PENTESTERRA
SEE THE REAL RISK

ATTACK | VALIDATE | STRENGTHEN

HUMAN RISK
REAL IMPACT
LOWER EXPOSURE

PHISHING SIMULATION MODULE

Real-World Phishing. Real Insights.

Test. Measure. Educate. Reduce Risk.

Run realistic phishing simulations to see how your people respond — and turn the results into actionable security improvements.

REALISTIC TEMPLATES
Modern, convincing scenarios

MEASURABLE RESULTS
Clicks, opens, macro-enabled doc interactions

EASY TO RUN —
From small teams to large enterprises

STRONGER PEOPLE
Reduce human risk over time

SOCIAL ENGINEERING STILL WORKS. BE PREPARED.

MULTI-VECTOR ATTACK TEMPLATES

Go beyond simple emails. Simulate the attacks that work in the real world.

Email Lures
Convincing, up-to-date templates

Macro Documents
Word / Excel with real macros (Document_Open)

PDF with JavaScript
Interactive PDFs with launch URL (Adobe Reader)

Link Tracking
Full click tracking and redirect control

Custom Templates
Create your own or use our library

TEMPLATE LIBRARY

Ready-to-use and customizable templates for any scenario.

Microsoft 365
Password Expiry
You need to update your password to continue using Microsoft 365.
Use Template

DHL
Delivery Notification
Your package is on hold. Please confirm delivery details.
Use Template

DocuSign
Document for Signature
You have a document waiting for your review and signature.
Use Template

Build Your Own
Create realistic lures tailored to your organization.
Use Template

PEOPLE & TARGETING

Choose who, how and when.

- Upload via CSV or sync from directory
- Target specific departments or roles
- Personalize with real data (name, company, role)
- Schedule and automate campaigns
- Auto-retry for non-delivered emails

DETAILED ANALYTICS

See the full picture, not just clicks.

- Delivery, open and click rates
- Attachment opened / macro enabled
- Submitted data (credentials, forms)
- Timeline and user-level details
- Export reports (PDF / CSV)

AWARENESS & IMPROVEMENT

Turn results into a stronger security culture.

- Identify high-risk users and groups
- Track progress over time
- Support targeted training and education
- Measure the impact of your security program
- Reduce risk with real behavioral data

HOW IT WORKS

1. **Select Targets** — Upload or choose from directory
2. **Choose Template** — Use library or create custom
3. **Launch Campaign** — Schedule or send now
4. **Track & Analyze** — Real-time results and detailed reports
5. **Improve** — Train, repeat, reduce risk

HUMAN AWARENESS IS A SECURITY CONTROL.

START A CAMPAIGN →

PEOPLE
PROCESS
TECHNOLOGY
STRONGER TOGETHER

PENTESTERRA

PHISHING & SOCIAL ENGINEERING SIMULATION

Phishing Tests That Use What an Attacker Would Actually Know

Real attackers research the target first. Pentesterra builds each scenario from OSINT - role, tooling, projects, and personal interests - then carries a successful phish into the attack chain to show impact, not just a click percentage.

OSINT

Every scenario is context-built, not templated

1:1

Spear-phishing against named, researched targets

Chain

A captured credential continues the attack

WHY THIS CONVERTS BETTER

Pentesterra's OSINT layer gathers more than a person's role and employer - it collects their public interests, hobbies, and recent social posts (opt-in). A pretext that references an actual hobby, a recent conference talk, or a side project the person posted about converts dramatically better than a generic "reset your password" email, because it reads as personal, not mass-sent. That's the same personalization a real attacker researches by hand; Pentesterra automates it so the simulation measures the real risk, not a lucky guess.

WHY NOW

Last year's awareness training had a 90%+ completion rate, and nobody remembers a word of it. One convincing email is still the fastest way into most companies. A generic simulated phish measures almost nothing close to what a real, researched attacker would actually send.

HOW IT WORKS

Context-Aware, Not Template Spam

Scenarios are built from real OSINT: the person's role, projects, tooling, public professional context, and personal interests. A pretext grounded in something the target actually cares about converts very differently from a generic blast.

- → Role-aware and department-aware targeting
- → Pretexts grounded in gathered company and people intelligence, including interests and hobbies
- → Spear-phishing against named high-value targets, not just broad blasts
- → Reuses the same intelligence layer as pentest and reporting

Full Campaign Toolkit

Sending profiles, landing pages, a templates library, and scheduling in one place. Build a campaign, pick the target list, choose the lure, and launch - with per-recipient tracking from delivery to credential submission.

- → Landing pages and credential-capture flows (non-destructive)
- → Sending profiles with domain and header control
- → Reusable template library across campaigns
- → Open, click, and submit tracking per recipient

Human Risk as a Measured Control

Phishing simulation is a security control test, not an HR exercise. Results feed the same risk model as technical findings, so "the human layer" stops being a blind spot in the report.

- → Click and submission rates by team, role, and seniority
- → Repeat campaigns to measure drift over time
- → Ties into awareness-training follow-up
- → Evidence suitable for compliance and audit

Part of an Attack Chain, Not a Silo

A captured credential or session is an artifact. Pentesterra can carry it into the next step - internal access, lateral movement, business impact - so a successful phish is shown as a full path, not an isolated statistic.

- → Credential and session artifacts feed the attack chain engine
- → Shows what a real attacker does after the click
- → Cross-references with external exposure and network findings
- → One report covering people plus infrastructure

FREQUENTLY ASKED QUESTIONS

How is this different from a generic phishing simulator?

Generic simulators send templated emails and count clicks. Pentesterra builds each scenario from OSINT about the target - their role, tooling, projects, and personal interests - and then carries a successful phish into the rest of the attack chain to show real impact, not just a click rate.

Is credential capture safe to run against real employees?

Yes. Capture flows are non-destructive and scoped: no real authentication happens, credentials entered on the landing page are recorded as an event and not stored as usable secrets, and every campaign has an explicit target list and schedule.

Can it do targeted spear-phishing, not just bulk campaigns?

Yes. You can run broad awareness campaigns or targeted spear-phishing against named high-value individuals, with pretexts tailored to each person - down to their real interests and public activity - from the intelligence layer.

Does phishing simulation connect to the rest of the platform?

Yes. It shares the OSINT intelligence layer with the pentest and reporting modules, and a captured credential or session becomes an artifact the attack chain engine can use in subsequent steps.

Launch your first campaign

Scenarios built from real OSINT on your own organization.

info@pentesterra.com
pentesterra.com/phishing-simulation