Effectiveness of a Phishing Warning in Field Settings

Weining Yang, Jing Chen, Aiping Xiong,
Robert W. Proctor, Ninghui Li
Purdue University

INTRODUCTION

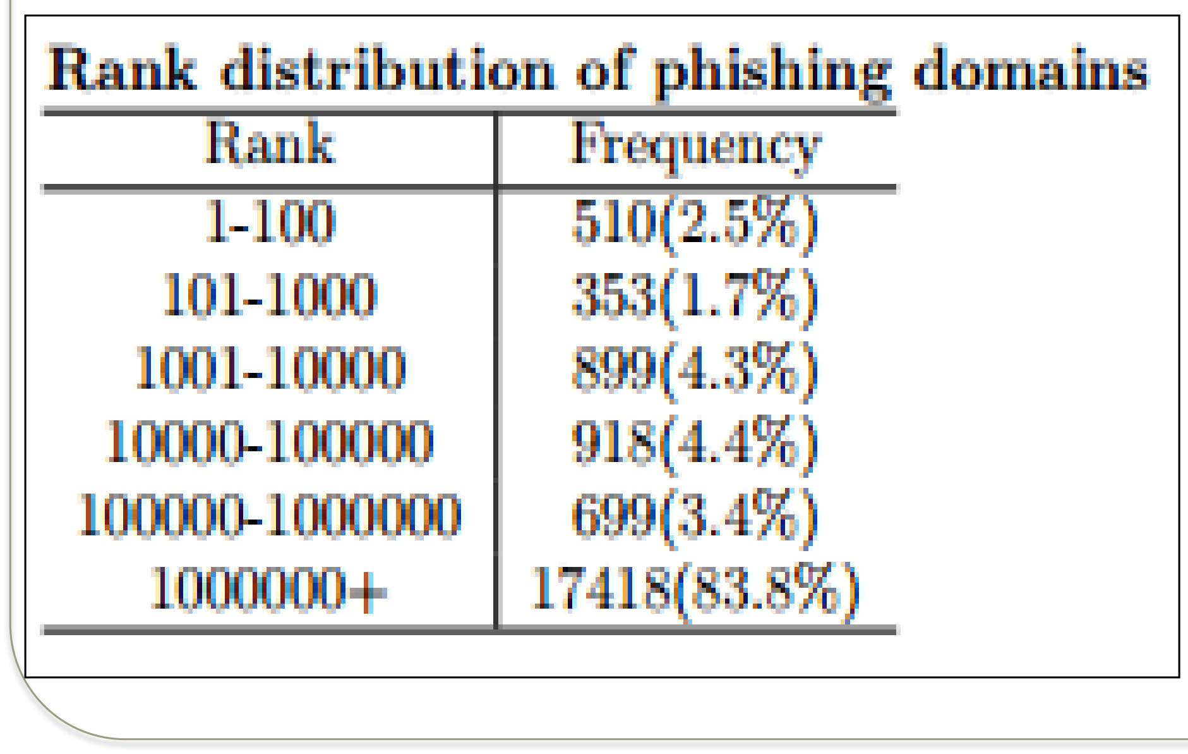
- Phishing attacks keep growing and evolving
- Users
  - are easily deceived
  - ignore bowser-based cues
  - do not understand active phishing warnings
- Detection of phishing websites
  - blacklist-based methods
  - heuristic methods

BROWSER EXTENSION DESIGN

Active warning presented with a Chrome extension

- popularity differences between phishing websites and legitimate popular websites
- phishing sites visited infrequently, with more than 91% of them having a rank > 10,000 (see Table 1)
- domain name extracted to aid user's decision about the website's legitimacy (see Figure 1)

