Real-World Decision Making: Logging Into Secure vs. Insecure Websites

Timothy Kelley **Bennett Bertenthal**

Developmental Cognitive Neuroscience Lab

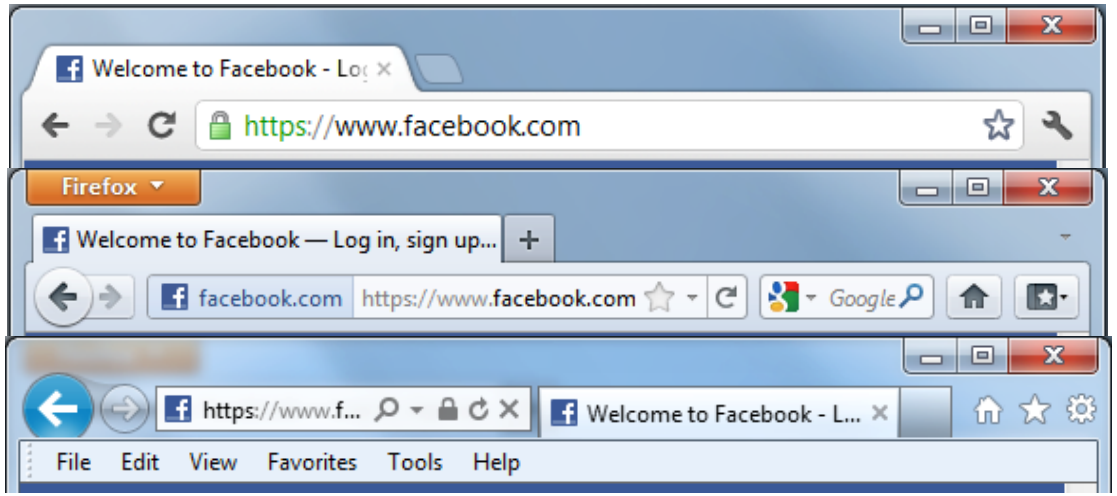
Department of Psychological & Brain Sciences

Indiana University Bloomington

kelleyt@Indiana.edu

The Purpose of Security Indicators

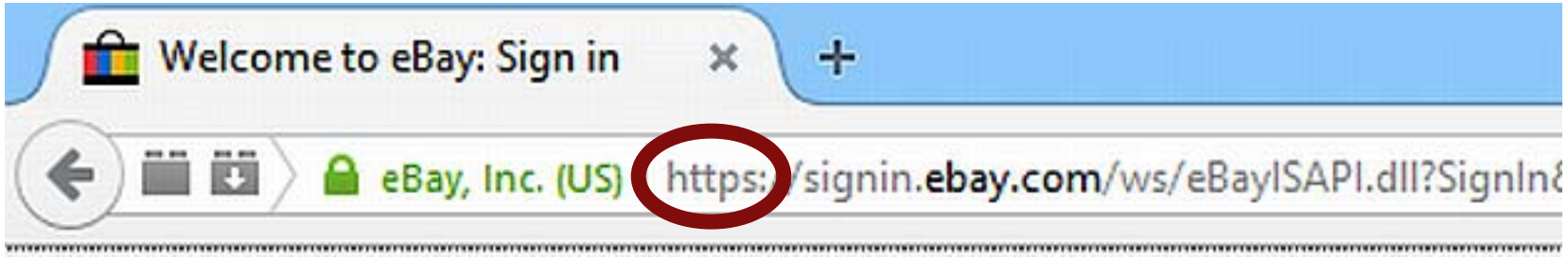
- Communicate to users:
  - Whether or not encryption is being used on a given website
  - The domain name is correctly identified in the issued SSL/TLS certificate (domain name mismatches throw security warnings)



M. Arianezhad, L. J. Camp, T. Kelley, and D. Stebila, "Comparative eye tracking of experts and novices in web single sign-on," in *Proceedings of the third ACM conference on Data and application security and privacy - CODASPY '13*, 2013, no. October, p. 105.

