Use of Phishing Training to Improve Security Warning Compliance: Evidence from a Field Experiment

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

Purdue University

Overview

- Problem: To protect users from entering information into an illegitimate website
- Domain traffic ranking as warning trigger
- Field Experiments
  - Pilot Study
  - Main Study
- Discussion

Problem

Phishing attacks keep growing and evolving

- Users
  - easily deceived
  - ignore bowser-based cues
  - do not understand active phishing warnings
- Detection of phishing websites
  - blacklist-based methods
  - heuristic methods
- But not 100% accurate

Problem

- High false negative rate
    - Phishing sites often not up long
    - Renders blacklisting ineffective
    - Infrequently used sites, but mimicking frequently used sites
    - Mismatches easy for users to understand
- Conducted experiments based on conveying this information to users in warnings

Domain Traffic Ranking

Phishing sites visited infrequently, with more than 91% of them having a rank > 10,000

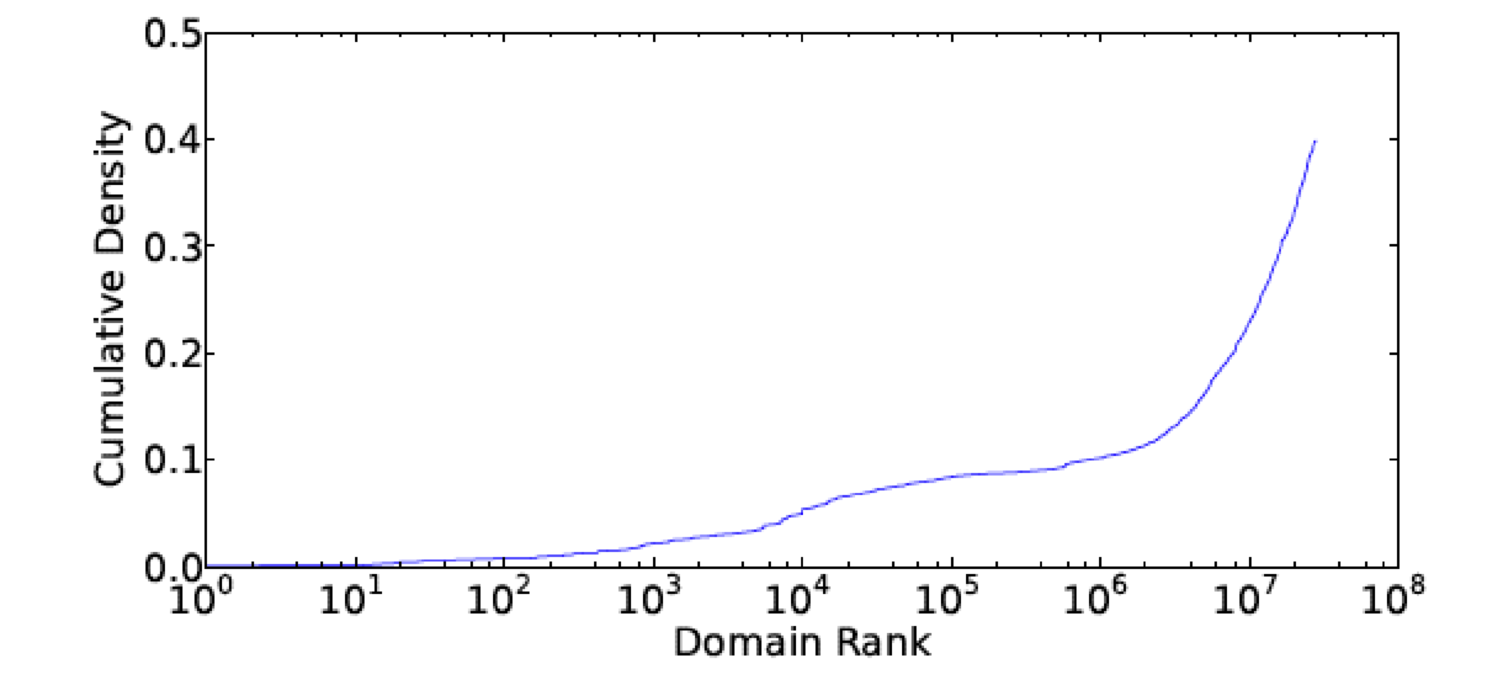


Figure 1: Cumulative density of reported phishing URLs in PhishTank based on traffic rankings

