RansomLeak

Security Training Syllabus

Every RansomLeak exercise, grouped by category and course, plus suggested learning paths by role. Each exercise is a 5-10 minute interactive module.

Updated November 2026 · ransomleak.com/syllabus

Learning paths by role

All employees

The baseline every person in the company should finish first: the inbox, the login prompt, the download and the report button.

1. Phishing
2. Spear Phishing
3. QR Code Phishing (Quishing)
4. Business Email Compromise
5. MFA Fatigue Attack
6. Password Manager Habits
7. Safe Browsing & Downloads
8. Ransomware
9. Data Classification Basics
10. Safe GenAI Usage
11. AI-Written Phishing
12. General Incident Reporting

Reinforced by: Email phishing, MFA fatigue, Quishing (QR code), Fake login page, Malicious attachment

Managers and executives

Leaders are the most impersonated people in a company. This path covers the calls, exceptions and sign-offs attackers aim at them.

1. Whaling With A Deepfake
2. Executive Voice Impersonation
3. Security Exception Requests
4. Help Desk Impersonation
5. Your Public Footprint
6. Delegated Mailbox Compromise
7. Quarterly Access Review
8. Vendor Risk Sign-off
9. Handling a Team Phishing Click
10. Ransomware Crisis Leadership

Reinforced by: Vishing (voice call), Deepfake, Social media / OSINT, Chat (Teams / Slack)

Finance and accounts payable

Payment fraud rarely looks like hacking. It looks like a supplier changing bank details or a director who needs a transfer today.

1. Invoice & Payment Fraud
2. Business Email Compromise
3. Verification Procedures
4. Callback Phishing
5. Double Barrel Phishing
6. Cloned Voice Payment Fraud
7. Deepfake Audio Detection
8. Supplier Bank Detail Fraud
9. Security Exception Requests

Reinforced by: Email phishing, Vishing (voice call), Attack chain, Malicious attachment, Deepfake

HR and people teams

HR holds the most personal data and runs the riskiest workflows: hiring, offboarding and data subject requests.

1. Deepfake Hiring Fraud
2. Personal Data Essentials
3. Employee Data Collection
4. Joiner-Mover-Leaver Awareness
5. Legitimate DSAR Processing
6. Fraudulent DSAR Detection
7. Identity Theft Prevention
8. Social Media Oversharing
9. Fake Recruiter Approaches

Reinforced by: Email phishing, Social media / OSINT, Chat (Teams / Slack), Deepfake

Front desk and retail staff

Patient and card data leak at the counter, not the server room. Built around HIPAA and PCI DSS duties for customer-facing roles.

1. Workstation Screen Privacy
2. Incidental Verbal Disclosures
3. Identity Verification Before Disclosure
4. Card Terminal Tampering Checks
5. Unverified Terminal Servicing
6. Card Details Taken by Phone or Email
7. Card Numbers on Paper
8. Technician Impersonation
9. Unlocked Workstations

Reinforced by: Smishing (SMS), Vishing (voice call), Quishing (QR code)

Software developers

Exploit the classic web and API flaws, then fix them. Ends with the new risks of AI coding assistants in the repository.

1. SQL Injection
2. Stored XSS
3. Broken Object Level Authorization
4. Server-Side Request Forgery
5. Insecure Deserialization
6. Secrets in Git History
7. Malicious Pull Requests
8. Dependency Chain Abuse
9. AI Package Hallucination
10. Untested AI Security Fix
11. Rules File Poisoning

Reinforced by: OAuth consent, AI chat data-leak, Fake login page, Chat (Teams / Slack)

Cloud and platform engineers

The account, the image, the cluster and the pipeline, each treated as a security boundary you can break and then lock down.

1. Over-Permissive IAM
2. Public Storage Buckets
3. Long-Lived Access Keys
4. Instance Metadata Abuse
5. Secrets in Image Layers
6. Insecure Kubernetes Workload Configurations
7. Overly Permissive Kubernetes Authorization
8. Secrets in Terraform State
9. Policy-as-Code Gate
10. Insecure CI/CD System Configuration

Reinforced by: OAuth consent, MFA fatigue, Fake login page

Teams building with AI

For anyone shipping LLM features, agents or MCP servers. Prompt injection first, then agency, tooling and the EU AI Act basics.

