The Impact of Secure Transport Protocols on Phishing Efficacy

Zane Ma, Joshua Reynolds, Joseph Dickinson, Kaishen Wang
Taylor Judd, Joseph D. Barnes, Joshua Mason, Michael Bailey

University of Illinois Urbana-Champaign

Phishing

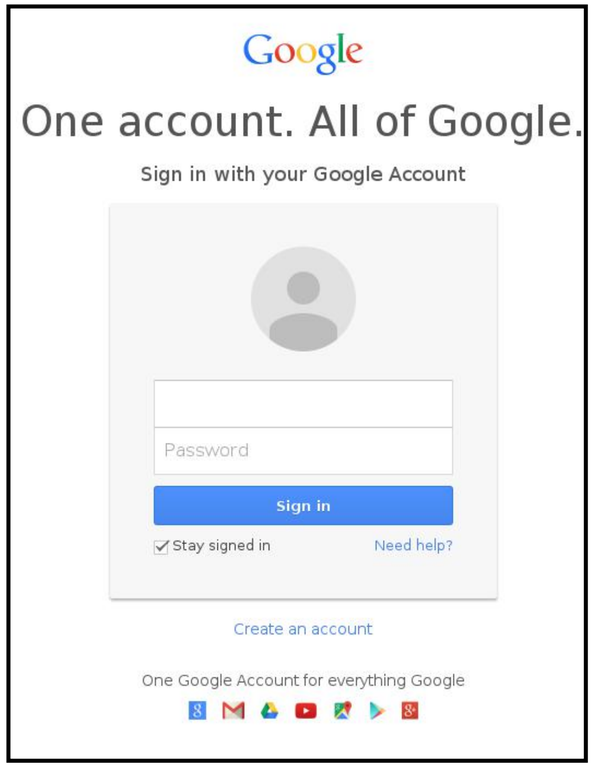
FBI estimated $12.5 billion in phishing losses from Oct 2013 - May 2018

Beyond financial impact:
Democratic National Convention emails

Root cause: misattribution of credibility/trust to an online entity

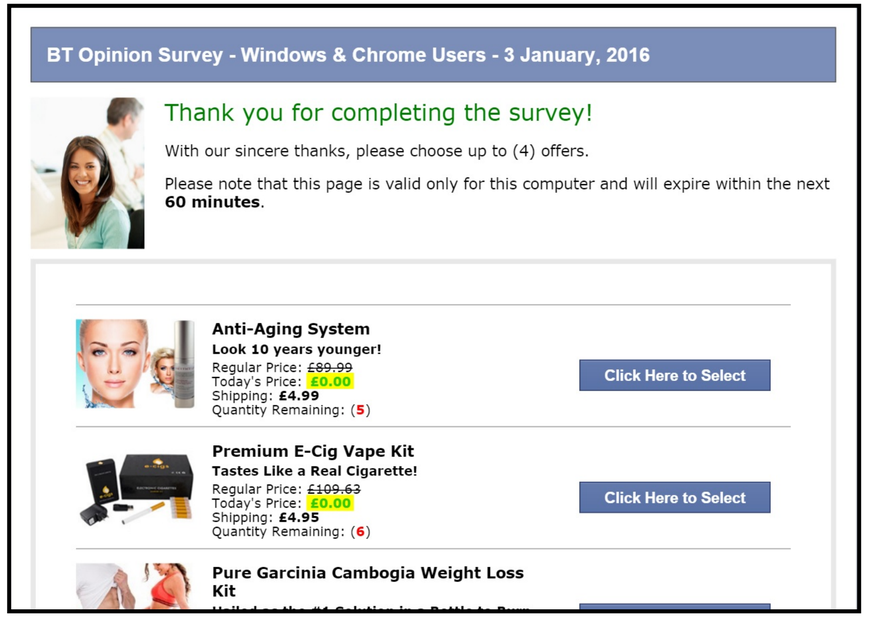
Misattribution of Trust

Mistaken trusted identity



accoounts-google.com

Mistaken credibility for new identity



questionsaboutisps.com

Existing Security Protocols Lack Credibility

Not designed to protect against phishing

TLS = Confidentiality + Integrity + Identity/Authenticity

Prior work:

1. Some users look at connection security indicators when exposed to phishing

2. Users confuse “connection security” and “site security”

Experimental Goals

1. Does the presence of secure transport protocols make phishing more effective?

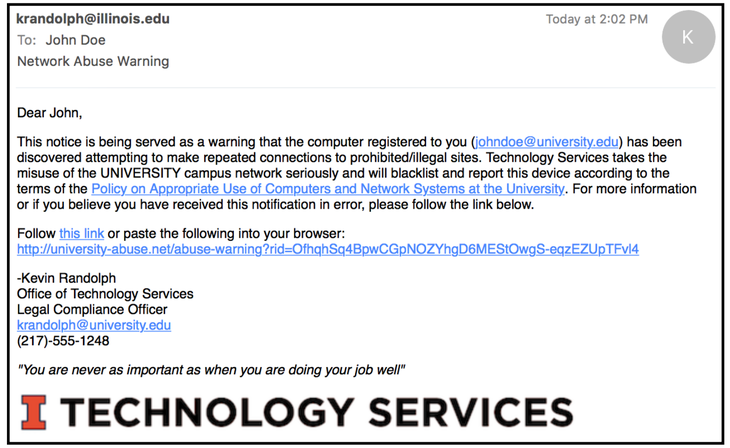
   Methodology: A/B test HTTP/HTTPS and SMTP/SMTP+TLS

2. Does browser URL bar UI (e.g. security indicators) influence phishing susceptibility?

   Methodology: Generate and feature code browser screenshots, correlate URL bar features with phishing outcomes

Phishing Experiment

1. Open Email



krandolph@illinois.edu
Today at 2:02 PM
To: John Doe
Network Abuse Warning

Dear John,

This notice is being served as a warning that the computer registered to you (johndoe@university.edu) has been discovered attempting to make repeated connections to prohibited/illegal sites. Technology Services takes the misuse of the UNIVERSITY campus network seriously and will blacklist and report this device according to the terms of the Policy on Appropriate Use of Computers and Network Systems at the University. For more information or if you believe you have received this notification in error, please follow the link below.

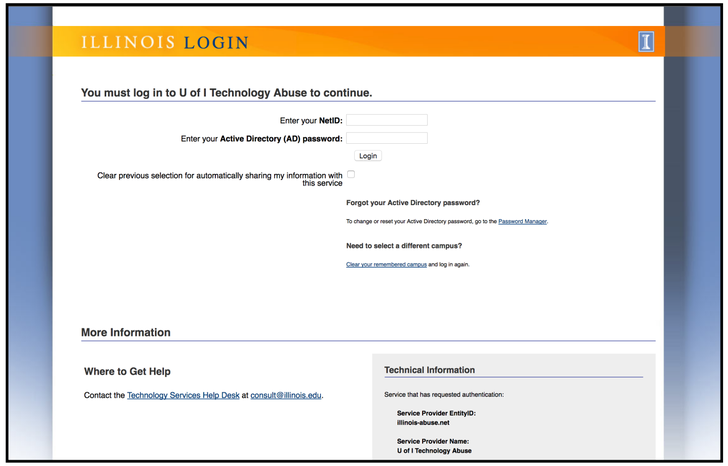
Follow this link or paste the following into your browser:
http://university-abuse.net/abuse-warning?rid=OfhqhSq4BpwCGpNOZYhgD6MEStOwgS-eqzEZUpTFvI4

-Kevin Randolph
Office of Technology Services
Legal Compliance Officer
krandolph@university.edu
(217)-555-1248

"You are never as important as when you are doing your job well"

TECHNOLOGY SERVICES

2. Access Site



ILLINOIS LOGIN

You must log in to U of I Technology Abuse to continue.

