IOWA STATE UNIVERSITY

Department of Electrical and Computer Engineering

Advanced Phishing Email Simulation Tool

Cpr E 599: Creative Component

Presenter: Raksha Ravindra Deshpande

Date: 04/24/2025

Abstract

- Phishing exploits human behavior, not just technical flaws.
- Project integrates Gophish, Mailtrap, and Hotjar.
- Tracks real-time interaction (Clicks, scrolls, and hover).
- Feedback via heatmaps improves awareness.
- Results show improved caution post-simulation.

Introduction

- Phishing is one of the most persistent cyber threats, driven by social engineering.
- This project aims to go beyond click-through analysis by capturing how users behave on phishing pages.
- The simulation setup uses a domain, secure VPS, ethical email routing, and detailed user behavior tracking.
- Goal: Build personalized awareness through real-world simulations and behavioral insight.

Related Work

Phishing research has shifted from technical analysis to a focus on human decision-making, which now drives the development of behavior-based simulations like this project.

- User Behavior and Psychological
- Detection and Prevention Techniques
- Experimental Design and Methodology
- Training and Awareness

Gaps Addressed by This Project

- Most tools stop at click tracking.
- This project analyzes post-click behavior, scrolls, and cursor movements.
- Adds heatmaps-based feedback.
- Delivers awareness strategy.

Research Question and Objective

Key Research Question:

“How do we track and analyze user behavior in phishing attacks to use tailored feedback which improves cybersecurity awareness?”

Objectives:

1. Controlled Phish Simulation.
2. User Behavior Tracking
3. User Classification
4. Feedback and Awareness

Methodology

- **Simulation Engine:** Gophish for email campaigns.
- **SMTP Relay:** Mailtrap to securely test email delivery.
- **Behavior Analytics:** Hotjar to record clicks, scrolls, and hovers.
- **Secure Hosting:** DigitalOcean VPS server, domain: raksha.me(Godaddy)

Experimental Setup

- Phishing emails imitate password resets and account password recovery.
- Landing pages were realistic replicas of login portals.
- Hotjar tracking scripts are embedded on pages.
- System tested phishing campaigns end-to-end ethically in the setup environment.