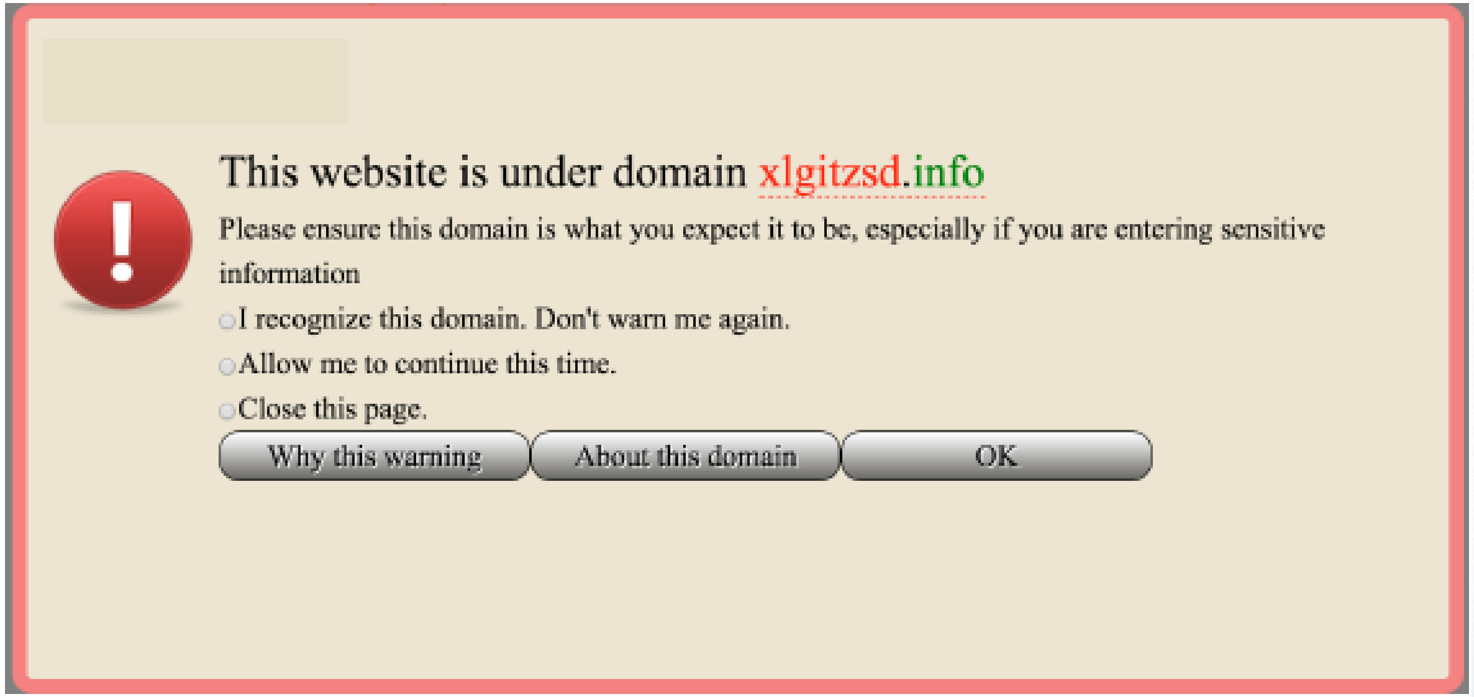
Domain Traffic Ranking

Active warning presented within a Chrome extension

- used traffic ranking as the criterion for phishing detection
- presented it as the reason why the warning was displayed in the warning interface.

Pilot Study: Warning

Domain name extracted to aid user’s decision about the website’s legitimacy



This website is under domain xlgitzsd.info

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.

