
Cyber Awareness Programme Design Training Course: Role Risk, Phishing Simulations and Measurement

19 – 23 September 2027
Zoom





Cyber Awareness Programme Design Training Course: Role Risk, Phishing Simulations and Measurement

Ref: 311_21050 Date: 19 – 23 September 2027 Location: Zoom Fees: 1700 GBP

Programme Summary

Cyber awareness programme design is the subject of this one-week training course for managers and heads of department responsible for staff security behaviour, ending in a cyber awareness programme plan for one organisation or division. Staff actions remain a leading route into incidents, yet awareness effort is often generic and unmeasured. The approach moves from purpose and audiences, through role risk and behaviour diagnosis, to content and simulation design, then to measurement and a worked plan. Mars Training Centre UK delivers this programme in cyber awareness programme design.

The Business Case

Awareness sessions that ignore role risk are quickly forgotten, and results reported as attendance say little about behaviour. Managers who target the roles and habits that create exposure, run realistic simulations and track what staff actually do can show which activities change behaviour and which should stop.

- Phishing Susceptibility: Falls as simulations and feedback focus on the roles and messages that fail most often.
- Incident Reporting Speed: Improves as a clear reporting route and positive feedback encourage staff to raise doubts early.
- Awareness Spend Effectiveness: Improves as measures of behaviour replace measures of attendance.

Principles and Evidence Base

- NIST SP 800-50 Rev. 1: Its guidance on building a cybersecurity and privacy learning programme structures the programme lifecycle work in Sessions 1 and 4.
- Fogg Behavior Model: Its link between motivation, ability and prompts guides the barrier analysis in Session 2 and the design choices in Session 3.
- Kirkpatrick Model: Its levels of reaction, learning, behaviour and results frame the evaluation work in Session 4.

Intended Participants

- Managers accountable for how their teams handle information and respond to suspicious messages.
- Heads of department who sponsor awareness activity and release staff time for it.
- Awareness and learning leads who plan content, channels and calendars.
- Security and risk contacts who supply incident data and set policy messages.

The programme serves banking, healthcare, government services and manufacturing organisations.



Learning Outcomes

1. Participants will be able to segment audiences and prioritise topics by role risk using a profile matrix.
2. Participants will be able to diagnose behaviour barriers from incident data, near misses and a phishing baseline.
3. Participants will be able to construct a phishing simulation brief with feedback and reporting routes.
4. Participants will be able to evaluate awareness activity against behaviour measures rather than attendance.
5. Participants will be able to justify reinforcement rules and escalation guidelines to a security lead.
6. Participants will be able to prioritise a channel and calendar plan within a limited budget.

Programme Structure

Day 1: Cyber Awareness Programme Design: Purpose and Audiences

What must the programme change, and for whom?

- Awareness Programme Charter
- NIST SP 800-50 Rev. 1 Programme Lifecycle
- Audience Segmentation Map
- Learning Needs Statement
- Case Review of Two Sector Incidents Caused by Staff Action

Day 2: Role Risk and Behaviour Diagnosis

Which roles and habits create exposure, and what stops staff acting safely?

- Role Risk Profile Matrix
- Incident and Near-Miss Review
- Phishing Susceptibility Baseline
- Fogg Behavior Model Barrier Analysis
- Policy Comprehension Gap Review

Day 3: Content, Channels and Simulations

What should each audience see, how, and when?

- Role-Based Topic Plan
- Phishing Simulation Design Brief
- Reporting Route and Feedback Loop
- Channel and Calendar Plan
- Manager Briefing Pack



Day 4: Measures, Reinforcement and Reporting

How is behaviour change shown and sustained?

- Behaviour Indicator Set
- Kirkpatrick Model Evaluation Levels
- Simulation Result Interpretation Rules
- Reinforcement and Escalation Guidelines
- Leadership Reporting Template

Day 5: Applying Cyber Awareness Programme Design to One Organisation

Is the programme plan ready for the sponsor and the security lead to approve?

- Applying the Session 1 Segmentation Map to the Chosen Organisation
- Testing the Session 2 Risk Matrix Against Sample Incident Data
- Checking Session 3 Simulation Brief Against the Topic Plan
- Applying the Session 4 Indicator Set to Open Issues
- Completing the Cyber Awareness Programme Plan

Methodology

The programme is built around structured exercises on an anonymised organisation and sample incident and simulation data. Participants profile roles, diagnose barriers, draft simulation briefs and select measures in small teams, then defend their plan before a simulated leadership panel. No technical security background is required.

- Suggested activity: Ranking six roles by exposure using sample incident and phishing data.
- Suggested activity: Drafting a simulation brief and feedback message for a finance team.
- Suggested activity: Replacing five attendance measures with behaviour indicators.

Capstone Output

Each participant completes a cyber awareness programme plan for one organisation or division. It contains a programme charter, a role risk matrix, a topic and channel calendar, a simulation brief, a behaviour indicator set and a reporting template. It is used to brief the sponsor and security lead and to launch the first awareness cycle.



Frequently Asked Questions

Is cyber awareness programme design suitable for managers without a security background?

Yes. Cyber awareness programme design is set at managerial level and assumes responsibility for staff behaviour or awareness activity, not technical security or programming skills.

Which models does cyber awareness programme design rest on?

Cyber awareness programme design rests on NIST SP 800-50 Rev. 1 for the programme lifecycle, the Fogg Behavior Model for barriers and the Kirkpatrick Model for evaluation.

How is the plan from cyber awareness programme design used at work?

You use the plan from cyber awareness programme design to brief your sponsor and security lead, launch the first awareness cycle and report behaviour results.

How does cyber awareness programme design differ from cyber security training for specialists?

Cyber awareness programme design centres on staff behaviour, role risk and measurement, while specialist cyber security training centres on technical defence and tools.