



SECURITY AWARENESS TRAINING

Course Catalog

Compliance frameworks &
topic-based courses

2026 EDITION • TRAINING TO PROTECT YOUR PEOPLE & DATA

infimasec.com

ABOUT THIS PROGRAM

Security awareness training, built for your team

Your IT provider delivers ongoing security awareness training to help your team recognize and stop the attacks that target businesses every day — phishing, social engineering, and the everyday mistakes that lead to a breach. This catalog shows the courses available to your organization, organized two ways: by the **compliance framework** your business is accountable to, and by **security topic** so training can be focused wherever your team needs it most.

26	9	15	5–20
Courses in the library	Topic areas covered	Compliance frameworks	Minutes per course

How the program works for your team

- **Short and practical** — most lessons run 5–20 minutes, so training fits into the workday.
- **Always current** — new team members are enrolled automatically and everyone stays up to date as threats evolve.
- **Reinforced with practice** — simulated phishing exercises turn lessons into habits and show where to focus next.
- **Mapped to your compliance needs** — completion lines up with the standards your business reports against, simplifying audits.
- **Fully managed for you** — your IT provider sets up, runs, and reports on everything, so there's nothing for your team to administer.

How this catalog is organized

1 • Compliance framework paths group the courses that satisfy a given standard's training requirement. If your business follows HIPAA, PCI DSS, SOC 2, or another framework, the matching path shows exactly which courses cover its awareness obligations.

2 • The topic-based library lists every course by subject, with its length. Your provider can assign a full path, target specific topics for certain roles, or follow up with a quick refresher after a simulated phishing test.

SECTION 1 — COMPLIANCE FRAMEWORK PATHS

Learning paths by framework

Each card pairs a framework's training requirement with the courses that satisfy it. If your business reports against one of these standards, this is the training that covers its awareness obligations.

CIS Controls v8

Organizations adopting the CIS benchmarks and safeguards

TRAINING REQUIREMENT ADDRESSED

Control 14 — Establish and maintain a security awareness program to influence behavior among the workforce.

COURSES IN THIS LEARNING PATH

phishing-2026 Phishing in the AI Age

social-2026 The Human Hack

CMMC Level 2

Defense Industrial Base suppliers and DoD contractors

TRAINING REQUIREMENT ADDRESSED

AT.L2-3.2.1 / AT.L2-3.2.3 — Deliver security awareness training, including insider-threat awareness, for all personnel.

COURSES IN THIS LEARNING PATH

privileged-users-2026 Privileged User Security

cui-2026 Handling Controlled Unclassified Information

insider-2026 Insider Threat Awareness

incident-response-2026 Incident Response Fundamentals

Cyber Insurance

Any organization carrying or seeking a cyber insurance policy

TRAINING REQUIREMENT ADDRESSED

Underwriting requirement — Cyber insurance carriers commonly require annual security awareness training as a condition of policy issuance and renewal.

COURSES IN THIS LEARNING PATH

phishing-2026 Phishing in the AI Age

Security Awareness Foundations

Any organization establishing or refreshing a baseline awareness program

TRAINING REQUIREMENT ADDRESSED

Baseline program — The minimum recommended awareness program for any organization, regardless of specific regulatory exposure.

COURSES IN THIS LEARNING PATH

phishing-2026 Phishing in the AI Age

FTC Safeguards Rule

Non-bank financial institutions covered by the FTC Safeguards Rule

TRAINING REQUIREMENT ADDRESSED

16 CFR §314.4(e) — Provide security awareness training to personnel as part of the qualified information security program; update as necessary as risks change.

COURSES IN THIS LEARNING PATH

pii-2026 Protecting Personal Information

GDPR

Organizations processing the personal data of EU residents

TRAINING REQUIREMENT ADDRESSED

Article 39 — Staff involved in processing operations must receive awareness training on data protection obligations.

COURSES IN THIS LEARNING PATH

[gdpr-2026](#) GDPR Awareness

[pii-2026](#) Protecting Personal Information

HIPAA

Healthcare providers and business associates handling PHI

TRAINING REQUIREMENT ADDRESSED

45 CFR §164.308(a)(5) — Implement a security awareness and training program for all members of the workforce.

COURSES IN THIS LEARNING PATH

[phi-2026](#) Protecting Health Information

[phi-data-2026](#) Handling PHI Day-to-Day

ISO 27001:2022

Organizations operating a certified ISMS

TRAINING REQUIREMENT ADDRESSED

Annex A 6.3 — Personnel shall receive appropriate information security awareness, education, and training.

COURSES IN THIS LEARNING PATH

[iso27001-orientation-2026](#) ISO 27001 Orientation
[vendor-risk-2026](#) Vendor Risk

[secure-development-2026](#) Secure Development
[phishing-2026](#) Phishing in the AI Age

NERC CIP

Bulk Electric System owners, operators, and registered entities

TRAINING REQUIREMENT ADDRESSED

CIP-004-7 R1 / R2 — Maintain a cybersecurity awareness program and training for personnel with authorized access to Bulk Electric System Cyber Systems.

COURSES IN THIS LEARNING PATH

insider-2026 Insider Threat Awareness

phishing-2026 Phishing in the AI Age

NIST AI RMF

Organizations developing, deploying, or using AI systems

TRAINING REQUIREMENT ADDRESSED

GOVERN 4 / MAP 2.1 — Establish and maintain workforce understanding of AI risks, responsibilities, and the safe and effective use of AI systems.

