NetSPI™

Social Engineering

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

Phishing continues to be one of the most prevalent attack vectors and one of the most expensive. In 2024, the average cost of a breach from phishing was $4.88M.[1]

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

Email and Text Message Testing (Phishing)

Security Awareness

Emails are crafted to direct 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 are used to persuade employees to take actions that 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 a customized email and text campaign to target select users based on your specific objectives, such as capturing high-value or proprietary information. We 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 made to a broad group of employees to focus on larger metrics of who does or does not detect the vishing attempt.

Capture The Flag

Utilizing realistic attack scenarios, we target identifying missing policies and edge case vulnerabilities to gain sensitive company information to emulate what a bad actor might do. Once obtained, we leverage discovered information throughout the test to build an overall attack narrative.

[1] IBM. Cost of a Data Breach Report 2024.

Physical and On-Site Social Engineering

Physical Social Engineering Assessment

Focused solely on the human component of your business with in-person interactions. NetSPI attempts to gain unauthorized access to sensitive areas, systems, and information through employees.

Physical Security Controls Assessment

During an on-site walk through, we review the property, building perimeter, office interior, and restricted or secured areas of your business location to discover potential weaknesses or vulnerabilities within physical security controls.

Physical On-Site 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 The NetSPI Platform

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

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

About NetSPI

NetSPI® pioneered Penetration Testing as a Service (PTaaS) and leads the industry in modern pentesting. Combining world-class security professionals with AI and automation, NetSPI delivers clarity, speed, and scale across 50+ pentest types, attack surface management, and vulnerability prioritization. The NetSPI platform streamlines workflows and accelerates remediation, enabling our experts to focus on deep dive testing that uncovers vulnerabilities others miss. Trusted by the top 10 U.S. banks and Fortune 500 companies worldwide, NetSPI has been driving security innovation since 2001. NetSPI is headquartered in Minneapolis, MN, and available on **AWS Marketplace**. Follow us on **LinkedIn** and **X**.