3

Brainstorm as a group

Have everyone move their ideas into the "group sharing space" within the template and have the team silently read through them. As a team, sort and group them by thematic topics or similarities. Discuss and answer any questions that arise. Encourage "Yes, and..." and build on the ideas of other people along the way.

15 minutes

TIP

You can use the **Voting session** tool above to focus on the strongest ideas.

Yosheppu.R

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

A demonstration of how hackers create phishing pages to steal login information.

Scripts to automate phishing attacks

Credential Harvester built on top of Python Flask for easier phishing to social media sites.-

This is an educational project for how a phising works

Vignesh C

This is a phishing site created to show users and create awareness about how easy it is to create phishing site and avoid it.

This is a phishing website for facebook made using Python(flask) and Storing in Database(MongoDB).

The dataset consists of different features that are to be taken into consideration while determining a website URL as legitimate or phishing.

PyShing is a powerful phishing tool which is built of Flask and uses Ngrok for tunneling

Phishing is a form of fraud in which the attacker tries to learn sensitive information such as login credentials

Thiyagaraj.K

Typically a victim receives a message that appears to have been sent by a known contact or organization.

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.

The main reason is the lack of awareness of users.

It begins with a protocol used to access the page, The fully qualified domain name identifies the server who hosts the web page.

Some threat intelligence companies detect and publish fraudulent web pages or IPs as blacklists, thus preventing these harmful assets by others is getting easier. (cymon, firehol)

Nivesan.T

the real domain name is active-userid.com, the attacker tried to make the domain look like paypal.com by adding FreeURL.

Cybersquatting (also known as domain squatting), is registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else.

Typosquatting, also called URL hijacking, is a form of cybersquatting which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser

There are a lot of algorithms and a wide variety of data types for phishing detection in the academic literature and commercial products.

URL is the first thing to analyse a website to decide whether it is a phishing or not.

Deepak Rana

The URL of phishing websites may be very similar to real websites to the human eye, but they are different in IP.

This project aims to detect fraud or phishing website using machine learning techniques.

The content-based detection usually refers to the detection of phishing sites through the pages of elements, such as form information, field names, and resource reference.

The antiphishing way using blacklist may be an easy way, but it cannot find new phishing websites

This chapter addresses the problem of selecting the best classification technique for website phishing detection that causes degradation in detection accuracy and high false alarm rate