User Behavior Scenarios

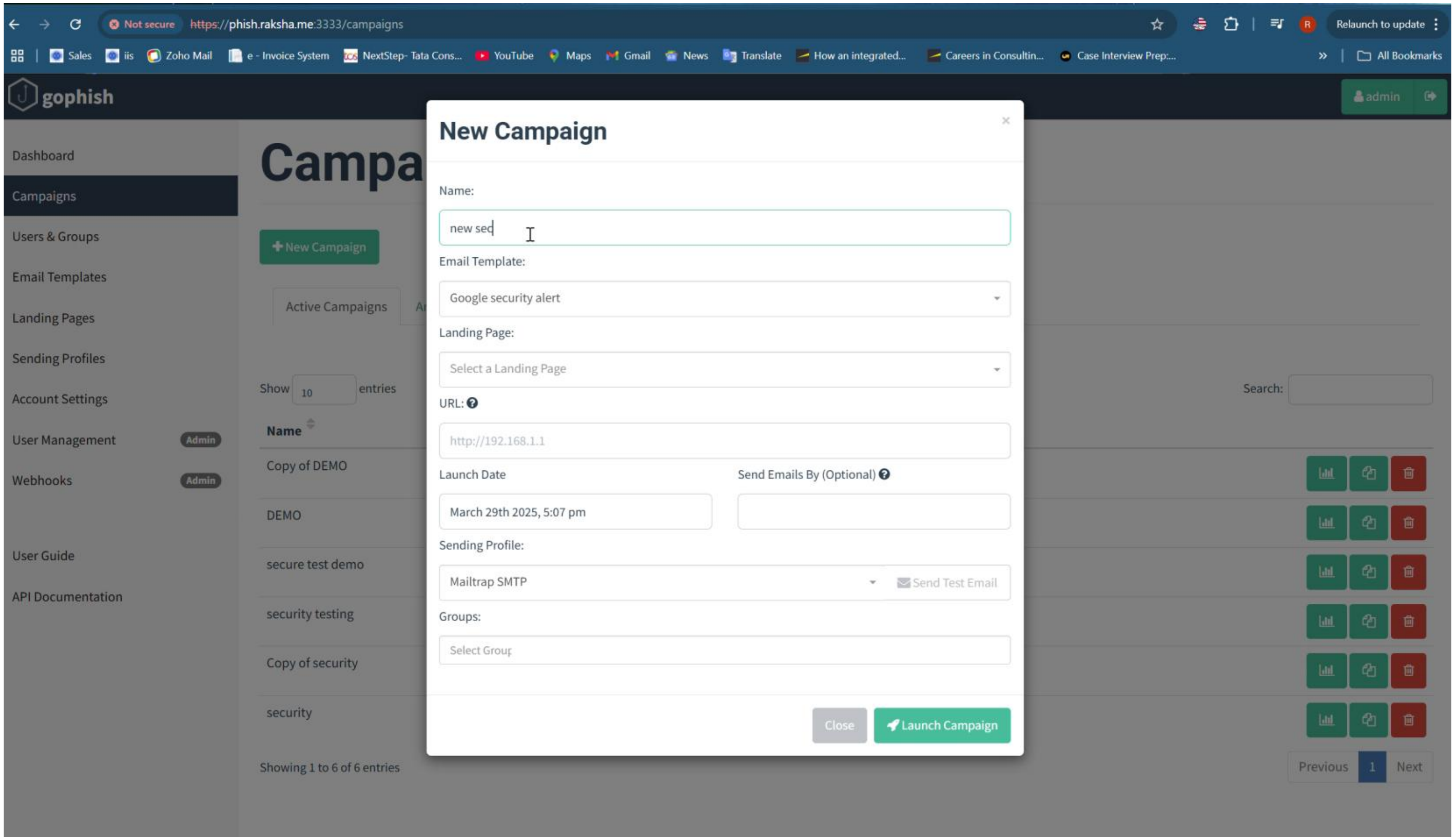
1. **High Risk:** Users clicked, changed passwords, or filled forms immediately.
2. **Moderate Risk:** Hovered, looked through, or scrolled before interacting.
3. **Low Risk:** Ignored the email, closed the page, or noticed suspicious content.

These patterns were used to assign users to risk categories for awareness strategy training.

Data Collection

- **Gophish:** Email sent, email opened, clicked link, submitted data.
- **Hotjar:** heatmaps, clicks, average scroll depths, cursor movements.
- **Mailtrap:** Test emails with fake login page URLs, urgency in the subject, and password resets.

Simulation Video



https://phish.raksha.me:3333/campaigns

New Campaign

Name: new sec

Email Template: Google security alert

Landing Page: Select a Landing Page

URL: http://192.168.1.1

Launch Date: March 29th 2025, 5:07 pm

Send Emails By (Optional):