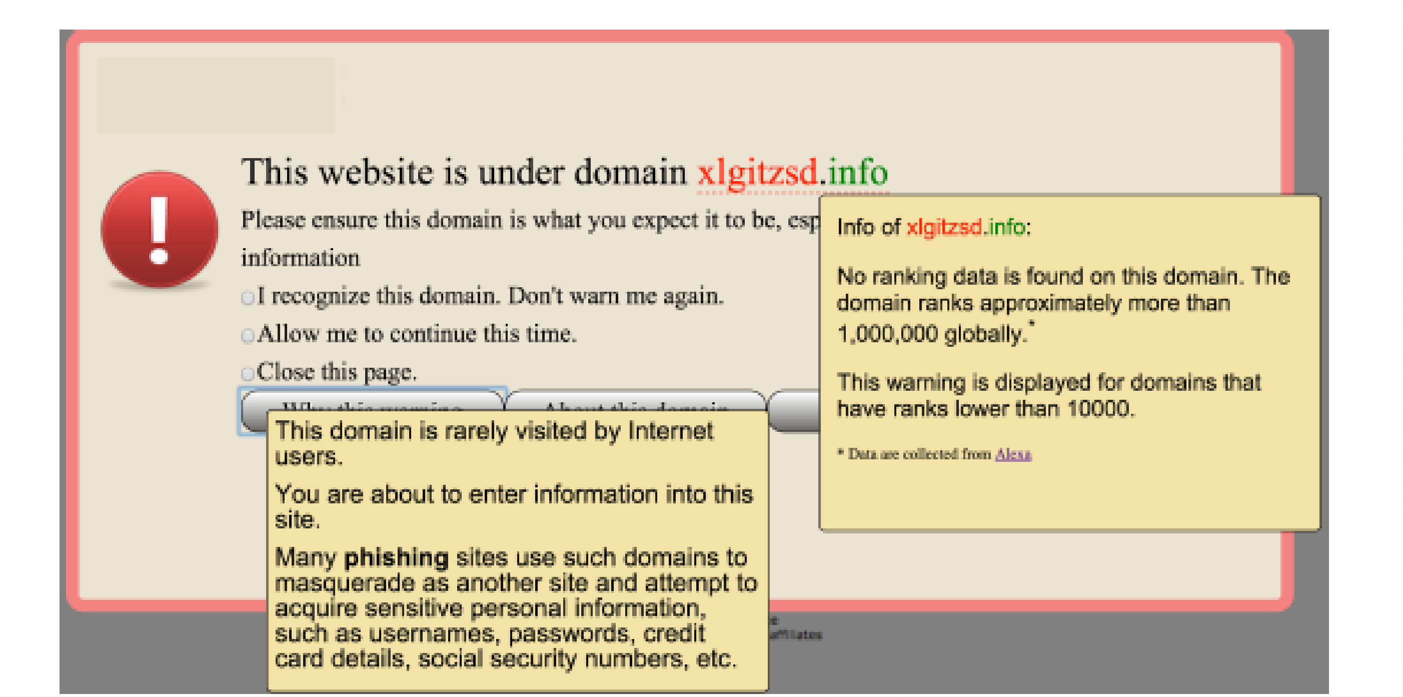
○ Allow me to continue this time.

○ Close this page.

Figure 2: Warning Display

Pilot Study: Warning

Domain name extracted to aid user's decision about the website's legitimacy



This website is under domain xlgitzsd.info

Please ensure this domain is what you expect it to be, esp

information

○ I recognize this domain. Don't warn me again.

○ Allow me to continue this time.

○ Close this page.

This domain is rarely visited by Internet users.

You are about to enter information into this site.

Many **phishing** sites use such domains to masquerade as another site and attempt to acquire sensitive personal information, such as usernames, passwords, credit card details, social security numbers, etc.

Info of xlgitzsd.info:

No ranking data is found on this domain. The domain ranks approximately more than 1,000,000 globally.*

This warning is displayed for domains that have ranks lower than 10000.