Enter your NetID:
Enter your Active Directory (AD) password:
Login
Clear previous selection for automatically sharing my information with this service

Forgot your Active Directory password?
To change or reset your Active Directory password, go to the Password Manager.

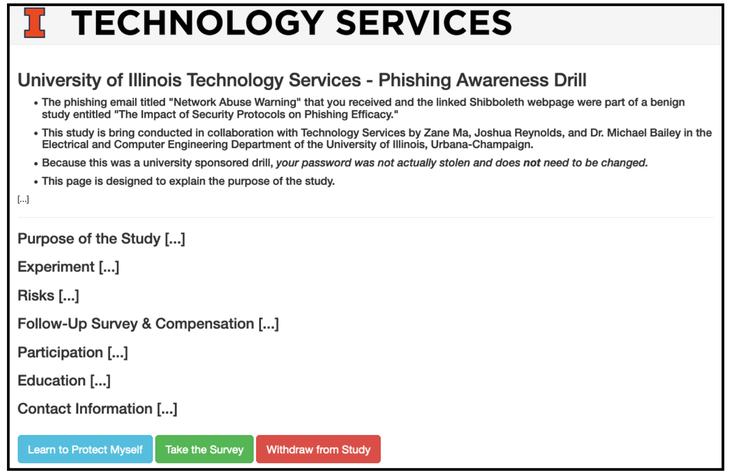
Need to select a different campus?
Clear your remembered campus and log in again.

More Information

Where to Get Help
Contact the Technology Services Help Desk at consult@illinois.edu.

Technical Information
Service that has requested authentication:
Service Provider EntityID:
illinois-abuse.net
Service Provider Name:
U of I Technology Abuse

3. Submit Credentials



TECHNOLOGY SERVICES

University of Illinois Technology Services - Phishing Awareness Drill

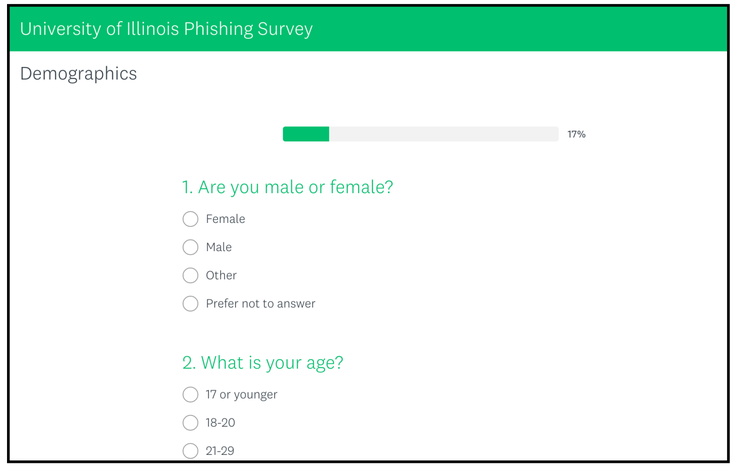
- The phishing email titled "Network Abuse Warning" that you received and the linked Shibboleth webpage were part of a benign study entitled "The Impact of Security Protocols on Phishing Efficacy."
- This study is bring conducted in collaboration with Technology Services by Zane Ma, Joshua Reynolds, and Dr. Michael Bailey in the Electrical and Computer Engineering Department of the University of Illinois, Urbana-Champaign.
- Because this was a university sponsored drill, *your password was not actually stolen and does not need to be changed.*
- This page is designed to explain the purpose of the study.

[...]

Purpose of the Study [...]
Experiment [...]
Risks [...]
Follow-Up Survey & Compensation [...]
Participation [...]
Education [...]
Contact Information [...]

