



Warning Users of Phishing Attacks with a Google Chrome Extension

8/5/2015 HCII

Jing Chen, Weining Yang, Aiping Xiong*, Ninghui Li, Robert Proctor

Funding for this research was provided by
the National Security Agency as part of a Science of
Security label through North Carolina State University



Phishing

Definition: Fraud perpetrated on the Internet; *spec.* the impersonation of reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

(The Oxford English Dictionary, 2015)

Phishing Lifecycle:

- starts from an unsolicited email sent by the deceiver posing as a legitimate party
- continues on the fraudulent webpage mimicking the authentic one after users' click on the link within the email
- ends with victims entering personal and credential information

Email

Dear Chase Customer:

We have received multiple failed login attempts from your online account. For your protection, we have locked your account.

To restore your online access click: [Log On to Chase](#) and proceed with the verification process.

Please don't reply directly to this automatically-generated e-mail message.

Sincerely,
Online Banking Team

© 2013 JPMorgan Chase & Co.

Webpage

https://www.chase.com.thisisnotchase.com

Personal | Business | Commercial Find a Branch or ATM | Contact Us | En Español

CHASE Search

Products & Services News & Stories Log In or Enroll

Welcome back

User ID Password Log In to Accounts

Forgot User ID/Password? Remember Me

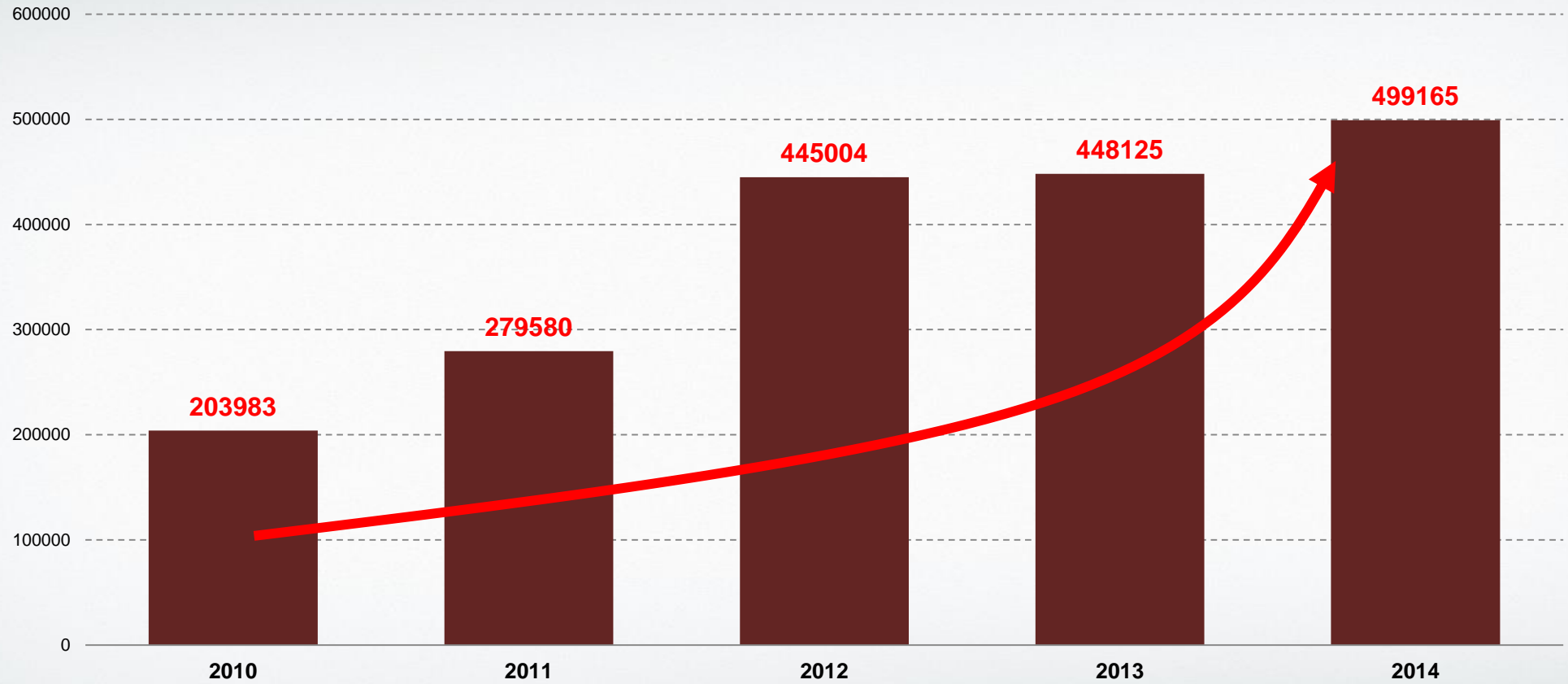
Quick and Simple Card Finder
In just **2 steps**, find the card that fits your needs.
[Get Started »](#)

