LivewirExperts
Make I.T Happens

LWE – Social Engineering

Social Engineering Test for Better Security

What Is Social Engineering?

Social engineering is a form of cyberattack where hackers utilize psychological manipulation to trick unwitting victims into making security blunders and handing over their personal data. Social engineering is the manipulation of human emotions like greed, fear, rage, curiosity, etc., to get victims to click on harmful URLs or participate in physical tailgaters.

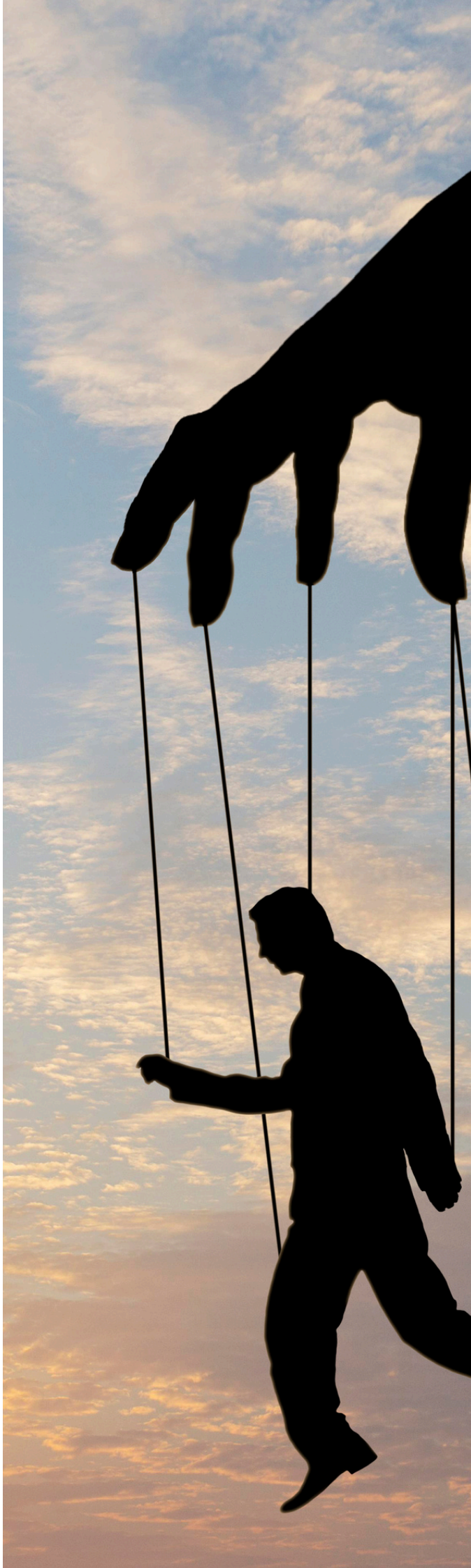
The purpose of Social Engineering attackers is one of two things:

- They want to disrupt a company's operation by tampering with its data, or
- They want to steal data and/or money.

When posing as IT helpdesk staff, for example, an intruder could act as a user and ask for personal information such as a username and password. The fact that so many individuals are willing to give over their personal information, especially if it appears to be coming from a reputable representative, is astonishing. Essentially, social engineering is the use of deception to persuade others to give up their personal information or data to gain access to it.

Social Engineering Penetration Test process

Social engineering penetration testers systematically design and execute attacks. They gather information about the target through reconnaissance and open-source intelligence (OSINT). They select victims and use tactics similar to real attackers. Testers define the scope, conduct tests, document findings, and report risks to management. The pen test report includes impact assessment and recommendations for risk mitigation.



Benefits of Social Engineering Penetration Testing

Identify Targeted Information or Assets: Social engineering pen tests reveal specific data or assets that attackers may target, enabling organizations to prioritize protection efforts and allocate resources effectively.

