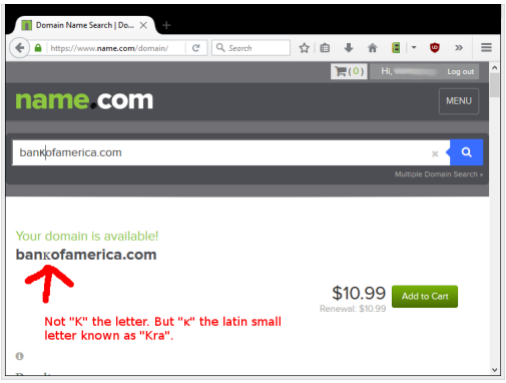
Ogadimma Chibuike
CYSE 494
May 31, 2023

Proposal

There is new technology and systems being created every day to help people get through day-to-day tasks. With the rapid advance of technology, also comes the creation of different methods used to exploit and hack into this technology. Two common ways people are hacked are by using typo-squatting and phishing tactics. Phishing and typo-squatting are two sneaky tricks that cybercriminals use to trick people online. Phishing happens when scammers pretend to be trustworthy organizations, like banks or email providers, to trick you into giving them your personal information, such as passwords or credit card numbers. Typo-squatting, on the other hand, takes advantage of common spelling mistakes people make when typing website addresses. These scammers create fake websites that look just like the real ones, and when you accidentally type the wrong address, they try to steal your information or infect your computer with malware. It's important to be aware of these tactics and stay cautious to protect yourself from falling into their traps.

Typo-squatting and phishing are a problem because they prey on a user's innocent mistakes while typing website addresses. When they make small spelling errors, cybercriminals take advantage of this and create these fake sites. Many of the sites just have a small error in the URL that a user probably wouldn't notice every time. Once we mistakenly enter the wrong address, these fake websites may trick us into giving away personal information or infect our devices with harmful software. It can lead to financial loss, identity theft, or other serious consequences. Therefore, it is crucial to be mindful of our typing and double-check website addresses to avoid falling victim to typo-squatting and protect ourselves from potential harm. For example, a user might be meaning to type in www.google.com, but instead they type www.joogle.com. Bad actors will buy this domain and infect the site so that when you enter the site your information is vulnerable. Another typo-squatting method hackers use is called an IDN homograph attack. They do this by using special characters that may look like normal letters but are different. For example, they might use a letter from a foreign language that looks like an English letter or replace a letter with a similar looking one. When we type in the website address, it looks right, but we end up on a fake website created by the hackers. They use this trick to try and fool us into giving away our personal information or infect our devices with harmful software. It's important to be cautious and double-check the website addresses we visit to avoid falling into these traps.



Ogadimma Chibuike
CYSE 494
May 31, 2023

In the figure above I have given an example of an IDN homograph attack where you can see that the letter ‘k’ in the Bankofamerica.com is not the regular letter k.

We have come up with what we think is the best solution to solve this issue. We have created a browser extension that scans URL and download links for mismatched file extension and malicious links. Our browser extension can scan for mismatched file extensions by intercepting and analyzing the URLs of downloaded files. When a user initiates a download, the browser extension can capture the URL and extract the file extension from it. Then, it can compare the extracted file extension with the actual file type of the downloaded file. If there is a mismatch between the file extension and the actual file type, the browser extension can raise an alert or provide a warning to the user. This comparison can be done by using predefined lists or databases that map file extensions to their corresponding file types. Additionally, the extension can leverage file signature analysis to verify the file's integrity and determine its true type. By implementing such checks, the browser extension can help users identify potentially malicious or misleading files that have mismatched file extensions.

There are a few potential barriers that we could face when developing a browser extension that scans for mismatched file extensions:

- Technical Limitations: Browser extensions work within the constraints enforced by the browser's extension API (application programming interface). The API may have limitations on the types of information that can be accessed or the level of access to system resources. These limitations can impact the effectiveness and accuracy of your extension's scanning capabilities.
- Privacy Concerns: Scanning and analyzing URLs and downloaded files can raise privacy concerns among users. It's important to handle user data securely and transparently, ensuring that sensitive information is not stored or transmitted without proper consent. Complying with privacy regulations and implementing robust data protection measures is crucial.
- False Positives and False Negatives: Developing an effective algorithm to detect mismatched file extensions accurately can be challenging. There is a risk of false positives, where legitimate files are flagged as mismatches, causing inconvenience to users. Conversely, false negatives can occur when potentially harmful files are not detected as mismatches, leading to a false sense of security.
- Performance Impact: Scanning and analyzing files in real-time can impose a performance overhead on the browser. Extensive processing or resource-intensive operations may slow down the browsing experience or strain system resources, negatively impacting user satisfaction.

Ogadimma Chibuike
CYSE 494
May 31, 2023

- Browser Compatibility: Different browsers have varying extension APIs and support different features. Ensuring compatibility across multiple browsers can be time-consuming and require additional development efforts.

To overcome these barriers, thorough testing, continuous improvements, and user feedback can help refine the scanning algorithm and address potential limitations. Open communication with users regarding privacy practices and offering customizable settings can help mitigate concerns and improve user trust in the extension.

We can determine the success of our browser extension by looking at the number of people who install and regularly use it, as well as the positive feedback and high ratings it receives from users. If more and more people are using our extension and finding value in its features, it indicates that it is successful. Additionally, if users engage with our extension frequently, use its different features, and provide positive reviews, it suggests that our extension is meeting their needs and enhancing their browsing experience.

Ogadimma Chibuike
CYSE 494
May 31, 2023

Reference:
https://github.com/SoftwareAddictionShow/IDN-homograph-attack