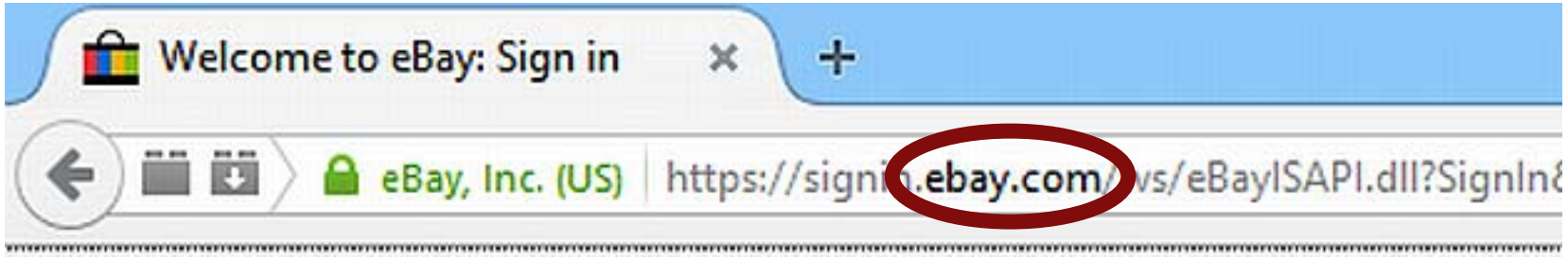
Four Key Features

- Does the URL in the location bar begin with https?



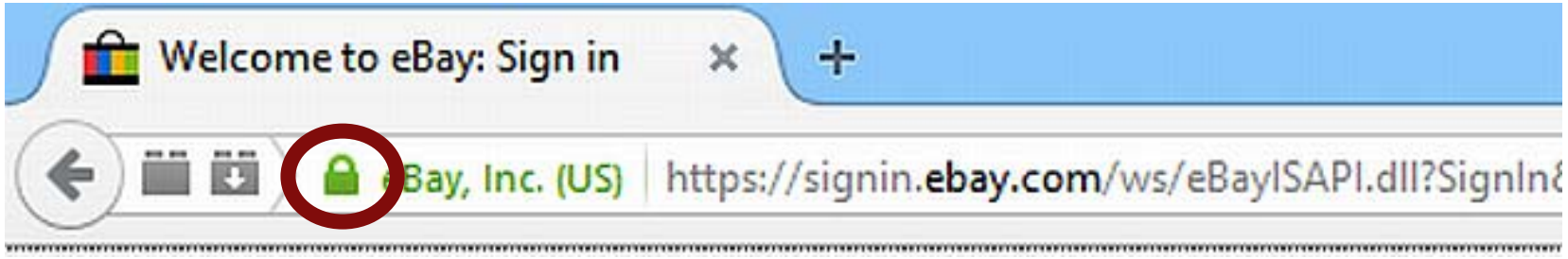
Four Key Features

- Does the URL in the location bar begin with https?
- Is the domain name of the URL in the location bar correct?



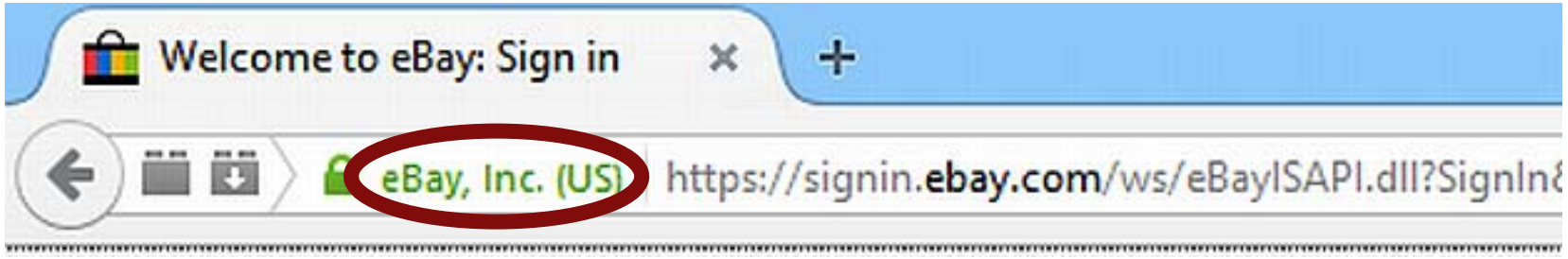
Four Key Features

- Does the URL in the location bar begin with https?
- Is the domain name of the URL in the location bar correct?
- Is the lock icon displayed somewhere in the browser chrome?



Four Key Features

- Does the URL in the location bar begin with https?
- Is the domain name of the URL in the location bar correct?
- Is the lock icon displayed somewhere in the browser chrome?
- Are there indicators present for an extended validation certificate? [1]



1. D. Stebila, “Reinforcing bad behaviour,” in *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction - OZCHI ’10*, 2010, p. 248.