1. LLM Prompt Injection
2. LLM Sensitive Information Disclosure
3. Over-Permissioned AI Agent
4. Agent Goal Hijack
5. Agent Tool Misuse & Exploitation
6. MCP Tool Poisoning
7. MCP Token Mismanagement & Secret Exposure
8. AI Risk Classification
9. Bias and Discrimination in AI

Reinforced by: AI chat data-leak, OAuth consent, Deepfake

Staff in sensitive technology

Operational security for people who build defence, dual-use or export-controlled products. What a photo, a trade show or a visitor gives away.

1. Photo Location Leaks
2. Fitness App Location Leaks
3. Trade Show Elicitation
4. Production Floor Visitors
5. Giveaway USB Devices
6. Need to Know
7. Removable Media and Air Gaps
8. Data Spill Reporting

Reinforced by: Social media / OSINT, Smishing (SMS), Chat (Teams / Slack)

Full curriculum

Security Awareness

Build a security-first culture with interactive exercises covering phishing, social engineering, device security, and more.

Phishing & Impersonation Attacks 17

Callback Phishing
Spot a fake fraud alert built to make you call.

Phishing
Spot a phishing email before you click.

Vishing
Handle a realistic voice phishing call.

Smishing
Detect fraud hiding in your text messages.

Double Barrel Phishing
Spot the phone call that sets up the phishing email.

Business Email Compromise
Spot a wire request from a hijacked colleague's account.

Social Engineering
Recognize manipulation before you comply.

Whaling With A Deepfake
Spot an AI-generated executive on a video call.

Spear Phishing
Your public profile is their attack playbook.

QR Code Phishing (Quishing)
That QR code skips every email filter you have.

WhatsApp Social Engineering
Your "boss" on WhatsApp isn't your boss.

Tech Support Scams
That virus warning is the actual attack.

SEO Poisoning Awareness
Top search results aren't always trustworthy.

Invoice & Payment Fraud
Catch a fraudulent vendor invoice using the 3-way match before it reaches the payment file.

Verification Procedures
Stop a vendor banking BEC by using your authoritative directory and an out-of-band callback.

Deepfake Audio Detection
Catch an AI-cloned executive voice on the phone before the wire goes out.

Calendar Invite Scams
Catch a spoofed calendar invite before the fake meeting page harvests your credentials.

Device Security 10

Backup Best Practices
Set up backups before a crash takes your work.

Encryption & Lock Discipline
Practice the habits that protect unattended devices.

OS Updates & Patching Basics
See why skipping updates opens real attack paths.

Ransomware
Survive a ransomware attack in real time.

USB Drop Attack
Think twice before plugging in that USB drive.

Endpoint Patching & EDR Alerts
Know what your EDR alert means and what to do next.

File Extension Awareness
It looks like a PDF. It runs like malware.

Safe Bluetooth Practices
Your headphones are broadcasting more than music.

Mobile Device Security
One fake text. Eight hours of stolen access.

Mobile App Permissions
Name the feature each permission powers, or revoke it.

Passwords & Account Security 8

Account Recovery Security
Defend account recovery from social engineering.

Credential Stuffing Awareness
See how breached passwords fuel automated attacks.

Joiner-Mover-Leaver Awareness
A leaver's account that nobody switched off.

Least Privilege Awareness
Keep access to the minimum your job requires.

MFA Setup & Best Practices
Set up multi-factor authentication the right way.

MFA Fatigue Attack
Your phone buzzes for the thirtieth time. Then a Slack message says approve.

Password Manager Habits
Build strong habits with your password manager.

Privileged Access Basics
Learn why admin accounts need special handling.

Web & Browser Safety 6

HTTPS & Website Security
Learn why the padlock icon is not proof of safety.

Safe Browsing & Downloads
Spot malicious downloads before they run.

Typosquatting Awareness
Catch the domain tricks attackers use against you.

Browser Autofill Risks
Hidden fields silently steal your autofilled data.

Browser Extension Safety
That helpful extension might be stealing everything.

Browser Notification Abuse
That CAPTCHA was a trap for push spam.

Incident Reporting 2

General Incident Reporting
Know when and how to report a security incident.

Reporting Culture
Report it, even when it is not your incident.

Safe Communication & Sharing 7

Cloud Sharing Controls
Audit who can see your shared files right now.

Guest Access Management
Control what external users can reach and for how long.

Secure Messaging Practices
Stop sensitive data from leaking through chat apps.

Social Media Policy
Learn what not to post on corporate accounts.

Social Media Oversharing
See how attackers exploit your public profiles.

Third-Party App OAuth Risks
Check what you gave permission to access.

Secure Online Meetings
Spot the drop-in attendee, remove them, lock the meeting, file the report.

