PhishNinja

13/10/2023

20201CCS0131	Umraz Khan
20201CCS0063	Jonathan R
20201CCS0132	Lenin E
20201CCS0070	Samrudh D Yash
20201CCS0046	K Rehan

Problem Statement

Phishing attacks are becoming common. The common man is sometimes duped of hard earned saving due to phishing attacks. Specially vulnerable are old people. They are targeted for their net banking/online wallet PIN or password. The developer should design a system to solve this problem. This problem cannot be solved using only technology. Special focus will have to be put on User Experience (UX) design and User Interface (UI) design. Solutions should keep in mind old users, users who are from villages, users who are not technically savvy and kids. These are specially vulnerable groups.

Problem Overview

In a world where the internet is booming, phishing attacks are imminent. These insidious cyber threats exploit the convenience and connectivity of the digital age. They involve deceptive tactics that impersonate legitimate entities, often arriving as convincing emails or messages. The unsuspecting victims are enticed to disclose sensitive information like passwords, credit card details, or personal data.
Phishing attacks leverage psychological manipulation and prey on human vulnerability. As our reliance on online platforms and communication grows, understanding the risks and implementing safeguards becomes paramount. In this age of interconnectedness, vigilance against phishing is crucial for safeguarding personal and organizational security.

Some of the services affected by phishing are:

- Net Banking
- Streaming services
- Online gaming accounts
- Subscription platform like Patreon, Onlyfans, etc
- Reward program accounts like Google play and Amazon gift cards
- Social accounts

Goals

- Chrome Extension Development: Create a Chrome extension designed to enhance the security of online/mobile wallets and net banking.

- Phishing Attack Prevention: Develop features within the extension aimed at preventing phishing attacks, including real-time analysis of web content and URLs for potential threats.

- User Awareness and Education: Incorporate educational components into the extension, such as pop-up notifications, tooltips, and guides, to increase user awareness regarding phishing threats and safe online banking practices.

- Reporting and Response Features: Integrate a user-friendly reporting mechanism within the extension, allowing users to report potential phishing incidents directly. Implement a quick response protocol to assist affected users.

- Phishing Incident Analytics: Collect and analyze data related to phishing incidents through the extension, including attack vectors and trends, to continually improve anti-phishing strategies.

- Continuous User Training: Offer in-extension training materials, tutorials, and webinars to keep users informed about evolving phishing tactics and security best practices.

Methodology

1. Project Initiation:

- Define project scope, objectives, and deliverables.
- Assemble a cross-functional team of developers.
- Allocate resources and establish project timelines

2. Requirements Analysis:

- Gather and document detailed functional and technical requirements based on the problem statement and objectives.
- Identify key features such as APIs, detection algorithms.

3. Technology Stack Selection:

- Backend (Python for server-side development)
- Database (Firebase Realtime Database or Firestore for data storage)
- Machine Learning (Python with relevant libraries, such as scikit-learn or TensorFlow)

4. Development:

- Browser Extension (JavaScript)
- Frontend (HTML, CSS)
- Database (mongoDB) - To store blacklisted domains

6. Data Integration:

- Integrate Firebase for data storage and authentication.
- Set up real-time data synchronization between browser extension and Firebase to provide live updates.

7. Testing

8. Deployment

Conclusion

In conclusion, we aim to produce a browser extension which when installed will help it's users from not getting coaxed into phishing scams. Our project will safeguard the user while also giving them knowledge on the how to, so they can use that knowledge and even pass it on to safeguard others. Our product will be rapidly evolving with the ever-growing knowledge base in the phishing sector and stay up-to-date.We strive to have it working efficiently

Guide Signature **Mr. Praveen Pawaskar**	**Reviewer Signature** **Dr. Mohana S D**