

Social Engineering

Sprocket Security | Continuous Offensive Security Platform



Humans are the largest risk to your business — assess how they respond before attackers exploit it.

74%

of breaches involve the human element.
Verizon Data Breach Investigations Report, 2023

No firewall stops a convincing phone call. No spam filter catches every well-crafted spear phishing email. Social engineering attacks bypass your entire technical security stack by targeting the one thing it can't patch - human behavior. Sprocket's Social Engineering service tests your people the same way real attackers do, and gives you the data to make them more resilient.

SCOPE COVERED

Phishing

Spear Phishing

Vishing / Voice

Pretexting

Credential Harvesting

Malware Delivery Simulation

Security Awareness Validation

Post-Exploitation Impact Demonstration

Key Capabilities

Phishing & Spear Phishing Campaigns

Sprocket designs multi-wave email campaigns using custom pretexts, spoofed sender identities, and cloned login pages built from public OSINT about your organization. Campaigns are specifically engineered to bypass email gateways and spam filters, and track clicks, credential submissions, and simulated malware execution at the individual level.

Vishing (Voice Phishing) & Pretexting

Testers conduct phone-based campaigns impersonating IT support staff, software vendors, executives, or other trusted figures attempting to trick employees into revealing credentials, approving password resets, or granting unauthorized system access. Every call is documented with outcome evidence.

Post-Exploitation Impact Demonstration

When employees fall victim, Sprocket doesn't stop at the click - they demonstrate the full downstream impact. This includes credential reuse against company resources, privilege escalation, and lateral movement inside the internal network, giving leadership a concrete picture of what a real breach would cost.

Why It Matters



Business Risk

Attackers target your employees every day with increasingly convincing pretexts. A single credential submission on a phishing page can be the starting point for a full network compromise and your technical controls won't stop it if the human says yes.



Compliance Driver

HIPAA Security Rule, PCI DSS v4, NIST 800-53, and CMMC all require organizations to regularly test and train employees against social engineering attacks as part of a complete security program.



Operational Value

Per-employee and per-department reporting identifies exactly where your human attack surface is weakest so security awareness training budgets go where they'll have the most impact, and progress can be measured through repeat campaigns over time.

ROI & Outcomes

 Campaigns conducted per engagement 4–6	 All campaigns documented with evidence 100%	 Per-department breakdown included Yes	 Post-exploitation impact demonstrated Full walkthrough included
--	---	---	---

Why Sprocket Security

- **Custom pretexts** built from real OSINT about your organization, industry, and personnel
- **Campaigns engineered to evade** email gateways, spam filters, and proxy controls
- **Per-employee and per-department metrics** to target awareness training precisely
- **Post-exploitation walkthrough** demonstrates real-world breach impact to leadership
- **Repeat campaigns** over time let you measure and prove improvement in human resilience

 Sprocket Security	Legacy / Point-in-Time
Custom pretexts built from your org's OSINT	Generic phishing templates
Multi-wave campaigns with trend data over time	Single campaign, single report
Full breach impact demonstrated	Click rate only - no post-exploitation
Per-employee and per-department breakdown	One aggregate report
Proactive - test, measure, improve, repeat	Reactive & compliance-driven

"Sprocket Security can be an extension of our team and give us the capability to stay on top of the latest vulnerabilities and attack vectors."

— IT Lead, Services Industry (Gartner Peer Insights)

