Workforce Phishing Defense and Cyber Safety Training Course

26 – 30 July 2027
Addis Ababa

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Workforce Phishing Defense and Cyber Safety Training Course

Ref: 758_223976 **Date:** 26 – 30 July 2027 **Location:** Addis Ababa **Fees:** 4500 Euro

Overview

Workforce Phishing Defense and Cyber Safety Training Course is a one-week foundation course for employees, team leaders, customer-facing staff, administrative teams, remote workers, and managers who leave with a Workforce Cyber Safety Action Plan. Participants practice phishing recognition, secure email habits, credential protection, safe remote work, incident reporting, and team reinforcement through workplace decisions and scenario analysis. The course turns general cybersecurity awareness into repeatable protective behavior. Agile Leaders Training Center develops workforce phishing defense and cyber safety practice.

Who Should Attend

- Business functions responsible for handling email, shared files, and collaboration messages
- Customer-facing functions responsible for protecting conversations, accounts, and submitted information
- Administrative functions responsible for documents, calendars, payments, and access requests
- Team leadership functions responsible for reinforcing safe digital behavior and reporting routes
- Remote and hybrid functions responsible for connecting to business systems outside managed workplaces

The course assumes participants routinely use workplace devices, accounts, email, or collaboration services, and leaves out security engineering, system administration, penetration testing, and incident investigation.

Departments and Industries

The course supports departments and industries that rely on people to protect accounts, communications, and shared information.

- Operations, administration, finance, and human resources
- Sales, customer service, procurement, and executive support
- Financial services and healthcare
- Retail, hospitality, and transportation
- Education, public services, and digital platforms

Learning Objectives

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

- Apply a message screening method to email, texts, and collaboration requests
- Analyze phishing cues, social engineering pressure, and impersonation attempts
- Use credential, multifactor authentication, update, and device protection practices
- Evaluate links, attachments, QR codes, and information requests before acting
- Apply incident reporting and account-containment steps
- Build a Workforce Cyber Safety Action Plan

Course Agenda

Day 1: Recognize Human-Centered Cyber Risk

- Cybersecurity Awareness Behavior and Decision Map
- Social Engineering Influence and Pressure Cue Checklist
- Phishing Channel and Attack Pathway Matrix
- Business Information Exposure Scenario Canvas
- Pause-Verify-Report Decision Method

Day 2: Inspect Messages and Requests

- Email Sender and Domain Verification Checklist
- Link, Attachment, and QR Code Inspection Routine
- Credential Harvesting Page Warning-Sign Guide
- Executive, Supplier, and Colleague Impersonation Test
- Suspicious Message Classification Worksheet

Day 3: Protect Accounts and Devices

- Strong Password and Password Manager Practice
- Multifactor Authentication Request Validation Guide
- Software Update and Device Protection Checklist
- Shared Data and Collaboration Permission Review
- Mobile and Removable Media Handling Rules

Day 4: Work and Report Safely

- Remote Connection and Public Network Safety Check
- Voice, Video, and Messaging Verification Protocol
- Phishing Incident Reporting Route Map
- Compromised Account First-Response Card
- Team Reinforcement and Learning Feedback Plan

Day 5: Practice Cyber Safety Decisions

- Exercise: Screen a Suspicious Email and Link
- Exercise: Challenge an Impersonation and Payment Request
- Exercise: Secure an Account and Remote Work Session
- Exercise: Report a Phishing Event and Reinforce the Lesson
- Capstone: Workforce Cyber Safety Action Plan

Practical Exercises

The course uses suggested activities based on healthcare, financial services, retail, hospitality, and education.

- Suggested activity: compare legitimate and deceptive messages using sender, context, urgency, link, attachment, and request cues.
- Suggested activity: respond to a supplier impersonation scenario without exposing credentials, payment data, or shared files.
- Suggested activity: apply account protection and remote-work checks to a realistic workday.
- Suggested activity: draft a reporting route and team reinforcement action for a phishing event.

FAQs

Who suits workforce phishing defense training, and what does it assume?

Employees, team leaders, customer-facing staff, administrators, remote workers, and managers suit the course; it assumes routine use of workplace accounts, devices, messages, or collaboration services.

How does workforce phishing defense differ from technical cybersecurity training?

Workforce phishing defense develops everyday recognition, verification, protection, and reporting behavior, while technical cybersecurity training focuses on configuring, monitoring, testing, or investigating security technologies.

What warning signs support phishing recognition?

Phishing recognition uses mismatched sender details, unusual context, pressure, secrecy, unexpected links or attachments, credential requests, payment changes, and requests that bypass normal verification routes.

How should employees report suspected phishing?

Employees should stop interaction, preserve the message, use the approved reporting route, provide relevant context, follow account-containment guidance, and avoid forwarding harmful content through ordinary channels.

How can teams reinforce cyber safety after training?

Teams can reinforce cyber safety through short scenario discussions, visible reporting routes, manager modeling, timely feedback, recurring reminders, and review of decisions without blaming the person who reported a concern.

Conclusion

Participants take back a Workforce Cyber Safety Action Plan connecting message checks, account protection, safe remote work, incident reporting, and team reinforcement. It changes vague awareness into clear choices people can repeat during everyday work. The plan supports consistent verification, faster reporting, safer handling of information, and practical learning from suspicious events.