Investigating Elderly Computer Users' Susceptibility to Phishing

This Internet2 CINC UP Call talk is based on the
research results of the NSF project (#1624149) titled
EAGER: Investigating Elderly Computer Users' Susceptibility to Phishing

Dr. Chuan Yue, chuanyue@mines.edu

EAGER: Investigating Elderly Computer Users' Susceptibility to Phishing

Award Number: NSF 1624149 (formerly 1359542)

Grant Period: February 1, 2014 ~ January 31, 2017

Investigators:

Chuan Yue (PI), Assistant Professor

Computer Science Department

Colorado School of Mines

Brandon Gavett (Co-PI), Assistant Professor

Psychology Department

University of Colorado Colorado Springs

Student Research Assistants and Publications

- A stable team of students


Rui Zhao
(CS, PhD)


Samantha John
(PSYC, PhD)


Stacy Karas
(CS, Undergrad)


Cara Bussell
(PSYC, Master)


Jennifer Roberts
(PSYC, Undergrad)


Daniel Six
(CS, Undergrad)

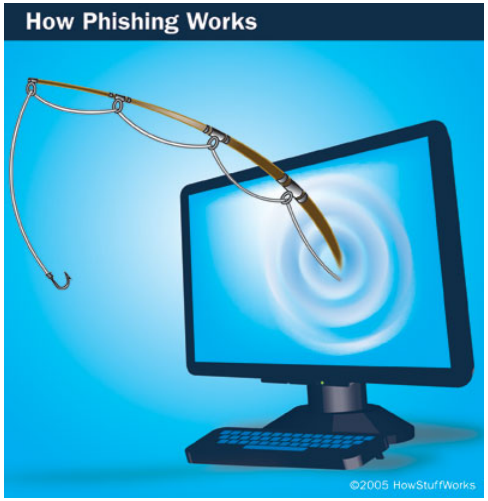
- Publications
  - **Design and Evaluation of the Highly Insidious Extreme Phishing Attacks.** By Rui Zhao, Samantha John, Stacy Karas, Cara Bussell, Jennifer Roberts, Daniel Six, Brandon Gavett, and Chuan Yue. In Journal of Computers & Security (COMPSEC), Elsevier, 70: 634--647, August 2017.
  - **Phishing Suspiciousness in Older and Younger Adults: The Role of Executive Functioning.** By Brandon Gavett, Rui Zhao, Samantha John, Cara Bussell, Jennifer Roberts, and Chuan Yue. In Journal of PLoS ONE, 12(2): e0171620, 2017.
  - **The Highly Insidious Extreme Phishing Attacks.** By Rui Zhao, Samantha John, Stacy Karas, Cara Bussell, Jennifer Roberts, Daniel Six, Brandon Gavett, and Chuan Yue. In proceedings of the IEEE International Conference on Computer Communication and Networks (ICCCN), 2016.
  - **Using Item Response Theory to Improve the Ecological Validity of Neuropsychological Tests: An Example of Phishing Susceptibility (poster).** By Brandon E. Gavett, Rui Zhao, Samantha E. John, Daniel Six, Cara Bussell, Stacy Karas, Jennifer R. Roberts, Jason Adams, and Chuan Yue. In proceedings of the 44th Annual Meeting in International Neuropsychological Society (INS), 2016.
  - **Age Group, Not Executive Functioning, Predicts Past Susceptibility to Internet Phishing Scams (poster).** By Jennifer R. Roberts, Samantha E. John, Cara A. Bussell, Katalin Grajzel, Rui Zhao, Stacy Karas, Daniel Six, Chuan Yue, and Brandon E. Gavett. In proceedings of the 35th Annual Conference of the National Academy of Neuropsychology (NAN), 2015.

Outline

- Background, Goal, and Hypotheses
- Phishing Susceptibility Testbed
- User Study and Results
- Conclusion

Phishing Attacks

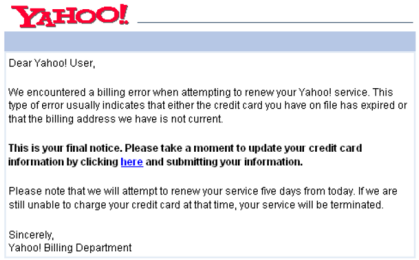
- Phishing: uses spoofed websites to steal users' passwords and online identities.



- Defense:
  - Blacklist-based
  - Heuristics-based
  - Whitelist-based
  - ……
- Phishing reporting and verification services:
  - APWG & PhishTank
- Phishing attacks are fast-evolving to evade the detection and defense.

Phishing: First-level Context [1]

- A spoofed email or instant message
  - To lure users to the phishing websites


YAHOO!

Dear Yahoo! User,

We encountered a billing error when attempting to renew your Yahoo! service. This type of error usually indicates that either the credit card you have on file has expired or that the billing address we have is not current.

This is your final notice. Please take a moment to update your credit card information by clicking here and submitting your information.

Please note that we will attempt to renew your service five days from today. If we are still unable to charge your credit card at that time, your service will be terminated.

Sincerely,
Yahoo! Billing Department

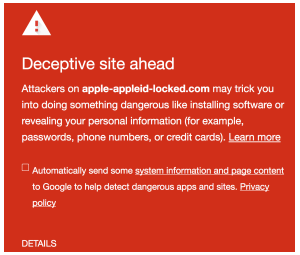
- The success is limited by two constraints
  - If phishing emails or instant messages are suspicious
    - Users would not click on phishing URLs

  - If phishing emails are captured by spam filters
    - Cannot even reach users in the first place

[1] C. Yue. The Devil is Phishing: Rethinking Web Single Sign-On Systems Security. In Proceedings of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2013

Phishing: Second-level Context [1]

