NETSPI®

Social Engineering

Identify and minimize company risk related to the people, policies, processes, and technical controls of real-time phishing & social engineering attacks.

There were more than 4.7 million phishing attacks in 2022, growing over 150% per year since 2019 according to APWG.

NetSPI's Social Engineering offers customized email, text message, phone-based, and physical engagements that leverage sophisticated scenarios used by modern real-world adversaries. Each engagement delivers actionable findings that allow you to improve security and meet key business goals.

Email & Text Message Testing (Phishing):

Security Awareness

Emails are crafted with a target of bringing employees to an external website designed to mimic a legitimate service but with a malicious sign-in form to gain credentials, or to have employees retrieve and execute a malicious payload to exfiltrate workstation details. These are sent to a broad group to focus on larger metrics of who does or does not detect phishing emails.

Account Takeover

Emails and text messages will be used to persuade employees to take actions which could compromise their accounts such as advanced credential harvesting pages to capture MFA and session cookie details, or OAuth and device code attacks to gather authentication tokens to access APIs. Once an account is compromised, we see what information we can find and extract.

Spearphishing Campaign

In collaboration with you we will build out a customized campaign to target select users based on your specific objectives, such as capturing high-value or proprietary information. We will use an open-ended approach, identifying missing policies and edge case vulnerabilities to build an overall attack narrative.

Phone-Based Testing (Vishing):

Following an audit-based or open-ended approach, identify and minimize risk as it relates to real-time phone-based attacks designed to gain sensitive information from employees based on publicly available information, allowing you to reduce the impact of real-world attacks.

Policy Check

With a goal of gathering specific information defined by you, we place calls using a standard script and pretext throughout each scenario. These calls are siloed, with information being reported, but not leveraged for further testing.

Capture The Flag

Utilizing an open-ended approach, we target identifying missing policies and edge case vulnerabilities to gain sensitive company information. Once obtained, we leverage discovered information throughout the test to build an overall attack narrative.

Physical & Onsite Testing:

Onsite Social Engineering Assessment

Focused solely on the human component of your business, NetSPI attempts to gain unauthorized access to sensitive areas, systems, and information through employees. Testers push controls and activities until they are detected or reported by employees.

Physical Security Controls Assessment

During an onsite walkthrough, we will review the property, building perimeter, office interior, and restricted or secured areas of your business location to discover potential weaknesses or vulnerabilities and provide remediation recommendations.

Full Onsite Pentest

Determine the risk presented by real-world threat actors attempting to gain unauthorized physical access to sensitive areas, systems, and information through a variety of actions such as tailgating, manipulating door locks, badge cloning, and more.

Testing Results Delivered in NetSPI's Resolve™, PTaaS Platform

- Real-Time Reporting – Get notified of vulnerabilities in platform as they are found.
- Remediation Guidance – Vulnerabilities are delivered with remediation instructions and consultant support.
- Project Management & Communication – Effortlessly assign responsibilities, track remediation status, communicate with teams, and more.
- Track & Trend Data – Analyze findings and discover trends over time.

To learn more about NetSPI's solution offerings, visit **www.netspi.com** or contact us.

NetSPI – The Global Leader in Offensive Security

Attack Surface Management | Breach and Attack Simulation | Penetration Testing as a Service:
Application Pentesting • Cloud Pentesting • Network Pentesting • Saas Security Assessment • AI/ML Pentesting • IoT Pentesting • Blockchain Pentesting • Secure Code Review • Strategic Advisory • Red Team Operations • Social Engineering • Threat Modeling

About NetSPI:

NetSPI is the global leader in offensive security, delivering the most comprehensive suite of penetration testing, attack surface management, and breach and attack simulation solutions. Through a combination of technology innovation and human ingenuity NetSPI helps organizations discover, prioritize, and remediate security vulnerabilities. Its global cybersecurity experts are committed to securing the world's most prominent organizations, including nine of the top 10 U.S. banks, four of the top five leading cloud providers, four of the five largest healthcare companies, three FAANG companies, seven of the top 10 U.S. retailers & e-commerce companies, and many of the Fortune 500. NetSPI is headquartered in Minneapolis, MN, with offices across the U.S., Canada, the UK, and India.