Security Policies & Your Role 5

Audit Mindset Basics
Think like an auditor to find compliance gaps.

Audit Portal Training
Navigate GRC portals and submit audit evidence.

Employee Security Responsibilities
Know your personal security duties at work.

ISMS Policy Awareness
Connect ISO 27001 policies to your daily work.

Internet & Email Acceptable Use
Stay within corporate internet and email policies.

Protecting Sensitive Information 7

Data Classification Basics
Label data correctly by sensitivity level.

Identity Theft Prevention
Spot identity theft tactics targeting employees.

Secure Sharing Practices
Share files safely without creating security gaps.

Data Leakage
Stop sensitive data from leaving your org.

Log Sensitivity Awareness
Production logs hold things you would never email out.

Metadata Awareness
A black rectangle over text does not remove the text.

Safe GenAI Usage
Use generative AI without leaking sensitive client data.

Workplace Security 17

Insider Threat (Intentional)
Recognize the warning signs of a malicious insider.

Shadow IT Awareness
Find out what happens when teams use unapproved apps.

Image-Based Attacks (Stegosploit)
That image file might be carrying more than pixels.

Insider Threat (Accidental)
One wrong attachment. Confidential data in the wrong inbox.

Collaboration Tool Hygiene
One shortcut in a team channel. Credentials everywhere.

Secure Document Disposal
Find out where a binned page actually ends up.

Clean Desk Basics
See what a passer-by does with the notes on your desk.

Unattended Printouts
A page in the tray belongs to whoever gets there first.

Printer Admin Security
The office printer still answers to admin / admin.

Visitor Sign-in Gaps
Nobody booked him in, but he has a ten o'clock.

Unescorted Visitors
A badge gets someone in. A host keeps them accounted for.

Intercom Tailgating
A courier at the door is not an ID card.

Badge Sharing
Lend your badge and the door log still says you.

Technician Impersonation
He has a toolbox, a badge and two minutes. Check anyway.

Shoulder Surfing
Your screen is readable from two metres behind you.

Unlocked Workstations
An awake screen is a signed-in session with a name on it.

Badge Door Tailgating
Treat holding a badge door as an access decision.

Remote & Home Office Security 3

VPN Usage & Safety
Configure and use your VPN without leaving gaps.

Home Router Security
Find out who else is on your home network.

IoT & Smart Device Security
Your smart camera scores 28 out of 100.

Working in Public Spaces 8

Captive Portal Phishing
More Wi-Fi time for your work password is not a deal.

Evil Twin Wi-Fi
The network's name proved nothing. Tether when unsure.

VPN on Public Wi-Fi
A VPN that drops mid-upload does not tell you. A kill switch does.

Tampered QR Codes
A QR code has no sender, and a sticker can replace it.

Juice Jacking
A charging port that asks for your files is not a charger.

Eavesdropping & Device Theft
Your voice carries further than your screen.

Boarding Pass Oversharing
See what a posted boarding pass hands a stranger.

Screen Privacy in Public
Keep your screen unreadable to the seat behind you.

Security for Managers & Executives 10

Delegated Mailbox Compromise
Your assistant's password was a key to your mailbox.

Quarterly Access Review
Approve all is a signature, not a shortcut.

Ransomware Crisis Leadership
The ransom note is addressed to the board. Lead, don't pay.

Deal-Driven Payment Fraud
The deal was in the news. That is what made the fraud work.

Help Desk Impersonation
Your help desk needs the authority to say no to you.

Security Exception Requests
The deadline is real. So is the hole you approve.

Executive Voice Impersonation
It sounds exactly like your CEO. That proves nothing.

Vendor Risk Sign-off
Your signature decides who holds your customers' data.

Handling a Team Phishing Click
Your reaction decides when the next one is reported.

Your Public Footprint
What a stranger can learn about you in an afternoon.

Privacy & Compliance Frameworks

Master GDPR compliance with hands-on exercises covering data protection, breach response, and privacy by design.

AI Basics for Everyone 4

What Counts as AI
Automatic is not the same as AI. Learn the legal test.

Labeling AI and Deepfakes
If it could pass for real, it needs a label.

Using AI Within the Law
What you paste, publish and switch on is all regulated.

When AI Use Goes Wrong
The fine is the company's. The consequences are yours too.

GDPR Compliance 18

Personal Data Essentials
Recognize personal data before you handle it.

Principles and Legal Bases
Pick the lawful basis before the work starts.

Everyday Privacy Duties
The three reflexes that keep a small problem small.

Employee Data Collection
Send the staff form twice: once wrong, once lawfully.

