



SAMPLE PROGRAM REPORT

Security Awareness & Training Report

A detailed sample of the evidence and management insight produced by a practical security-awareness and phishing-readiness program.

Security Awareness & Training Report

A management-ready view of assigned training, completion, assessment performance, phishing-simulation outcomes, follow-up learning, and evidence retained.

Reporting period	Q3 2026 • Scope: all active personnel in the illustrative organization • Training data is presented as program evidence, not as a disciplinary scorecard.
------------------	---

Program snapshot

Assigned	Completed	Overdue	Assessment pass rate
142	94%	8	91%
Active personnel	134 of 142	Follow-up required	Across completed modules

Training completion by module

Training module	Assigned	Completed	Completion	Assessment pass rate	Status
Cybersecurity essentials	142	134	94%	92%	On track
Phishing & social engineering	142	132	93%	90%	On track
MFA & password security	142	136	96%	94%	On track
Data handling & privacy	142	129	91%	89%	Attention
AI and company data	142	126	89%	88%	Attention
Incident reporting	142	134	94%	93%	On track

Phishing simulation and reporting

Delivered	Reported safely	Clicked	Simulated action
138	37%	13%	4.3%
Of 142 targeted	51 employees	18 employees	6 employees

Interpretation: Reporting behavior is improving, while benefits- and identity-themed scenarios remain a reinforcement opportunity. The organization should measure trend over time and use results to guide training content, not to publicly rank or shame employees.

Follow-up learning

Follow-up action	Population	Progress	Owner	Due
Phishing refresher assigned after click or simulated action	18 employees	14 complete; 4 overdue	Security Owner	Oct 18
AI data-handling microlearning	16 employees with incomplete module	6 complete; 10 in progress	Operations	Oct 25
Manager reminder for overdue core training	8 employees	Scheduled	People Operations	Oct 10

Evidence retained

Evidence	Record kept in Unboredly
Training assignment	Module version, assigned audience, assignment date, due date, and reminder history
Completion	Employee completion time, acknowledgement where applicable, and assessment outcome
Phishing exercise	Campaign template, target audience, delivery record, reports, clicks, safe simulated actions, and follow-up assignment
Management review	Quarterly program summary, priority actions, and responsible owner

Next-quarter recommendation	Prioritize data-handling and AI-use training completion, repeat a lower-difficulty phishing scenario focused on reporting, and report improvement trends to leadership alongside overdue-training remediation.
------------------------------------	--