Are web browser security indicators actually helping?

- Several studies have evaluated whether users correctly use security indicators (e.g., [2 – 4]), but there has been little systematic quantification about how knowledge of these indicators and familiarity affect behavior.
- There has been little work in identifying the underlying processes that are responsible for a given decision.

2. S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators an evaluation of website authentication and the effect of role playing on usability studies," in *Proceedings - IEEE Symposium on Security and Privacy*, 2007, vol. 0, pp. 51–65.3.
3. R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI '06*, 2006, no. November 2005, p. 581.
4. M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *Int. J. Hum. Comput. Stud.*, vol. 82, pp. 69–82, 2015.

Study Questions

- How do technical security knowledge and familiarity influence participants' likelihood to login?
- What factors affect the participants' behavior prior to their final decision?

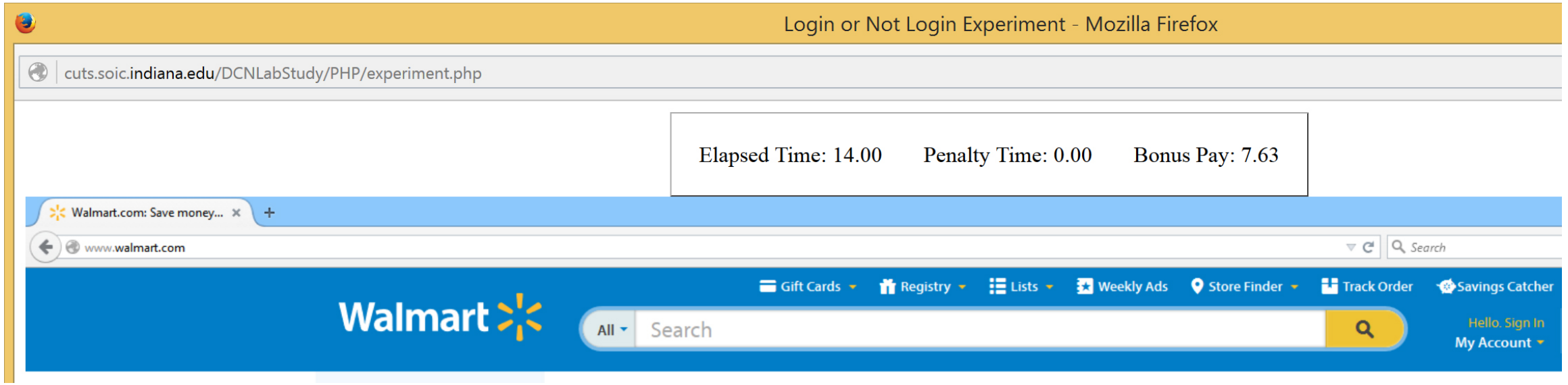
Study Questions

- How do technical security knowledge and familiarity influence participants' likelihood to login?
- What factors affect the participants' behavior prior to their final decision?
- What are the conditions that make security indicators effective (if any)?

