SOCIAL ENGINEERING

Harden Your Human Perimeter—Stop Social Threats Before They Disrupt Your Business

Technology no longer decides whether an attacker gets in. People do.

AI-generated voice calls, deepfake video, and hyper-targeted phishing have turned employees, contractors, and front-desk staff into the easiest, fastest path into your environment. One convincing pretext now bypasses:

- Email gateways and endpoint tools
- Segregated networks and MFA policies
- Policy binders and awareness "check-the-box" training

Regulators, auditors, and boards now look directly at how well your human controls actually work—not how often users completed training.

When human controls are untested, external reviewers treat them as a blind spot. After an incident, the questions are simple and unforgiving:

- Did you test your people and processes against realistic attacks?
- Can you prove it with metrics, evidence, and corrective actions?

If the answer is no, even a well-designed security stack and training program can still fail where it matters most: in the moment a person decides to trust or challenge a request.

eSurelTy's Social Engineering Assessments exist to change that answer.

How eSurelTy Changes the Conversation With Attackers and Reviewers

Most organizations approach social engineering as a training problem. Attackers treat it as a campaign.

eSurelTy aligns your side with theirs: targeted, persistent, data-driven. Our Social Engineering Assessments are built to:

- Mirror how real adversaries research, plan, and execute campaigns
- Test people, process, and physical controls in one integrated program
- Tie every finding to measurable business risk and operational impact

You move from "we trained our users" to "we tested our defenses, fixed the gaps, and can prove it."

The Human Attack Surface Is Now the Weakest Link

Attackers now operate at scale with AI-enhanced deception:

- Synthetic voices that mimic executives and vendors
- Deepfake videos and spoofed collaboration invites
- Phishing and smishing tailored to specific roles and workflows

A single misstep can:

- Expose credentials and data
- Circumvent payment and approval workflows
- Trigger regulatory and contractual reporting
- Erode customer, partner, and board confidence in your controls

Independent assessors increasingly expect evidence that human-factor controls have been tested under realistic, adversary-style conditions—not just trained in a classroom.

eSurelTy's framework quantifies human risk across email, voice, text, and physical entry, generating the proof auditors and oversight bodies expect.

How We Simulate Attacks To Strengthen Your Defenses

Red team specialists conduct controlled, ethical attack simulations modeled on current attacker tradecraft. Each engagement is tuned to your industry, regulatory obligations, and risk profile.

Our methodology includes:

- Recon & Profiling
  - Targeted intelligence gathering from public and internal sources to craft realistic phishing, vishing, and pretexting campaigns against high-impact roles.
- Multi-Vector Simulations
  - Coordinated use of email, SMS, phone, collaboration tools, and web lures to stress-test layered defenses, escalation paths, and reporting channels.
- Physical Breach Drills
  - Onsite testing of tailgating, badge cloning, visitor management, and front-desk procedures to validate how well the "last mile" of security holds up.
- AI-Enhanced Deception
  - Synthetic voices, spoofed domains, and deepfake-style visuals used to test resilience against advanced social engineering that bypasses "gut feel."

Each campaign is documented with response metrics, risk scoring, and corrective actions mapped to NIST 800-53, ISO 27001, and HIPAA-aligned human control requirements.

Contact Us
info@eSurelTy.com
www.eSurelTy.com

Measurable Human Risk Reduction, Not Generic Training Stats

You receive actionable visibility into how your people and controls behave under pressure—not vanity metrics.

Deliverables may include:

- **Employee Susceptibility Scores**
  - Benchmarks by user, role, and department across phishing, smishing, and vishing attempts.
- **Behavioral Risk Analytics**
  - Clear view of who clicked, who complied, who reported, and who ignored, tied to specific scenarios and timelines.
- **Physical Security Gap Analysis**
  - Assessment of door controls, reception and visitor handling, badge usage, and how staff respond to on-site pretexts.
- **Training and Policy Roadmap**
  - Targeted awareness, procedural, and control improvements prioritized by business risk and oversight expectations.
- **Executive-Ready Reporting**
  - Summaries designed for board decks, audit packets, and to satisfy typical cyber insurance coverage requirements for demonstrating that human-factor controls have been realistically tested.

What We Test

A comprehensive suite covering human and physical vectors where attackers most often succeed.

- **Email Phishing and Spear Phishing -** Custom lures targeting high-value users in finance, HR, IT, and executive roles.
- **Smishing and Vishing -** SMS and voice-based impersonation of vendors, leadership, banks, and service providers.
- **Physical Impersonation and Onsite Intrusion -** Tailgating, badge cloning, fake visitors, and contractor pretexts to test real-world access control.
- **Removable Media and USB Testing -** Device drop exercises and controlled malware simulations to identify unsafe behaviors and process gaps.
- **Web and Application Deception -** Watering-hole pages, cloned portals, and spoofed login screens designed to capture credentials or trigger unsafe actions.
- **Dumpster Dive and Paper Trail -** Validation of shredding, disposal, and document-handling practices for sensitive information.

Each vector is selected and scoped to reflect your actual risk profile and regulatory environment.

The outcome is a defensible, metrics-backed narrative of your human and physical security posture.

Why Organizations Choose eSurelTy

- **Risk and Governance Alignment:** Testing and reporting structured around what boards, auditors, and regulators need to see to understand and challenge human-factor risk.
- **Certified Red Team Operators:** CISSP, CEH, OSCP, CISA, and other certified professionals leading each engagement with consistent, repeatable methodology.
- **U.S.-Based Operations:** All testing performed domestically to support data sovereignty, privacy, and sector-specific requirements.
- **25+ Years in Regulated Industries:** Deep experience across healthcare, financial services, energy, and utilities where regulators and auditors scrutinize human controls.
- **Flexible Engagement Models:** Full-scope social engineering programs, focused micro-tests, or quarterly simulation campaigns that align with budget and audit cycles.

Run the same plays attackers run—on your terms, with your data, and with clear evidence of how your people and processes perform under pressure.

Schedule a focused 15-minute consultation with eSurelTy to scope your Social Engineering Assessment and get an initial view of your highest human and physical exposure points.

Contact Us

info@eSurelTy.com

www.eSurelTy.com