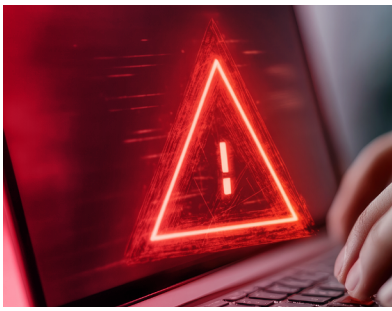
Plurilock
CRITICAL SERVICES

Social Engineering Testing Services

Simulate Social Engineering Attacks by Sophisticated Adversaries

75% of data breaches are enabled in some way by the manipulation of **human behavior.**

Most successful cyberattacks are caused by **human behavior**—by deviations from established processes and controls that undermine chains of authority, incident response, resistance to lateral movement, or safeguards against account takeovers and privilege escalation.



True-to-life, Real-world Attacks

Plurilock's social engineering testing emulates malicious attack activity more completely than traditional phishing simulation (focused on a single, primitive tactic) or penetration testing (focused on technology without evaluating behavior or defenses-in-depth).

Our service attempts to gain access to your data and systems through carefully crafted, true-to-purpose attacks on the places where technical systems and human behavior intersect.

We Don't Stop Prematurely

We don't arti icially stop and merely note a "vulnerability" once access is gained. Instead, we continue to maintain persistence and do what attackers do—attempt to achieve privilege escalation, lateral movement, or data ex iltration.

Social Engineering Tactics We May Employ

Based on research and reconnaissance about your organization, we may employ these or other social engineering techniques as we attempt to penetrate your environment.

- Business email compromise (BEC)
- Deep-fake voice or face impersonation
- Social media impersonation
- Smishing (SMS phishing), vishing (voice phishing), phone number spoofing
- Consent phishing and MFA bypass attacks
- Pretexting, malvertising, recruitment scams

Deep Fakes, Cloned Faces, Cloned Voices

Defenses against today's social engineering attacks must be ready for video and other deep fakes, containing cloned faces and voices and armed with reconnaissance for hyper-realistic social pressure or coercion.

Advanced Social Engineering Tactics

Rather than just testing resistance to phishing for training purposes, we'll work to bypass MFA, break entry and approval workflows, and gain the ability escalate privileges, move laterally, or exfiltrate data.

Plurilock's social engineering testing emulates malicious attack activity more completely than traditional phishing simulation or penetration testing.

Contact Plurilock
info@plurilock.com

Contact Us

+1 (888) 282-0696 (USA West)
+1 (908) 231-7777 (USA East)
+1 (866) 657-7620 (Canada)

Advanced cybersecurity and Zero Trust
Security assessments and consulting
IT products and solutions
Professional services
Managed services

© 2025 Plurilock

Plurilock Services

Zero Trust

Design and implementation of zero trust architectures (ZTAs)

Data Protection

Protection of intellectual property and digital assets

Identity and Access Management

Design, implementation, and integration of complete identity and access management (IAM)

Public Key Infrastructure

Design and implementation of modern public key infrastructure (PKI) deployments

Offensive Security

Security assessments and tests with a hacker mindset

Penetration Testing as a Service (PTaaS)

Managed service providing continuous penetration testing to rapidly surface emerging vulnerabilities

Data Protection as a Service (DPaaS)

Managed data protection service to operate DLP and insider threat capabilities as a service

Emergency Support

Immediate, cross functional team for urgent and high impact IT and cyber problems

Selection of current and past customers that can be publicly represented

Plurilock CRITICAL SERVICES

© 2025 Plurilock