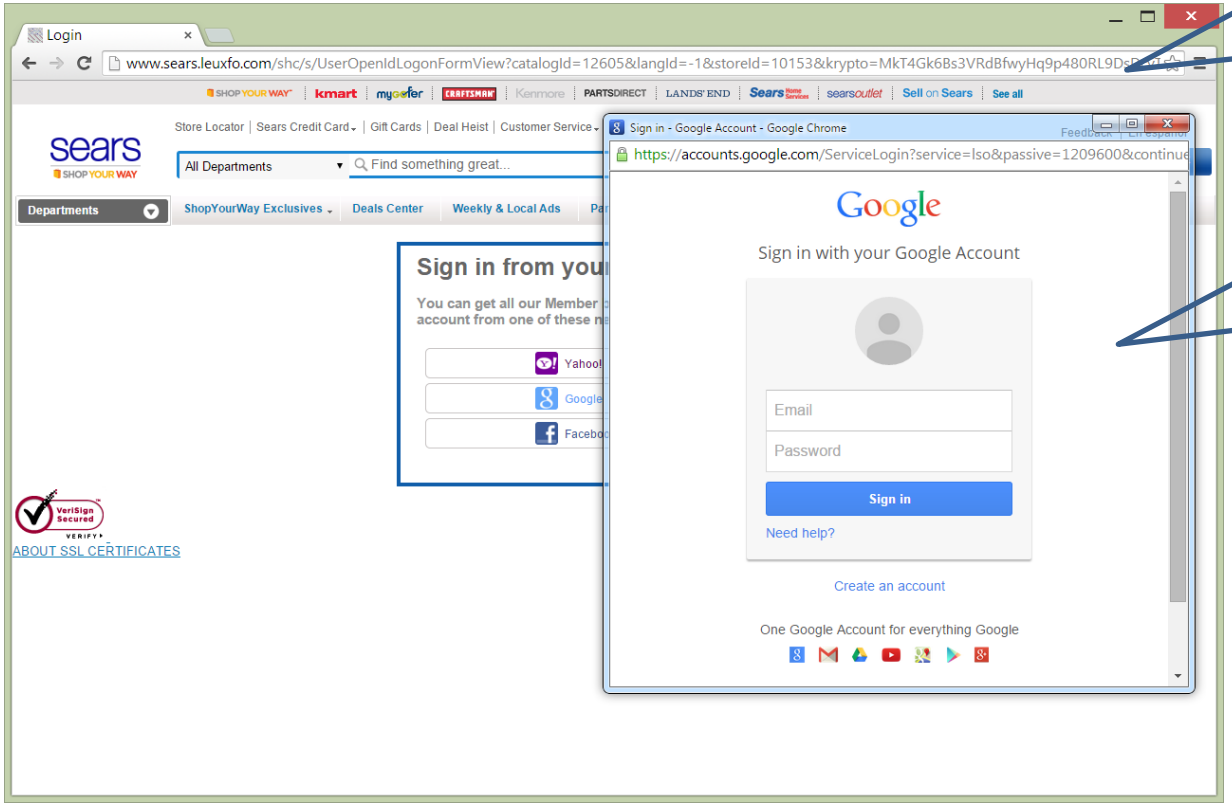
- The look and feel of a phishing site are similar to that of a targeted legitimate website
  - To lure users to submit their login credentials
- The success is limited by two constraints
  - If browsers detect the phishing websites and give warnings



  - If the look and feel of the undetected phishing websites are suspicious

[1] C. Yue. The Devil is Phishing: Rethinking Web Single Sign-On Systems Security. In Proceedings of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2013

Look and Feel of Traditional and Web SSO Phishing



Traditional phishing can be very stealthy with the look and feel of phishing sites almost identical to the targeted legitimate sites.

Web Single Sign-On (SSO) phishing can be more profitable, insidious, and harder to detect than traditional phishing.

As the elderly population continues to grow rapidly, older computer users have also become very attractive targets for online fraud.

Goal, Hypotheses, and Tasks of the Project

- Goal
  - Systematically compare younger and older computer users' susceptibility to both the traditional phishing and the newly emergent Web SSO phishing.
- Hypotheses
  - Older users differ from younger ones in terms of their susceptibility to both types of phishing.
  - This susceptibility can be explained by differences in cognitive abilities, specifically executive functioning and decision-making skills.
- Tasks
  - Build a comprehensive testbed that measures traditional and Web SSO phishing susceptibility in realistic environments.
  - Perform a user study to test the hypotheses.

Outline

- Background, Goal, and Hypotheses
- Phishing Susceptibility Testbed
- User Study and Results
- Conclusion

Phishing Susceptibility Testbed Design Objectives

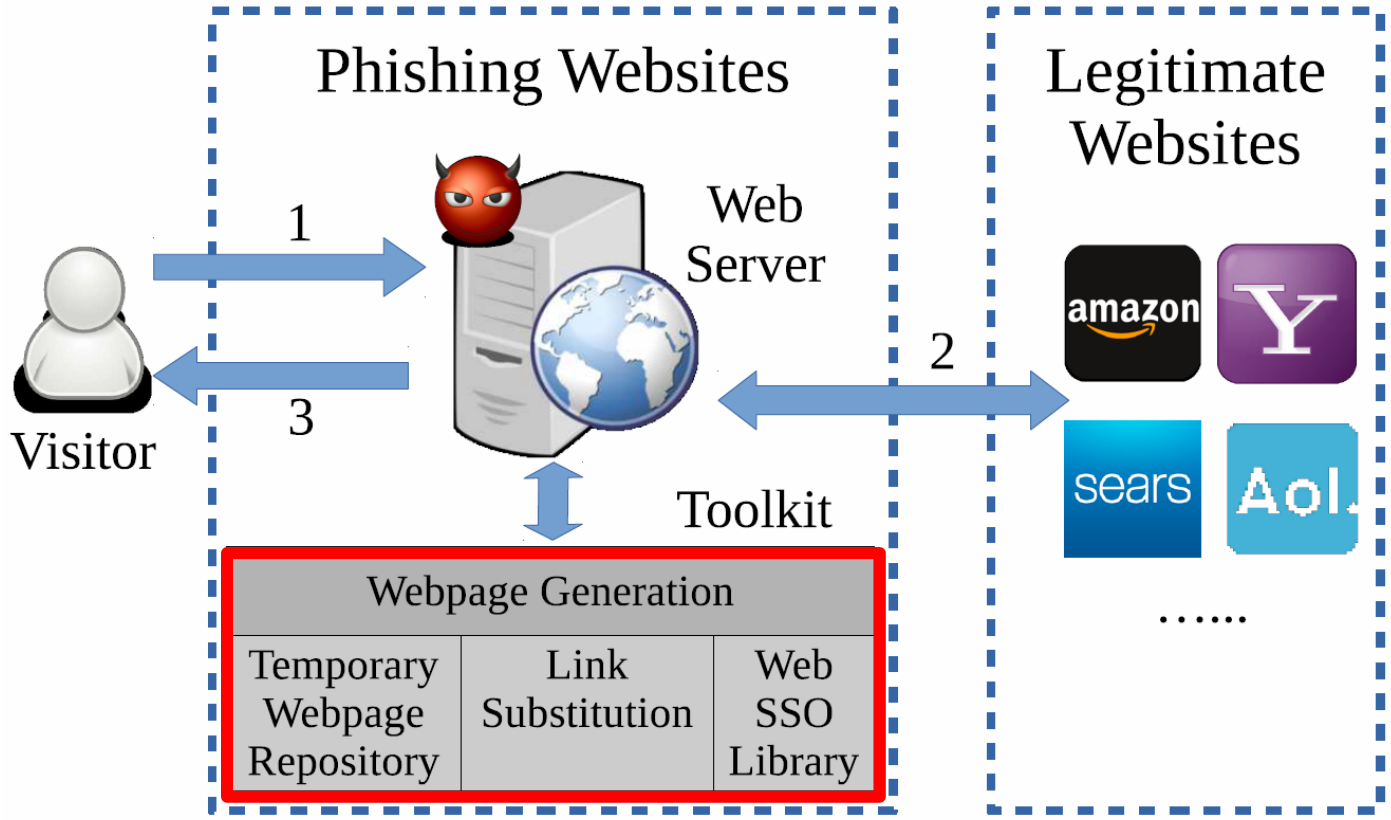
- Comprehensive
  - The testbed supports both traditional forms of phishing and the newly emergent Web Single Sign-On (SSO) phishing [1].
- Realistic
  - Participants use their favorite Web browsers, e.g., Internet Explorer, Firefox, Google Chrome, Safari, and Opera.
  - Participants use their real website login credentials to perform real browsing activities.
- Ethical
  - It does not expose participants to any risk – participants' login credentials will neither be sent to any third party nor be recorded by us.