Marketing Consent Management
Segment a marketing list by the consent each contact gave.

Data Breach Response
Report a misdirected-email breach inside the 72-hour clock.

Privacy by Design Review
Evaluate a product feature through a privacy-first lens.

Legitimate DSAR Processing
Process a data subject access request end to end.

PII Document Redaction
Redact personal data from a report before it goes to auditors.

Fraudulent DSAR Detection
Spot fake data access requests used for social engineering.

Third-Party Data Processor Vetting
Find the gaps in a vendor's DPA before signing.

Security Incident Response
Spot a live breach in the SOC and escalate it to the DPO.

Cross-Border Data Transfers
Navigate transfer mechanisms for data leaving the EEA.

Data Protection Impact Assessment
Run a DPIA for a high-risk data processing activity.

Data Mapping and Records of Processing
Review a healthcare provider's Article 30 processing register.

Cookie Consent Management
Fix a cookie banner a regulator has already flagged.

Data Retention Compliance
Decide what to delete, retain, hold, or anonymize.

Breach Response Tabletop
Take the privacy seat on a live ransomware bridge.

EU AI Act Compliance 16

AI Literacy Essentials
Earn the AI literacy required by Article 4 before touching company AI tools.

AI Risk Classification
Sort real AI deployments into the four EU AI Act risk tiers.

Prohibited AI Practices
Stop banned AI deployments before they go live.

High-Risk AI: Deployer Obligations
Block a high-risk AI launch with compliance gaps in any of seven areas.

Provider vs. Deployer: Who's Responsible?
A compliant vendor product does not make your deployment compliant.

AI Transparency and Disclosure
Label AI chatbots and synthetic media correctly under Article 50.

Meaningful Human Oversight
Override an AI loan recommendation when the evidence does not match.

AI Data Governance
Block AI training that uses a leaky, biased, or oversharing dataset.

AI and Data Protection
Run a healthcare AI through both EU AI Act and GDPR at once.

Bias and Discrimination in AI
Investigate proxy variables hiding inside a resume-screening model.

Fundamental Rights Impact Assessment
Run a FRIA before a social housing AI ever assigns a benefit decision.

AI Incident Reporting
Report a discriminatory AI rejection pattern under Article 73.

AI Governance in Your Organization
Build an AI registry and shut down shadow AI in your company.

General-Purpose AI Model Obligations
Map GPAI provider and downstream deployer duties for systemic-risk models.

Using AI Tools Responsibly at Work
Make compliant AI choices through a normal working day.

EU AI Act Penalties and Enforcement
Map the three-tier penalty structure to real enforcement scenarios.

OWASP Top 10 Privacy Risks 10

Privacy Breach via Web Application Vulnerabilities
A valid login is not a key to everyone's record.

Operator-sided Data Leakage
The leak came through your own support console.

Insufficient Data Breach Response
You cannot notify the right people if you never logged reads.

Consent on Everything
The ad pixel fired before anyone said yes.

Non-transparent Policies
The notice said never. The data map said nightly.

Insufficient Deletion of User Data
The delete button removed one copy out of six.

Insufficient Data Quality
Same name, different person, one account.

Missing or Insufficient Session Expiration
She pressed Log out. The kiosk kept her signed in.

Inability of Users to Access and Modify Data
She asked for all her data. She got four fields.

Collection of Data Not Required for the User-consented Purpose
The sign-up wanted her birthday, her friends and her location.

Handling Controlled Information 8

CMMC Level 2 in Practice
Answer a CMMC assessor from what you actually do.

BYOD and Controlled Data
Keep controlled documents off a personal phone.

Need to Know
Share the pages someone needs, not the whole package.

Secure Printing and Disposal
Number, collect and shred every controlled copy.

Removable Media and Air Gaps
Cross an air gap the approved way, not with a personal USB stick.

Export-Controlled Data Sharing
Learn why showing a drawing can be an export.

Data Spill Reporting
Report a misdirected controlled file in the first minute.

Controlled Document Marking
Keep each customer's marking on what you write.

HIPAA Compliance 6

Workstation Screen Privacy
Keep patient records off a screen the waiting room can read.

Incidental Verbal Disclosures
Confirm patient details without the queue hearing them.

Identity Verification Before Disclosure
Verify a caller before sharing anything about a patient.

Shared Workstation Logins
Never work in a session logged in as someone else.

Paper PHI Handling and Disposal
Keep printed patient records out of trays and bins.

Facility Access Control
Stop a stranger with a toolbox at the staff door.

