Online Fraud Investigation Techniques 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 economy, online fraud is evolving faster than ever. From phishing scams and identity theft to cryptocurrency fraud, cybercriminals use sophisticated techniques to exploit digital vulnerabilities. As a result, the demand for skilled professionals in cyber fraud detection, digital forensics, and fraud analytics has never been higher. Training Course on Online Fraud Investigation Techniques provides an in-depth understanding of online fraud investigation techniques, equipping law enforcement professionals, cybersecurity experts, and compliance officers with the tools necessary to mitigate and investigate online threats effectively.

Participants will gain practical knowledge of the investigative process, understand data trail mapping, and utilize open-source intelligence (OSINT) tools, dark web monitoring, and blockchain analysis. Whether you’re conducting investigations in a corporate, legal, or government setting, this course will empower you with real-world case studies, evidence-gathering strategies, and advanced technology integration to combat online fraud head-on.

Programme Curriculum

Online Fraud Investigation Techniques Training Course

Introduction

In today’s hyper-connected digital economy, online fraud is evolving faster than ever. From phishing scams and identity theft to cryptocurrency fraud, cybercriminals use sophisticated techniques to exploit digital vulnerabilities. As a result, the demand for skilled professionals in cyber fraud detection, digital forensics, and fraud analytics has never been higher. Online Fraud Investigation Techniques Training Course provides an in-depth understanding of online fraud

investigation techniques, equipping law enforcement professionals, cybersecurity experts, and compliance officers with the tools necessary to mitigate and investigate online threats effectively.

Participants will gain practical knowledge of the investigative process, understand data trail mapping, and utilize open-source intelligence (OSINT) tools, dark web monitoring, and blockchain analysis. Whether you're conducting investigations in a corporate, legal, or government setting, this course will empower you with real-world case studies, evidence-gathering strategies, and advanced technology integration to combat online fraud head-on.

Course Objectives

1. Understand core principles of online fraud investigation.
2. Identify different types of cyber fraud schemes and patterns.
3. Master the use of digital forensics tools for evidence extraction.
4. Analyze financial trails using blockchain analytics.
5. Apply OSINT techniques for digital footprint tracing.
6. Conduct professional email header analysis for fraud detection.
7. Learn to track IP addresses and geolocate digital suspects.
8. Explore dark web markets for identifying fraud-related content.
9. Use threat intelligence platforms to assess cyber threats.
10. Learn social engineering detection techniques.
11. Understand legal frameworks surrounding cybercrime investigations.
12. Develop incident response strategies for fraud mitigation.
13. Build cross-border cooperation strategies for international fraud cases.

Target Audiences

1. Cybercrime investigators
2. Law enforcement officers
3. IT security professionals
4. Financial crime analysts
5. Compliance and risk managers
6. Digital forensics specialists
7. Fraud prevention teams
8. Legal and regulatory authorities

Course Duration: 10 days

Course Modules

Module 1: Introduction to Online Fraud

- Definition and evolution of online fraud
- Common fraud schemes: phishing, vishing, spoofing
- Economic and social impact of fraud
- Cyber fraud vs traditional fraud: Key differences

- Overview of global fraud statistics
- **Case Study: The 2020 Twitter Bitcoin Scam**

Module 2: Fundamentals of Digital Forensics

- Types of digital evidence
- Chain of custody in digital environments
- Disk imaging and memory capture
- Metadata analysis techniques
- Using forensic software (FTK, Autopsy)
- **Case Study: Corporate Data Breach and Evidence Collection**

Module 3: Open-Source Intelligence (OSINT)

- Introduction to OSINT
- OSINT tools: Maltego, Shodan, Spiderfoot
- Techniques for social media intelligence
- Monitoring paste sites and forums
- Legal/ethical implications of OSINT
- **Case Study: Tracking a Romance Scam via OSINT**

Module 4: Email Header and IP Analysis

- Anatomy of an email header
- Identifying forged email addresses
- Tracing IP addresses and server logs
- Understanding SMTP relay exploits
- Using tools like MXToolbox and MailXaminer
- **Case Study: Phishing Attack Investigation**

Module 5: Identity Theft and Synthetic Identities

- Understanding synthetic identity fraud
- Cloning and impersonation methods
- Techniques to detect fake identities
- Document verification systems
- Role of biometric authentication
- **Case Study: E-commerce Platform Identity Theft Case**

Module 6: Financial Fraud and Money Laundering

- Basics of money laundering online
- Transaction monitoring tools
- Red flags in financial fraud
- Know Your Customer (KYC) compliance
- Cryptocurrency laundering tactics
- **Case Study: Crypto Exchange Laundering Scheme**

Module 7: Blockchain and Cryptocurrency Investigations

- Blockchain architecture overview
- Crypto wallet tracing
- Smart contract vulnerabilities
- Tools: Chainalysis, CipherTrace
- Understanding mixer/tumbler services
- **Case Study: Tracing Bitcoin in a Ransomware Case**

Module 8: Dark Web Investigations

- Understanding Tor and I2P networks
- Darknet marketplaces and vendors
- Dark web monitoring tools
- Risks and limitations of undercover work
- Evidence collection from hidden services
- **Case Study: Dark Web Credit Card Ring**

Module 9: Social Engineering and Human Factors

- Psychology behind social engineering
- Types: baiting, pretexting, tailgating
- Phishing simulation tools
- Employee training programs
- Social engineering in business email compromise
- **Case Study: CEO Fraud via Social Engineering**

Module 10: Cyber Law and Legal Frameworks

- Overview of cybercrime laws
- GDPR, CCPA, and digital rights
- International law enforcement cooperation
- Legal standards for evidence admissibility
- Ethics in cyber investigations
- **Case Study: Legal Dispute Over Email Evidence**

Module 11: Cyber Threat Intelligence (CTI)

- Basics of CTI and its application
- Tools: AlienVault, ThreatConnect, MISP
- Indicators of compromise (IOCs)
- Threat actor profiling
- Integration with SIEM systems
- **Case Study: Preventing Bank Fraud with CTI**

Module 12: Mobile Device Forensics

- Mobile data acquisition methods

- Encrypted app investigation
- Deleted data recovery
- Geo-location tracking
- Bypassing screen locks ethically
- **Case Study: Mobile App Fraud in Loan Application**

Module 13: Cloud and SaaS Fraud

- Cloud security basics
- SaaS and API vulnerabilities
- Cloud log analysis
- Identity federation exploits
- Shared responsibility model
- **Case Study: SaaS Subscription Fraud Detection**

Module 14: Incident Response Planning

- Developing a cyber incident response plan
- Roles and responsibilities in a crisis
- Communication during incidents
- Evidence preservation under pressure
- Integrating fraud detection tools
- **Case Study: Financial Institution Fraud Response Drill**

Module 15: Cross-Border Investigations and Cooperation

- Challenges in international investigations
- MLAT and Interpol cooperation
- Cyber jurisdiction issues
- Data sharing and privacy laws
- Building an international task force
- **Case Study: Global eCommerce Fraud Investigation**

Training Methodology

- Interactive lectures with industry experts
- Hands-on labs using real tools and simulated fraud environments
- Case study analysis to apply theory to practice
- Quizzes and assessments to test knowledge retention
- Group discussions for knowledge exchange
- Access to online resources and toolkits post-training

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
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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