

BRAIN STORMING SESSION

DEFINING PROBLEM STATEMENT

Web Phishing Detection

There are a number of users who purchase products online and make payments through e-banking. There are e-banking websites that ask users to provide sensitive data such as username, password & credit card details, etc., often for malicious reasons. This type of e-banking website is known as a phishing website. Web service is one of the key communications software services for the Internet. Web phishing is one of many security threats to web services on the Internet.

Common threats of web phishing:

- 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.
- Large organizations may get trapped in different kinds of scams.

This Guided Project mainly focuses on applying a machine-learning algorithm to detect Phishing website.

Brainstorm:

Group ideas:

Several different techniques to combat phishing, including legislation and technology created specifically to protect against phishing.

These techniques include steps that can be taken by individuals, as well as by organizations. Phone, web site, and email phishing can now be reported to authorities

Filtering out phishing mails:

Specialized spam filters that will reduce the number of phishing mail

Some specific filters to are

1. Requests for login credentials
2. Requests for credit/debit card credentials.
3. Obvious claims that you've won a prize.

Rohith.R

Because Phisher
software is diverse,
current filters can
still mis-classify
emails.

Commonly featured
keywords in current
Phishers need to be
used as part of the
test data

Predicting future
mutation of such
evolving emails and
taking preventive
measures could be
looked into.

Sifting through
algorithms like Bayesian
networks and the
multilayer perceptron
algorithm, to find which
yields the most accuracy
in results is important.

Srivanth.S

Tools to
categorise and
cluster the data
need to be
researched.

Phishers are often
disguised as trusted
brands and
institutions. This
software must verify
against that

Analyze the salutation
(legitimate
organization will often
use a personal
salutation with your
first and last name)

Strong
authentication

Dhanush.G

There are anti-phishing websites which publish exact messages that have been recently circulating the internet.

Once a phishing email is detected, A pop-up notification and further clear instructions should be given.

Reporting the email and run a security scan over your computer.

The emails will usually contains a logo or images that have been taken from website

Tarun.M.K

Based on White and black list

Check your online accounts regularly

No legitimate organisation will send emails from an address that ends '@gmail.com.'

The phisher messages often creates a sense of urgency. We need to frame a set of filters to detect this.

Our priority is listed below:

PRIORITIZE CHART:

