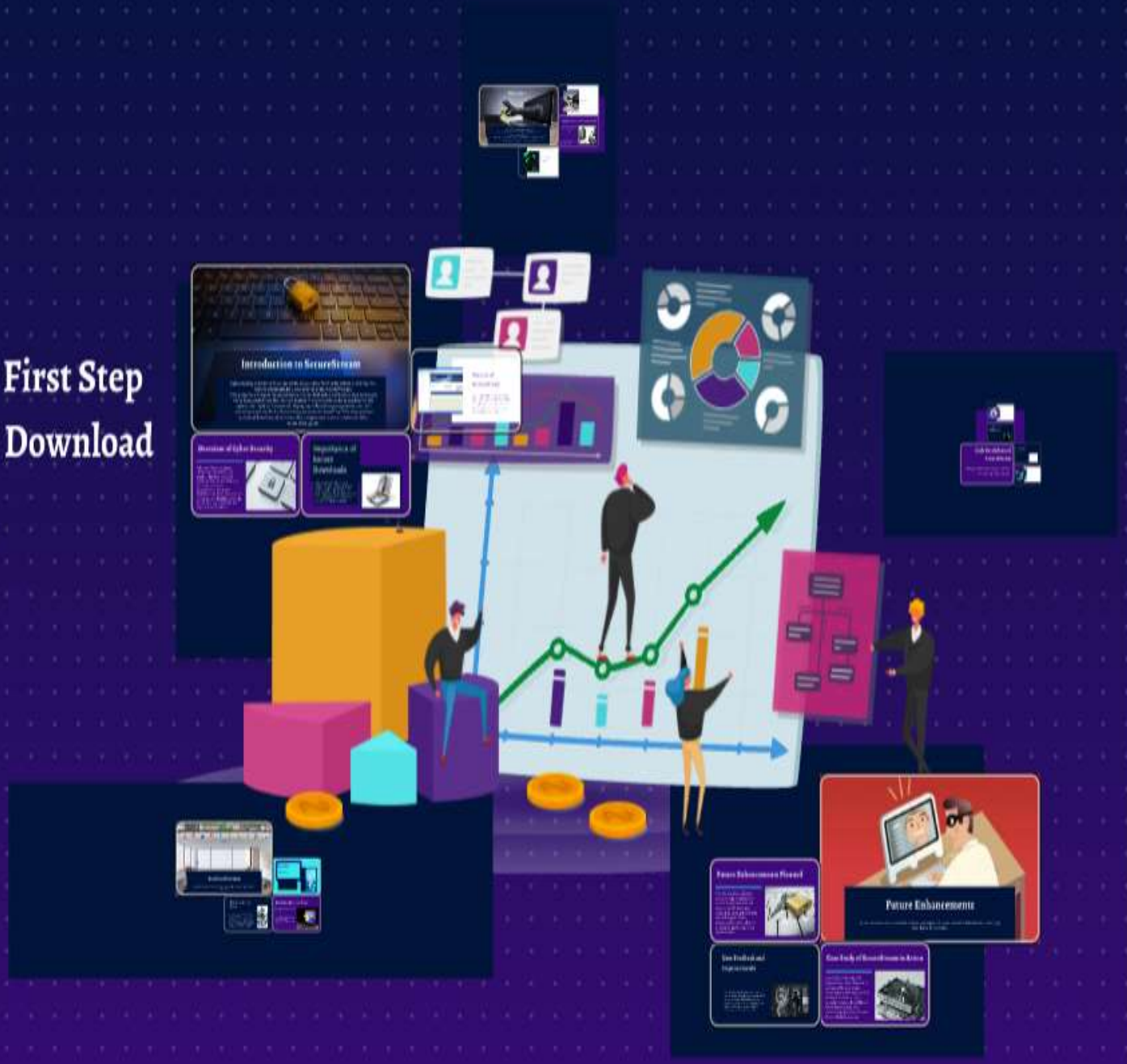
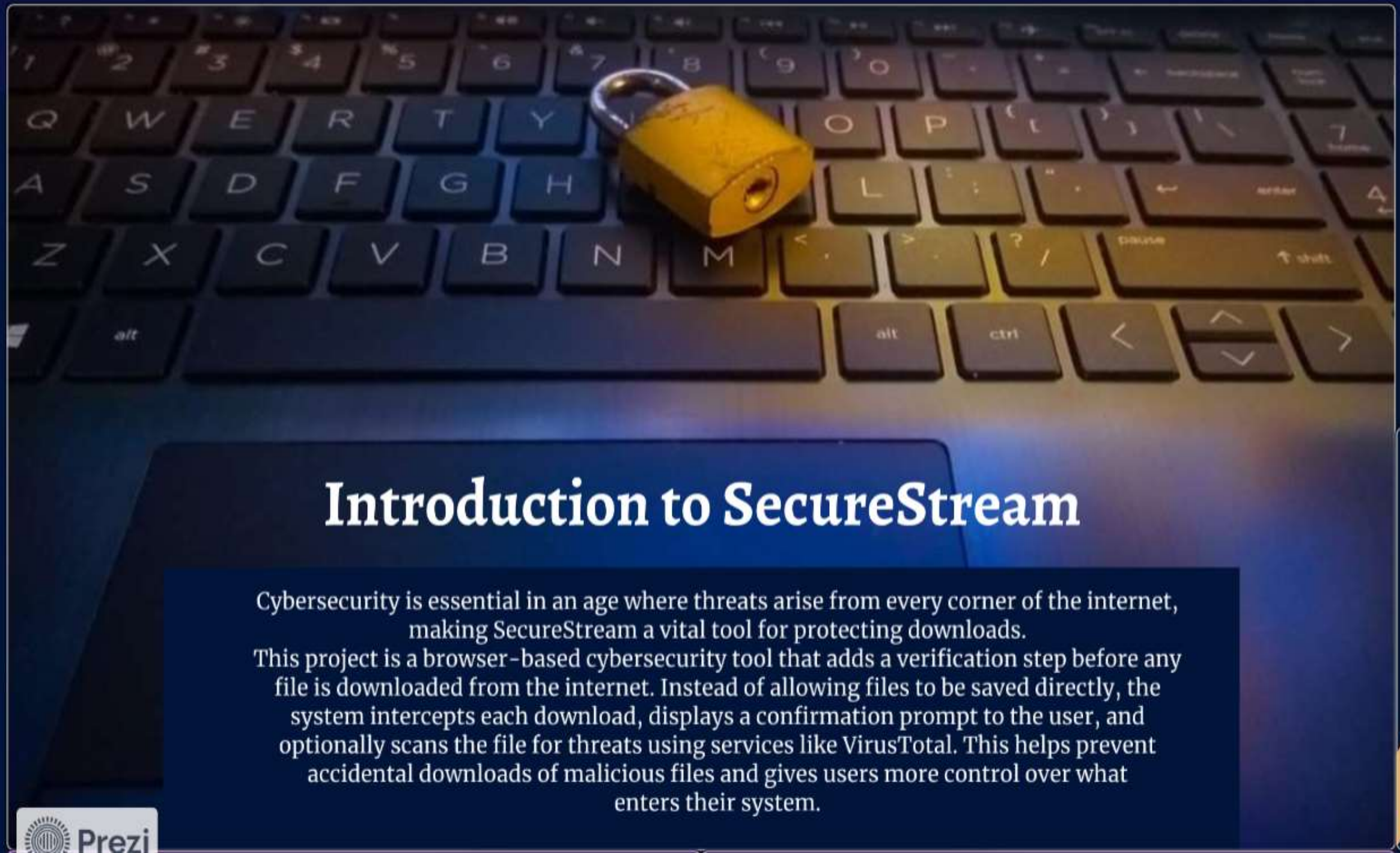
SecureStream: Your First Step of Defense for Every Download

