TEVORA

One Spectrum Pointe Drive, Suite 200
Lake Forest, California 92630
t: 949.250.3290 | **e:** info@tevora.com

SOCIAL ENGINEERING

Guarding your organization's assets can be a vast undertaking. Tevora's elite threat team combines years of industry experience with exceptional outside-the-box thinking skills and industry certifications to provide you with the answers you need. By going beyond simple automation tools testing, we can help you understand whether your current controls are effective in protecting you from external and internal threats.

SOCIAL ENGINEERING

Social engineering is one of the most prevalent attack methods used to gain unauthorized access to corporate networks. Many organizations implement policies and technical controls to combat this threat, but network intrusions through social engineering attacks are still highly successful. An effective way to mitigate this risk is to test the effectiveness of existing technical and organizational protections.

Tevora's elite threat team helps pinpoint genuine and relevant security weaknesses by educating your users on the techniques and mindset of hackers. Our services are designed to pinpoint breakdowns in protections using proven methodologies, developed over dozens of engagements, to evaluate weaknesses in organizational identification and response activities. The assessment is tailored specifically to your organizational requirements.

TEVORA SOCIAL ENGINEERING SERVICES INCLUDE:

- **Spear Phishing –** Targeted emails to designated personnel
- **Open Source Intelligence Gathering –** Information gathered from publically available sources
- **Cold-calling –** Phone-based social engineering
- **Physical –** Onsite activities to gain access

1 RECON

- Enumeration of public data regarding employees
- Mapping of target employees
- Social engineering campaign creation

2 ASSESS

- Social engineering campaign execution
- Measurement of target susceptibility to social engineering attacks, including technical controls and human error
- Impact measurement
- Leveraging foothold to gain further access to sensitive areas and data

3 REPORT

- Executive summary for management
- Detailed findings report with recommended remediation
- Retesting with validation
- Executive presentation
- Full list of raw data of email campaigns