Training Course on Responding to Business Email Compromise (BEC) Attacks

Professional Development Training Course Outline

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

Course Introduction

Business Email Compromise (BEC) is one of the most financially damaging cyber threats targeting modern organizations. In this age of digital transformation, attackers exploit human vulnerabilities and misconfigured systems through sophisticated phishing, spoofing, and social engineering tactics. Training Course on Responding to Business Email Compromise (BEC) Attacks equips IT security professionals, executives, and staff with practical skills and robust strategies to detect, prevent, and respond to BEC incidents in real-time.

With the rise in spear-phishing and CEO fraud schemes, it's vital to have a strategic response plan. Our course blends real-world case studies, cybersecurity awareness, incident response planning, and actionable frameworks to empower teams to combat and recover from BEC threats. Participants will gain hands-on knowledge in email security protocols, behavioral analytics, forensic investigation, and cross-functional communication for business continuity.

Programme Curriculum

Training Course on Responding to Business Email Compromise (BEC) Attacks

Introduction

Business Email Compromise (BEC) is one of the most financially damaging cyber threats targeting modern organizations. In this age of digital transformation, attackers exploit human vulnerabilities and misconfigured systems through sophisticated phishing, spoofing, and social engineering tactics. Training Course on Responding to Business Email Compromise (BEC) Attacks equips IT security professionals, executives, and staff with practical skills and robust strategies to detect, prevent, and respond to BEC incidents in real-time.

With the rise in spear-phishing and CEO fraud schemes, it's vital to have a strategic response plan. Our course blends real-world case studies, cybersecurity awareness, incident response planning, and actionable frameworks to empower teams to combat and recover from BEC threats. Participants will gain hands-on knowledge in email security protocols, behavioral

analytics, forensic investigation, and cross-functional communication for business continuity.

Course Objectives

1. Understand the anatomy of BEC attacks and their impact on organizations.
2. Identify email phishing tactics using advanced threat intelligence.
3. Implement DMARC, SPF, and DKIM for secure email infrastructure.
4. Analyze real-world CEO fraud and invoice scams.
5. Enhance cybersecurity awareness across departments.
6. Design an incident response plan specific to BEC events.
7. Execute digital forensics and email trace-back analysis.
8. Apply AI-based phishing detection tools.
9. Train employees using simulated phishing attacks.
10. Collaborate with law enforcement and cybercrime reporting bodies.
11. Use cloud email security gateways to filter malicious content.
12. Recover compromised systems with cyber resilience frameworks.
13. Establish email security policies and conduct regular audits.

Target Audience

1. IT Security Managers
2. Cybersecurity Analysts
3. Email Administrators
4. Financial Controllers and CFOs
5. Legal and Compliance Officers
6. Small Business Owners
7. HR and Operations Managers
8. Incident Response Teams

Course Duration: 5 days

Course Modules

Module 1: Understanding Business Email Compromise (BEC)

- Definition and types of BEC attacks
- Tactics used by threat actors
- Financial and reputational impacts
- Common targets and threat vectors
- Emerging BEC trends in 2025
- **Case Study:** How a multinational lost $5M through fake vendor invoices

Module 2: Recognizing Email-Based Social Engineering

- Psychology of social engineering
- Red flags and language cues in phishing emails
- Spear-phishing vs. mass phishing
- Deepfake videos and impersonation tactics
- Tools for verifying sender authenticity
- **Case Study:** Executive impersonation leads to wire fraud

Module 3: Securing Email Systems

- Implementing SPF, DKIM, and DMARC
- Email server hardening techniques

- Email encryption and MFA
- Third-party email gateway solutions
- Automated alerts and monitoring tools
- **Case Study:** BEC blocked using email authentication protocols

Module 4: Employee Awareness and Training

- Building a culture of security
- Phishing simulation exercises
- Cybersecurity training programs
- Behavior analytics and reporting mechanisms
- Gamification for employee engagement
- **Case Study:** Mid-size firm reduces phishing click rate by 75%

Module 5: Incident Response to BEC

- Identifying and containing the breach
- Communicating with stakeholders and regulators
- Legal and compliance considerations
- Evidence preservation and analysis
- Coordinating with law enforcement and FBI
- **Case Study:** Successful recovery through timely incident response

Module 6: Email Forensics and Investigation

- Email header analysis
- Tracing IP origins and spoofed domains
- Preserving chain of custody
- Using forensic tools like EnCase and FTK
- Correlating with SIEM and logs
- **Case Study:** Tracking stolen funds via email analysis

Module 7: Recovery and Mitigation Strategies

- Post-incident audit and review
- Restoring trust and operational continuity
- Revising policies and protocols
- Insurance and risk transfer options
- Long-term monitoring plans
- **Case Study:** Organization rebounds from BEC with a resilience framework

Module 8: Building a Proactive Defense Posture

- Email threat intelligence integration
- Zero trust architecture for communication
- Ongoing training and red-teaming
- Business continuity planning
- Annual BEC simulation drills
- **Case Study:** Enterprise achieves zero BEC incidents in 12 months

Training Methodology

- Interactive instructor-led sessions
- Real-world case study breakdowns
- Role-based simulations and red teaming
- Hands-on labs for email analysis

- Assessment quizzes and policy drafts
- Post-training knowledge check and certification

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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