YOUR PEOPLE ARE THE TARGET

A security aware workforce protects the enterprise.
Build readiness before attackers test your defenses

Simulate | Measure | Train | Prove It

91%
of breaches start with a phishing attack

Real
attack scenarios - not generic test emails

Proven
reduction in human risk - measurably, over time

THE REALITY

Attackers Don’t Hack Systems Anymore, They Manipulate Human Assets

Perimeter defenses, firewalls, and endpoint tools protect your infrastructure. But no technology canprevent an employee from clicking a convincing link, submitting credentials on a fake login page, orapproving a fraudulent request.

Attackers know this. That's why social engineering now leads the majority of successful breaches and why security awareness training that happens once a year, in a classroom, simply doesn't change behavior under real attack conditions.

Risk Is Invisible Without Measurement

Without simulation, you have no idea which teams, roles, or individuals carry the highest human risk in your organization.

Awareness Alone Isn't Enough

A policy document or annual training session doesn't prepare employees for the convincing, context-aware attacks they face today.

People Are The Primary Target

Attackers specifically craft campaigns to exploit human trust, urgency, and authority not technical vulnerabilities.

THE SOLUTION

TechOwl Phish Shield - turn your employees into the strongest shield of your organization.

TechOwl Phish Shield is an intelligent phishing simulation and human risk management platform. It goes beyond awareness training to continuously test, measure, and improve how your people respond to real-world social engineering attacks. Every simulation is an opportunity to identify risk before attackers do and every failure becomes an immediate, targeted learning moment that changes behavior for good.

01

SIMULATE

Launch realistic, targeted phishing campaigns tailored to your teams, roles, and the tactics attackers actually use.

02

MEASURE

MEASURETrack susceptibility by person, team, and department. See where your human risk actually lives, not where you assume it does.

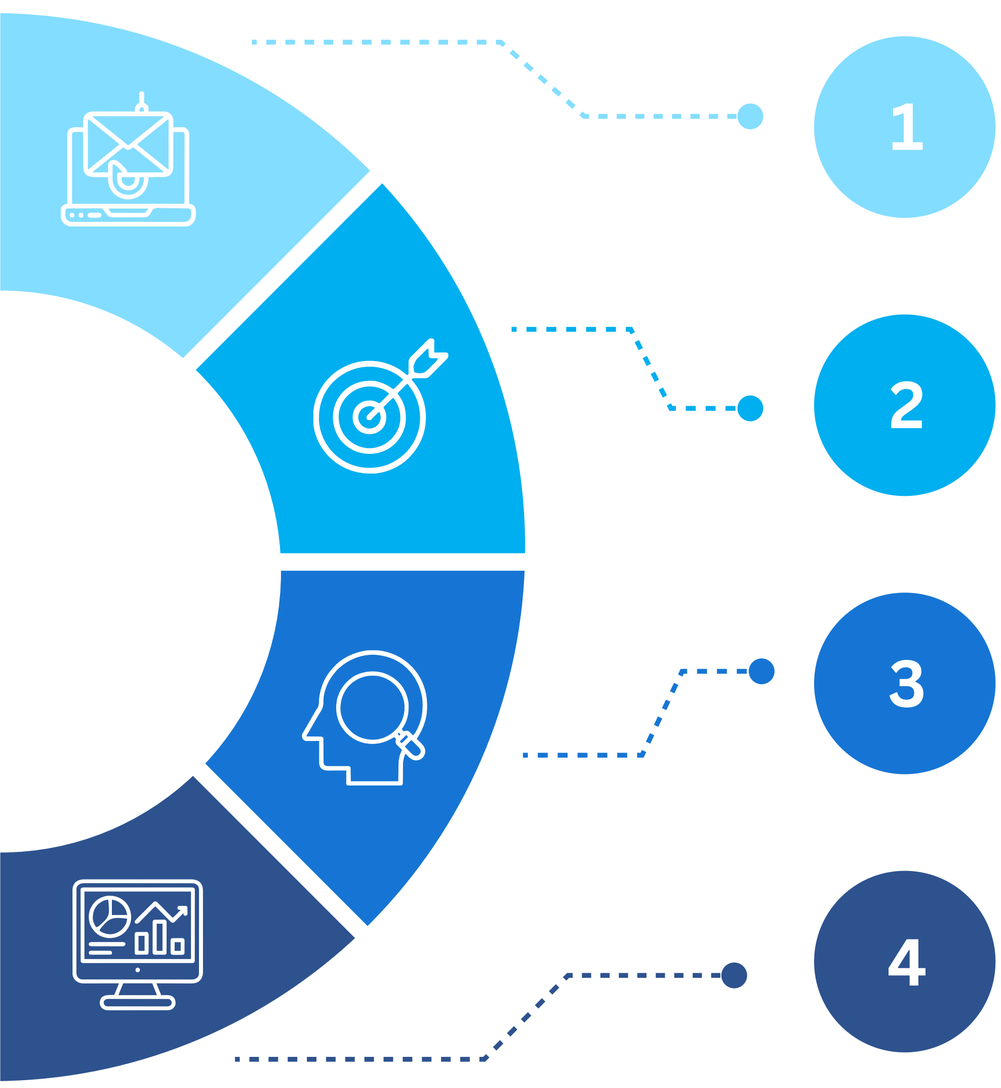
03

IMPROVE

Trigger instant, targeted micro-learning the moment someone fails, turning every mistake into a behavior change that sticks.

