

SOCIAL ENGINEERING ASSESSMENT SERVICES

Your People Are a Target. Are They Ready?

Attackers target people because they know that social engineering works. Now, advances in AI have made these attacks easier, faster, and more convincing than ever before.

Humans often open the door to the most damaging breaches. GuidePoint Security's Social Engineering Assessment Services simulate the full spectrum of human-focused attack techniques to reveal how far a determined adversary could infiltrate an organization. GuidePoint experts deliver real-world findings to provide organizations the evidence and strategies they need to close critical gaps before real attacks succeed.

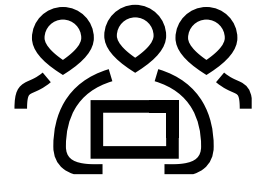
Make People the Strongest Perimeter

Attackers rely on social engineering because people are quick to trust and easy to exploit. AI has made these attacks startlingly more realistic. Social engineering attacks are evolving to become precise, convincing, and tailored to their victims. AI-powered reconnaissance enables adversaries to craft highly personalized pretexts using publicly available information and deepfake audio and video make impersonation attacks more believable than ever. And when it comes to onsite security, physical security controls mean little when an attacker simply walks in wearing a uniform and a perfectly replicated badge.

GuidePoint Security Social Engineering assessment services expose human and physical perimeter vulnerabilities before threat actors can exploit them. Highly certified GuidePoint experts use the same tactics, techniques, and approaches that adversaries use to uncover an organization's weakest links and recommend solutions to shore up defenses.

Through tailored social engineering assessments, we help organizations:

- ✓ **Understand how far a determined adversary could get** using human-focused attacks
- ✓ **Identify gaps and weaknesses** in procedures, awareness, and physical security
- ✓ **Validate employee awareness** of and resistance to social engineering attacks
- ✓ **Strengthen security awareness training** and procedural controls
- ✓ **Build the case for security investment** with evidence-based findings
- ✓ **Satisfy compliance requirements** through documented evidence of awareness tests and training



Stronger Together. Protecting What's Next.

Working with GuidePoint, your organization will be backed by our elite team of highly-trained cybersecurity engineers, architects and consultants who come from organizations of all sizes, including Fortune 100 companies, the Department of War, and U.S. intelligence agencies.



Social Engineering Assessments That Mirror Real-world Attacks

Effective social engineering assessments are built on the same methodology attackers use in the wild. GuidePoint's approach follows the full attack lifecycle, from reconnaissance and pretext development through execution and impact assessment. The team ensures that findings discovered during remote and onsite social engineering assessments reflect genuine risk and illuminate gaps in understanding, procedure, and perimeter defenses so customers can build a more resilient, attack-proof organization.



Remote Social Engineering

Attackers do not need to be in the building to compromise the organization. GuidePoint combines in-depth reconnaissance with carefully developed pretexts to simulate advanced techniques, revealing the procedural and awareness gaps that create the greatest human risk—even from a distance. Remote tactics include:

- Phishing/spear phishing, vishing, smishing, & QR code phishing
- Vendor, supplier, and internal impersonation
- Business email compromise (BEC)
- Credential harvesting, device code phishing, and browser-in-the-middle attacks
- AI deepfakes and voice impersonation
- Malicious file and link delivery

Onsite Social Engineering

Physical security controls are only as strong as the people enforcing them. GuidePoint's onsite assessments test the organization's adherence to procedural and physical security measures, revealing how far a determined attacker could get once they set foot onsite. Onsite tactics include:

- Badge cloning and access control bypass
- Dumpster diving, document acquisition, and clean desk sweeps
- Network device drops and rogue device placement
- Vendor, contractor, and employee impersonation
- Lock picking, tailgating, and covert methods of entry
- Asset and data acquisition from unsecured areas

Why GuidePoint Security

When attackers target people, human defenses matter as much as technical controls. GuidePoint's social engineering assessments are built on real-world tactics and tailored to each organization's specific environment, delivering findings that strengthen awareness, shift behaviors, and inform the processes that keep people from becoming the path of least resistance. Accelerate your business with confidence – and protect what matters most.

About Us

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow. Stronger Together. Protecting What's Next.