Digital Identity Theft and Fraud Investigation Training Course

Professional Development Training Course Outline

Category	Criminology	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's hyper-connected digital world, digital identity theft and cyber fraud have emerged as top threats to personal, corporate, and governmental security. The rise of sophisticated attack vectors such as phishing, social engineering, SIM swapping, and synthetic identity fraud demands a new breed of trained professionals equipped to prevent, investigate, and respond effectively. Training Course on Digital Identity Theft & Fraud Investigation provides learners with practical and cutting-edge knowledge on tracking, analyzing, and mitigating cyber fraud schemes targeting digital identities.

Whether you're a cybersecurity professional, law enforcement officer, IT analyst, or compliance officer, this training will arm you with actionable skills to detect anomalies, trace fraudulent activities, conduct investigations using forensic tools, and collaborate across sectors to secure digital ecosystems. With hands-on case studies, real-time threat analysis, and compliance frameworks, this course is your key to mastering digital identity protection in an evolving threat landscape.

Programme Curriculum

Digital Identity Theft and Fraud Investigation Training Course

Introduction

In today's hyper-connected digital world, digital identity theft and cyber fraud have emerged as top threats to personal, corporate, and governmental security. The rise of sophisticated attack vectors such as phishing, social engineering, SIM swapping, and synthetic identity fraud demands a new breed of trained professionals equipped to prevent, investigate, and respond effectively. Digital Identity Theft and Fraud Investigation Training Course provides learners with practical and cutting-edge knowledge on tracking, analyzing, and mitigating cyber fraud schemes targeting digital identities.

Whether you're a cybersecurity professional, law enforcement officer, IT analyst, or compliance officer, this training will arm you with actionable skills to detect anomalies, trace fraudulent activities, conduct investigations using forensic tools, and collaborate across sectors to secure digital ecosystems. With hands-on case studies, real-time threat analysis, and compliance frameworks, this course is your key to mastering digital identity protection in an evolving threat landscape.

Course Objectives

1. Understand the fundamentals of digital identity ecosystems and vulnerabilities.
2. Investigate identity theft tactics used in cybercrime.
3. Detect and prevent account takeover fraud (ATO).
4. Apply cyber forensic techniques in fraud investigations.
5. Analyze behavioral biometrics and digital footprint tracking.
6. Learn how to combat synthetic identity fraud.
7. Explore financial fraud trends in online banking and e-commerce.
8. Master tools for digital forensics and evidence gathering.
9. Implement real-time fraud detection systems.
10. Understand the legal and regulatory aspects of cyber fraud.
11. Respond to identity breaches with incident response frameworks.
12. Collaborate across institutions for fraud intelligence sharing.
13. Develop enterprise-wide identity security strategies.

Target Audiences

1. Cybersecurity professionals
2. Digital forensic investigators
3. Fraud detection analysts
4. Banking and fintech security teams
5. Law enforcement and intelligence officers
6. Risk management and compliance officers
7. IT and network security managers
8. Legal and regulatory enforcement teams

Course Duration: 10 days

Course Modules

Module 1: Introduction to Digital Identity Theft

- Overview of digital identity components
- Common vectors for identity theft
- Threat actors and motives
- Global trends and statistics
- Regulatory frameworks overview
- **Case Study:** The 2023 Experian identity breach

Module 2: Account Takeover (ATO) Fraud

- Definition and anatomy of ATO
- Credential stuffing and brute-force attacks
- Detection through user behavior analytics
- Tools to prevent ATO
- Real-time monitoring solutions
- **Case Study:** Twitter celebrity account hack

Module 3: Synthetic Identity Fraud

- What is synthetic identity fraud?
- Common creation tactics (SSN fraud, DOB mismatches)
- Impact on financial institutions
- Machine learning for detection
- Authentication measures
- **Case Study:** U.S. credit union synthetic ID scam

Module 4: Social Engineering & Phishing

- Tactics in social engineering
- Phishing, smishing, vishing methods
- Email spoofing detection
- Employee training & awareness
- Phishing simulation tools
- **Case Study:** Business email compromise (BEC) in Africa

Module 5: SIM Swapping & Mobile Fraud

- How SIM swap attacks work
- Telecom vulnerabilities
- Impact on two-factor authentication
- Prevention through multi-layered security
- Role of mobile carriers in fraud prevention
- **Case Study:** Cryptocurrency theft via SIM swap

Module 6: Behavioral Biometrics in Fraud Detection

- What is behavioral biometrics?
- Typing patterns and mouse movement tracking
- AI/ML for behavior profiling
- Use in fraud risk scoring
- Challenges and ethical concerns
- **Case Study:** Behavioral detection in online banking fraud

Module 7: Digital Forensics Tools & Techniques

- Basics of cyber forensics
- Tools: EnCase, FTK, Autopsy, Volatility
- Evidence collection and chain of custody
- Recovering deleted data
- Report writing and court admissibility
- **Case Study:** Forensic analysis of identity theft ring

Module 8: Financial Fraud & Digital Identity

- Online banking and fintech fraud
- Card-not-present (CNP) fraud
- Real-time transaction monitoring
- AML/KYC compliance
- Fraud triangulation techniques
- **Case Study:** PayPal fraud and digital laundering case

Module 9: Identity Verification & Authentication Systems

- 2FA, MFA, and biometrics
- Passwordless authentication

- Document verification technologies
- Liveness detection
- Fraud-resistant onboarding
- **Case Study:** Fake passport ID fraud on an e-wallet

Module 10: Cloud Identity Security

- Identity management in cloud environments
- Access control protocols (SAML, OAuth, OpenID)
- Risks in cloud-based identity systems
- Best practices in IAM deployment
- Zero Trust architecture
- **Case Study:** AWS IAM misconfiguration breach

Module 11: Cyber Threat Intelligence in Identity Fraud

- Role of CTI in fraud prevention
- Dark web monitoring for stolen identities
- Indicators of compromise (IoCs)
- Sharing intelligence across sectors
- CTI platforms and tools
- **Case Study:** Identity data sold on the dark web

Module 12: Incident Response for Identity Breaches

- Steps in breach response
- Communication and notification strategies
- Forensics during incident response
- Coordinating with legal & PR teams
- Post-incident auditing
- **Case Study:** Marriott hotel identity breach

Module 13: Legal & Regulatory Compliance

- GDPR, CCPA, and international privacy laws
- Cybercrime laws by region
- Responsibilities in handling identity data
- Compliance risk assessments
- Reporting requirements and penalties
- **Case Study:** Equifax settlement case

Module 14: Cross-Sector Collaboration

- Public-private partnerships
- Information sharing protocols
- National CERTs and ISACs
- Industry-specific threat briefings
- Collaborative simulation exercises
- **Case Study:** FBI and fintech joint fraud sting

Module 15: Building Enterprise Identity Fraud Defense

- Creating fraud prevention policies
- Training employees at all levels
- Monitoring and auditing processes
- Risk-based authentication strategies

- Incident playbooks and simulations
- **Case Study:** A bank's internal fraud prevention overhaul

Training Methodology

- Interactive instructor-led virtual or in-person sessions
- Real-world simulations and use-case-based learning
- Hands-on lab exercises with forensic tools
- Peer-reviewed assessments and scenario evaluations
- Group-based fraud investigation assignments
- Access to online resource library and fraud detection toolkits

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

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

Register Online Now

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