Sending Profile: Mailtrap SMTP

Groups: Select Group

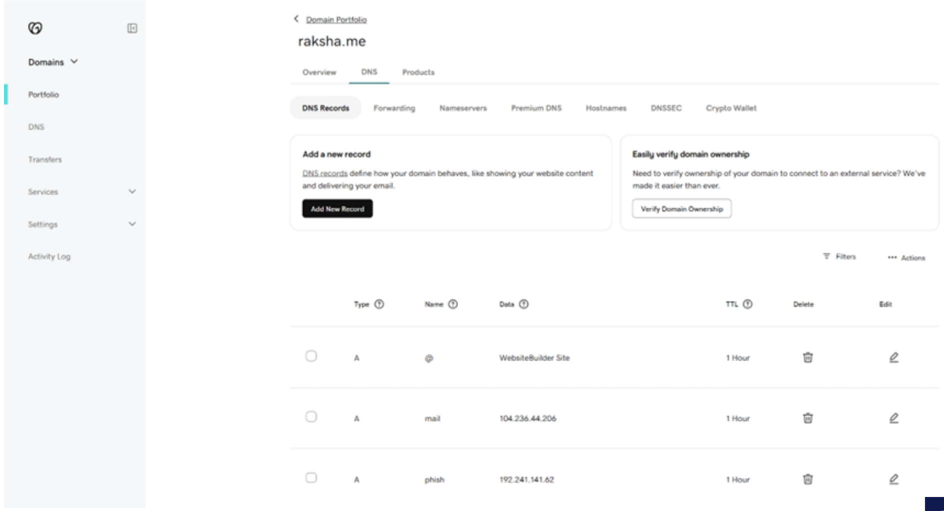
Campaigns

Name
Copy of DEMO
DEMO
secure test demo
security testing
Copy of security
security

Showing 1 to 6 of 6 entries

Simulation Outputs

GoDaddy Domain name raksha.me:



raksha.me

Add a new record

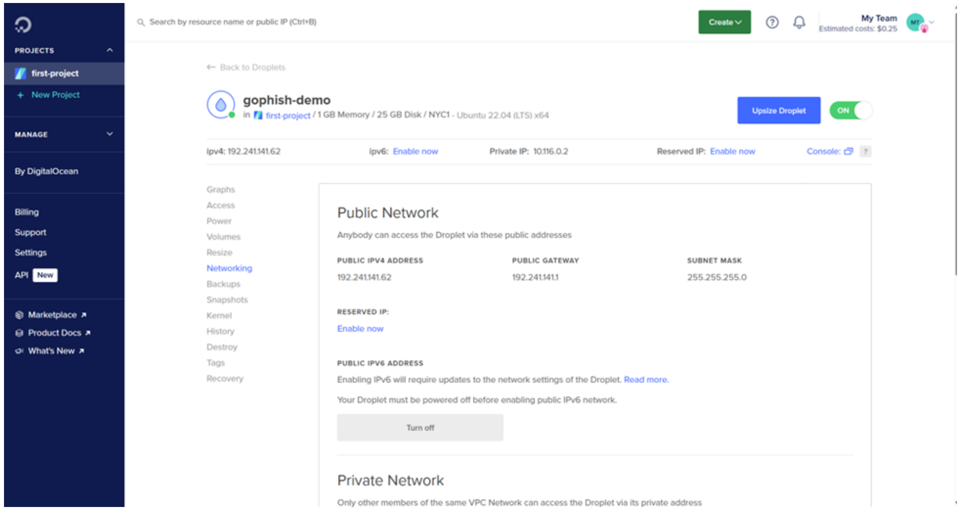
DNS records define how your domain behaves, like showing your website content and delivering your email.

Easily verify domain ownership

Need to verify ownership of your domain to connect to an external service? We've made it easier than ever.

	Type	Name	Data	TTL	Delete	Edit
□	A	@	WebsiteBuilder Site	1 Hour		
□	A	mail	104.236.44.206	1 Hour		
□	A	phish	192.241.141.62	1 Hour		

Digital Ocean- VPS SERVER: Gophish Demo:



Estimated costs: $0.25

gophish-demo

in first-project / 1 GB Memory / 25 GB Disk / NYC1 - Ubuntu 22.04 (LTS) x64

ipv4: 192.241.141.62 ipv6: Enable now Private IP: 10.116.0.2 Reserved IP: Enable now Console:

Public Network

Anybody can access the Droplet via these public addresses

PUBLIC IPV4 ADDRESS	PUBLIC GATEWAY	SUBNET MASK
192.241.141.62	192.241.141.1	255.255.255.0

RESERVED IP:
Enable now

PUBLIC IPV6 ADDRESS

Enabling IPv6 will require updates to the network settings of the Droplet. Read more.

