

Security Awareness Training Catalog

SCAMS & SOCIAL ENGINEERING

Phishing

Covers common phishing techniques, warning signs, and how attackers use social engineering to trick users into clicking links or sharing sensitive information.

Smishing

Explains how SMS based phishing works, common red flags, and how to safely handle suspicious texts.

QR Phishing

Teaches how attackers use QR codes to hide malicious links and how to verify QR codes before scanning.

Vishing

Explains voice based scams, caller manipulation tactics, and how to verify requests made over the phone.

Social Media Scams

Covers scams that target users through social platforms, including fake profiles, messages, and impersonation attempts.

Impersonation Scams

Explains how attackers pose as trusted individuals or organizations to gain access or steal information.

AI Scams

Covers how attackers use artificial intelligence to make scams more convincing and harder to detect.

Deepfake Awareness

Explains how deepfake audio and video are used in fraud, impersonation, and misinformation campaigns.

Ransomware

Explains how ransomware attacks spread, common infection methods, and what actions employees can take to prevent incidents and limit damage.

CORE SECURITY FUNDAMENTALS

Cyber Security

Provides a practical overview of everyday cybersecurity risks and how employee actions impact organizational security. Builds a shared baseline so everyone understands how small decisions can create or reduce risk.

Password Security

Teaches how to create, store, and manage strong passwords while avoiding common password mistakes. Addresses one of the most common causes of account compromise across all industries.

Multi Factor Authentication

Explains how MFA works, why it is critical, and how it significantly reduces account compromise. Shows how a single additional step can stop the majority of credential-based attacks.

Device Security

Covers best practices for securing laptops, mobile phones, and tablets against theft, malware, and misuse.

WiFi Security

Explains how to secure home, public, and corporate WiFi networks and avoid common wireless threats.

Secure Internet Browsing

Teaches safe browsing habits, how to spot unsafe websites, and how to avoid malicious downloads.

Defense in Depth

Explains layered security strategies and why relying on a single control is never enough.

Situational Awareness

Helps learners recognize suspicious behavior and potential threats in both digital and physical environments.

WORKPLACE & INSIDER RISK

Remote Working

Covers security risks associated with remote work and how to keep data and systems safe outside the office.

Secure Traveling

Provides guidance on protecting devices, data, and accounts while traveling for work.

Physical Security

Focuses on protecting offices, equipment, and physical assets through awareness and access control.

Insider Threats

Explains risks posed by insiders, whether intentional or accidental, and how those risks can be reduced.

Shadow IT

Covers risks created by unauthorized tools and services and how they impact security and compliance.

Privileged User Best Practices

Focuses on securing high level accounts and reducing risks tied to elevated access.

PRIVACY & COMPLIANCE

Privacy Awareness

Introduces core privacy principles and how to responsibly handle personal and sensitive information.

HIPAA

Explains how to properly handle protected health information and maintain regulatory compliance.

GDPR Fundamentals

Provides an overview of GDPR requirements and how organizations can protect personal data.

SOC 2 Fundamentals

Introduces SOC 2 principles and the importance of security, availability, and confidentiality controls.

ISO 27001 Fundamentals

Explains ISO 27001 standards and how they support effective information security management.

CCPA

Covers California's Consumer Privacy Act and consumer data rights.

Privacy Act Australia

Provides an overview of Australia's Privacy Act and key compliance responsibilities.

PSPF Fundamentals Australia

Explains the Protective Security Policy Framework and its role in Australian government security.

PDPA Singapore

Covers Singapore's data protection requirements and organizational obligations.

DPA United Kingdom

Explains the UK Data Protection Act and its alignment with GDPR principles.

PIPL China

Provides an overview of China's Personal Information Protection Law and compliance expectations.

POPI Act South Africa

Covers South Africa's POPI Act and responsible handling of personal data.

DPDP Act India

Introduces India's Digital Personal Data Protection Act and compliance basics.

Privacy Act New Zealand

Explains New Zealand's privacy laws and data handling expectations.

NIST CSF United States

Introduces the NIST Cybersecurity Framework and how it supports risk management.

Secure Credit Card Handling

Covers best practices for securely handling payment card data and reducing fraud risk.

NIS2 Fundamentals

This training explains what NIS2 is, why it matters, and how it raises cybersecurity expectations.

EU AI Act

This training gives a brief overview of the EU AI Act, why it matters, and what it means for organizations using AI.

TECHNOLOGY & EMERGING RISK

Secure Software Development

Introduces secure coding principles and reducing vulnerabilities throughout the development lifecycle.

Supply Chain Risk

Explains cybersecurity risks within supply chains and how to manage third party risk.

Threat Actors

Explains different types of cyber threat actors, their motivations, and common attack methods.

Using Artificial Intelligence Securely

Explains how to use AI tools responsibly while protecting sensitive data.

Web3.0 & Blockchain Security

Introduces security considerations related to blockchain and decentralized technologies.

INDUSTRY SPECIFIC TRAINING

Education Provider Best Practices

Addresses cybersecurity risks specific to education environments and protecting students and staff.

Small Business Best Practices

Provides practical cybersecurity guidance tailored to small businesses with limited resources.

Financial Industry Best Practices

Focuses on security and compliance needs unique to financial organizations.

Healthcare Industry Best Practices

Covers cybersecurity challenges in healthcare and protecting patient data.

Critical Infrastructure Best Practices

Explains security responsibilities for organizations supporting essential services.

Government Best Practices

Outlines cybersecurity expectations, policies, and risk management practices for government environments.

ROLE SPECIFIC TRAINING

Cybersecurity for Executives

Explains how authority, urgency, and decision-making pressure can be exploited, and how leaders reduce risk through deliberate verification.

Cybersecurity for HR

Explains how trust, empathy, and sensitive employee requests are exploited through impersonation and account compromise.

Cybersecurity for Finance

Explains how payment workflows and late-stage changes are targeted to redirect funds through fraud and impersonation.

Cybersecurity for Legal

Explains how authority, deadlines, and formal communications are exploited to deliver malware or extract sensitive information.

Cybersecurity for Sales

Explains how urgency, opportunity, and deal momentum are used to lure sales professionals into phishing attacks.

Cybersecurity for Real Estate Agents

Explains how high-value transactions and last-minute changes are exploited to intercept payments and sensitive details.

Cybersecurity for Students

Introduces how phishing uses urgency and fear of disruption to steal student credentials and access accounts.

Cybersecurity for Teachers

Explains how routine communications and internal trust can be exploited to spread malware or compromise systems.

Cybersecurity for Medical Professionals

Explains how urgency and patient-focused messaging are used to compromise clinical systems and sensitive data.

HR COMPLIANCE TRAINING

Sexual Harassment Prevention

Learn how to recognize, prevent, and respond to inappropriate behavior that can make others feel unsafe, uncomfortable, or disrespected at work.

Bullying And Harassment Prevention

Understand how repeated harmful behavior can affect people and workplace culture, and what to do when conduct crosses the line.

Workplace Emotional Intelligence

Learn how self-awareness, self-control, and understanding others can improve communication, teamwork, and decision-making at work.

Workplace Health And Safety

Understand how to identify risks, follow safe practices, and help prevent injury or illness in the workplace.

Discrimination Prevention

Learn how unfair treatment can show up at work, why it matters, and how to help create a fair and inclusive workplace.