



Cyber Hygiene and Safe Digital Behavior Training Course

14 – 18 March 2027
Nairobi

Cyber Hygiene and Safe Digital Behavior Training Course

Ref: 761_157925 **Date:** 14 – 18 March 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Cyber Hygiene and Safe Digital Behavior Training Course is a five-day foundation course for employees, contractors, supervisors, and nontechnical digital users who leave with a Workplace Cyber Hygiene Action Plan. Participants build repeatable habits for protecting accounts, devices, communications, and data while recognizing suspicious activity and reporting it promptly. The course uses decision cards, checklists, and workplace scenarios instead of technical administration. Agile Leaders Training Center develops cyber hygiene and safe digital behavior practice.

Who Should Attend

- Workforce functions responsible for handling accounts, messages, files, and shared systems
- Supervisory functions responsible for reinforcing safe digital routines
- Remote and hybrid work functions responsible for secure access and communications
- Customer-facing functions responsible for protecting information during service delivery
- Contractor and partner functions responsible for using organizational digital resources

The course assumes participants use workplace accounts, devices, messaging, or business data, and leaves out penetration testing, security engineering, system administration, and certification preparation.

Departments and Industries

The course supports departments and industries that depend on safe everyday digital behavior.

- Human resources, administration, finance, and customer service
- Healthcare and education
- Financial services and insurance
- Retail, hospitality, and logistics
- Public services and technology-enabled operations

Learning Objectives

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

- Apply a cyber hygiene habit checklist to daily work
- Use stronger account, authentication, and device routines
- Analyze messages and requests for phishing indicators
- Prioritize safe handling of files, data, and communications
- Evaluate remote-work and browsing choices before acting



- Build a Workplace Cyber Hygiene Action Plan

Course Agenda

Day 1: Build Everyday Cyber Hygiene

- Personal Digital Exposure Mapping Worksheet
- Cyber Hygiene Habit Baseline Checklist
- Account and Device Responsibility Matrix
- Human Error and Threat Decision Map
- Safe Digital Behavior Commitment Card

Day 2: Protect Accounts and Devices

- Strong Passphrase and Password Manager Practice
- Multifactor Authentication Decision Guide
- Software Update and Patch Habit Checklist
- Device Lock, Storage, and Disposal Routine
- Lost Device and Account Recovery Action Card

Day 3: Detect Social Engineering

- Phishing Indicator Inspection Method
- Sender, Link, and Attachment Verification Checklist
- Urgency, Authority, and Emotion Trigger Map
- Voice, Message, and QR Deception Decision Tree
- Suspicious Communication Reporting Route

Day 4: Handle Data and Remote Work Safely

- Data Sensitivity and Sharing Decision Card
- Safe Browsing and Download Checklist
- Public Wi-Fi and Remote Access Risk Guide
- Cloud File and Collaboration Permission Review
- Workspace Privacy and Screen Protection Routine

Day 5: Practice Safe Digital Behavior

- Exercise: Diagnose Account and Device Habit Gaps
- Exercise: Evaluate Phishing and Social Engineering Scenarios
- Exercise: Choose Safe Data and Remote-Work Actions
- Exercise: Rehearse Prompt Incident Reporting
- Capstone: Workplace Cyber Hygiene Action Plan

Practical Exercises

The course uses suggested activities based on office, healthcare, retail, education, and remote-work situations.

- Suggested activity: inspect messages, links, attachments, and requests using a phishing decision card.
- Suggested activity: audit account, authentication, update, backup, and device-lock habits.
- Suggested activity: choose safe sharing, browsing, Wi-Fi, and collaboration actions in workplace scenarios.
- Suggested activity: practice reporting a suspicious event with the information responders need.

FAQs

Who suits cyber hygiene training, and what does it assume?

Employees, contractors, supervisors, and nontechnical users suit cyber hygiene training; it assumes routine use of workplace accounts, devices, communications, or data.

How does cyber hygiene training differ from technical cybersecurity training?

Cyber hygiene training develops repeatable user behaviors and decisions, while technical cybersecurity training focuses on configuring, testing, monitoring, or defending systems.

Which cyber hygiene habits reduce everyday account risk?

Cyber hygiene habits include separate passphrases, password-manager use, multifactor authentication, prompt updates, sign-in review, device locking, and immediate reporting of unexpected access requests.

How should safe digital behavior respond to suspicious messages?

Safe digital behavior pauses the request, checks the sender and context through a trusted channel, avoids unknown links or attachments, preserves relevant details, and follows the reporting route.

What belongs in a workplace cyber hygiene action plan?

A workplace cyber hygiene action plan records priority habits, responsible actions, reporting routes, review points, and changes needed for accounts, devices, communications, data, browsing, and remote work.

Conclusion

Participants take back a Workplace Cyber Hygiene Action Plan connecting account protection, device care, phishing decisions, data handling, remote work, and reporting. It changes scattered precautions into visible daily routines. The plan supports safer choices, quicker escalation, shared expectations, and periodic review of behavior gaps.