HORIZONSHIELD

Securing Your Digital Future, Today.

HUMAN RISK SERIES · BOOK 12 OF 16

Social Engineering Defence Guide

Human Hacking — Awareness, Defence & Simulation 2026

Understand and defend against the full spectrum of social engineering: phishing, vishing, smishing, pretexting, and physical intrusion. Includes security awareness programme design and phishing simulation frameworks.

ATTACK TYPES	AWARENESS MODULES	SIMULATION TYPES
15+	8	5

LEVEL

All Levels

Contents

SOCIAL ENGINEERING DEFENCE 2026

CHAPTER 01

Psychology of Social Engineering

Attackers exploit predictable human psychology, not just technical vulnerabilities. Understanding the attack is the first step to defence.

CIALDINI | COGNITIVE BIAS | TRUST EXPLOITATION | HUMAN FACTORS

The Psychology Behind Every Social Engineering Attack

Robert Cialdini's six principles of influence provide the psychological foundation for social engineering. Attackers weaponise these natural, adaptive human tendencies at industrial scale — because they reliably work.

Principle	How Attackers Exploit It	Real Attack Example	Defence
Authority	Impersonate CEO, IT, HMRC, police, legal counsel	CEO Fraud: "This is your CEO — I need an urgent wire transfer processed today, I am in a meeting and cannot call"	Verbal verification policy. Never process financial requests based solely on email.
Urgency / Scarcity	Create time pressure to bypass rational decision-making	IT Support: "Your account will be suspended in 2 hours — click here to verify your identity immediately"	Slow down when pressure is applied. Urgency is a manipulation tactic, not a reason to bypass process.
Social Proof	Reference colleagues or trusted institutions	Vendor Invoice Fraud: "As discussed with your CFO, please use the new bank account details"	Verify any references independently via known contact methods — not numbers provided in the message.

Principle	How Attackers Exploit It	Real Attack Example	Defence
Reciprocity	Offer help before making the ask	Tech Support Scam: Fix a fake problem on the computer, then request AnyDesk access "to install the fix"	Unsolicited help from unknown parties is a manipulation attempt, not generosity.
Liking / Similarity	Build rapport, reference shared connections, match communication style	LinkedIn research: "Hi John — I met you at the Security Summit last March. I need a quick favour..."	Familiarity in professional context does not equal legitimacy. Verify identity independently.
Commitment	Get small yes before larger ask — foot-in-the-door	Establish rapport over multiple contacts before requesting sensitive information or action	Be alert to escalating requests. Early commitments do not obligate compliance with later asks.

High-Value Social Engineering Targets

Target	Why High-Value	Common Attack	Defence
Finance staff	Authorise payments, access banking platforms	BEC wire fraud, fake vendor invoice update	Dual-authorisation for any wire > $10K. Verbal confirmation policy.
IT helpdesk	Can reset passwords, create accounts, grant access	Call as executive: "I need my password reset immediately, I am locked out before a critical meeting"	Identity verification protocol. Never reset via voice call without verification code.
HR staff	Access payroll, employee PII, can process requests	Payroll diversion: email from "employee" to change direct deposit account	Verify ALL direct deposit changes via a separate authenticated channel to the employee.
Executive assistants	Calendar access, can act on behalf of C-suite	Targeted spear phishing with CEO travel schedule details from LinkedIn	Need-to-know information sharing. Verify any unusual requests from executives.
New employees	Unfamiliar with processes, eager to help, unsure what is normal	"Hi, this is IT support — as part of your onboarding we need your temporary password"	Security onboarding: first day training on social engineering attacks. Specific IT process documentation.

THE WEAKEST LINK FALLACY

People are not the weakest link — they are the last line of defence when technical controls fail. Blaming users for social engineering incidents is counterproductive and demoralising. The goal is to build systems where the secure path is the easy path, and to give people the knowledge and permission to say NO to unusual requests without fear of career consequences.

CHAPTER 06

Security Awareness Programme Design

An effective security awareness programme changes behaviour, not just knowledge. Compliance-focused training fails to reduce incidents.

BEHAVIOUR CHANGE | TRAINING | PHISHING SIMULATION | METRICS

Security Awareness That Changes Behaviour

1

Baseline Assessment

MONTH 0 — BEFORE TRAINING

Run phishing simulation before any training to establish baseline click rate. Survey staff on security knowledge gaps. Review past incident data for recurring human factors. This baseline measures actual improvement, not self-reported knowledge.

2

Content Development

MONTH 1

Develop training content for your specific threat profile. Generic compliance training fails — content must reference real incidents that match your industry and threat landscape. Formats: video (5 minutes max), interactive scenarios, in-person workshops, posters, monthly security tips.

3

Delivery & Reinforcement

MONTHS 2-12

Annual compliance training is not a security programme — it is a compliance checkbox. Effective awareness requires monthly touchpoints: monthly phishing simulations, quarterly short training modules (5-10 minutes), bi-annual in-person workshops, security incident debrief communications after real incidents.

4

Measure & Improve

4

ONGOING

Track: phishing simulation click rate (target < 5%), report rate (target > 30%), training completion rate (target 100%), security incidents attributed to human factors. Use improvement data to brief leadership and justify programme budget.

Training Module	Delivery Format	Duration	Frequency	Key Outcome
Phishing Recognition	Simulated phishing + instant education page for clickers	Ongoing	Monthly simulation + immediate training for failures	Reduce click rate from ~25% to <5% within 6 months
Password & MFA Security	Video + interactive quiz	8 minutes	Annual + when new policy introduced	100% MFA adoption, password manager usage
Social Engineering Scenarios	Role-play scenarios + video examples	15 minutes	Quarterly	Employees able to identify and report SE attempts
Data Classification & Handling	Interactive with real business data examples	10 minutes	Annual	Correct classification and handling of sensitive data
Working Remotely Securely	Short video series (5 parts, 3 min each)	15 minutes total	Annual + for new remote workers	VPN usage, screen privacy, home WiFi security
Incident Reporting Culture	Short video + in-person discussion	20 minutes	Annual + after incidents	Removal of fear around reporting — "no blame" culture

HS

H O R I Z O N S H I E L D

Securing Your Digital Future, Today.

Social Engineering Defence Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.