* Data are collected from Alexa

Figure 3: Warning Display

Pilot Study: Method

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

- control group (no warning) and exp. group (warned when trying to type information on domains ranked greater than 10,000)
- participants required to fill out a survey on a web-site through a link in weekly email sent by us
- in week 6, links in the email were associated with newly registered “phishing” domain maintained by us, simulating phishing attacks
- At end, semi-structured interview

Pilot Study: Results

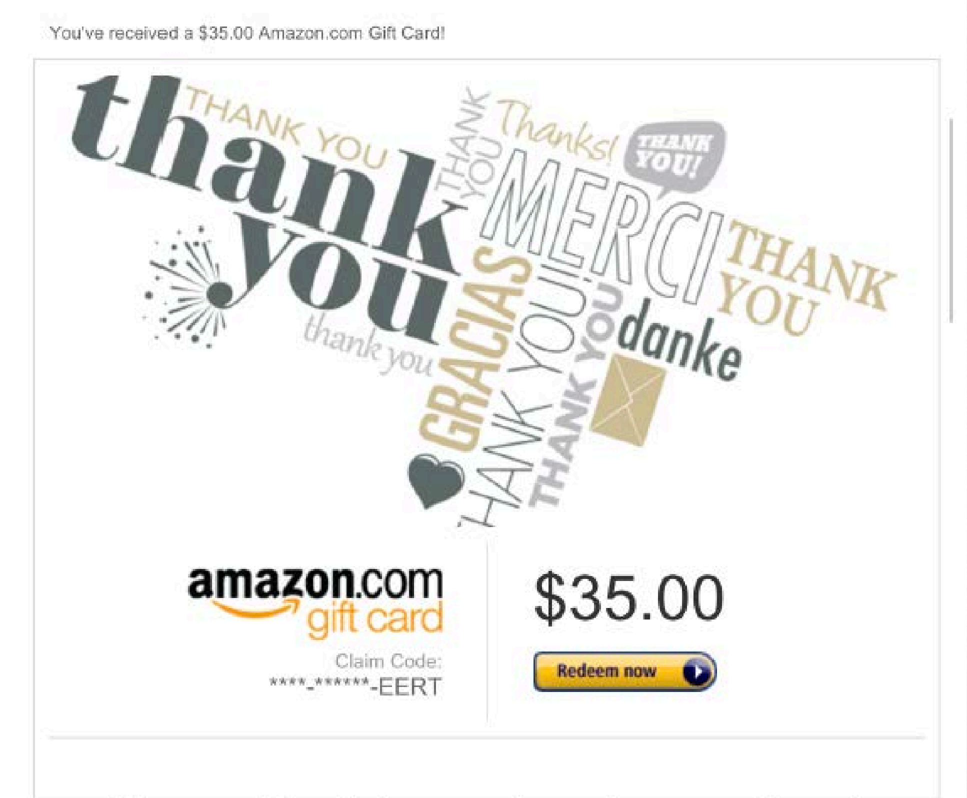
- No participants in experimental group chose “Close the page” or closed the tab
- However, only 1 of 6 provided correct passwords during the “phishing” week
- Wrong passwords observed mainly due to keying errors
- Tended to ignore the warning due to mainly the mandatory survey task and partly to the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

Main Study

- 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

Phishing Email Message

Amazon Gift Card



You've received a $35.00 Amazon.com Gift Card!