[1] C. Yue. The Devil is Phishing: Rethinking Web Single Sign-On Systems Security. In Proceedings of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2013

Sophisticated and Highly Insidious Phishing Attacks

- Phishing attacks emulated by our testbed are sophisticated and highly insidious; we call them *extreme phishing* attacks.
  - Any level of webpages from legitimate websites can be dynamically generated and presented to users, making it very difficult for users to identify phishing simply based on the look and feel of the websites.
  - A compromised Web SSO IdP (identity provider) account can allow attackers to impersonate the victim on a large number of RP (relying party) websites.
- Attackers can realistically create similar phishing websites to effectively deceive users and obtain their valuable login credentials!

High Level Design of a Phishing Susceptibility Testbed (also A Phishing Toolkit)

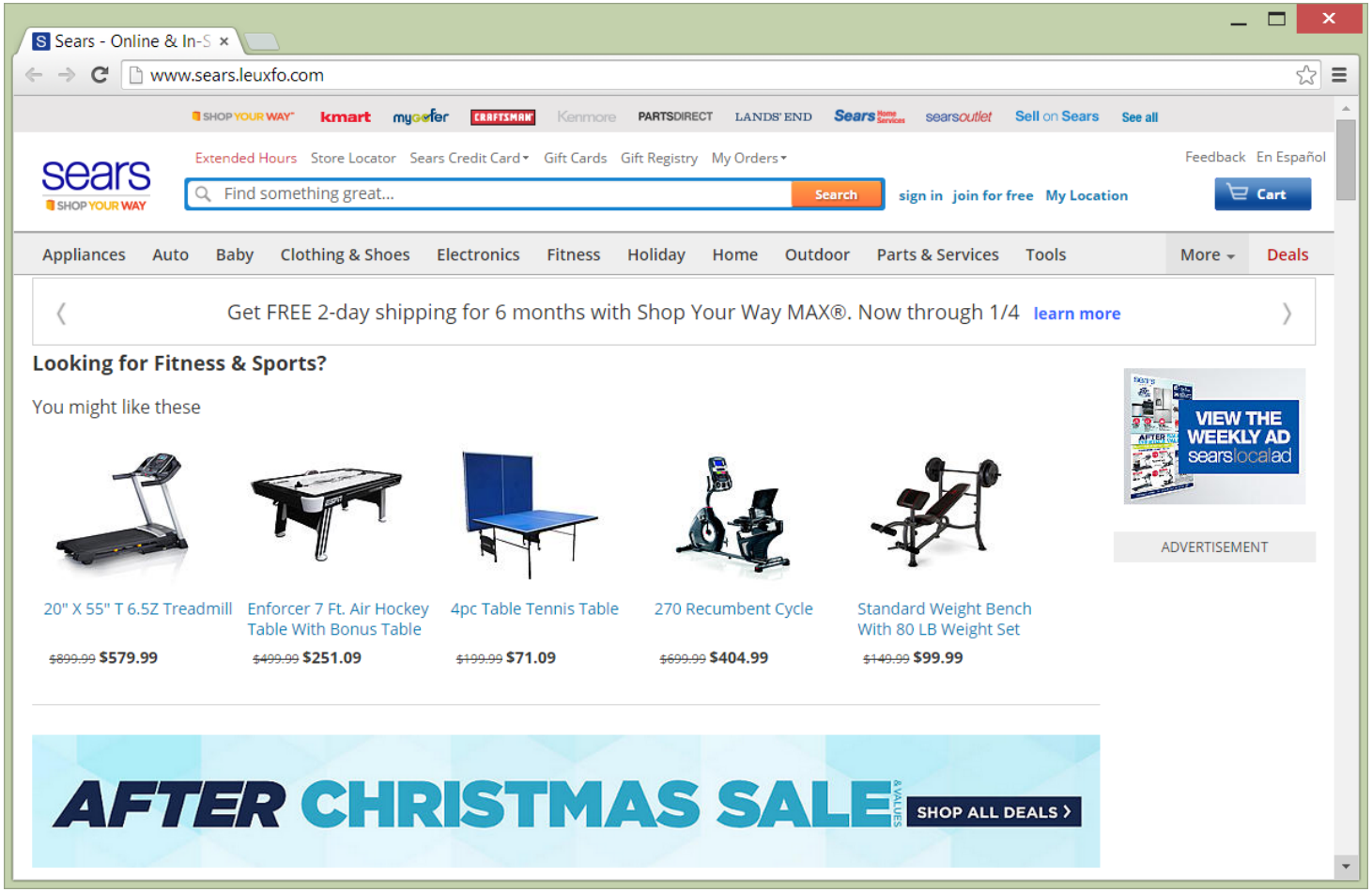


The Apache Web server and our Toolkit on the phishing website act like a proxy between the browsers and the legitimate websites, and send the modified webpages to browsers.

