

SECURITY

Security Awareness at Work: A Practical Handbook

Fewer clicks on bad links, faster reporting, a measurably lower human-risk score.

A TriLMS eBook





People are the attack surface

Most breaches start with a person, not a server: a convincing phishing email, a reused password, a file that shouldn't have been opened. Security awareness training turns your workforce from the weakest link into an active sensor network — but only if it's continuous, measured and paired with realistic practice.

What a modern program covers

- Phishing & business email compromise — how to spot and report, not just delete.
- Passwords & MFA — why length beats complexity, and why reuse is the real risk.
- Data handling — classification, least-privilege, safe sharing.
- Safe web, remote work and physical security.
- Incident response — what to do in the first five minutes.

Simulate, measure, remediate

Knowledge fades; behavior is what matters. Run phishing simulations against domains you own, measure the phish-prone rate (clicked vs reported), and auto-assign short remedial training to anyone who clicks. Track the score over time — a falling phish-prone rate is a board-ready metric.

Quick checklist

- Deliver a full awareness curriculum
- Run phishing simulations on domains you own
- Measure phish-prone rate (clicked vs reported)
- Auto-assign remedial training to clickers
- Re-certify annually
- Report the trend to leadership

Try it in TriLMS

TriLMS ships a security-awareness curriculum plus a phishing-simulation engine with phish-prone scoring and auto-remediation — all in one platform. Demo at trilms.com.