QUICK REFERENCE

Employee Training Starter Kit

A plug-and-play curriculum for new hires and quarterly refreshers — built for businesses without a dedicated security team.

Why Training Is Your Best ROI

95% of security breaches involve human error. The most expensive security tools cannot protect you if employees click bad links or reuse weak passwords. Trained employees are your strongest defense — and training is among the cheapest investments you can make.

Week 1 — New Employee Orientation (1 hour)

Passwords (15 minutes)

- How to create a strong password (12+ characters, unique per site)
- How to set up the company password manager
- Why sharing passwords — even with coworkers you trust — is off limits
- Hands-on: help them set up the password manager before they leave the session

Phishing (20 minutes)

- What phishing looks like — show 3 real examples from your inbox
- Red flags: urgency, unexpected attachments, lookalike domains, requests for credentials
- What to do if you get one — report to [designated email], do NOT forward
- What to do if you already clicked — report immediately, no punishment for fast reports

Physical Security (10 minutes)

- Lock your screen every time you step away
- No tailgating — do not let strangers follow you in
- Shred sensitive documents
- Do not leave laptops visible in parked cars

When Something Goes Wrong (10 minutes)

- Who to call — have the name and number written down
- Report immediately, do not hide mistakes
- You will not get in trouble for reporting honest errors

Policies (5 minutes)

- Acceptable use of company systems
- Social media and AI guidelines
- Employee signs acknowledgment of training

Quarterly Refresher Topics (30 min each, rotate)

✓ **Q1 — Phishing & Email:** Recent examples from YOUR inbox, reporting refresher

✓ **Q2 — Passwords & Accounts:** Password manager tips, MFA coverage check, account hygiene

✓ **Q3 — Physical & Mobile:** Lost device procedure, working from public places, home network basics

✓ **Q4 — Year in Review:** General lessons from the year's incidents (no naming), new policies, upcoming changes

Simulated Phishing Program

Once a quarter, send a test phishing email to every employee. Not to trick them — to train them.

- Use a tool like KnowBe4, Proofpoint, or the free tier of Hook
- **If they click:** redirect to a short training page. No shame, no punishment — it is training
- **If they report it correctly:** thank them publicly. Reward reporting behavior.
- Track your click rate over time — it should drop quarter over quarter

Materials Checklist for Your Training Pack

✓ Slide deck or printed handout covering the five Week-1 topics
✓ Three real phishing examples (screenshots)
✓ Contact card — security email, phone, manager escalation
✓ Password manager setup guide for your chosen tool
✓ MFA setup guide for email and primary apps
✓ Signed acknowledgment form

The Culture That Makes Training Work

Training fails when people are afraid to report mistakes. The moment you punish an honest phishing click, every future click gets hidden — and hidden clicks become breaches. Thank every report, public or private. The fastest-improving security cultures are the ones where "I clicked something I should not have" is said openly.