

No. 142

CYBERSECURITY

Security Awareness Training Programs

Building a programme that changes behaviour, not just ticks boxes

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 142

Security Awareness Training Programs

Building a programme that changes behaviour, not just ticks boxes

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Security Awareness Training Programs
Building a programme that changes behaviour, not just ticks boxes

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product, framework and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why people matter 5
2 The human element 6
3 Why training often fails 7
4 Behaviour change 8
5 Maturity 9
6 The programme cycle 10
7 Goals 11
8 Stakeholders 12

PART II · DESIGNING THE PROGRAMME

9 Assessing human risk 14
10 Topics 15
11 Role-based training 16
12 New starters 17
13 A yearly calendar 18
14 Content design 19
15 Behavioural science 20
16 Channels 21
17 Security champions 22
18 Accessibility and inclusion 23
19 Languages and locations 24

PART III · SIMULATIONS AND MEASUREMENT

20 Phishing simulations 26
21 Beyond email simulations 27
22 Ethics 28
23 Feedback 29

FREE SAMPLE · ojayo.com

24 Reporting 30
25 Metrics 31
26 Calculating trends 32
27 Dashboards 33
28 Culture surveys 34

PART IV · CULTURE AND PRACTICE

29 Security culture 36
30 Leadership 37
31 Turning incidents into lessons 38
32 AI and deepfakes 39
33 Requirements 40
34 Budget and tools 41
35 Common mistakes 42
36 A worked example 43
37 Careers 44
38 A first-year roadmap 45
Checklists 46
Glossary 47
Further reading 48

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Most cyberattacks involve people somewhere: a convincing phishing email, a reused password, a fake call to the help desk, a payment sent to a fraudster. A **security awareness programme** helps people recognize and resist these attacks, use secure habits and report problems quickly.

This beginner's book shows how to build a programme that changes behaviour rather than just ticking compliance boxes: understanding human risk, choosing topics and audiences, designing short engaging content, running ethical phishing simulations, measuring what matters, building a positive security culture and meeting regulatory requirements.

What this book covers

- Why people matter and why traditional training often fails.
- Maturity, planning, topics and role-based training.
- Content design, channels and behavioural science.
- Phishing simulations, done ethically.
- Metrics, culture, AI and deepfakes.
- Requirements, budgets and a first-year roadmap.

Who this book is for

- **Security teams** responsible for awareness.
- **HR, learning and communications professionals.**
- **Managers** who want a security-aware team.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–8): why people matter, the human element, why training fails, behaviour change, maturity, the programme cycle, goals and stakeholders.
- **Part II — Designing the programme** (Chapters 9–19): assessing risk, topics, role-based training, new starters, a yearly calendar, content design, behavioural science, channels, champions, accessibility and languages.
- **Part III — Simulations and measurement** (Chapters 20–28): phishing simulations, other kinds of tests, ethics, feedback, reporting, metrics, the report rate, dashboards and surveys.
- **Part IV — Culture and practice** (Chapters 29–38): culture, leadership, learning from incidents, AI and deepfakes, requirements, budgets, mistakes, a worked example, careers and a roadmap.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in real programmes.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on screens

Screens are **simplified illustrations**, not real product screens.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain why people are central to security and how to think about changing behaviour.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why people matter

People are targets and defenders.

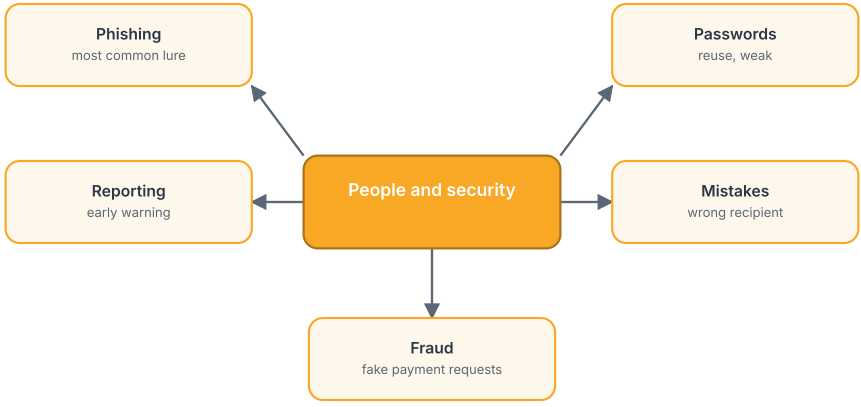


Figure 1.1 Where people make the difference

People as sensors

Staff who spot and report a phishing email quickly can stop an attack for everyone. Awareness turns people from targets into an early warning system.

KEY IDEA

The aim is not perfect people; it is people who notice, pause and report.

FREE SAMPLE · ojayo.com

CHAPTER 2

The human element

The data on human involvement.

Verizon's **2026 Data Breach Investigations Report** found human involvement in **62%** of breaches, such as falling for social engineering, misusing access or making errors. It also found shadow AI had become the third most common non-malicious insider action in its data loss prevention data.

FREE SAMPLE · ojayo.com

CHAPTER 3

Why training often fails

Why many programmes fail.



Figure 3.1 Ticking boxes versus changing behaviour

Knowledge is not behaviour

People may know they should not click suspicious links, but under time pressure they still do. Programmes must make the secure action easy, practised and expected.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs (you are…

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Security Awareness Training Programs

Enjoyed it? The full book has 53 pages and 38 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.