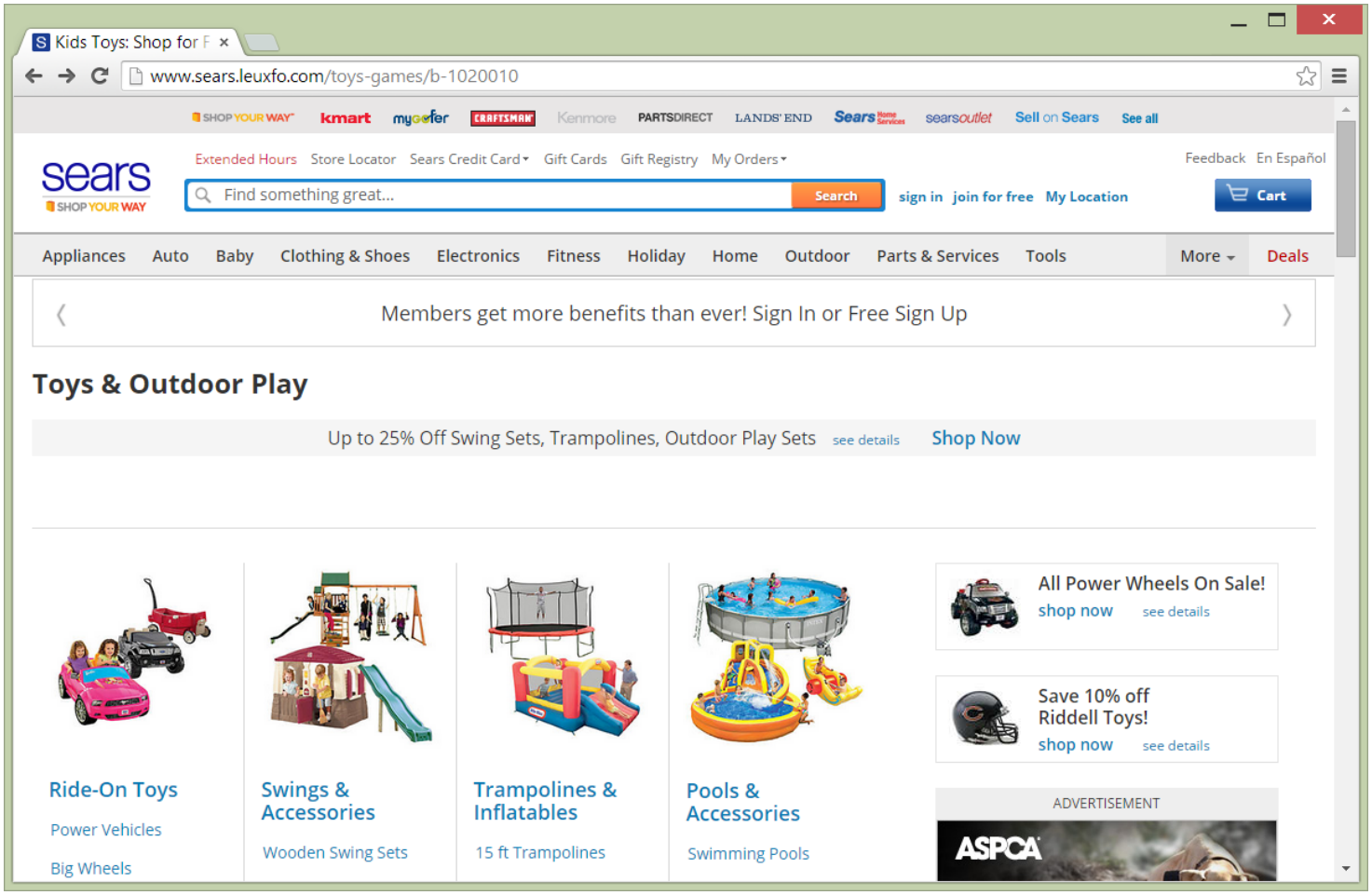
A dynamically generated homepage on the **Amazon** phishing website (it presents the same content as that is actually displayed on the legitimate Amazon website)

A dynamically generated deep-level webpage on the **Amazon** phishing website (any level of webpages can be generated and presented to users in real-time)