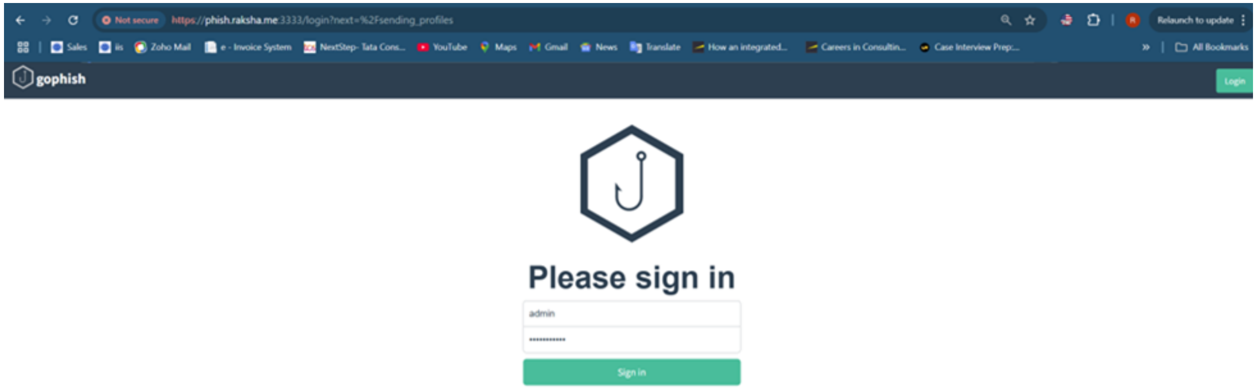
Your Droplet must be powered off before enabling public IPv6 network.

Private Network

Only other members of the same VPC Network can access the Droplet via its private address

Simulation Outputs

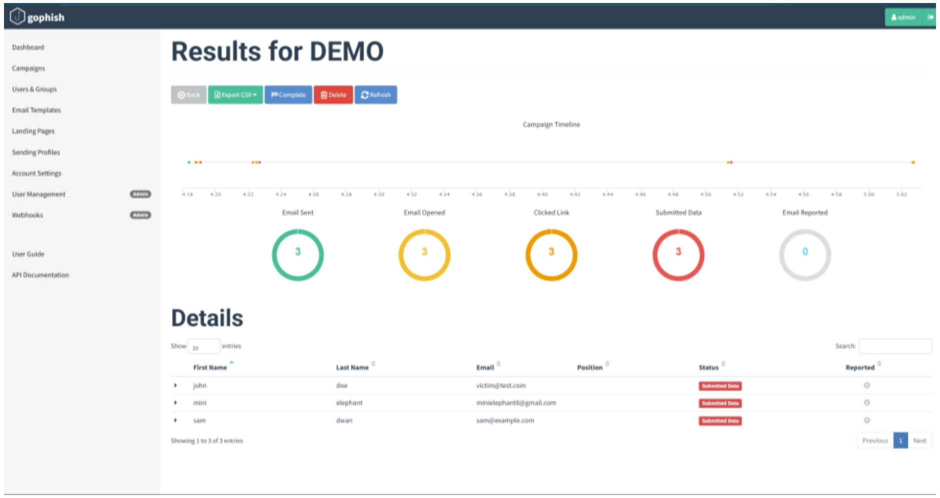
Gophish Login Page:



Please sign in

admin

Phishing Campaign Simulation Result:



Results for DEMO

Email Sent 3

Email Opened 3

Clicked Link 3

Submitted Data 3

Email Reported 0

Details

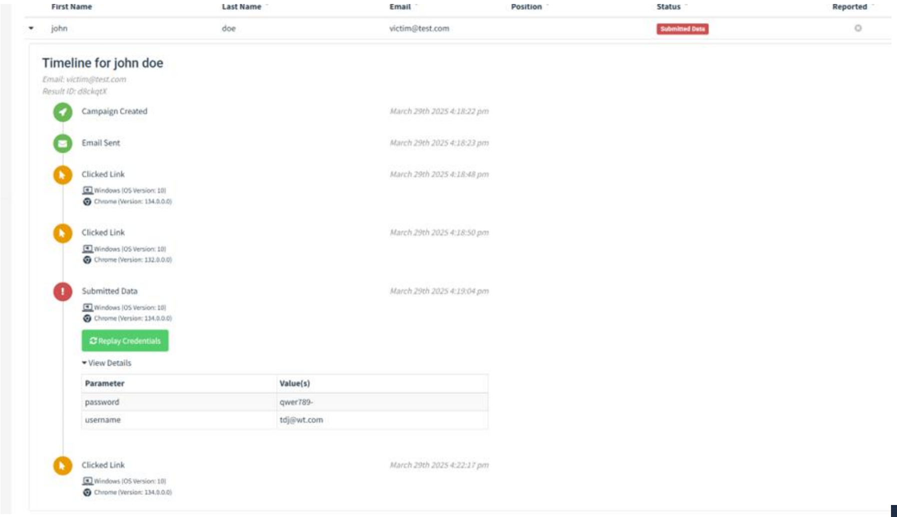
Show 10 entries

First Name	Last Name	Email	Position	Status	Reported
john	doe	victim@test.com		Submitted Data	○
mini	elephant	minielephant8@gmail.com		Submitted Data	○
sam	dwan	sam@example.com		Submitted Data	○

Showing 1 to 3 of 3 entries

Simulation Outputs

User Phished Data-Demo Campaign:



First Name	Last Name	Email	Position	Status	Reported
john	doe	victim@test.com		Submitted Data	

Timeline for john doe

Email: victim@test.com
Result ID: d8ckqtX

Campaign Created — *March 29th 2025 4:18:22 pm*

Email Sent — *March 29th 2025 4:18:23 pm*

Clicked Link — *March 29th 2025 4:18:48 pm*
Windows (OS Version: 10)
Chrome (Version: 134.0.0.0)

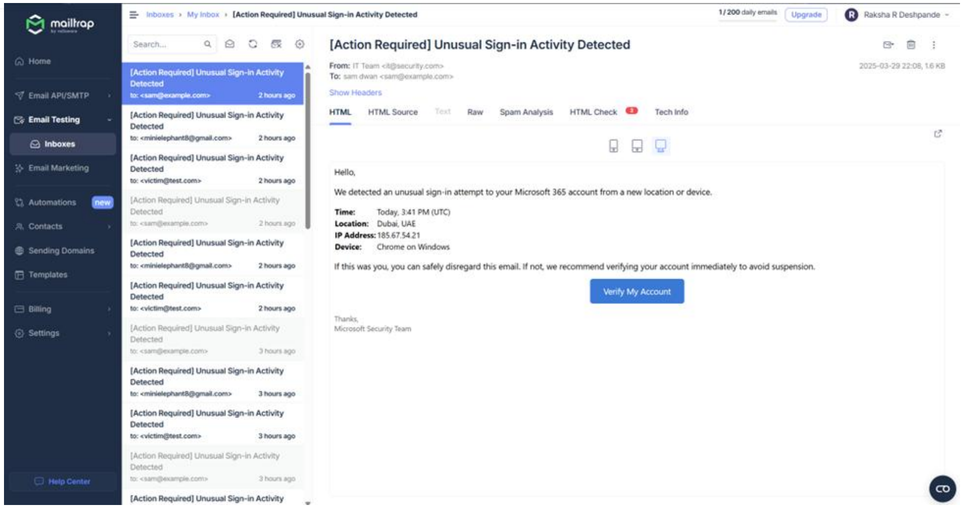
Clicked Link — *March 29th 2025 4:18:50 pm*
Windows (OS Version: 10)
Chrome (Version: 132.0.0.0)

Submitted Data — *March 29th 2025 4:19:04 pm*
Windows (OS Version: 10)
Chrome (Version: 134.0.0.0)

Parameter	Value(s)
password	qwer789-
username	tdj@wt.com

Clicked Link — *March 29th 2025 4:22:17 pm*
Windows (OS Version: 10)
Chrome (Version: 134.0.0.0)

MAILTRAP SMTP: User Test Emails:



[Action Required] Unusual Sign-in Activity Detected
to: <sam@example.com> 2 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <minielephant8@gmail.com> 2 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <victim@test.com> 2 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <sam@example.com> 2 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <minielephant8@gmail.com> 2 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <victim@test.com> 2 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <sam@example.com> 3 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <minielephant8@gmail.com> 3 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <victim@test.com> 3 hours ago

[Action Required] Unusual Sign-in Activity Detected
to: <sam@example.com> 3 hours ago

[Action Required] Unusual Sign-in Activity

[Action Required] Unusual Sign-in Activity Detected

From: IT Team <it@security.com>
To: sam dwan <sam@example.com>
2025-03-29 22:08, 1.6 KB

Hello,

We detected an unusual sign-in attempt to your Microsoft 365 account from a new location or device.

