JUPITER PRIME
Consulting • Training • Advisory
جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Cyber Security Awareness Culture for Managers Training Course

2 – 13 August 2027
Milan

Cyber Security Awareness Culture for Managers Training Course

Ref: 195_5922 **Date:** 2 – 13 August 2027 **Location:** Milan **Fees:** 12400 GBP

Cyber Security Awareness Culture for Managers is a 2-week training course for line managers, HR partners and department heads who shape how staff behave around email, passwords and sensitive files, and it ends with a team awareness campaign blueprint ready to launch. Most breaches still begin with a person clicking, sharing or reusing something they should not, so everyday habits now decide exposure. Jupiter Prime Training offers this course to managers who own that behaviour.

Why Cyber Security Awareness Culture Matters Now

Three pressures meet in this subject: phishing and impersonation scams that now imitate executives and suppliers convincingly, hybrid working that moves sensitive files onto home networks and personal devices, and boards and auditors that ask for evidence that staff behaviour is improving rather than a record of slides watched. An organisation with a strong security culture sees suspicious messages reported within minutes; one without it learns of a fraud weeks later. The course draws on the awareness and competence expectations of ISO/IEC 27001:2022, the international standard for information security management systems.

Who Gains Most from Cyber Security Awareness Culture

- Line managers who set daily expectations for how their teams handle email, files and devices
- HR partners who embed security conduct in induction, appraisal and disciplinary policy
- Department heads who sign off access requests and data sharing with outside parties
- Internal communications leads who shape the tone and timing of security messages
- Awareness coordinators who schedule simulations and report behaviour trends upward

A management layer that sends managers from several departments together gains most, because consistent expectations across functions stop staff hearing conflicting security messages.

Cyber Security Awareness Culture Capabilities

Participants leave able to turn security expectations into habits their staff actually keep and to show that change in numbers.

- Assess the current security culture through surveys, incident reports and simulation results — priorities for the awareness budget
- Design phishing simulations matched to the real lures each department receives — campaign owners and HR
- Specify password, multi-factor and access hygiene rules staff can follow — IT and line managers
- Apply data classification and handling rules to everyday tasks — data owners and compliance leads
- Build behaviour metrics that track reporting rates and repeat clickers — executive sponsors
- Communicate security messages through managers rather than mass email — staff trust and engagement

Key Cyber Security Awareness Culture Terms

- Social engineering — Manipulating people into revealing information or taking unsafe actions, often by posing as a trusted colleague, supplier or authority.
- Phishing simulation — A controlled fake attack email sent to staff to measure who clicks, who reports and where coaching is needed.
- Business email compromise — A fraud in which attackers impersonate an executive or supplier to redirect payments or obtain sensitive files.
- Multi-factor authentication — A sign-in method that requires two or more proofs of identity, such as a password and a phone prompt.
- Report rate — The share of simulated or real suspicious messages that staff report to the security team instead of ignoring.
- Just culture — An approach that treats honest mistakes as learning opportunities while holding deliberate or reckless behaviour to account.

Cyber Security Awareness Culture Day by Day

Day 1: The Human Side of Cyber Risk

- Human Factor in Breach Patterns — Where Staff Behaviour Creates Exposure
- Security Culture Maturity Models — Starting Point for Each Department
- ISO/IEC 27001:2022 Awareness Expectations — Evidence Auditors Will Ask For
- Manager Accountability Map — Who Owns Which Security Habit
- Culture Diagnostic Survey — Baseline Attitudes and Blind Spots

Day 2: Phishing and Social Engineering Tactics

- Phishing Lure Anatomy — Signals Staff Can Spot in Seconds
- Voice and Text Message Scams — Verification Steps Before Acting
- Business Email Compromise Scenarios — Payment Approval Safeguards
- Pretexting and Tailgating Cases — Physical and Reception Controls
- Deepfake Impersonation Risks — Call-Back Rules for Senior Requests

Day 3: Passwords, Identity and Access Hygiene

- Passphrase and Password Manager Policy — Usability Versus Strength
- Multi-Factor Authentication Rollout — Resistance Points and Exceptions
- Joiner, Mover and Leaver Access Reviews — Manager Sign-Off Duties
- Shared Account Elimination — Accountability for Every Login
- Privileged Access Requests — Approval Criteria for Department Heads