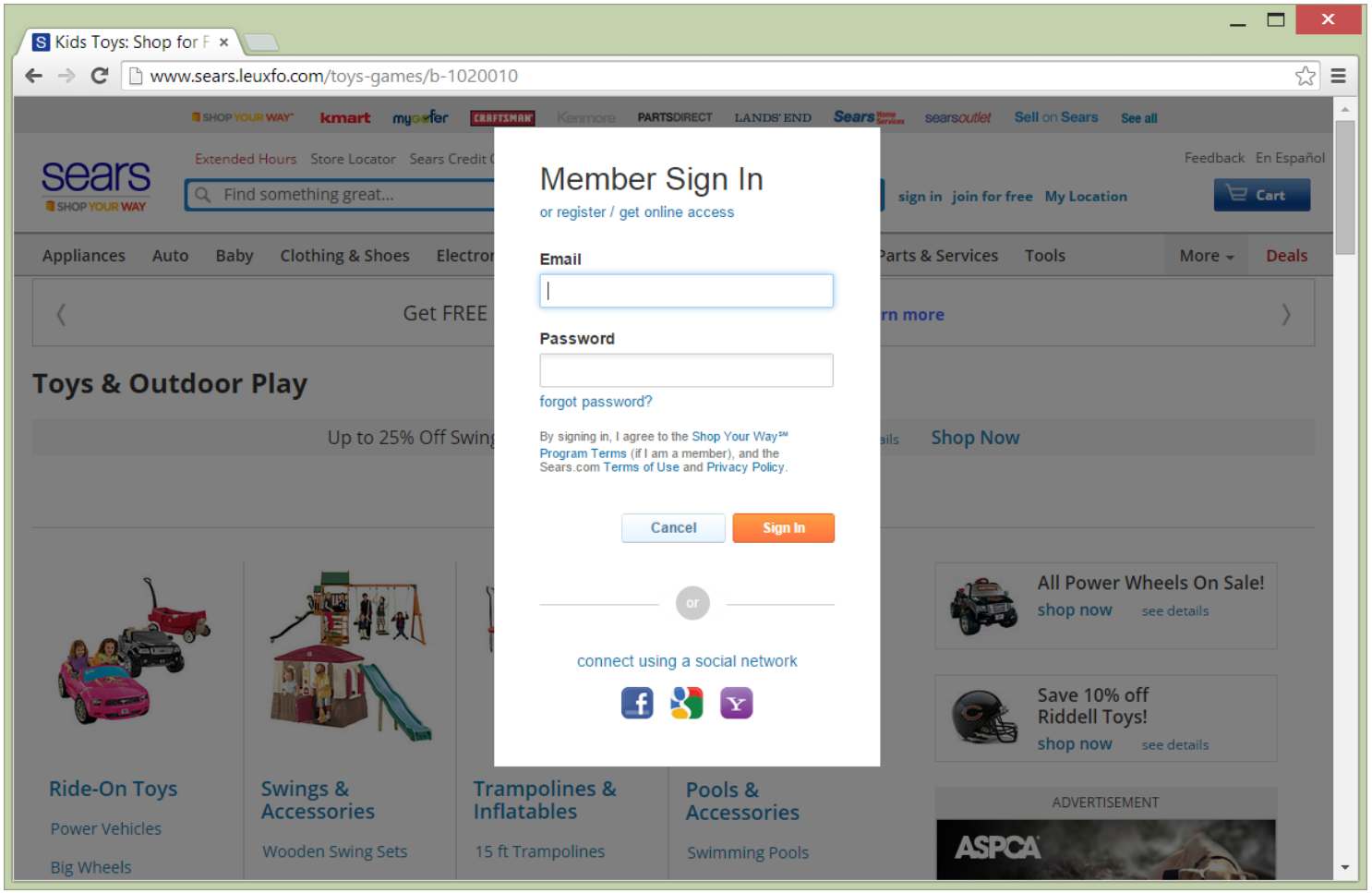
A dynamically generated homepage on the **Sears** phishing website (it presents the same content as that is actually displayed on the legitimate Sears website)



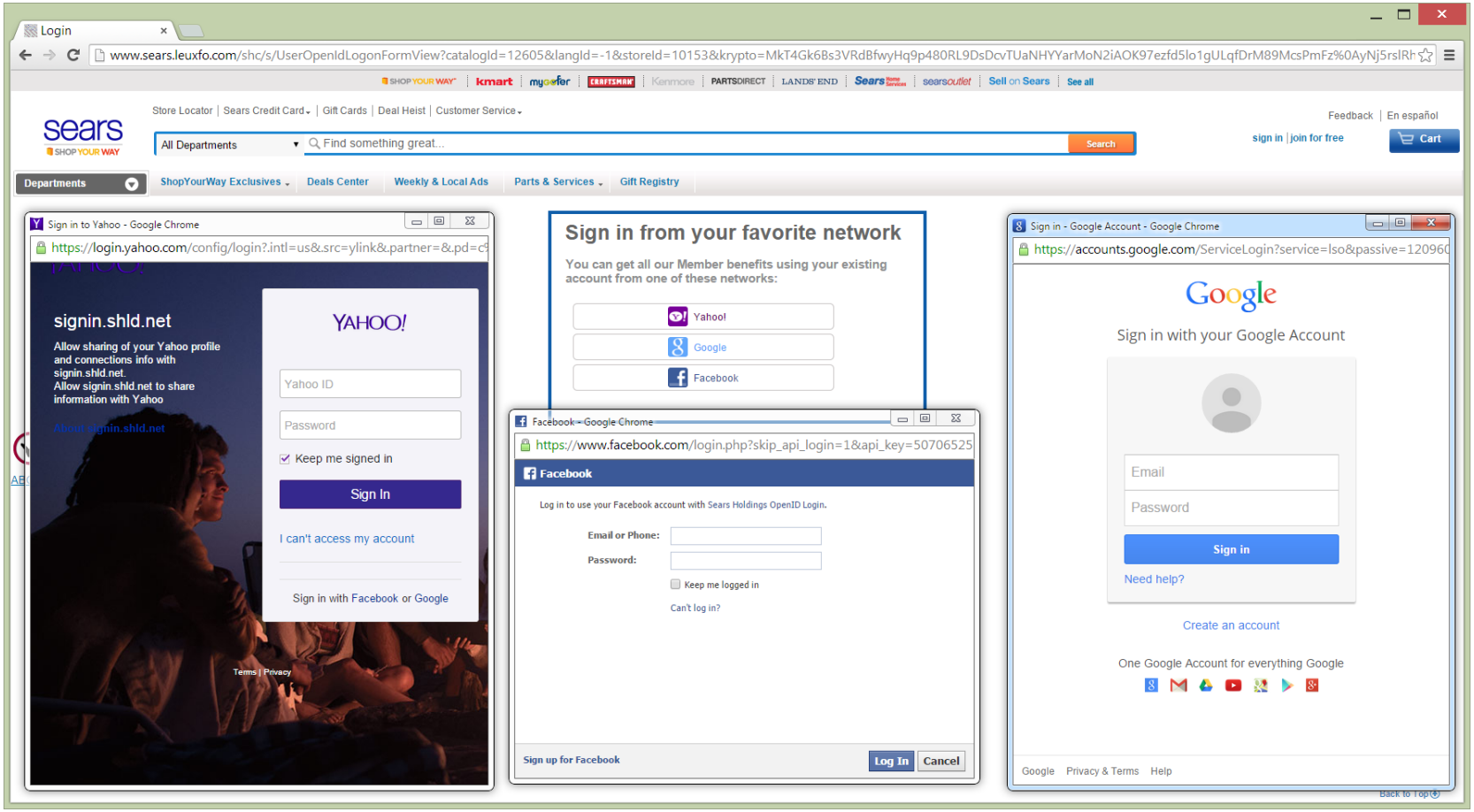
A dynamically generated deep-level webpage on the **Sears** phishing website (any level of webpages can be generated and presented to users in real-time)



