DETECTION OF WEB PHISHING

PROBLEM STATEMENT

Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity. It will lead to information disclosure and property damage. This paper mainly focuses on applying a deep learning framework to detect phishing websites.

PROBLEMS:

Malicious links will lead to a website that often steals login credentials or financial information like credit card numbers. Attachments from phishing emails can contain malware that once opened can leave the door open to the attacker to perform malicious behavior from the user's computer.

Phishing attack examples

- A spoofed email ostensibly from myuniversity.edu is mass-distributed to as many faculty members as possible.
- The email claims that the user's password is about to expire. Instructions are given to go to myuniversity.edu/renewal to renew their password within 24 hours.
- Email phishing scams:
- Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can net significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates.For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same phrasing, typefaces, logos, and signatures makes the messages appear legitimate.In addition, attackers will usually try to push users into action by creating a sense of urgency. For example, as previously shown, an email could threaten account expiration and place the recipient on a timer. Applying such pressure causes the user to be less diligent and more prone to error.Lastly, links inside messages resemble their legitimate counterparts, but typically have a misspelled domain name or extra subdomains.In the above example,the myuniversity.edu/renewal URL was changed to myuniversity.edurenewal.com. Similarities between the two addresses offer the impression of a secure link, making the recipient less aware that an attack is taking place.So for this problem . we came with the solution of web phishing detection