PCI DSS for Frontline Staff 6

Card Terminal Tampering Checks
Check the card machine for tampering at the start of a shift.

Unverified Terminal Servicing
Verify a technician before they touch the card machine.

PIN Capture by Hidden Camera
Find the hidden camera watching customers type their PIN.

Card Numbers on Paper
Never write a customer's card number down.

Card Details Taken by Phone or Email
Keep card numbers out of the inbox and off the phone notes.

Rogue Devices on the Payment Network
Notice the extra device plugged into the payment network.

AI & LLM Security

Prepare for AI-powered threats including prompt injection, deepfake attacks, and LLM manipulation.

AI at Work 15

AI-Written Phishing
Spot a phishing email with perfect spelling and your project name.

AI Voice Phishing Calls
Take a scam call from an AI that answers every question.

Cloned Voice Payment Fraud
Handle a payment request sent as your manager's voice note.

Voice Clone Impersonation
Handle the fallout when a clone of your voice calls a colleague.

Deepfake Hiring Fraud
Run a liveness check on a remote candidate mid-interview.

AI Support Chatbot Scam
Spot a fake AI support chat that asks for your login code.

Unapproved AI Notetakers
Find the AI notetaker sitting in a confidential HR meeting.

Prompt Injection in Documents
Trace an AI summary back to hidden text inside a PDF.

Unreviewed AI Output
Cut the internal details out of an AI-drafted client reply.

Shadow AI Tools
Photograph a roadmap into a free AI app, then put it right.

AI Agent Payment Fraud
Watch a web page redirect the payment your AI agent makes.

AI Assistant Oversharing
Check the source when an assistant answers with colleagues' salaries.

Shared Agents Share Access
Share an assistant built on your files and watch it answer with your access.

Browser Agent Data Leak
It acts as you, on every site you're signed into.

The Agent Clicked Allow
It approved the permission screen you never saw.

OWASP Top 10 for LLM Applications 10

LLM Prompt Injection
Stop a hidden prompt from hijacking your AI assistant mid-task.

LLM Sensitive Information Disclosure
See what happens when confidential data enters a consumer AI tool.

AI Supply Chain
Deploy an AI plugin that hides a backdoor in plain sight.

AI Data and Model Poisoning
Watch poisoned documents corrupt your AI's answers in real time.

Unsafe AI Output Handling
Exploit an AI whose outputs flow unchecked into live systems.

Over-Permissioned AI Agent
Manipulate an AI assistant into misusing its own permissions.

Hidden Context Exposure
Extract hidden instructions from a customer-facing AI chatbot.

Vector and Embedding Weaknesses
Exploit a RAG pipeline to access documents beyond your clearance.

AI Misinformation
Catch fabricated statistics and fake citations in an AI report.

AI Denial-of-Service Attack
Launch a denial-of-wallet attack against an unprotected AI API.

OWASP Top 10 for Agentic Applications 10

Agent Goal Hijack
Spot the moment an AI agent's goal is quietly rewritten.

Agent Tool Misuse & Exploitation
Catch the fraudulent items an agent's tools slip into your queue.

Agent Identity & Privilege Abuse
Find the agent that has been quietly widening its own access.

Agentic Supply Chain Vulnerabilities
A backdoored MCP server mirrors every query your agents make.

Unexpected Code Execution by AI Agents
Read the AI's pull request before you approve the backdoor.

Agent Memory & Context Poisoning
One poisoned memory entry keeps steering the agent for weeks.

Insecure Inter-Agent Communication
Forge one message on an unauthenticated agent bus and it obeys.

Multi-Agent Cascading Failures
One bad record, five agents, and a filed regulatory report.

Human-Agent Trust Exploitation
Weeks of accurate approvals are the setup, not the reassurance.

Rogue AI Agents
Healthy metrics, clean output, one agent acting on its own.

OWASP MCP Top 10 10

MCP Tool Poisoning
Agents read tool descriptions as instructions, not as docs.

MCP Command Injection & Execution
A semicolon in a tool argument becomes a shell command.

MCP Intent Flow Subversion
Text an agent reads is not a command it should obey.

Shadow MCP Servers
Your client's server list is not what is actually listening.

MCP Supply Chain & Dependency Tampering
Installing an MCP server runs its code before you read it.

Lack of MCP Audit & Telemetry
Logging turned on today cannot recover yesterday.

Insufficient MCP Authentication & Authorization
Approving a server is not the same as authenticating it.

MCP Privilege Escalation via Scope Creep
An agent reaches as far as its token, not its brief.