A dynamically generated sign-in webpage on the Sears phishing website



The Single Sign-On login windows on the Sears phishing website (the fake Yahoo, Facebook, and Google login “windows” have the almost identical look and feel as those of legitimate login windows)



Outline

- Background, Goal, and Hypotheses
- Phishing Susceptibility Testbed
- User Study and Results
  - *Design and Evaluation of the Highly Insidious Extreme Phishing Attacks*. By Rui Zhao, Samantha John, Stacy Karas, Cara Bussell, Jennifer Roberts, Daniel Six, Brandon Gavett, and Chuan Yue. In Journal of Computers & Security (COMPSEC), Elsevier, 70: 634--647, August 2017.
  - *Phishing Suspiciousness in Older and Younger Adults: The Role of Executive Functioning*. By Brandon Gavett, Rui Zhao, Samantha John, Cara Bussell, Jennifer Roberts, and Chuan Yue. In Journal of PLoS ONE, 12(2): e0171620, 2017.
- Conclusion

User Study

- We provided a computer for all the participants
  - Modified the *hosts* file
  - Installed and configured *five popular browsers*
- The testbed – Realistic!
  - Allows participants to use their real login credentials
  - Perform real browsing activities
- IRB (Institutional Review Board) approval
- Participants - 194 adults
  - 91 younger (18-44 years), 103 older (50-88 years)
  - 135 female, 59 male

User Study – Procedure and Data Collection

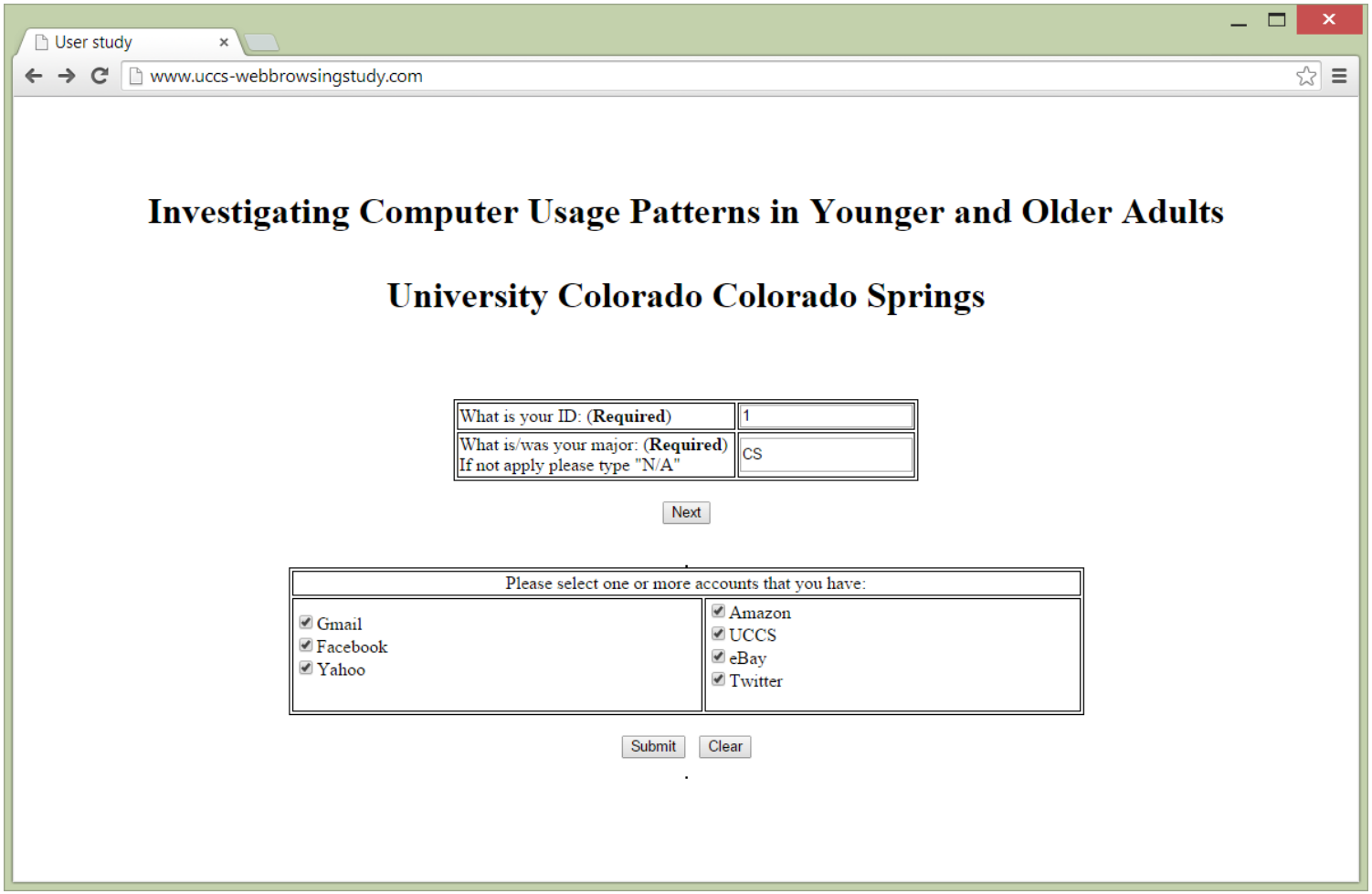
- Procedure
  - Participants were administered the informed consent without the mention of phishing
  - We provided handout instructions for using SSO
  - Each participant performed 4 tasks on 4 websites
    - 2 were extreme phishing websites (traditional, SSO)
    - 2 were legitimate websites (traditional, SSO)
  - Each task – browse the corresponding website as the participant usually does, log into it, and sign out

