Social Engineering Attacks Preparedness

PLETHORA offers in-depth **Social Engineering Attacks Preparedness Assessment** to help you strengthen the processes and technology to mitigate the threat of phishing attacks.

Problem

The Social Engineering Risk:

- Few years back, it was common practice for hackers to focus on Internet facing assets for their attacks. The assets were generally not well defended and focusing on it was low risk and high reward for most attacker objectives. Times have now changed and Internet facing assets are typically better defended, and attackers are finding more success when targeting people and process. This shift has occurred, but many organizations have failed to keep their threat model up to date.

- **Did you know:**
  - Social engineering attacks were responsible for the theft of over $5 billion worldwide during a recent three-year period.
  - 55% of all emails are spam.
  - 97% of all attacks use some form of social engineering.
- **Social engineering is a real-world threat.** The impact and likelihood of such an attack succeeding against an organization typically needs to be understood. A social engineering test hands that knowledge to an enterprise and helps feed into a robust cyber security strategy.

Service Overview

Use Security email phishing service to conduct the real-world attack scenarios on to identify security awareness and personnel gaps.

- Creating **Security Awareness Program Roadmap** for the organization.
- Assistance in creating the **Information Security policies and procedures**.
- **Actionable** Awareness Content and Sessions.
- **Client Success Support** over email and calls.
- Conducting the **tests of participants** with respect to the sessions.
- **Employee-wise and Organization-wise Reports** on Email Phishing & awareness.
- Follow-up sessions with the target employees.
- Digital Certificate of Completion.

Key Benefits

Create an end-to-end security culture by training and preparing your employees to protect information and assets of your organization.

- **Expertise -** Our Subject Matter Experts are having years of Infosec experience.
- **Compliance -** Regularly training your employees is a critical component of compliance and security.
- **Culture -** Cyber-attack and breach prevention happens when an organization has a culture of security awareness.
- **Metrics -** Demonstrate the effectiveness of your security awareness program with objective data with Questionnaire tests and Social Engineering Real life scenarios Tests.
- **Customization -** Tailor your security awareness training program to meet your specific needs.
- **Flexibility -** Conduct sessions as per the availability of the participants

How it works

- The prevalence and success of phishing make it one of the most dangerous social engineering tactics. Several business tools are available to test and train against phishing. **Our security professionals create the phishing attack scenarios along with the client to conduct their phishing tests with the help of customized emails.**

- The goal is to assess how target employees will react when receiving these suspicious emails. Calls for action include convincing targets to do any of the following:
  - Visit malicious websites
  - Reveal vital personal information
  - Break security rules and regulation

REQUEST A CONSULTATION

Scope Definition

Name of the Organization/Company:	
Business Industry:	
Approx. Number of Total Employees:	
Approx. Number of the Subsidiaries or the Sister concerns of the Organization/Company:	
Number of Scenarios – Phishing / Spear-phishing / Whaling	
List the Business Domain(s):	
List the Email Domain(s):	
Location of Office Headquarters:	
Locations of Business Operations:	
Locations of Subsidiaries or the Sister concerns:	
Frequency of the SET (Social Engineering Test) – Quarterly / Bi-annually / Annually – Number of tests required –	