

OBJECTIVES OF WEB PISHING DETECTION

Phishing is a form of the attacker tries to learn sensitive information such as login credentials or account information by sending as a reputable entity or person in email or other communication channels.

Typically, a victim receives a message that appears to have been sent by a known contact or organization. The message contains malicious software targeting the user's computer or has links to direct victims to malicious websites in order to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Phishing is popular among attackers, since it is easier to trick someone into clicking a malicious link which seems legitimate than trying to break through a computer's defense systems.

A protocol used to access the page the server who hosts the web page. A Host name consists of a subdomain name and a domain name. The attacker can register any domain name that has not been registered before. This part of URL can be set only once. The phisher can change Free URL at any time to create a new URL. The reason security defenders struggle to detect phishing domains is because of the unique part of the website domain (the Free URL). When a domain detected as a fraudulent, it is easy to prevent this domain before a user access to it.