ALEPH TAV
TECHNOLOGIES

Security Testing at its best

Anti-phishing Campaign

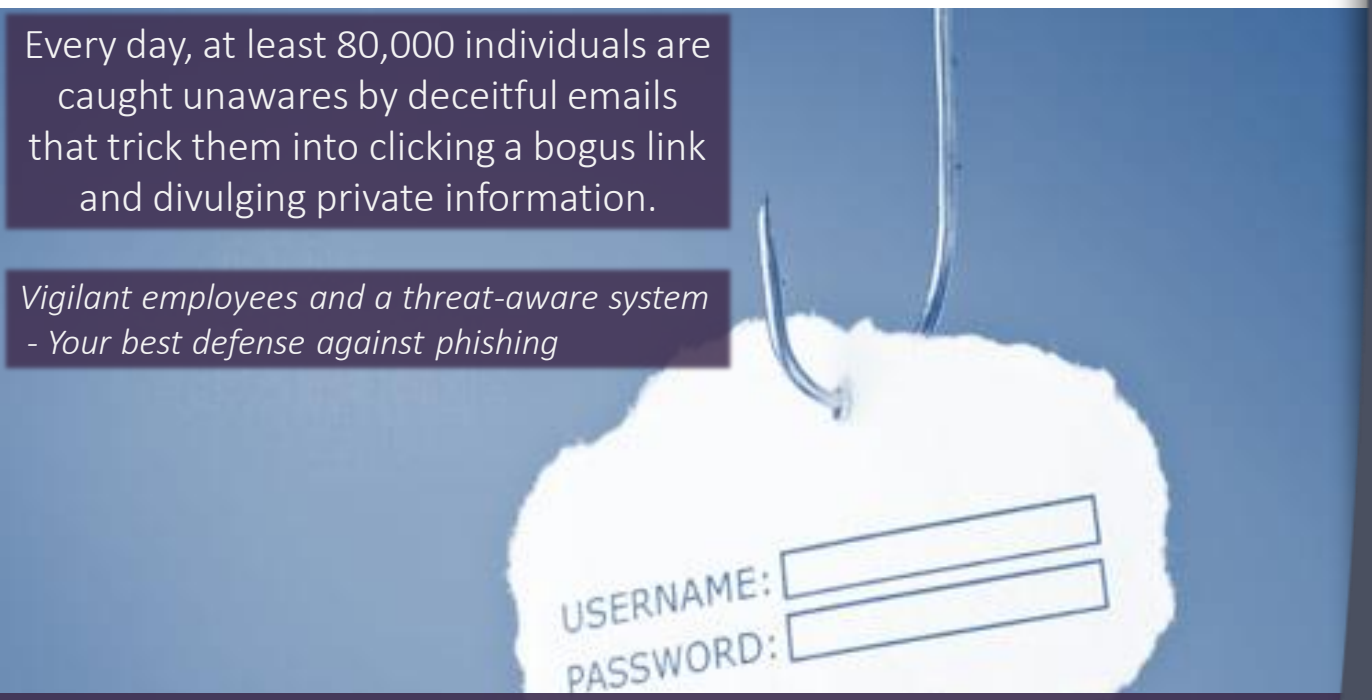
User Behavior Profiling Program

- A powerful protection strategy against Phishing attacks

Assessing **Security** for the **Enterprise**

Every day, at least 80,000 individuals are caught unawares by deceitful emails that trick them into clicking a bogus link and divulging private information.

Vigilant employees and a threat-aware system - Your best defense against phishing



Aleph Tav Technologies looks beyond conventional social engineering.
Our Insider Behavior Profiling Services presents an anti-phishing campaign you can use to assess your enterprise-wide security posture against phishing scams.

The program strives to provide insight into essential system hardening that can prevent clone attacks.

Can one simple email bring down your business empire?

If you answered No, think again. Not elaborate exploits, not zero-day vulnerabilities. It is the Phishing scams that are wreaking havoc in enterprise networks. Often, all they need is just one naive click.

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

-Even individuals who are not particularly gullible can fall for one such email message. Panic is the most common trigger-point phishers capitalize on.

Effects of a successful phishing attack:

Loss of user credentials leading to system compromise

-Using a compromised network system, the attacker can move laterally across the network, snooping around critical servers.
-Once a leeway is gained, it is only a matter of time before the attacker sniffs out access credentials to all critical systems and data assets.

Loss of client/customer information

Your client databases with confidential information could be leaked.

Denial of Service and Defacement attacks

Availability and credibility of your data is at stake

Entry into mission-critical control system networks

Critical tasks could be triggered and privileged information could be leaked.

Financial loss

Transfer of funds could be effected by a malicious hacker.
Ambushed global companies have incurred losses up to an average of $144 million per attack.

How we can help

We evaluate your posture against cyber crime with an investigative study of employees' level of prudence while interacting with the web.
We do this by launching **pseudo-phishing attacks** that are **controlled and harmless.**

1. **Initial test**: Also launched through the internal email server to employees, the email message mimics a login prompt to a regular, enterprise user login page but redirects the user to a cloned, phony login page.
2. **Cognizance Check**: Users who click on the phony web link and proceed to submit login credentials are then redirected to an awareness message on secure online culture in the enterprise. This also logs the number of tricked users and immediacy of their response.
3. **Advanced test vector:** The initial test is replicated from an external server, carrying an 'offer' or 'caution' message as bait.

Our **two-pronged approach** analyzes the network environ, identifying flaws in authentication policies. **This user behavior profiling program** will culminate in employee-centric sensitization. The effectiveness of the campaign can be enhanced by detecting vulnerabilities arising out of misconfiguration and insecure interfaces.
Our experts will also assess the resilience of firewalls, malware filters and junk filters.

Achieve total control over insider risks, sustainably.

We're here to guide you.

+91 44 3010 6900

engage@alephtavtech.com

alephtavtech.com

ALEPH TAV TECHNOLOGIES

2E, Gee Gee Emerald, 312 Village Road, Nungambakkam, Chennai 600 034. India