Study Design

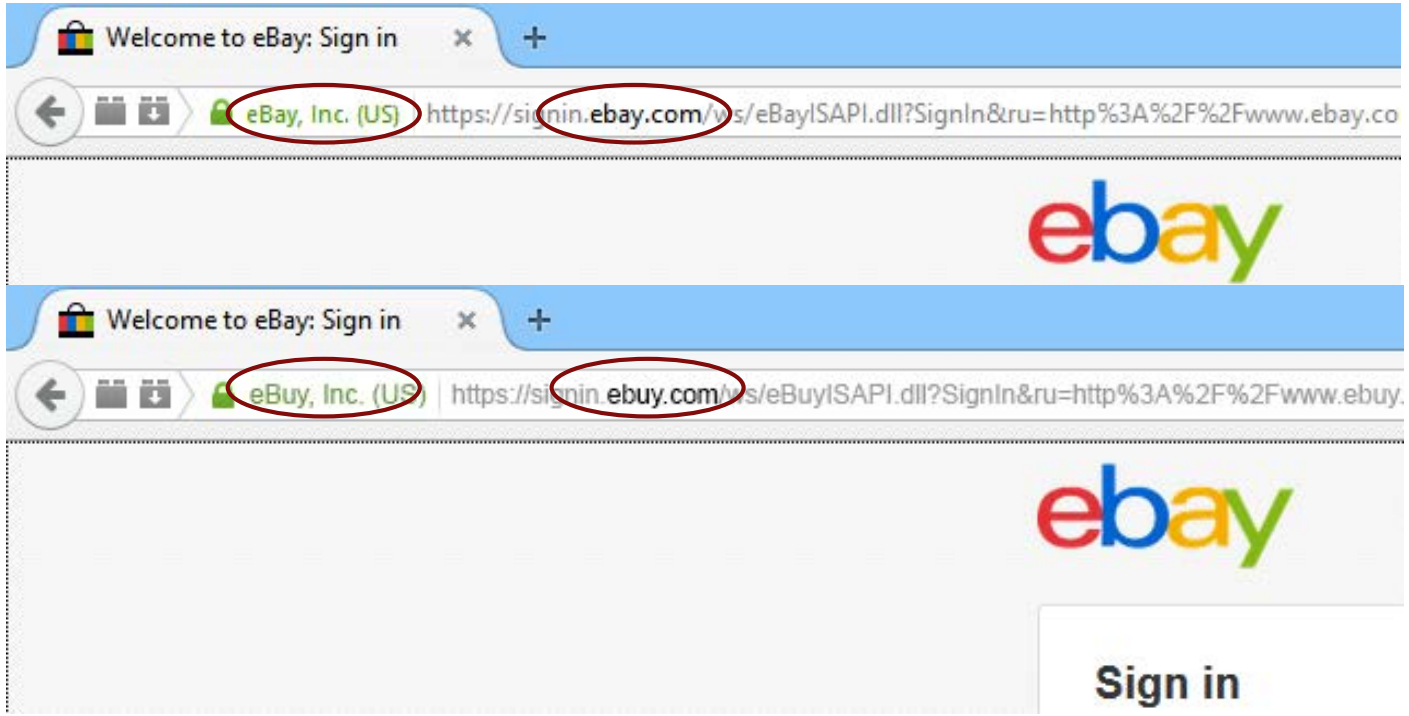
- Two Studies
  - HTTPS/HTTP
    - 8 Trials
      - 4 HTTPS (1 EV, 2 FE, 1 PE)/4 HTTP (NE)
  - No Spoof/Spoof
    - 6 Trials
      - 3 No Spoof (1 EV, 1 FE, 1 PE)/3 Spoof (1 EV, 1 FE, 1 PE)
- Post-Study Survey

The Key Components: Time & Money



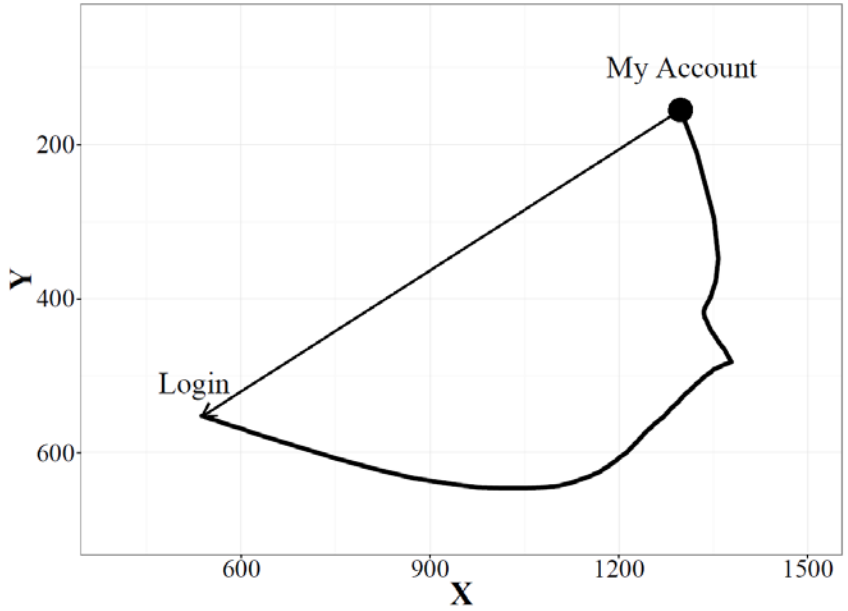
Experimental Task: In this experiment, you will be presented with a series of websites, and you will need to decide whether or not to sign-in to each of these sites based on whether or not they are secure. All of the websites are designed to simulate real websites viewed with a Firefox browser, but just like in the real world, the Firefox browser may not be able to ensure the protection of your credentials.