PLATFORM CAPABILITIES

Everything You Need to Manage Human Risk



Advanced Simulation Engine

Realistic campaigns covering spear-phishing, credential harvesting, brand impersonation, and attachment-based attacks — built around the techniques your adversaries actually use today.

Instant Adaptive Training

When someone fails a simulation, Phish Shield automatically delivers a targeted micro-learning module - role-specific, threat-specific, and timed exactly when attention is highest.

Human Risk Intelligence

Move beyond click rates. Phish Shield scores behavioral risk at the individual and department level — revealing your real exposure, not just your average awareness score.

Executive Risk Dashboard

Board-ready reporting that tracks risk reduction over time, campaign performance, and awareness maturity giving leadership clear evidence that the program is working.

SIMULATION REALISM

Built Around How Attackers Actually Operate

Generic phishing tests don't prepare your team for the real thing. Phish Shield simulations are built around current attacker playbooks — so your employees face the same tactics, pressure, and deception they'd encounter in an actual attack.

Invoice Fraud

Urgent payment requests from spoofed vendors or finance contacts.

MFA Fatigue

Repeated push notification attacks designed to wear down approval resistance.

Credential Reset Scams

Fake IT or security alerts demanding immediate password or access verification.

HR Impersonation

Payroll, benefits, or policy notifications crafted to extract sensitive information.

Vendor Compromise

Trusted third-party lookalike campaigns that exploit supply chain relationships.

BUSINESS OUTCOMES

What Changes When Human Risk Is Managed

Fewer Security Incidents Originating From People

Identifying and correcting risky behavior before attackers exploit it directly reduces breach exposure.

Visibility Into Your Highest-Risk Individuals And Teams

Know exactly where to focus attention and prove that targeted intervention is working over time.

A Measurable Security Culture, Not Just Policy

Employees trained through repeated simulation develop genuine security instincts, not just compliance habits.

Security That Runs Continuously, Not Annually

Automated campaign scheduling means your workforce is always tested — without any operational overhead.

Clear Evidence For Auditors, Boards, And Regulators

Campaign reports, risk scores & improvement trends give you documented proof that human-layer controls are active & improving.

Faster Threat Recognition Across The Organization

People who've been simulated recognize suspicious patterns faster — because they've seen them before, safely.

PRECISION TARGETING

The Right Campaign, for the Right Person, at the Right Time

Not every team carries the same risk. Finance is targeted differently than IT. A new hire faces different threats than a senior executive. Phish Shield lets you design campaigns that reflect these realities — so your simulation program is as precise as the attacks it prepares people for.

By Department

Finance, HR, IT, Legal — each team gets scenarios relevant to their role and risk exposure.

By Designation

Executives, managers, and frontline staff face appropriately calibrated simulation difficulty.

By Geography

Regional or country-specific campaigns that reflect local threat context and language.

By Risk Profile

High-risk individuals and repeat clickers receive increased simulation frequency and intensity.

GOVERNANCE & COMPLIANCE

Proof That Your Human Layer Is Under Control

Regulators and auditors are no longer satisfied with awareness training policies. They want evidence — that employees are tested, that risk is tracked, and that your program demonstrably improves over time. Phish Shield generates exactly that evidence.

Compliance Support

- Employee Security Awareness Validation
- Social Engineering Resilience Evidence
- Security Control Effectiveness Testing
- Incident Preparedness Maturity Documentation
- Risk Reduction Tracking And Reporting
- Awareness Program Accountability Records

Governance Value

- Demonstrates Active, Continuous Human-Layer Testing
- Provides Documented Evidence Of Risk Reduction
- Satisfies Regulators That Awareness Is Measurable
- Supports BFSI, Healthcare & Regulated Sector Audits
- Moves Security Culture From Policy To Proof
- Shows Boards That Human Risk Is Actively Managed

Documented policy alone is no longer considered sufficient. Regulators increasingly expect measurable evidence of effectiveness.

WHY PHISH SHIELD

Beyond Generic Awareness - What Makes the Difference

Most organizations run some form of security awareness program. Very few can measure whether it actually changes behavior under real attack conditions. That's the gap Phish Shield closes.

NO.	CAPABILITY	TRADITIONAL AWARENESS	TECHOWL PHISH SHIELD
1	Annual awareness training only	✗	✓
2	Generic phishing test emails	✓	✓
3	Spear-phishing & targeted simulation	✗	✓
4	Behavioral risk scoring per user	✗	✓
5	Departmental exposure heatmaps	✗	✓
6	Immediate micro-learning on failure	✗	✓
7	Threat-aligned simulation templates	✗	✓
8	Risk trend tracking over time	✗	✓
9	Board-ready compliance reporting	Limited	✓
10	Campaign scheduling automation	✗	✓

SERVICES

Part of TechOwl SHIELD Platform

TechOwl SHIELD
Attack Surface Monitoring

TechOwl DMARC SHIELD
Email Trust Assurance

TechOwl VendorShield
Third-Party Risk Intelligence

TechOwl CloudShield
Cloud Security Visibility

TechOwl PhishShield
Employee Risk Readiness

TechOwl ThreatPulse
Threat Signal Intelligence

TechOwl THREATLAB
Advanced Threat Detonation

Validate Trust Before Attackers Exploit It.

TechOwl Phish Shield transforms awareness into measurable defense - so you know your people are ready when it matters most.

sanchita@techowl.com