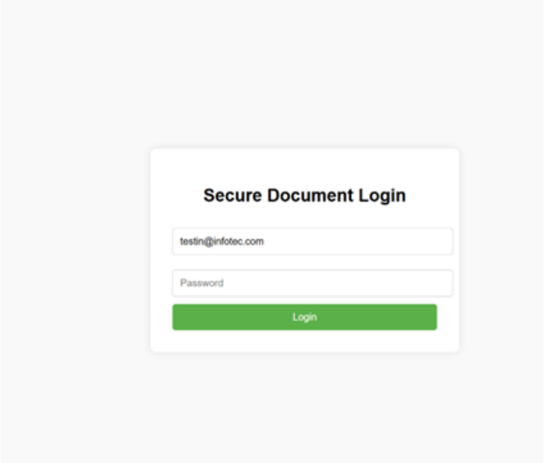
Time: Today, 3:41 PM (UTC)
Location: Dubai, UAE
IP Address: 185.67.54.21
Device: Chrome on Windows

If this was you, you can safely disregard this email. If not, we recommend verifying your account immediately to avoid suspension.

Thanks,
Microsoft Security Team

Simulation Outputs

Fake Login Page:



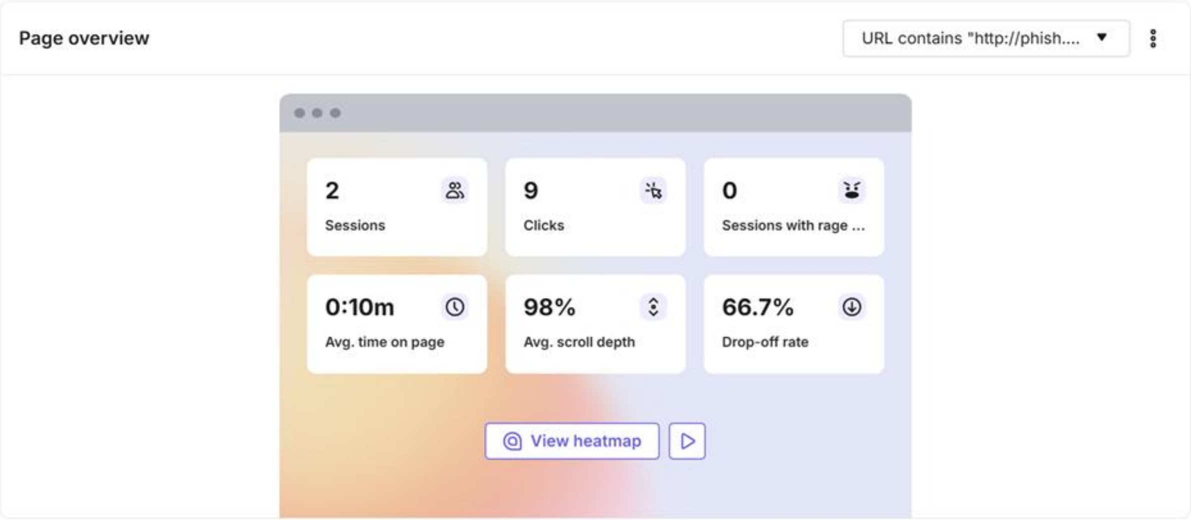
Secure Document Login

testin@infotec.com

Password

Login

Hotjar-Phished User Behavior Overview:



Page overview

URL contains "http://phish....