Implementing a Cyber Security Verification Process for File Downloads





Introduction to SecureStream

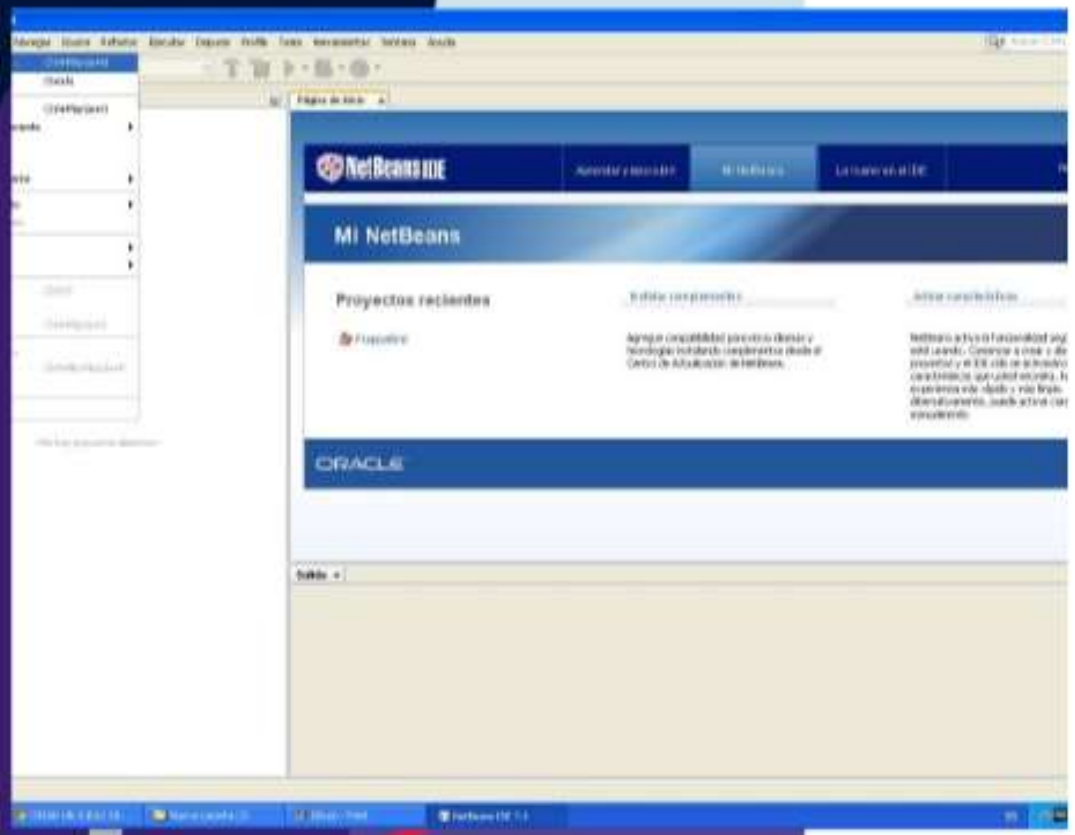
Cybersecurity is essential in an age where threats arise from every corner of the internet, making SecureStream a vital tool for protecting downloads.
This project is a browser-based cybersecurity tool that adds a verification step before any file is downloaded from the internet. Instead of allowing files to be saved directly, the system intercepts each download, displays a confirmation prompt to the user, and optionally scans the file for threats using services like VirusTotal. This helps prevent accidental downloads of malicious files and gives users more control over what enters their system.

Overview of Cyber Security

Cybersecurity encompasses technologies, processes, and practices designed to protect networks, devices, and data from unauthorized access, vulnerabilities, and attacks. Awareness and robust measures are critical as cyber threats continue to evolve, affecting individuals and organizations worldwide.

Importance of Secure Downloads

Secure downloads are crucial to prevent malware, ransomware, and phishing attacks. By verifying files before downloading, users can mitigate risks, protect personal information, and maintain system integrity.