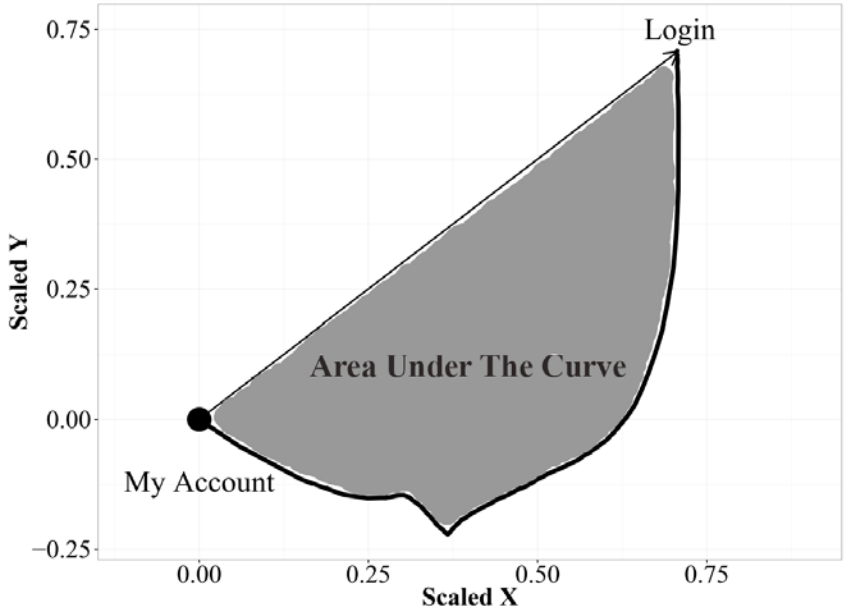
Example Stimuli



Example Stimuli

Mouse Tracking Data





Survey

- **Demographic** – age, gender, race, education
- **Computer experience** – browser, familiarity of websites, data loss, programming languages, etc.
- **Practical security knowledge** – identification of security indicators, password management, data loss, etc.
- **Technical security knowledge** – firewall, phishing, DDoS, SSL, etc.

Demographics

Sample size = 172 participants

Mean age = 32.6 (*9.58*)

Males = 100; **Females** = 72

Technical expertise score (0-1) = 0.5 (*0.24*)

Prop. of identified security indicators = .59 (*.31*)

Familiarity (1-5) = 2.90 (*1.65*)

Study Details

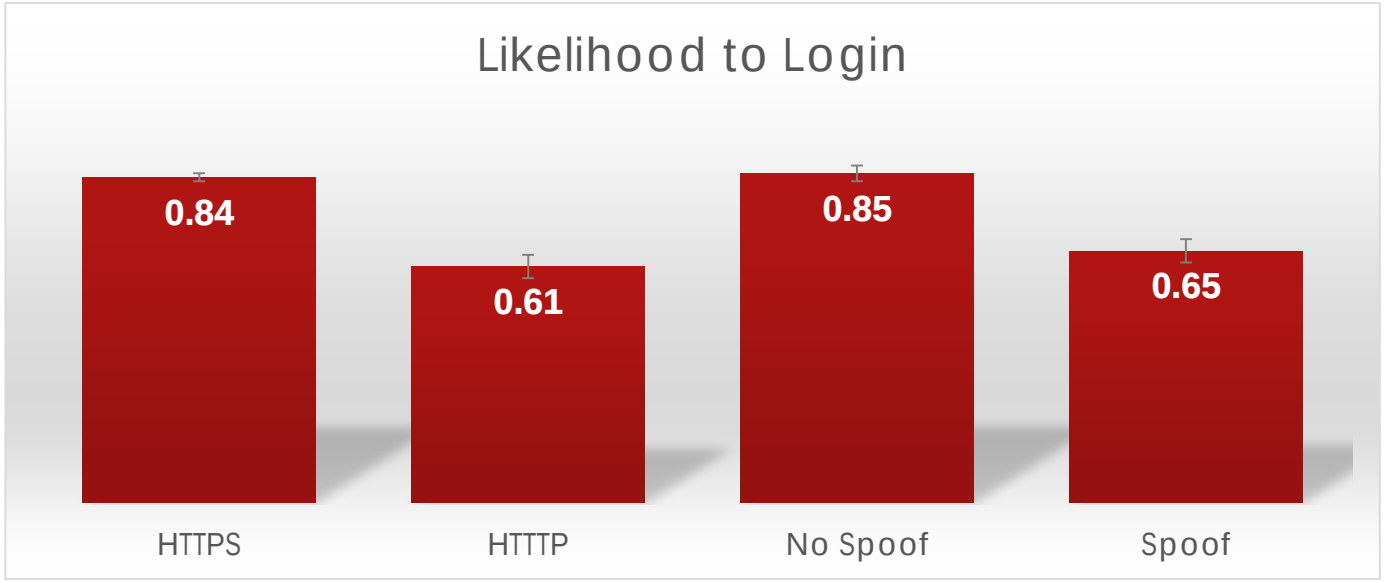
Mean Time Per Site = 9.07 sec. (6.74)