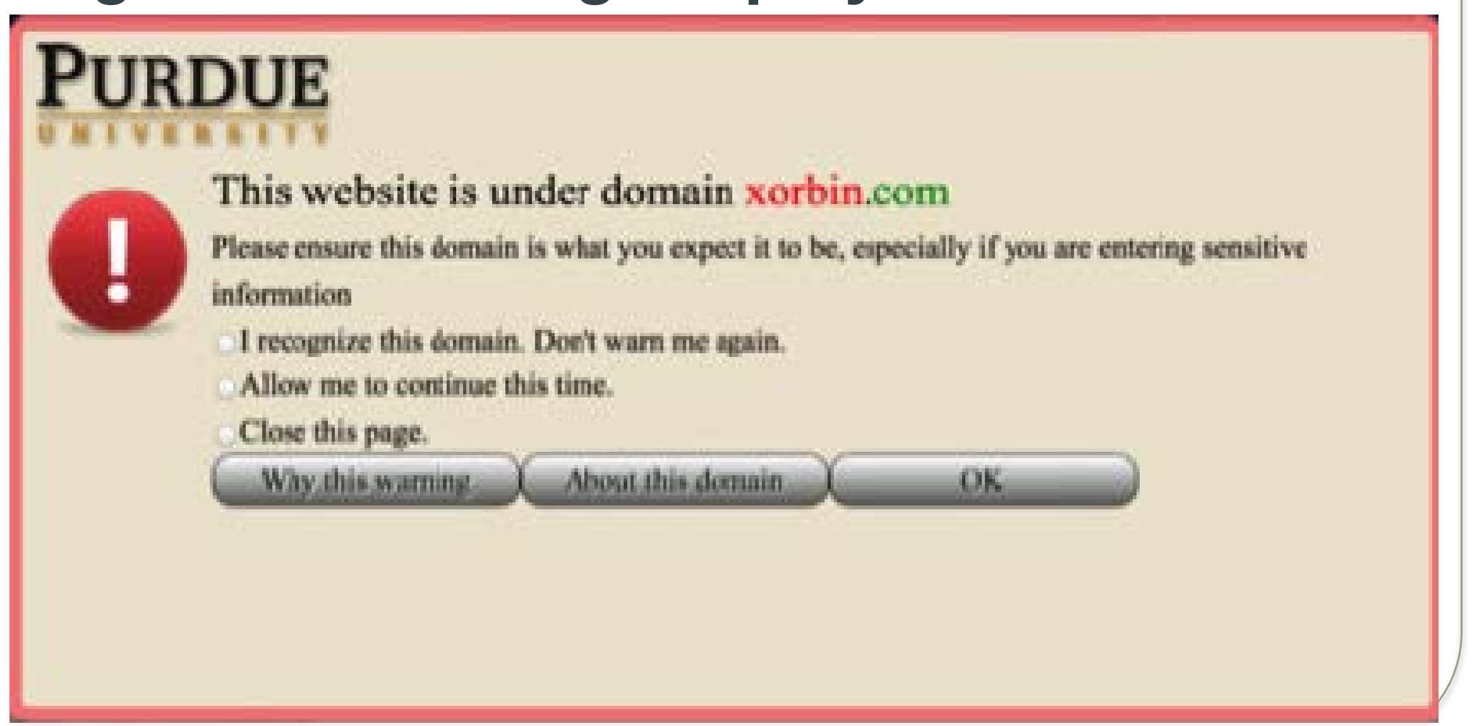
Table 1:



Rank distribution of phishing domains

Rank	Frequency
1-100	510(2.5%)
101-1000	353(1.7%)
1001-10000	899(4.3%)
10000-100000	918(4.4%)
100000-1000000	699(3.4%)
1000000+	17418(83.8%)

Figure 1: Warning Display



This website is under domain xorbin.com

Please ensure this domain is what you expect it to be, especially if you are entering sensitive information

○ I recognize this domain. Don't warn me again.
○ Allow me to continue this time.
○ Close this page.

PRELIMINARY EXPERIMENT

A 6-week field experiment using the phishing warning Chrome extension for daily computer use:

- control group (no warning) and experimental group (warned when trying to type information on domains ranked greater than 10,000)
- participants required to fill out a survey on a website through a link in weekly email sent by us
- in weeks 4 and 6, links in the email were associated with two newly registered "phishing" domains maintained by us, simulating phishing attacks

RESULTS

- 1 of 6 participants in experimental group provided correct passwords during the "phishing" weeks
- No participants chose "Close the page" or closed the tab
- Wrong passwords observed mainly due to keying errors
- Tended to ignore the warning due to mainly the mandatory survey task and partly to the interface design
- About half the participants did not understand the meaning of phishing

NEXT STEP

A full study redesigned with

- a new phishing scenario that replicates a popular commercial website promotion requesting only a voluntary response
- a redesigned warning interface
- participants' lack of knowledge of phishing taken into consideration

http://hot-sos.org/

The Science of Security initiative is
funded by the National Security Agency.