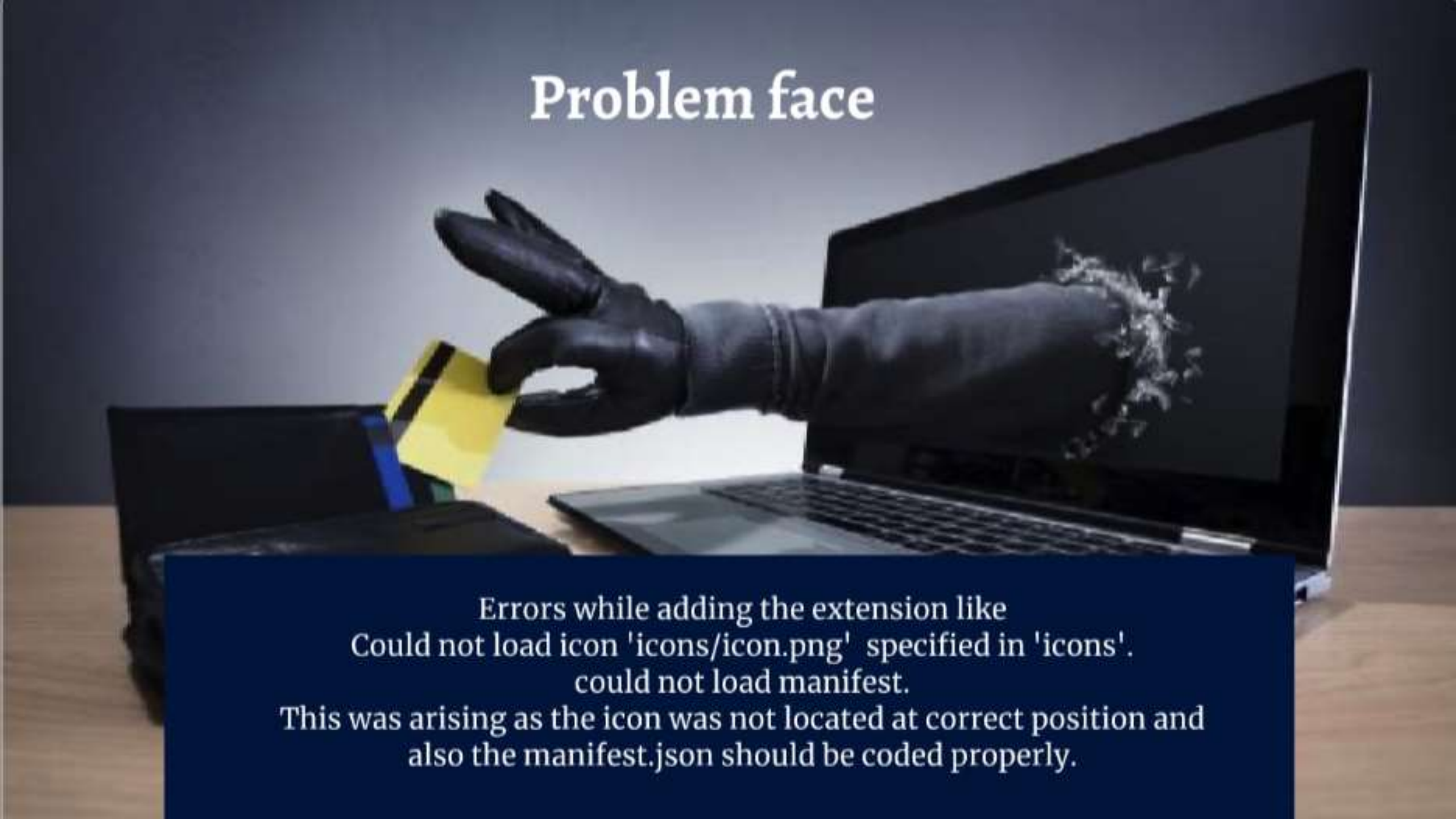
Purpose of SecureStream

SecureStream serves as a verification step before any file is downloaded from the web, ensuring that users only receive safe and verified files. This reduces the likelihood of harmful software infiltrating user systems, enhancing overall digital safety.

How SecureStream Works

The browser extension monitors all download attempts. When a file is about to be downloaded, it pauses or cancels the action, then shows a popup asking the user to verify the download. The user can choose to allow or block it. Optionally, the extension can send the file URL to a scanning service like VirusTotal to check for malware before allowing the download to proceed.

Problem face



Errors while adding the extension like
Could not load icon 'icons/icon.png' specified in 'icons'.
could not load manifest.
This was arising as the icon was not located at correct position and also the manifest.json should be coded properly.

Solution

Locating the icon.png in proper location. Correcting the code in manifest also it should be placed in root folder.

Rise of Cyber Threats

Recent statistics show that cyber threats have increased significantly, with a 200% rise in ransomware attacks in the past three years. This alarming trend highlights the urgent need for robust cybersecurity protocols in file downloading processes.

Risks Associated with Unverified Downloads

Downloading files without verification exposes users to malware, data breaches, and identity theft. Ignoring these risks can lead to significant financial and reputational damage for both individuals and organizations.

Verification Process Steps

The verification process consists of several steps: scanning the file for viruses, checking against blacklists, and validating the source's authenticity. Only files passing all checks are allowed download, creating multiple layers of security.

RealLife usecase.

Enterprise security
Parental control
Educational institutions
public access computer

JSON Structure for Verification

The JSON structure used in SecureStream outlines essential file information such as file type, size, source URL, and hash value for verification. This structured format allows for efficient data handling and facilitates secure checks during the download process.

JavaScript Implementation

SecureStream utilizes JavaScript to execute the verification process upon a user's download request. The script checks the integrity of the file against the recorded hash value, ensuring the downloaded content is safe and unaltered.

Future Enhancements Planned

To enhance SecureStream, plans include integrating AI-driven threat detection for smarter verification and expanding compatibility with more file types. These enhancements aim to bolster protection against evolving cyber threats.