Learn to Protect Myself | Take the Survey | Withdraw from Study

4. Opt-In To Survey



University of Illinois Phishing Survey

Demographics

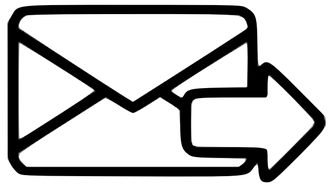
17%

1. Are you male or female?
- Female
- Male
- Other
- Prefer not to answer

2. What is your age?
- 17 or younger
- 18-20
- 21-29

Phishing Campaign

Target population: 266 employees of a university IT organization



0. Send Email

266 Users
100%

1. Open Email

140 Users
53%

2. Access Site

92 Users
35%

3. Submit Credentials

57 Users
21%

Q1: Phishing Effectiveness

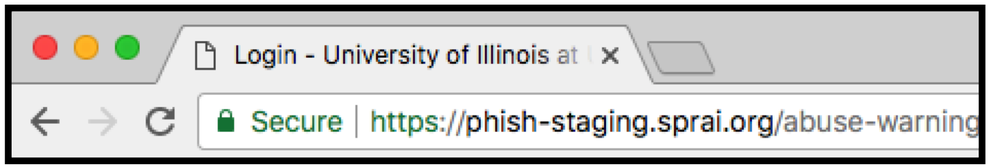
	2. Access Site		3. Enter Credentials	
HTTP	45/75 = 60.0%	p = 0.17	25/45 = 55.6%	p = 0.31
HTTPS	47/65 = 72.3%		32/47 = 68.0%	
TLS Email	45/71 = 63.3%	**p = 0.96**	30/47 = 63.8%	**p = 0.87**
No TLS Email	45/69 = 65.2%		27/45 = 60.0%	

Q2: Browser UI Correlation

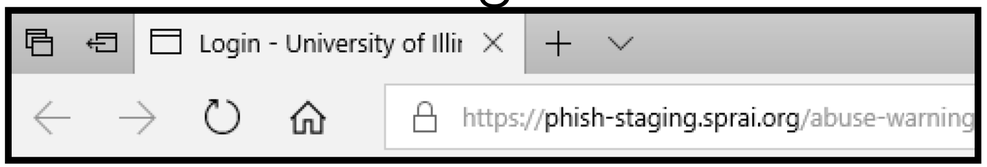
Feature coded 2,882 screenshots across different browsers / platforms / OS