MCP Token Mismanagement & Secret Exposure
A token in your MCP config is a token your assistant reads.

MCP Context Injection & Over-Sharing
When one agent serves many customers, its context is data.

Secure AI-Assisted Development 12

AI Package Hallucination
The assistant named a package. Nobody checked it was real.

Untested AI Security Fix
The assistant said it was safe. It wasn't.

AI Context Secret Leak
The assistant read a file you never handed it.

Rules File Poisoning
The rule looked like a note. The assistant obeyed it.

Prompt Injection via Issues
Anyone could file a bug. The bot merged it.

Hollow AI-Written Tests
Twelve green tests. Not one checked the case that leaked.

Ambient Cloud Credentials
The assistant ran your delete with your laptop's production key.

Unreviewed AI-Built App
An assistant built it in a weekend. Nobody reviewed it.

Insecure Generated IaC
It planned cleanly. It shipped public.

AI Code License Contamination
The assistant wrote it. Someone else owns it.

Unbounded Agent File Access
Your project ends at the workspace root. The assistant's reach did not.

Disabled AI Guardrails
Three controls off. One dependency did the rest.

Real-World Incidents

Learn from actual security breaches. Walk through the MGM Resorts attack, BEC fraud cases, and more.

Incident walkthroughs 4

OneNote Email Attack
A trusted partner's email, a fake sign-in page, six minutes.

HTTP2Shell RCE
One compressed request, no login, a shell on your box.

PHP2Shell RCE
One request, no login, a shell on your server.

MGM Resorts Breach
Relive the 10-minute helpdesk call that cost $100M.

OPSEC

Operational security for staff who build sensitive technology. Notice what photos, apps, trade shows, visitors and friendly questions give away, then close each gap and report it.

OPSEC Essentials 5

Linked Device Takeover
See what one tap on Link hands a stranger.

Fitness App Location Leaks
Stop a fitness app from mapping where you live and work.

Group Chat Membership
Check who is really in the work group chat.

Photo Location Leaks
Check what a photo gives away before you post it.

Fake Recruiter Approaches
Spot a friendly approach that is really elicitation.

OPSEC: Industry 10

Demo Unit Tampering
Check a demo unit after strangers have been near it.

Exhibitor Badge Sharing
Keep your exhibitor badge on you, even for ten minutes.

Family and Home Oversharing
Find what family posts reveal about your work.

Giveaway USB Devices
Leave the free USB stick from the show unplugged.

Overnight Stand Security
Close a trade-show stand so nothing walks overnight.

Prototype Photos and Video
See what a short test-range clip tells strangers.

Supplier Bank Detail Fraud
Verify a supplier's new bank account before paying.

Trade Show Elicitation
Answer friendly questions at the stand without oversharing.

Unattended Demo Laptop
Lock the demo laptop every time you step away.

Production Floor Visitors
Challenge a visitor nobody is escorting.

Application Security

Exploit the OWASP Top 10 for web, API and mobile, then ship the fix. Hands-on secure-coding practice for developers.

OWASP Top 10 for Web Applications 26

Clickjacking
Steal a click on a bank approval button.

Command Injection
Chain a second command onto a server-side tool.

Components with Known Vulnerabilities
Get code execution through an outdated library.

Cross-Site Request Forgery
Move money from a page the victim never trusted.

Directory Traversal
Read system files through a download link.

DOM XSS
Trigger XSS the server never sees.

Forced Browsing
Pull an employee PII export from an unlinked route.

Horizontal Privilege Escalation
Change one digit and read another customer.

Host Header Injection
Redirect a password-reset email to a lookalike domain.

Insecure URL Redirect
Hide a phishing page behind a real login.

Leftover Debug Code
Pull production secrets from a forgotten debug route.

PII in URL
Lift personal data straight out of a link.

Reflected XSS
Craft a malicious URL that runs the moment it opens.

Server-Side Request Forgery
Make the server fetch its own cloud credentials.

Session Fixation
Plant a session id and inherit the victim login.

SQL Injection
Dump a database through one unguarded lookup form.

Stored XSS
Plant a script in a comment and watch it fire.

Token Exposure in URL
Replay a session token harvested from a referrer log.

User Enumeration
Harvest a verified customer list from a login form.

Vertical Privilege Escalation
Forge a role claim and become an administrator.

Weak Randomness
Predict a password-reset token and take the account.

XXE Injection
Read the password file through an XML upload.

Weak Password Hashing
A stolen hash table is only safe if the hashing is.

Checkout Workflow Bypass
Skip the payment step, ship the order anyway.

