CSW Cyber SecurityWorks

# CSW - Social Engineering Penetration Testing

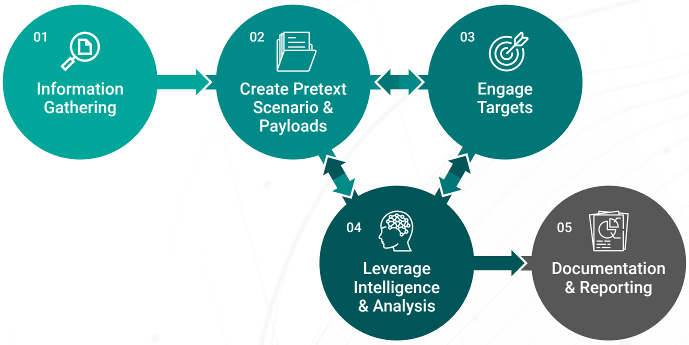
## Introduction

The human aspect of security is often overlooked. Security breaches attributed to social engineering are growing rapidly. As an easier route to an organization's confidential information, cybercriminals have switched their focus from attacking the technology perimeter to compromising the user. The largest cybersecurity vulnerability at any company is its employees. Social engineering is a non-technical intrusion that tricks unsuspecting employees into breaking normal security procedures and giving network access to attackers. Social engineering attacks are based on fundamental psychological principles about human behaviour. Attackers use these human weaknesses to gainaccess to sensitive data or information.

We tailor assessments based on attack vectors to be tested and your end objective (employee security awareness, attack mitigation, etc.). Testing activities remain in a controlled environment, and assessment results provide actionable remediation.

CSW specializes in advanced social engineering techniques and practices that identify areas for improvement.

## Our Approach


01
Information Gathering
02
Create Pretext Scenario & Payloads
03
Engage Targets
04
Leverage Intelligence & Analysis
05
Documentation & Reporting

**01.** Often neglected in social engineering services, information gathering is a critical phase and often determines the success of the campaign. We use publicly available information to gather intelligence and inform targeted social engineering attacks.

**02.** Once enumeration of the client organization and its employees is complete, we look into the pretext scenarios and payloads for the social engineers.

**03.** Using the predetermined tactics, our team will send phishing emails to employees and try to get the intended information.

**04.** Based on the outcome of the campaign and the information gathered our team will use all the information collected to gain access and showcase greater impact to the organization.

**05.** Upon completion, assessment results are aggregated, and the social engineering report is created. This report outlines both an executive summary and a detailed technical report with POC

## Benefits

- Identification of weaknesses in the human factor of security.
- Identification all vulnerable areas within a company and prioritizing them.
- Reduce the risk of information leakage by employees when faced with a social engineering attack.
- Validation of company's operational processes to prevent a social engineering attack.
- Recommendations to improve the company's training procedures and security policies.
- Recomendations to improve the company's training procedures and security policies.

## Deliverables

CSW will furnish a comprehensive report detailing:

- Describing of the attack vectors employed
- Which vectors were successful/not successful with particular employees

We can also work with your team to help design security awareness training focused on thwarting social engineering attacks.

PCI Security Standards Council
APPROVED SCANNING VENDOR

**Corporate Office Address:**
IITM Research Park, No.6 A-Block, 3rd Floor, Kanagam Main Road,Taramani, Chennai - 600 113.
**P: +91 44 4208 9337 | E: info@cybersecurityworks.com | W: www.cybersecurityworks.com**