Social Engineering and Human Risk

- Social engineering principles: authority, urgency and familiarity.
- Pretexting calls, fake engineers and impersonation attacks.
- Tailgating, shoulder surfing and physical access trickery.
- Verifying identity before granting access or information.
- Handling pressure, unusual requests and escalation attempts.
- Building a challenge culture without blocking legitimate work.
- Workshop: working through social engineering scenarios and responses.

Day 3: ATM Physical Security and Fraud Techniques

- Skimming devices, card trapping and cash trapping.
- Shimming on chip card readers and detection methods.
- Terminal inspection routines and tamper evidence checks.
- Jackpotting and black box attacks on dispensers.
- Cash replenishment security and route awareness.
- Reporting suspicious activity and preserving the scene.
- Workshop: running a terminal tamper inspection checklist.

Day 4: Digital Threats, Data Protection and Safe Habits

- Phishing, smishing, vishing and business email compromise.
- Malware delivery routes and unsafe device behaviour.
- Password, multi-factor authentication and remote access discipline.

- USB devices, personal equipment and unauthorised software.
- Payment card data handling and confidentiality duties.
- Data protection principles applied to customer records.
- Workshop: identifying phishing attempts and unsafe practices.

Day 5: Incident Response, Reporting and Security Culture

- Recognising and reporting a security incident quickly.
- Escalation routes and who to contact at each stage.
- Evidence preservation and incident documentation.
- Supporting investigations and post-incident reviews.
- Learning from near misses and security lessons shared.
- Building everyday security habits into daily routine.
- Workshop: presenting an incident report and lessons learned.

Conclusion

By successfully completing Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats Training Course, participants will have acquired the knowledge to recognise physical and digital threats before they cause loss. They will understand social engineering, skimming and terminal tampering, jackpotting and malware, phishing and data protection duties, incident reporting and escalation, and everyday security practice. As a result, delegates reduce fraud losses and protect customer trust. Gentex Training Center builds the programme around current threat patterns and operational practice.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

FAQs for the Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats course

Q1 What is the "Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats" course about?

It builds awareness of the threats facing ATM operations and financial data. You learn social engineering, skimming, shimming and jackpotting, malware and phishing, card data handling, incident reporting and the daily security habits that prevent loss.

Q2 What are the key benefits of the "Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats" course?

You gain the ability to spot an attack in progress rather than discovering it afterwards. You also reduce cash and data losses, respond faster to incidents with clear escalation, meet awareness training obligations, and strengthen a security culture across branches and field teams.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q3 What skills will I gain from the "Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats" course?

You will gain ATM threat recognition and physical tamper detection, social engineering awareness and verification practice, phishing and malware recognition with safe device habits, and incident reporting, escalation and payment data protection.

Q4 What tools, methods, or standards are covered in the "Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats" course?

The course covers skimming and shimming detection methods, card trapping and cash trapping indicators, jackpotting and black box attack patterns, terminal tamper inspection checklists, cash replenishment security routines, social engineering pretexting techniques, phishing, smishing, vishing and business email compromise recognition, malware and ransomware delivery routes, password and multi-factor authentication discipline, USB and unauthorised software policy, payment card data handling and confidentiality rules, data protection principles for customer records, incident escalation routes, evidence preservation practice, and near-miss review.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q5 How is the "Security Awareness: Protecting ATM Operations and Financial Data from Modern Security Threats" course applied in real-world practice?

Graduates apply it to inspect terminals for tampering during routine visits, verify identity before granting access or sharing information, challenge unusual requests politely, recognise and report phishing attempts, handle card and customer data carefully, escalate suspected incidents promptly, preserve evidence for investigation, and contribute lessons learned to team briefings.