Anti-Phishing Strategies for Banks Training Course

Professional Development Training Course Outline

Category	Banking Institute	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Financial institutions are prime targets for phishing attacks, business email compromise (BEC), credential theft, social engineering, ransomware, AI-powered phishing, QR code phishing (quishing), deepfake fraud, mobile banking attacks, and account takeover (ATO). As digital banking, cloud computing, fintech integration, and remote work continue to expand, cybercriminals are leveraging artificial intelligence (AI), machine learning, automated phishing kits, and sophisticated malware to bypass traditional security controls. Banks must implement zero trust security, phishing-resistant authentication, advanced email security, threat intelligence, cyber resilience, fraud detection, and employee awareness programs to protect customer information, financial assets, and regulatory compliance. A comprehensive anti-phishing strategy strengthens organizational resilience while minimizing operational, financial, and reputational risks.

Anti-Phishing Strategies for Banks Training Course equips banking professionals with practical knowledge, industry best practices, and globally recognized cybersecurity frameworks to identify, prevent, detect, respond to, and recover from phishing attacks. Participants will explore AI-driven threat detection, security awareness, digital identity protection, multifactor authentication (MFA), behavioral analytics, Security Operations Center (SOC) practices, incident response, cloud security, regulatory compliance, cyber risk management, and continuous security monitoring. Through real-world banking case studies, phishing simulations, and interactive exercises, learners will develop the expertise required to build a proactive cybersecurity culture and defend against emerging phishing threats.

Programme Curriculum

Anti-Phishing Strategies for Banks Training Course

Introduction

Financial institutions are prime targets for phishing attacks, business email compromise (BEC), credential theft, social engineering, ransomware, AI-powered phishing, QR code phishing (quishing), deepfake fraud, mobile

banking attacks, and account takeover (ATO). As digital banking, cloud computing, fintech integration, and remote work continue to expand, cybercriminals are leveraging artificial intelligence (AI), machine learning, automated phishing kits, and sophisticated malware to bypass traditional security controls. Banks must implement zero trust security, phishing-resistant authentication, advanced email security, threat intelligence, cyber resilience, fraud detection, and employee awareness programs to protect customer information, financial assets, and regulatory compliance. A comprehensive anti-phishing strategy strengthens organizational resilience while minimizing operational, financial, and reputational risks.

Anti-Phishing Strategies for Banks Training Course equips banking professionals with practical knowledge, industry best practices, and globally recognized cybersecurity frameworks to identify, prevent, detect, respond to, and recover from phishing attacks. Participants will explore AI-driven threat detection, security awareness, digital identity protection, multifactor authentication (MFA), behavioral analytics, Security Operations Center (SOC) practices, incident response, cloud security, regulatory compliance, cyber risk management, and continuous security monitoring. Through real-world banking case studies, phishing simulations, and interactive exercises, learners will develop the expertise required to build a proactive cybersecurity culture and defend against emerging phishing threats.

Course Duration

5 days

Course Objectives

By the end of this training, participants will be able to:

1. Understand the latest AI-powered phishing threats targeting financial institutions.
2. Identify social engineering techniques used by cybercriminals.
3. Implement Zero Trust Security Architecture to reduce phishing risks.
4. Strengthen Email Security Gateway (SEG) controls and secure communications.
5. Deploy Multi-Factor Authentication (MFA) and Phishing-Resistant Authentication.
6. Detect Business Email Compromise (BEC) and CEO fraud attacks.
7. Protect digital banking platforms against Credential Theft and Account Takeover (ATO).
8. Utilize Threat Intelligence for proactive phishing detection.
9. Improve Security Awareness Training using phishing simulations.
10. Develop effective Incident Response and Cyber Resilience strategies.
11. Ensure compliance with ISO 27001, NIST CSF, PCI DSS, SWIFT CSP, and GDPR security requirements.
12. Apply Behavioral Analytics and AI-based Fraud Detection for early threat identification.
13. Design a comprehensive Enterprise Anti-Phishing Framework for banking institutions.

Target Audience

- Chief Information Security Officers (CISOs)
- Information Security Managers
- Banking Risk and Compliance Officers
- IT Security Administrators
- Security Operations Center (SOC) Analysts
- Fraud Prevention and Financial Crime Teams
- Internal Auditors and Cyber Risk Professionals
- Digital Banking, FinTech, and Technology Managers

Course Modules

Module 1: Phishing Threat Landscape in Banking

- Evolution of phishing attacks in financial services
- AI-generated phishing and deepfake scams
- Banking malware and credential harvesting
- Attack lifecycle and cyber kill chain
- Global phishing trends affecting banks
- **Case Study:** Analysis of a major banking phishing campaign leading to customer credential theft.

Module 2: Social Engineering and Human Risk Management

- Psychology behind phishing attacks
- Spear phishing and whaling attacks
- Business Email Compromise (BEC)
- Voice phishing (Vishing) and SMS phishing (Smishing)
- Security awareness best practices
- **Case Study:** CEO impersonation attack resulting in fraudulent wire transfers.

Module 3: Advanced Email Security and Authentication

- Secure Email Gateway (SEG)
- SPF, DKIM, and DMARC implementation
- Anti-spoofing technologies
- Secure email encryption
- Email threat detection platforms
- **Case Study:** Preventing domain spoofing using DMARC implementation.

Module 4: Identity Protection and Zero Trust Security

- Zero Trust Architecture
- Multi-Factor Authentication (MFA)
- Passwordless authentication
- Identity and Access Management (IAM)
- Privileged Access Management (PAM)
- **Case Study:** Preventing account takeover through phishing-resistant MFA.

Module 5: AI-Powered Detection and Threat Intelligence

- Artificial Intelligence in cybersecurity
- Machine learning for phishing detection
- Threat Intelligence Platforms (TIP)
- Behavioral analytics
- Fraud detection technologies
- **Case Study:** AI-based phishing detection preventing large-scale banking fraud.

Module 6: Incident Response and Cyber Resilience

- Phishing incident response lifecycle
- Digital forensics fundamentals
- Threat containment strategies

- Business continuity planning
- Cyber resilience framework
- **Case Study:** Coordinated incident response following a phishing breach.

Module 7: Regulatory Compliance and Governance

- ISO 27001 security controls
- NIST Cybersecurity Framework
- PCI DSS requirements
- SWIFT Customer Security Programme (CSP)
- Regulatory reporting obligations
- **Case Study:** Compliance improvements following regulatory cybersecurity findings.

Module 8: Building an Enterprise Anti-Phishing Program

- Enterprise phishing risk assessment
- Security awareness campaigns
- Phishing simulation exercises
- Continuous monitoring and metrics
- Future trends in banking cybersecurity
- **Case Study:** Developing a bank-wide anti-phishing strategy that reduced phishing success rates and improved security awareness.

Training Methodology

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Online	$1,000
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Online	$1,000
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Online	$1,000
28 Sep 2026	02 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com