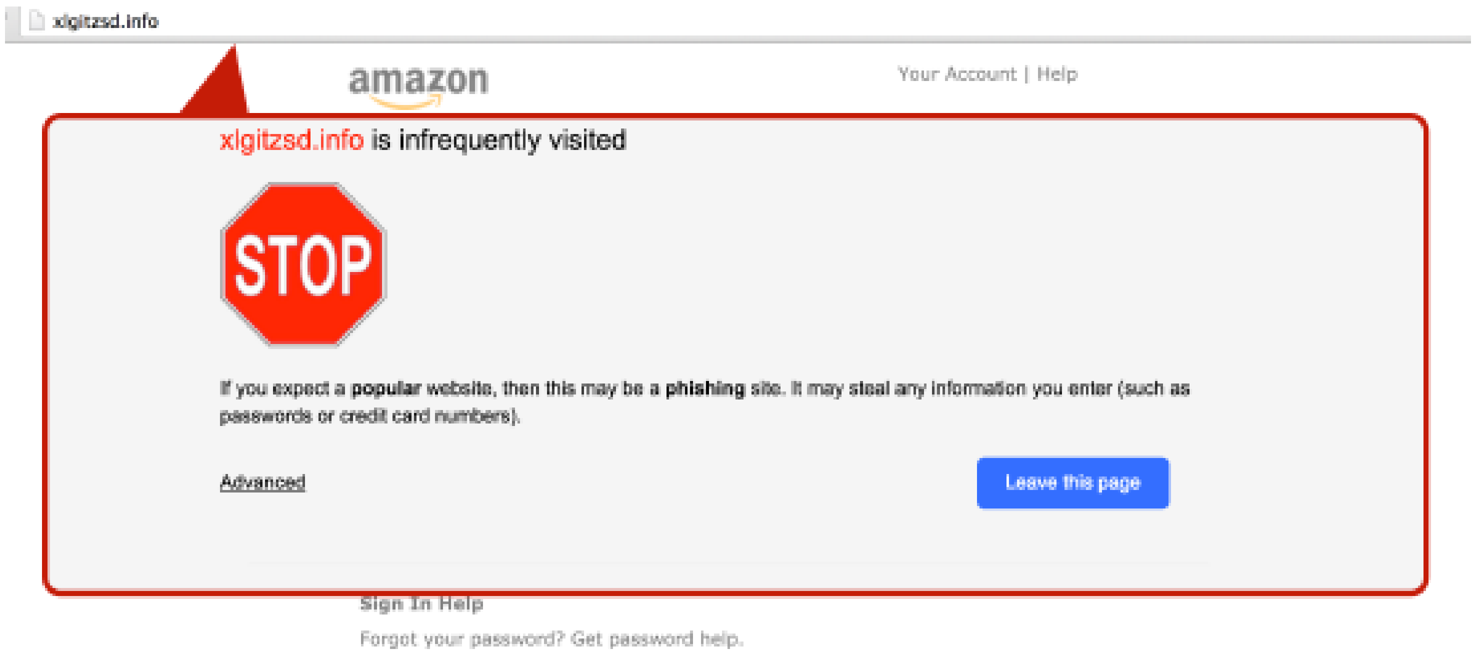
amazon.com gift card

$35.00

Claim Code:
****-******-EERT

Figure 5: Email that spoofs an Amazon gift card

New Warning Interface

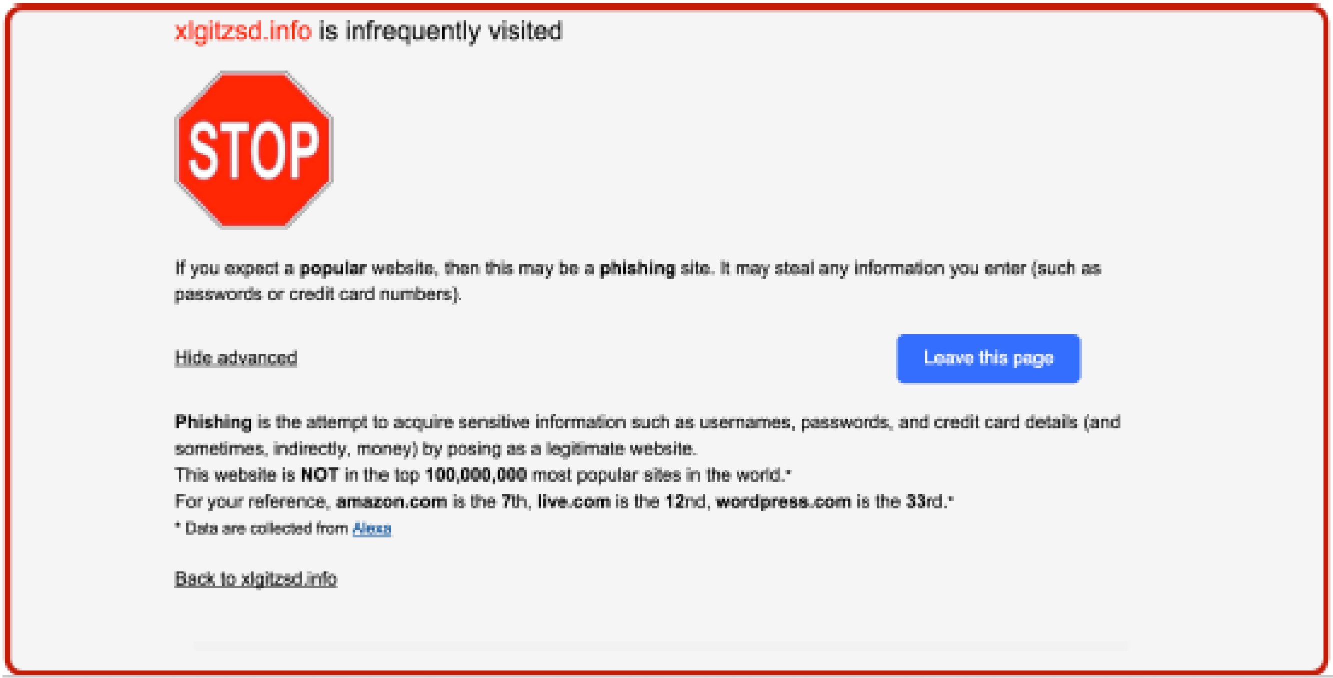


xlgitzsd.info is infrequently visited

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).

Figure 3: New Warning Interface.

New Warning Interface



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).

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 is **NOT** in the top **100,000,000** most popular sites in the world.*
For your reference, **amazon.com** is the 7th, **live.com** is the **12**nd, **wordpress.com** is the **33**rd.*
* Data are collected from Alexa

Back to xlgitzsd.info

Figure 4: New Warning Interface after clicking on "Advanced".

Brief Phishing Training