COURSES IN THIS LEARNING PATH

ai-safety-2026 Safe AI Usage

PCI DSS v4.0

Any organization that stores, processes, or transmits cardholder data

TRAINING REQUIREMENT ADDRESSED

Requirement 12.6 — Maintain a formal security awareness program; train personnel at onboarding and at least once every 12 months.

COURSES IN THIS LEARNING PATH

phishing-2026 Phishing in the AI Age

pci-2026 PCI DSS for Cardholder Data Handlers

SOC 2 Type II

SaaS and service organizations reporting against the Trust Services Criteria

TRAINING REQUIREMENT ADDRESSED

Common Criteria CC1.4 / CC2.2 — Demonstrate that personnel receive security awareness communications and understand their responsibilities.

COURSES IN THIS LEARNING PATH

phishing-2026 Phishing in the AI Age

incident-response-2026 Incident Response Fundamentals

privileged-users-2026 Privileged User Security

SOX

Publicly traded U.S. companies and personnel involved in financial reporting controls

TRAINING REQUIREMENT ADDRESSED

Sections 302 / 404 — Internal control over financial reporting includes IT security controls and training for personnel with access to financial systems.

COURSES IN THIS LEARNING PATH

phishing-2026 Phishing in the AI Age

StateRAMP

Cloud service providers authorized to serve state, local, and education entities

TRAINING REQUIREMENT ADDRESSED

NIST 800-53 AT-2 / AT-3 — Provide basic security awareness training to all personnel and role-based training to personnel with security responsibilities.

COURSES IN THIS LEARNING PATH

phishing-2026 Phishing in the AI Age

incident-response-2026 Incident Response Fundamentals

Texas DIR

Texas state agencies, public higher education, and their contractors

TRAINING REQUIREMENT ADDRESSED

TAC §202.74 — State agencies must complete a certified cybersecurity training program annually for all employees with access to state information resources.

COURSES IN THIS LEARNING PATH

texas-dir-2026 Texas DIR Cybersecurity Training

These mappings reflect common interpretations of each standard's awareness and training requirements and are provided to help plan your program. They are not legal advice or a certification of compliance; confirm scope with your auditor or compliance advisor.

SECTION 2 — TOPIC-BASED COURSE LIBRARY

26 courses across 9 topic areas

Every available course, grouped by subject. Your IT provider draws from this library to assign full paths, target specific topics for certain roles, or follow up with a quick refresher after a simulated phishing test.

Fundamentals

CODE	COURSE	LENGTH
phishing-2026	Phishing in the AI Age	8 min
social-2026	The Human Hack	7 min
hygiene-2026	Small Habits, Big Protection	5 min
data-2026	Data Has Consequences	6 min

Threat Awareness

CODE	COURSE	LENGTH
socialattacks-2026	Social Engineering Attacks	15 min

CODE	COURSE	LENGTH
malware-2026	Malware Awareness	15 min
passwords-2026	Password Security	12 min
wire-2026	Preventing Wire Fraud	15 min

AI & Emerging Threats

CODE	COURSE	LENGTH
aithreats-2026	AI-Powered Threats & Deepfakes	15 min
ai-safety-2026	Safe AI Usage	15 min

Incident Response

CODE	COURSE	LENGTH
incident-response-2026	Incident Response Fundamentals	10 min

Data Protection

CODE	COURSE	LENGTH
pii-2026	Protecting Personal Information	10 min
insider-2026	Insider Threat Awareness	12 min

Compliance

CODE	COURSE	LENGTH
phi-2026	Protecting Health Information	8 min
phi-data-2026	Handling PHI Day-to-Day	12 min
pci-2026	PCI DSS for Cardholder Data Handlers	15 min
gdpr-2026	GDPR Awareness	15 min
cui-2026	Handling Controlled Unclassified Information	15 min
iso42001-2026	ISO 42001: AI Management Systems	20 min

CODE	COURSE	LENGTH
phishing-k12-2026	Phishing Awareness for K-12 Teachers	15 min

Specialized Topics

CODE	COURSE	LENGTH
privileged-users-2026	Privileged User Security	12 min
guardian-2026	The Data Guardian	12 min

Remote Work

CODE	COURSE	LENGTH
remote-2026	Security Beyond the Office	15 min

Workplace Conduct

CODE	COURSE	LENGTH
harassment	Sexual Harassment in the Workplace	—
bullying	Bullying in the Workplace	—
violence	Violence in the Workplace	—

NEXT STEPS

Bringing this training to your team

Rolling out security awareness training is straightforward — your IT provider handles setup and ongoing management, so your team simply receives short lessons over time. Here is what getting started looks like.

1 Enroll

Your team is added and assigned a starting path based on the standards your business follows.

2 Train

Short, regular lessons and simulated phishing exercises build lasting habits over time.

3 Improve

You receive clear reports showing completion, progress, and where to focus next.

Getting your team started

Your IT provider manages this program from start to finish — enrolling your people, scheduling training and simulated phishing, and reporting on progress against the standards your business follows. There's nothing for your team to install or administer.

Talk to your IT provider to build the right program for your organization.

Delivered on the INFIMA security awareness platform · infimasec.com