2 Sessions

9 Clicks

0 Sessions with rage ...

0:10m Avg. time on page

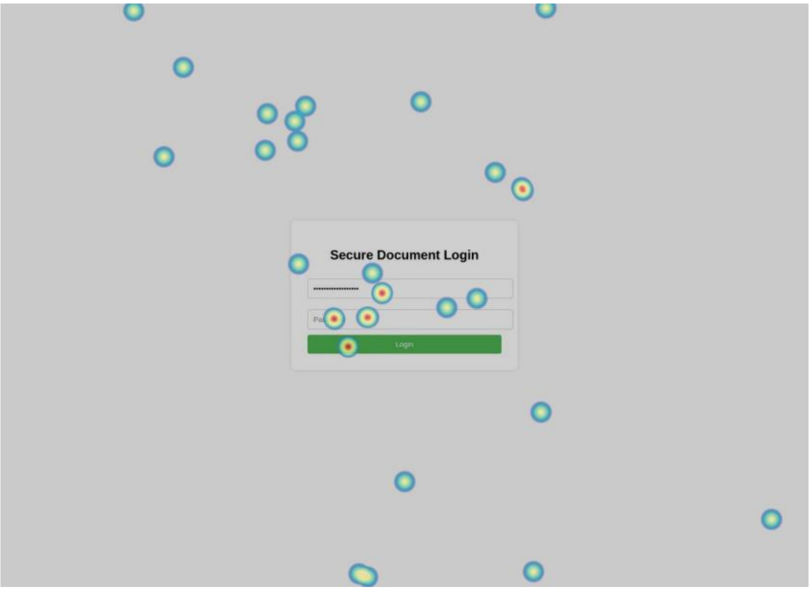
98% Avg. scroll depth

66.7% Drop-off rate

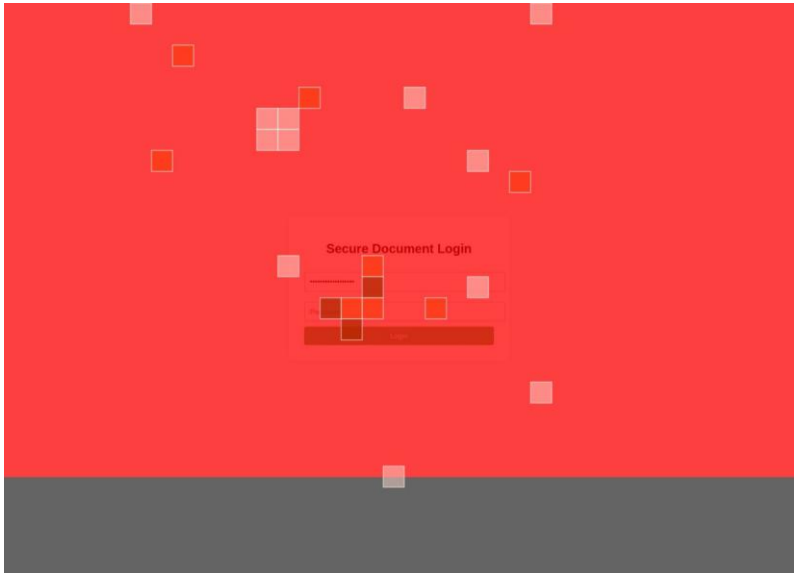
View heatmap

Simulation Outputs

Phished User Movements on Desktop:



Phished User Scrolls on Desktop:



Awareness Strategies and Why its more Effective

Awareness Strategies:

- **Real phishing-style emails with urgency**.
- Hotjar recording user behavior.
- Users are classified into risk-based levels on interaction style.

Why is it more effective?

- Users learn better through real simulations than lectures.
- Heatmaps reveal the user's blind spots in decision-making.
- Visual recordings provide realistic judgments for the awareness strategy.

Limitations

- Small participants limit scalability.
- Hotjar’s free plan restricts session recording duration.
- Mailtrap’s free plan limits for email receiving.

Conclusion

The tool successfully merges phishing simulation with behavioral analytics. By analyzing real-time actions and giving visual feedback, it transforms passive learning into interactive awareness training. It’s ethical, deployable, and scalable for academic settings.

Future Work

- Expand simulation to cover SMS phishing, social media, and vishing.
- Incorporate machine learning for predictive risk scoring.
- Build a phishing training platform with automated feedback and behavioral profiling.

THANK YOU

“Knowing who’s Susceptible allows you to take preventative steps.”