- The definition of phishing was provided and a banking phishing email example was presented. Participants were also taught how to evaluate the legitimacy of a URL by identifying the domain name.
- In addition, participants were tested with a list of URLs that included both legitimate and fraudulent types, with feedback provided.

Results

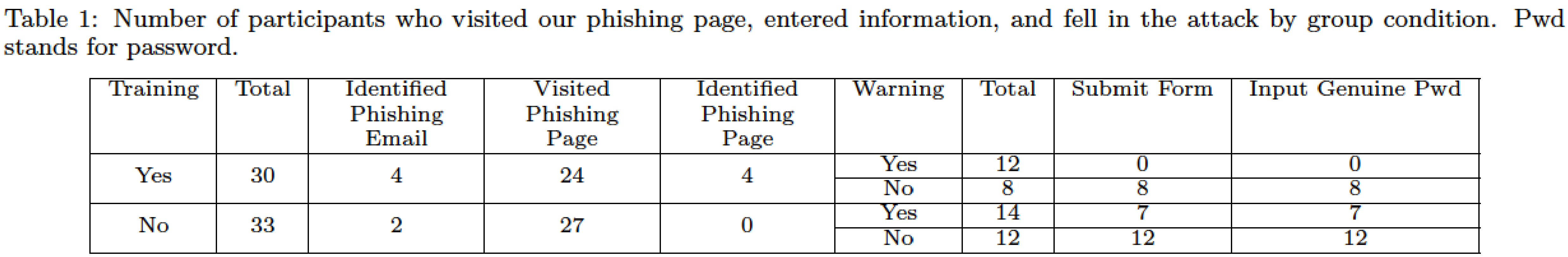


Table 1: Number of participants who visited our phishing page, entered information, and fell in the attack by group condition. Pwd stands for password.

Training	Total	Identified Phishing Email	Visited Phishing Page	Identified Phishing Page	Warning	Total	Submit Form	Input Genuine Pwd
Yes	30	4	24	4	Yes	12	0	0
					No	8	8	8
No	33	2	27	0	Yes	14	7	7
					No	12	12	12

Discussion

- Knowledge gained from the training enhances the effectiveness of phishing warnings
- The knowledge by itself was not sufficient to provide phishing protection
- Field experiment : time consuming vs. ecological validity