- Data collection through behavioral observation & questionnaire

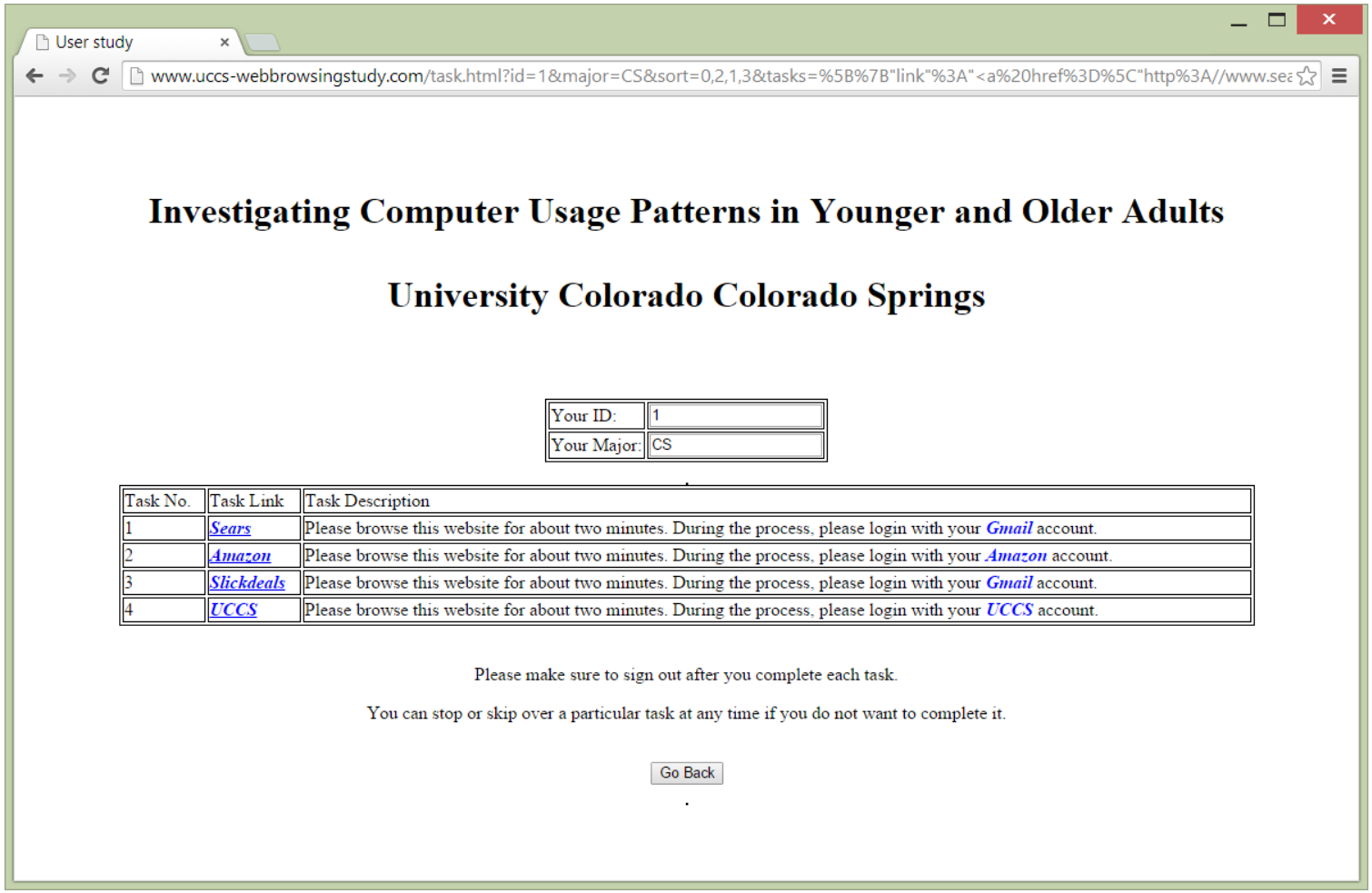
User Study – Phishing Websites

- **Amazon**: traditional sign-on
  - *www.amazon.jigdee.com*
- **Yahoo**: both traditional sign-on & Web SSO
  - *www.yahoo.ibancu.com*
  - Google and Facebook SSO
- **Sears**: both traditional sign-on & Web SSO
  - *www.sears.leuxfo.com*
  - Google, Facebook, and Yahoo SSO
- **AOL**: both traditional sign-on & Web SSO
  - *www.aol.keirtu.com*
  - Google, Facebook, Yahoo, and Twitter SSO

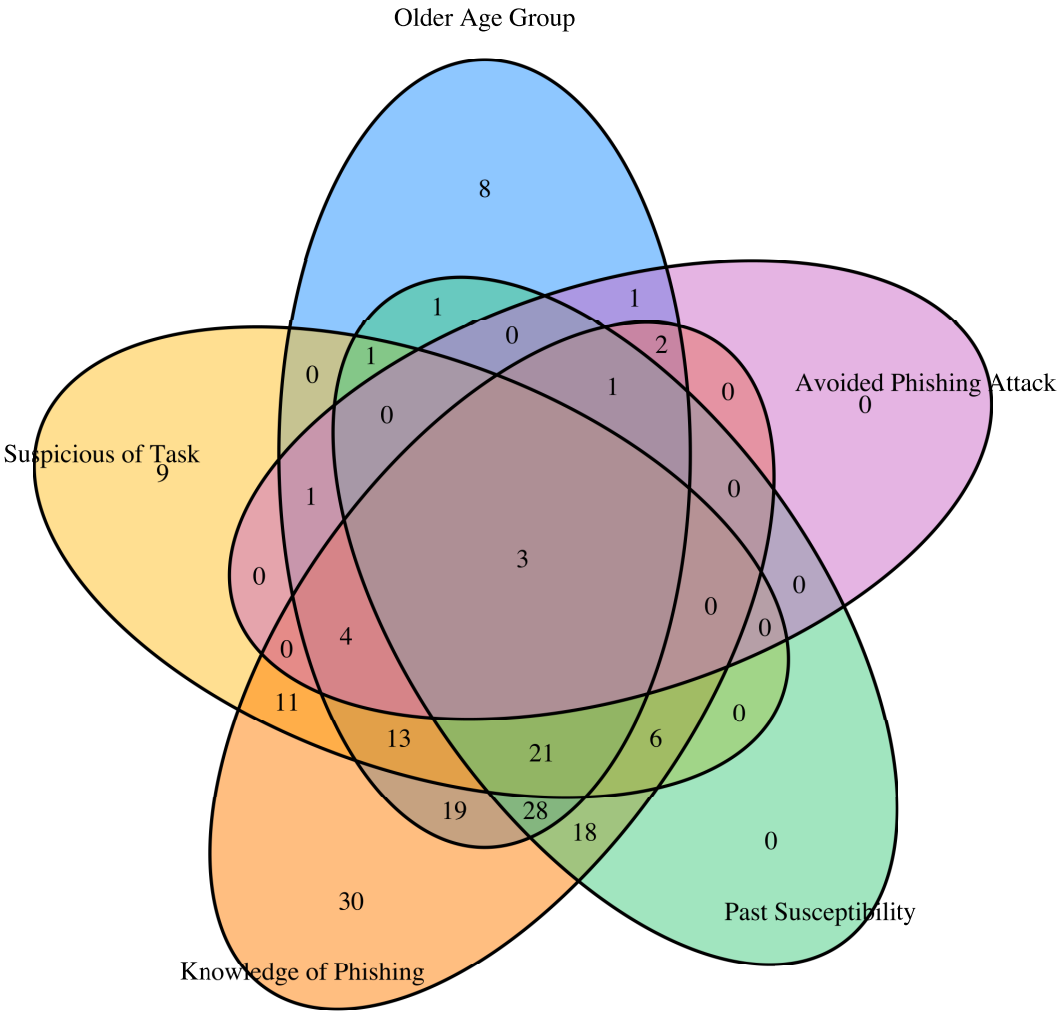
Task Webpages Presented to the Participants (account selection)