Rates Are Low Again—Lock In Today
Buying a new home? Refinancing? Shop smart by prequalifying for a new Chase mortgage.
[See Low Rates »](#)

Insights, News and Stories
Helpful articles ranging from finance to community.
[Learn more »](#)

More from Chase ▾

Phishing Attack Volume



Source: <http://www.emc.com/domains/rsa/index.htm>

Research Against Phishing Attacks

- Focus is on computational technologies, such as automated tools to detect/inhibit phishing emails, website blacklists
- Final decision of webpage legitimacy is made by user; decision aid tools developed to assist users to detect fraudulent websites

Research Against Phishing Attacks

Limited success, ineffectiveness and usability problems generally found across assistant tools evoked further investigation which indicates:

- Users' attention is dominated by visual cues reinforcing webpage legitimacy, while ignoring the browser-based security cues;
- Users not familiar with phishing attacks and have difficulty understanding security warnings

A Chrome Extension Warning

User's attention:

- Stop sign to attract attention
- Domain name extracted from URL to aid user's decision about the website's legitimacy

User's understanding:

- Specific and complete identification of the risk
 - Without technical language
 - Not so lengthy that it takes time and effort to read the warning
- Explicit explanation of consequences if exposed to the risk

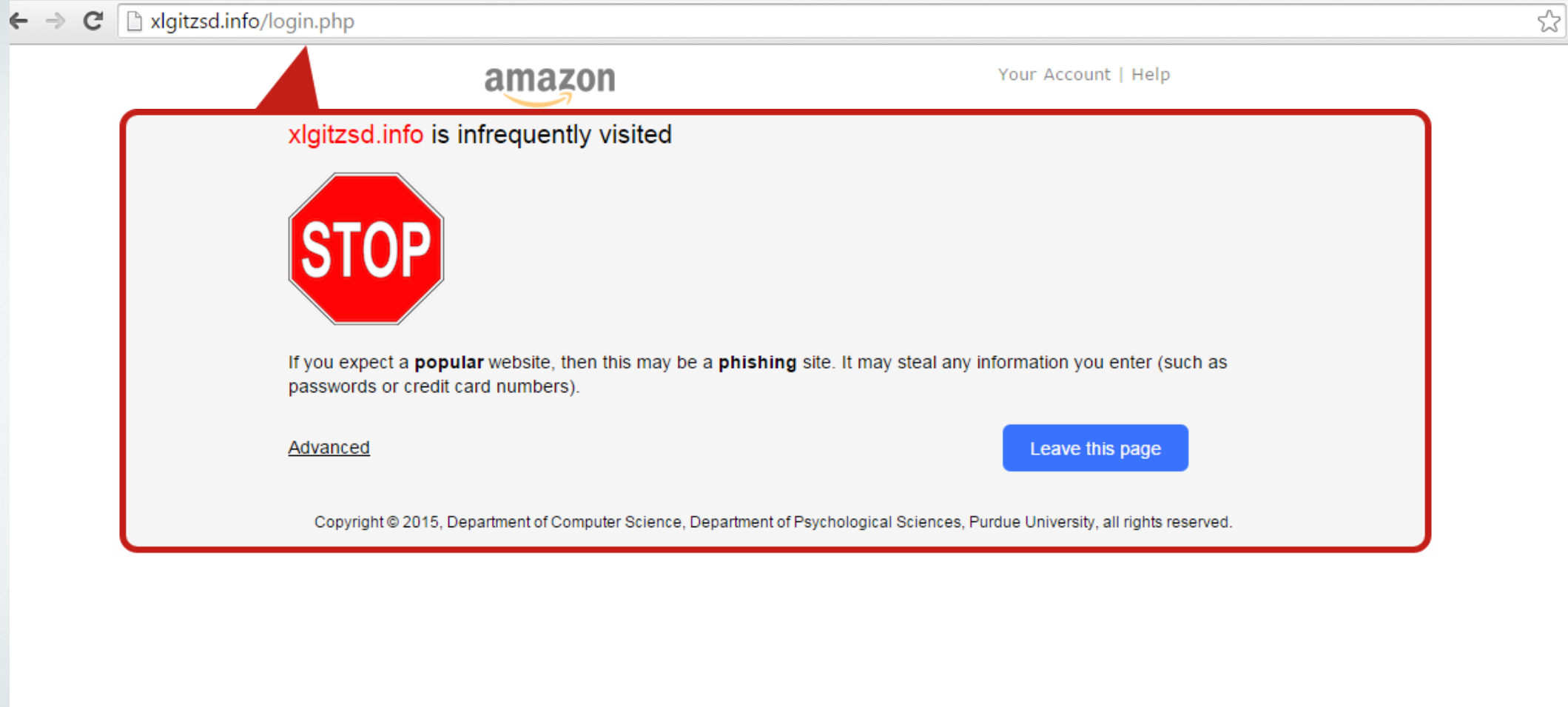
User's action:

- Highlight the recommended action

A Chrome Extension Warning


- Popularity difference between phishing websites and legitimate popular websites
- Phishing sites visited infrequently, with more than 89.5% of them with a rank $> 100,000$

Warning Interface



The screenshot shows a web browser window with the address bar containing "xlgitzsd.info/login.php". The page header features the "amazon" logo and "Your Account | Help" links. A large red-bordered warning box is centered on the page, containing the following text and elements:

xlgitzsd.info is infrequently visited



If you expect a **popular** website, then this may be a **phishing** site. It may steal any information you enter (such as passwords or credit card numbers).

[Advanced](#) [Leave this page](#)


Copyright © 2015, Department of Computer Science, Department of Psychological Sciences, Purdue University, all rights reserved.

Warning Interface

← → ↻ xlgitzsd.info/login.php ☆

amazon Your Account | Help

xlgitzsd.info is infrequently visited



If you expect a **popular** website, then this may be a **phishing** site. It may steal any information you enter (such as passwords or credit card numbers).

[Hide advanced](#) [Leave this page](#)

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by posing as a legitimate website.
This website **NOT** in the top **100,000,000** most popular sites in the world.*
For your reference, **yahoo.com** is the **5th**, **wordpress.com** is the **33th**, **ups.com** is the **216th**.*
* Data are collected from [Alexa](#)

[Back to xlgitzsd.info](#)

Copyright © 2015, Department of Computer Science, Department of Psychological Sciences, Purdue University, all rights reserved.

Experiment Design

- A 3-week field experiment using the phishing warning Chrome extension for daily computer use
- Participants were informed that they were taking part in a study about browser behavior of daily use
- Phishing scenario that replicates a popular commercial website promotion
- Two groups:
 - control (no warning)
 - experiment (warning pop ups when user types information on domains ranked greater than 100,000)
- In week 3, an email of Amazon gift card including links associated with a newly registered “phishing” domains maintained by us, simulating phishing attacks

Results to Date

- All 11 participants (control group) who did not see the warning provided correct passwords during the “phishing” week.
- 5 of 7 participants (experiment group) who saw the warning chose “Leave this page” or closed the tab. Interview of two participants fell into phishing:
 - One saw the warning during the first two weeks when he visited a pet tracking website that was 100% secure. Thus, he thought the warning was a bug of Chrome.
- Participants who saw the warning:
 - understood the most important information delivered from the warning.
 - the frequency of the warning was thought to be rare and acceptable.

Summary

- Users understand the warning based on the current interface design.
- The chrome extension warning compliance rate is over 70%, indicating the domain name ranking difference is promising to aid user's decision of webpage's legitimacy.
- False positives will result in not trusting the extension.

Next Step

- Recruit more participants to verify the effectiveness of the warning obtained with the first 18 participants.

Thank you!