Correlate features with HTTP User-Agent for susceptible users

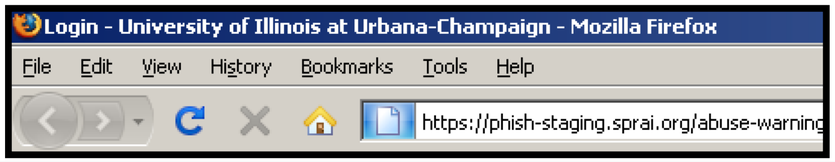
Mac 10.13 Chrome 63



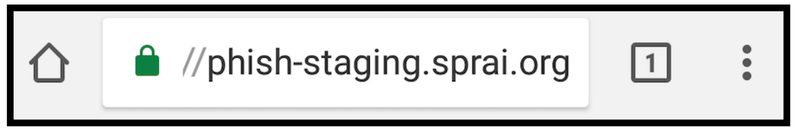
Windows 10 Edge 16



Windows XP SP2 Firefox 3.0



Galaxy S7 Android 70 Mbl. Chrome 63



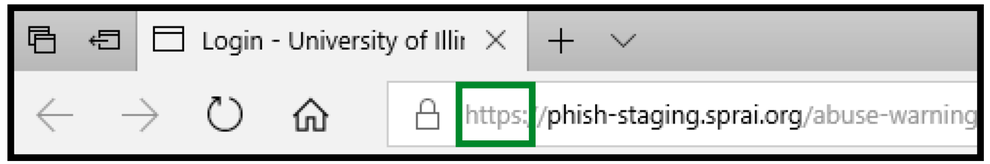
iPhone 8 iOS 11 Mbl Safari 11.0

https://github.com/teamnsrg/url-bar-coding

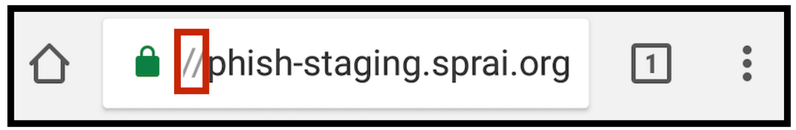
Q2: Browser UI Correlation

Feature	p_{exp}
Any Icon?	0.25
Lock Icon?	0.32
Lock Position	0.98
Lock Color	0.55
Detailed Lock?	0.54
Lock Additions	0.27
Favicon?	0.56
Favicon Position	0.32
Default Favicon	0.06
Protocol Visible?	0.07
Protocol Emphasis	0.63
Additional Text?	0.62
Add. Text Emphasis	0.62
Add. Text Background	0.97
Icon/URL Separator?	0.42

14/16 = 87.5% of users who saw protocol submitted credentials



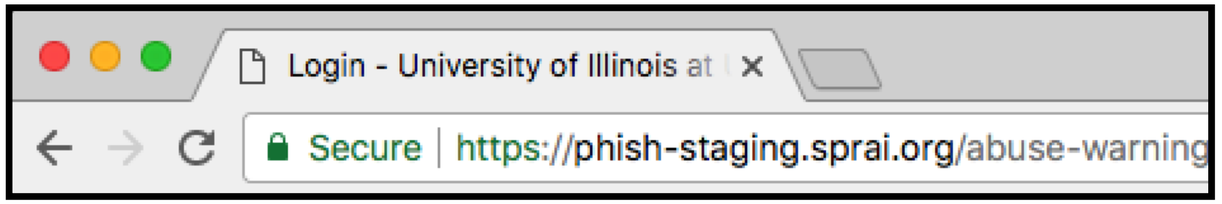
27/46 = 58.7% of users who did not see protocol submitted credentials



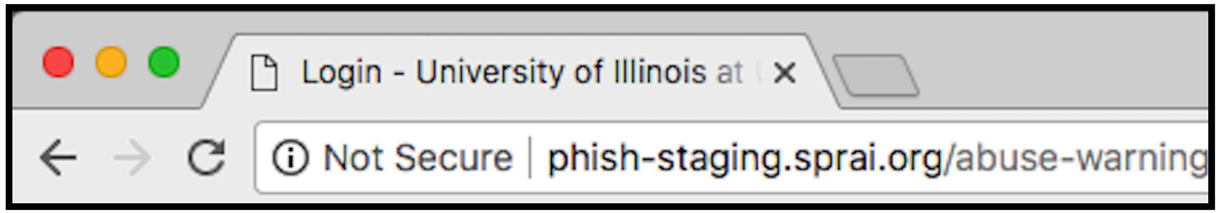
Q2: Browser UI Correlation

Feature	p_{exp}
Any Icon?	0.25
Lock Icon?	0.32
Lock Position	0.98
Lock Color	0.55
Detailed Lock?	0.54
Lock Additions	0.27
Favicon?	0.56
Favicon Position	0.32
Default Favicon	0.06
Protocol Visible?	0.07
Protocol Emphasis	0.63
Additional Text?	0.62
Add. Text Emphasis	0.62
Add. Text Background	0.97
Icon/URL Separator?	0.42

9/10 “Secure” submitted credentials



8/10 “Not Secure” submitted credentials



Takeaways

- The presence of HTTPS in phishing tended to increase effectiveness, but…need more data, more diverse target population
- Protocol presence may increase phishing susceptibility, while “Secure/Not Secure” had minimal distinction
- Another hint that users conflate credibility/trustworthiness with connection security

Questions?

zanema2@illinois.edu