Task Webpages Presented to the Participants (four tasks)



The Venn Diagram for the Main Questionnaire and Observation Results



COLORADOSCHOOLOFMINES engineering the way

Main Questionnaire Results

- **Suspicious of Task:** "Did you notice anything suspicious about the websites that you visited during this study?"
  - Only 69 (35.6%) participants reported noticing something suspicious about the visited websites.
  - Only 16 (8.2%) participants were actually suspicious about the phishing websites
    - 9 for look and feel of websites, 7 for website URL addresses, and 2 for public key certificates
  - There was no significant difference in identification of suspicious websites between older and younger adults.
- **Aware of phishing**: "Are you aware of phishing attacks?"
  - 156 (80.4%) participants reported the awareness
  - Older adults were relatively more aware of phishing than younger adults
- **Past Susceptibility:** "Have you been susceptible to any phishing attacks in the past?"
  - 79 (40.9%) participants reported "yes"
  - Older adults were relatively more likely to have been a victim than younger adults

Observed & Questionnaire Results Correlation - 1

- Only 12 (6.2%) participants chose not to enter their username and password on both traditional and Web SSO phishing websites.
  - This observed number is smaller than the number for *Suspicious of Task* obtained from the questionnaire.
  - Some participants would still log into a phishing website while noticing something suspicious perhaps due to **authoritarian attitudes** of participants.
- 146 (93.6%) of 156 participants who reported awareness of phishing still submitted their credentials to our phishing sites.
- 73 (92.4%) of 79 participants who reported as victims of phishing still submitted their credentials to our phishing sites.

Observed & Questionnaire Results Correlation - 2

- There was a significant difference in the lack of susceptibility to both types of phishing between older (n=12, 11.8% of 103) and younger (n=0, 0% of 91) adults.
- Only 19 (9.84%) participants chose not to enter their username and password when confronted with traditional phishing webpages.
  - There was a significant difference in this lack of susceptibility to traditional phishing between older and younger adults with 4 (4.4%) of 91 younger adults avoiding susceptibility compared to 15 (14.7%) of 103 older adults avoiding susceptibility.
- Only 22 (11.5%) participants chose not to enter their username and password when confronted with SSO phishing webpages.
  - There was a significant difference in this lack of susceptibility to SSO phishing between older and younger adults with 3 (3.3%) of 91 younger adults avoiding susceptibility compared to 15 (14.7%) of 103 older adults avoiding susceptibility.

Observed & Questionnaire Results Correlation - 3

- There was a significant difference in this lack of susceptibility to SSO phishing between those with (n=22, 14.3% of 156) and without (n=0, 0% of 38) prior knowledge of phishing.

- There was a significant difference in this lack of susceptibility to SSO phishing between those who did (n=13, 18.8% of 69) and did not (n=9, 7.3% of 125) report noticing something suspicious about the web browsing activity.

Web SSO Related Questionnaire Results

- "Had you heard of Web Single Sign-On before coming in today?"
  - 62 (32.1%) had heard of Web SSO before the study.
  - There was a significant difference in past exposure to SSO between older (n = 23, 22.5% of responses) and younger (n = 39, 42.9% of responses) adults.

- "Do you prefer to create a dedicated account for a website to sign into it or do you prefer to sign into the website using your Google, Facebook, or Yahoo account?"
  - 43 (23.5%) participants reported a preference for SSO-based logins, compared to traditional logins.
  - There was a significant difference in this preference between older (n = 12, 12.5% of responses) and younger (n = 31, 35.6% of responses) adults.

Phishing Suspiciousness in Older and Younger Adults: The Role of Executive Functioning

(In Journal of PLoS ONE, 12(2): e0171620, 2017)

- The Executive Functions Module from the *Neuropsychological Assessment Battery (NAB)* and the *Iowa Gambling Task* were the primary cognitive predictors of the reported phishing suspiciousness.
- Overall, the results failed to support our hypothesis that older adults would be more susceptible to phishing than younger adults.
- A logistic regression model predicted phishing suspiciousness with 73.1% accuracy, and revealed three statistically significant predictors for phishing suspiciousness:
  - the main effect of education
    - Adults with more years of education are more suspicious.
  - the interactions of age group with prior awareness of phishing
    - Older adults with prior phishing knowledge are more suspicious.
  - performance on the NAB Mazes test
    - Older adults with better scores are more suspicious.
    - A partial support to our hypothesis on the prediction capability of executive functioning tests.

Conclusion

- Both traditional and Web SSO phishing attacks can be sophisticated and highly insidious.
- Technical solutions are needed to address phishing attacks.
- Educational efforts are needed to address phishing attacks.
- Three predictors for phishing suspiciousness.

Thank You! Q & A