**LITERATURE SURVEY**

Phishing is a social engineering attack that aims at ex ploiting the weakness found in system processes as caused

by system users. For example, a system can be technically

secure enough against password theft, however unaware end

users may leak their passwords if an attacker asked them to

update their passwords via a given Hypertext Transfer Protocol

(HTTP) link, which ultimately threatens the overall security of

the system.

Moreover, technical vulnerabilities (e.g. Domain Name Sys tem (DNS) cache poisoning) can be used by attackers to

construct far more persuading socially-engineered messages

(i.e. use of legitimate, but spoofed, domain names can be far

more persuading than using different domain names). This

makes phishing attacks a layered problem, and an effective

mitigation would require addressing issues at the technical and

human layers.

Since phishing attacks aim at exploiting weaknesses found

in humans (i.e. system end-users), it is difficult to mitigate

them. For example, as evaluated in [1], end-users failed

to detect 29% of phishing attacks even when trained with

the best performing user awareness program. On the other

hand, software phishing detection techniques are evaluated

against bulk phishing attacks, which makes their performance

practically unknown with regards to targeted forms of phishing

attacks.