Insecure Deserialization
An uploaded backup that runs the attacker's code.

Fail-Open Refund Check
Make the risk check fail, and the refund pays out.

OWASP Top 10 for API Security 10

Broken Function Level Authorization
Call staff-only endpoints from a read-only account.

Broken Object Level Authorization
Swap an id and read another rider.

Broken API Authentication
Brute-force a six-digit login code.

Excessive Data Exposure
Read the fields the UI never shows.

Improper Inventory Management
Read records through a retired API version.

Injection
Turn a search box into a full database read.

Insufficient Logging & Monitoring
Look up a customer and leave no trace.

Mass Assignment
Mint a loyalty balance with two extra keys.

Security Misconfiguration
Read a signed-in account from any website.

Unrestricted Resource Consumption
Scrape a catalog with one oversized request.

OWASP Mobile Top 10 13

Improper Credential Usage in Mobile Apps
Every install of the app carried the company's SMS gateway key.

Inadequate Mobile Supply Chain Security
An SDK update the team never chose shipped inside their app.

Unsigned Over-the-Air Updates
An update nobody signed reached every user at launch.

Biometric Unlock Without Crypto
The fingerprint check said yes without anyone touching it.

Insecure Mobile Authentication/Authorization
The app said he was staff, and the API believed it.

Insufficient Input/Output Validation in Mobile Apps
A link decided who got paid, and the user never saw it.

Exposed WebView Bridge
A help article's widget could read the user's session.

Insecure Mobile Communication
The app trusted any certificate, so anyone on the Wi-Fi could read it.

Inadequate Mobile Privacy Controls
Users' health data was sitting in a crash dashboard.

Insufficient Mobile Binary Protections
Someone rebuilt the app and gave themselves free rewards.

Mobile Security Misconfiguration
The release build still shipped its debug menu.

Insecure Mobile Data Storage
A second-hand tablet still held a working session.

Insufficient Cryptography in Mobile Apps
The backups were encrypted with a key every copy of the app shared.

Git & CI/CD Security

Treat the repository and the pipeline as security boundaries. Pull secrets out of commit history, poison a build, abuse a runner, then lock the default branch and the deploy path down.

Git & Repository Security 8

Secrets in Git History
Recover a live API key from the commit that removed it.

Exposed .git Directory
Rebuild an entire codebase from one public URL.

Committed Secret Files
Clone a public repo and read its committed .env.

Commit Author Spoofing
Land a backdoor wearing a maintainer's name.

Branch Protection Bypass
Force-push over main and skip review and CI.

Leaked Access Tokens
Clone private repos with a token from a public gist.

Malicious Pull Requests
Catch a backdoor hidden inside a friendly test fix.

CI/CD Secret Exposure
Lift a deploy key straight out of a public build log.

OWASP Top 10 CI/CD Security Risks 10

Insufficient CI/CD Flow Control Mechanisms
Branch protection means nothing if a deploy skips the pipeline.

Inadequate CI/CD Identity and Access Management
The contractor was offboarded. Their CI token never was.

Dependency Chain Abuse
The name was exactly right. The registry it came from was not.

Poisoned Pipeline Execution
The workflow was correct. A lint config ran the attacker's code.

Insufficient Pipeline-Based Access Controls
A repository secret is in every job, including a stranger's pull request.

Insufficient CI/CD Credential Hygiene
One key, everywhere, and nobody can say what rotating it breaks.

Insecure CI/CD System Configuration
Job two inherits whatever job one left on the runner's disk.

Ungoverned Usage of Third-Party Services
A trial from two years ago still reads every private repo.

Improper Artifact Integrity Validation
The artifact that deployed was not the artifact that was built.

Insufficient CI/CD Logging and Visibility
The pipeline is where code becomes production, and it logged almost nothing.

Cloud Security

Treat the account, the image and the cluster as security boundaries. Read a bucket nobody meant to publish, escape a privileged pod, take over a cluster through RBAC, then gate Terraform with policy as code.

Cloud Infrastructure Security 9

Public Storage Buckets
List a bucket with no credentials and take the customer export.

Over-Permissive IAM
Escalate a boring build credential into a full administrator.

Long-Lived Access Keys
Replay a key that leaked months ago and still authenticates.

Instance Metadata Abuse
Turn a URL-fetching feature into cloud credential theft.

Cloud Network Exposure
Connect straight to a production database with no application in the path.

Subdomain Takeover
Serve your own login page from a domain the company really owns.