Day 4: Handling Sensitive Information Day to Day

- Data Classification Labels — Choices Staff Make When Saving Files
- Secure File Sharing and Email Encryption — External Collaboration Rules
- Clean Desk and Screen Lock Habits — Office and Home Working Exposure
- Removable Media and Personal Cloud Use — Leakage Paths to Close
- Records Disposal and Retention — Paper and Device Destruction Choices

Day 5: Hybrid Working and Device Security

- Home Network and Public Wi-Fi Guidance — Remote Access Conditions
- Bring-Your-Own-Device Agreements — Privacy and Control Trade-Offs
- Software Update and Patch Habits — Staff Responsibilities on Endpoints
- Lost Device Reporting Procedure — Speed of Remote Wipe Decisions
- Collaboration Platform Settings — Guest Access and Link Sharing Limits

Day 6: Behavioural Science for Security Habits

- Nudge Techniques and Defaults — Making the Secure Choice Easiest
- Habit Loops and Reminders — Timing of Security Prompts
- Security Champions Networks — Peer Influence Inside Departments
- Just Culture and Reporting Without Fear — Disciplinary Policy Alignment
- Gamification and Recognition Schemes — Motivation Without Fatigue

Day 7: Designing Phishing Simulations

- Simulation Ethics and Consent Rules — Trust Between Staff and Security
- Difficulty Grading of Templates — Fair Comparison Across Departments
- Landing Page Micro-Learning — Coaching at the Moment of a Click
- Repeat Clicker Support Pathway — Coaching Versus Escalation
- Report Button Adoption — Turning Staff into Early Warning Sensors

Day 8: Measuring Security Behaviour

- Behaviour Metrics Framework — Click, Report and Dwell Indicators
- Awareness Dashboard for Executives — Trends Worth Board Attention
- Incident Root Cause Tagging — Linking Human Error to Coaching
- Pulse Surveys and Focus Groups — Attitude Shift Over Time
- Banking and Healthcare Case Comparisons — Sector Culture Patterns

Day 9: Communicating Security Through Managers

- Message Framing for Different Audiences — Frontline, Office and Executive Staff
- Team Briefing Scripts — Five-Minute Security Moments in Meetings
- Induction Security Module — First-Week Expectations for New Starters
- Incident Story Telling — Lessons Shared Without Blame
- Campaign Calendar Planning — Themes Across the Year

Day 10: Practising the Team Awareness Campaign Blueprint

- Culture Diagnostic Applied to a Live Department — Priority Behaviours
- Simulation Plan Drafting — Templates, Timing and Coaching Steps
- Metrics Selection and Dashboard Mock-Up — Sponsor Reporting Format
- Peer Critique of Campaign Messages — Clarity and Tone Checks
- Team Awareness Campaign Blueprint Completion — Owners, Milestones and Measures

Applying Cyber Security Awareness Culture After the Course

- Run a baseline phishing simulation for one department using the graded templates and coaching pathway practised in the course
- Hold a security moment in each weekly team meeting for a month and track report rates on the behaviour dashboard

Cyber Security Awareness Culture Questions FAQ

What is cyber security awareness culture and why does it matter now?

Cyber security awareness culture is the set of shared habits that lead staff to spot, report and avoid threats without being told each time. It matters now because phishing and impersonation target people first, and hybrid working widens the places mistakes happen.

Which roles gain most from cyber security awareness culture training for managers?

Line managers, HR partners, department heads and awareness coordinators gain most. You benefit if you approve access, set team routines or handle staff conduct, because your daily signals shape security behaviour more than annual e-learning does.

How does cyber security awareness culture training differ from basic staff awareness training?

It prepares managers to lead behaviour change rather than simply teaching staff to spot threats. You design simulations, metrics and messages for others, and learn to link coaching, HR policy and reporting into one sustained effort.

What do you bring back from cyber security awareness culture training?

You bring back a campaign blueprint for your own team. It sets priority behaviours, a simulation schedule, coaching steps, communication themes and the metrics your sponsor will see, so the first activities can start within weeks.

Cyber Security Awareness Culture: The Way Forward

The team awareness campaign blueprint first informs which behaviour to target in the opening quarter and how the first simulation is graded. Line managers run it, HR aligns policy to it and executive sponsors read its dashboard. After the first cycle, revisit the coaching pathway for repeat clickers, since early results show whether support or escalation changes behaviour faster.