

The Effect of Repeated Login Prompts on Phishing Susceptibility

Peter Snyder¹, Mike K. Reiter², Chris Kanich¹

1. University of Illinois at Chicago

2. University of North Carolina at Chapel Hill

Topic and Goals

- Several popular “best practices” for security
- These “best practices” carry their own costs
- **Research Question:**
Do some “best practices” encourage insecure behaviors?

Do web users become more susceptible to phishing if they log into more websites?

Methodology: Overview

- Recruit test subjects
- Induce some subjects to authenticate with websites more often than others subjects
- Simulate a phishing attack on both groups
- See if the test subjects are successfully phished more often than control subjects

Methodology: Extension

- Firefox and Chrome browser extension
- Randomly assign users control or test group

Control Group

- “Heartbeat”
- Domains visited
- # of passwords entered

Test Group

- All of “Control Group”
- Limit lifetime of select session cookies

Methodology: Recruitment

- Email to university students, faculty and staff
- Regular web users
- Keep extension installed for two months
- \$30 in Amazon gift cards
- IRB approved deception

Methodology: Phishing

- Two months of browsing
- Two emails sent to participants

“Study Over” Message

- “Trusted” address (...@uic.edu)
- Extension removal appointment

“Survey” Message

- “Untrusted” address (...@uic-auth.com)
- Request for a survey
- Link to fake university login page

Subject Protections

- **Browser Extension**
 - Users identified by unmapped identifiers
 - Passwords were uniquely salted and hashed
- **Phishing attack**
 - HTTPS
 - Entered password not sent to the server

Results

	Control	Test
Members	43	46
Clicked Link	17 (39.5%)	19 (38.8%)
Entered Password	17 (100%)	18 (94.7%)
Completed Survey	17	17
“Noted Domain”	5	6

Findings

- **Phishing is effective**
 - 40.4% of participants clicked the link in the email
 - 97.2% of those entered some password
- **No observed difference**
 - Roughly equal phishing susceptibility

Possible Improvements

- **Try to increase difference between groups**
 - More than 8 popular sites
 - More than 2 months
 - More participants
- **Better understand magnitude of effect of treatment**
 - Measure pre-experiment authentication rates
- **Account of “treatment mitigation” tools**
 - Password management tools

Results, continued

- Average # passwords entered:
185.74
- Average # of domains authenticated to:
28.69
- etc...

Thanks!

The Effect of Repeated Login Prompts on Phishing
Susceptibility

Peter Snyder¹, Mike K. Reiter², Chris Kanich¹

1. University of Illinois at Chicago

2. University of North Carolina at Chapel Hill