SOCIAL ENGINEERING ASSESSMENT

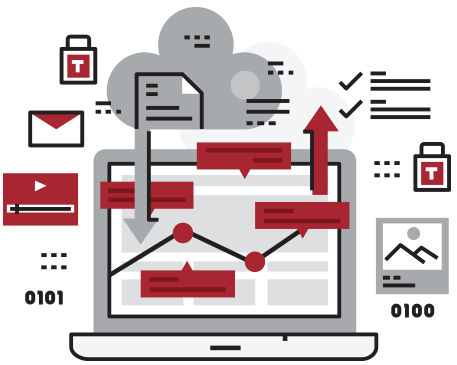
The Impact of Social Engineering Attacks

While technical risks are often the primary focus during a security audit, many times malicious attackers target employees directly, tricking them into providing passwords or downloading malware.

These attacks – known as social engineering - can range from simple email phishing to sophisticated campaigns using multiple communication techniques.

Rhino Security Labs offers a range of expert-driven social engineering engagements for testing both employee training and technical controls.

Whether traditional spearphishing (email), vishing (voice calls), or on-site assessments and attempting access into the physical building, we have trained experts at the ready.



ASSESSMENT TYPES

- Spearphishing (Directed Email Campaigns)
- Vishing (Incorporating Voice Calls)
- On-site Engagement (Tailgating, dropping USB drives, etc.)

PHISHING IN ADVANCED CAMPAIGNS

Often basic social engineering engagements are successful by strategically targeting sensitive information or access, but not all attacks are so direct. In more advanced engagements, operators may request basic office information such as organizational structure or who's on vacation.

This information serves as building blocks for coercing more prepared users, leveraging shared knowledge to develop trust and legitimacy.

Conducting a social engineering assessment with Rhino Security Labs can pinpoint the risk and impact of a social engineering - as well as the company's ability to respond to such an attack.

- *Understand the risk of social engineering attacks*
- *Prepare and train users against similar attacks*
- *Set the priority of security training for employees*
- *Test incident responders to phishing attacks*

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122

ASSESSMENT DETAILS AND METHODOLOGY

At Rhino Security Labs, each social engineering engagement follows a proven methodology to ensure highly targeted, consistent engagements. Each engagement is executed with the following steps:

Information gathering on target organization and personnel

1. Reconnaissance

Information gathering is a critical phase of social engineering and often determines the success of the rest of the assessment. Using a 'black box' approach, our security experts perform in-depth research to extract information on the target company.

Create pretext scenarios, preparing for execution

2. Create Pretext Scenarios And Payloads

Once the target has been fully enumerated, focus turns to crafting the payload. These specifics include identifying departments, user roles, and associated pretext scenarios. These details ensure each user is researched thoroughly for the most successful, targeted engagements.

Engage targets, safely exploiting phishing pages

3. Engage Targets

Using carefully structured tactics and pretext, Rhino Security Labs' security analysts engage employees via phishing emails or phone calls. For on-site assessments, a series of tests are started, such as tailgating users and baiting employees with USB drives 'lost' in the building. automated services.

Detailed, risk-prioritized report with remediation steps

4. Assessment Reporting And Debrief

After completing the campaign and aggregating results, a final report is delivered, providing both executive summary and specific details.

Remediation steps and training guidance are also provided, guiding the client in resolving the training and policy issues identified.

(Optional) Social engineering training and education for employees

5. (Optional) Employee Education

As an optional addition, Rhino Security Labs provides user training sessions for client employees. Whether hosted in a recorded online webinar or an in-house training session, Rhino Security provides quality security awareness training – by the same experts who performed the original engagement.

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.

info@RhinoSecurityLabs.com | 888.944.8679

464 12th Ave, Suite 300 | Seattle, WA 98122