



Brainstorm

Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.

- 🕒 10 minutes to prepare
- 🕒 1 hour to collaborate
- 👤 2-8 people recommended



Before you collaborate

A little bit of preparation goes a long way with this session. Here's what you need to do to get going.

🕒 10 minutes

- A

Team gathering
Define who should participate in the session and send an invite. Share relevant information or pre-work ahead.
- B

Set the goal
Think about the problem you'll be focusing on solving in the brainstorming session.
- C

Learn how to use the facilitation tools
Use the Facilitation Superpowers to run a happy and productive session.

Open article →

1

Define your problem statement

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

🕒 5 minutes

Analytical



As online transactions grew in popularity, cybercrimes also grew quickly. Because of the anonymity offered by the internet, hackers try to trick users by using techniques like phishing, SQL injection, malware, man-in-the-middle attacks, domain name system tunneling , ransomware, web trojans, and other forms of attack. Phishing is said to be the most misleading of all of these tactics.

2

Brainstorm

Write down any ideas that come to mind that address your problem statement.



TEAM
ID:PNT2022TMID50410
WEB PHISHING DETECTION

Kalai selvi G(Team Leader)

Difficult to block "redirecting pages," as these URLs can be disguised

To keep track of all potential phishing techniques, use an intelligent online security gateway.

comparison of trustworthy and fraudulent websites

Anushya M(Team member 1)

Web phishing detection with advanced deployment

Maintaining web phishing records with a spam repository

Observation of resource loading times to identify fraudulent websites' tendencies to display just costs rather than their functionality

Paul Reshmin M(Team member 2)

Link pathways are being traced after detection of tampering

By contrasting it with real online domain names, homograph spoofing can be identified.

To check for extended links and prevent link shortening because most fraudulent websites use the "bit.ly" extension

Kartiga devi K(Team member 3)

Incorrectly worded keywords and odd website changes

Requesting confirmation of unrelated qualifications

Verify secure web protocols like "https" visually