Audit Logging Gaps
Investigate an incident where the trail covered one region and the intruder deleted the rest.

Serverless Over-Privilege
Drive a public function URL into an account-wide role.

Multi-Account Boundaries
Walk a sandbox credential into production, then put a ceiling above the account.

Container & Image Security 8

Secrets in Image Layers
Read a live token out of a layer the build tried to clean up.

Privileged Containers
Turn a shell in a container into root on the host.

Exposed Docker Daemon
Take a production host through an unauthenticated Docker API.

Vulnerable Base Images
Exploit a CVE in the OS layer nobody audits.

Malicious Base Images
Trace a cryptominer back to one line in a Dockerfile.

Container Registry Exposure
Pull a private image, then replace the tag they deploy.

Container Network Exposure
A port mapping puts a production database on the internet.

Minimal Container Images
Cut a 412MB runtime down to what actually has to ship.

OWASP Kubernetes Top Ten 13

Insecure Kubernetes Workload Configurations
One privileged pod, and the whole node is open.

Overly Permissive Kubernetes Authorization
One temporary cluster-admin binding, and a contractor reads payroll.

Kubernetes Secrets Management Failures
The Secret was locked down. Its value was in a crash log.

Lack of Cluster Level Policy Enforcement
Move the tag, and production pulls it on its own.

Missing Kubernetes Network Segmentation
One web pod, and every internal service is in reach.

Overly Exposed Kubernetes Components
No credential needed: the cluster answers anyone.

Misconfigured and Vulnerable Cluster Components
The API server was locked. The kubelet was not.

Cluster-to-Cloud Lateral Movement
A pod takes the node's cloud identity and walks out of the cluster.

Broken Authentication in Kubernetes
A pod that never calls the API still carries a key to it.

Outdated and Vulnerable Cluster Add-ons
An ingress controller nobody upgraded reads every Secret.

Inadequate Kubernetes Logging and Monitoring
A miner ran for weeks because nothing was watching.

Unsigned Container Images
Every gate passed. None checked the base image.

Exposed etcd Backups
One snapshot, and the whole cluster's Secrets are readable.

Infrastructure as Code Security 7

Policy-as-Code Gate
A gate nobody can bypass, or it is only advice.

Terraform Blast Radius
A rename plans one line of destroy, and the apply runs it.

Terraform Drift
Close the port in the console, and the next apply reopens it.

Terraform Plan Leaks
The plan printed a database password in a public comment.

Secrets in Terraform State
The password is in no .tf file. The state file still has it.

Untrusted Terraform Modules
A module pinned to a branch can change under you.

Untrusted Terraform Plan
A plan runs code, and CI runs plan with full credentials.

Reinforced by microlearning

Between modules, short drills keep the same instincts sharp. Each one is a 2-4 minute attack in a real format, sent on a schedule or right after someone clicks a simulation.

Email phishing 2 min
Spot the tells in a credential-harvesting email before you click.

Smishing (SMS) 2 min
Catch the courier-impersonation text hiding in a normal phone inbox.

Vishing (voice call) 3 min
Hear out a caller who wants your MFA code, and choose when to hang up.

Chat (Teams / Slack) 3 min
Read a chat from an outside account posing as internal support.

MFA fatigue 2 min
Approve or deny a flood of MFA prompts you never started.

Quishing (QR code) 2 min
Decide whether to scan a pay-here QR code stuck on a meter.

Fake login page 2 min
Inspect a pixel-perfect Microsoft sign-in clone before you type.

AI chat data-leak 3 min
Use a public AI assistant without pasting in data it should never see.

Attack chain 4 min
Track one BEC scam as it jumps from email to text to a phone call.

OAuth consent 2 min
Read a consent screen before you grant an app full access to your mail.

Malicious attachment 2 min
Check an overdue-invoice attachment before you open it.

Social media / OSINT 3 min
Find what a cheerful first-day post hands an attacker.

Deepfake 3 min
Tell a real executive recording from an AI-generated one. Coming soon.

And a two-minute lesson in Slack or Teams, every working day

Drills teach people to spot an attack. Chat lessons make sure they keep doing it. Short lessons and 30-second spot-it checks land in the chat app your team already has open, and they start and finish right there: no login, no course to open.

On your schedule. Every working day, twice a week or monthly, each person in their own timezone, with daily and weekly limits.

Just in time. Clicked a phishing simulation? A 60-second lesson on that exact lure arrives within minutes.

Report to Security. One click on any suspicious message sends it to your security team.

Recorded like any exercise. Completions show in reports and exports and count toward the Human Risk Score.