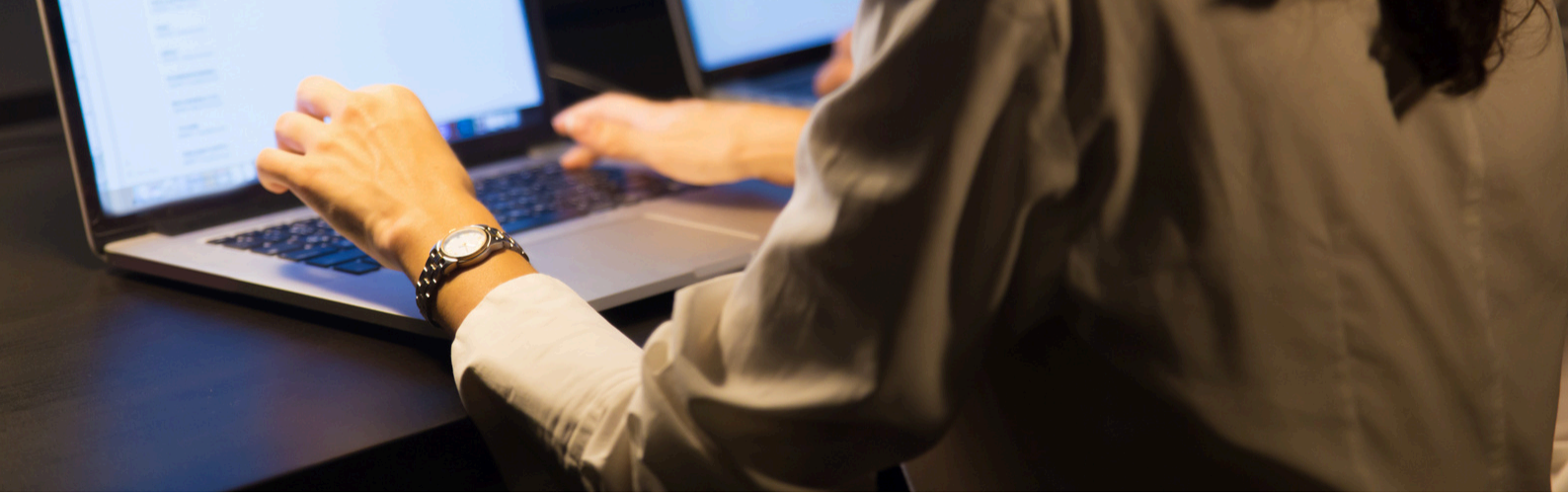
Develop or Improve Security Awareness Training: By monitoring how employees react to social engineering tactics, companies can customize their security training programs. This helps employees better recognize and counteract social engineering attempts, thereby reducing the risk of successful attacks.

Effectiveness of Security Controls Summary: Social engineering penetration tests measure how well current security measures prevent social engineering threats. These tests mimic real attacks, helping organizations spot and improve weak areas in their security to better guard against such attacks.

Determining New Security Controls: Social engineering pen tests reveal critical areas for security enhancement. They guide the adoption of robust authentication, improved email filtering, and cutting-edge threat detection to proactively upgrade security in response to identified vulnerabilities and attack trends.

Organizations can also prevent social engineering attacks by implementing these controls:

- Regular security awareness training.
- Clear password policies.
- Multifactor authentication (MFA).
- Incident response planning.
- Regular security assessments (including pen tests).
- Security monitoring systems.
- Identity and access management (IAM) controls.
- Zero trust security.
- Software and systems patching.



Social engineering penetration tests best practices

Social engineering pen testing should provide a company with information about how easily an intruder could convince employees to break security rules or divulge (or provide access) to sensitive information. The test results should also provide a better understanding of how successful the company's security training is and how the organization stacks up, security-wise, compared to its peers. To promote this understanding, a detailed pen test report, written in audience-friendly language, is crucial.

But even before the test starts, it's important to perform thorough reconnaissance about the target and gather as much information as possible about them. This information helps to clarify the test scope and ensure it's executed correctly.

Finally, it's important to address all the vulnerabilities identified during the pen test and implement all required measures to plug the gaps and prevent an actual attack.

LivewirExperts' Overview

LivewirExperts was born from a shared passion for IT solutions and a vision to revolutionize the industry. Founded by a team of seasoned professionals with years of collective expertise, our company emerged as a response to the growing demand for innovative, reliable IT services. Fueled by a commitment to excellence and a drive to exceed expectations, LivewirExperts delivers cutting-edge solutions and unparalleled customer satisfaction. Today, we continue to push the boundaries of technology, empowering businesses worldwide to thrive in the digital era.

CONTACT US:

LivewirExperts
Contacts: +1 (787) 699-2067 / +1 (561) 441-8281
Email: info@lwexperts.com / sales@lwexperts.com