Mean Total Time = 145.11 (*45.69*)

Mean Bonus Pay = 2.37 (1.36)

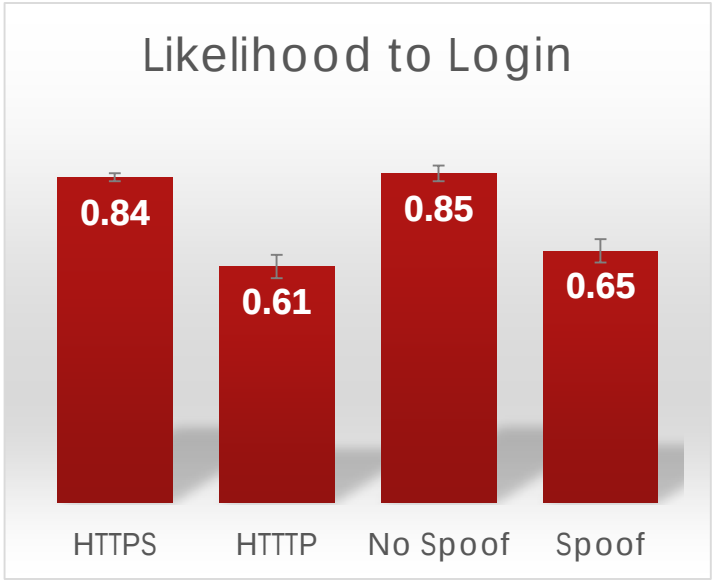
Results

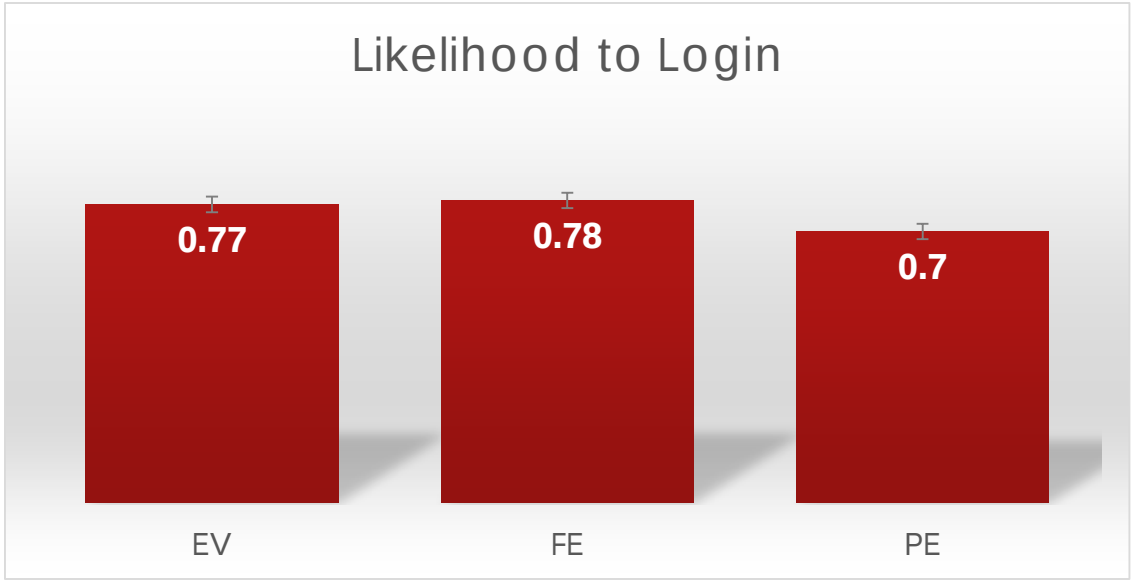
- Participants do not ignore security indicators.



Results

- Participants do not ignore security indicators.



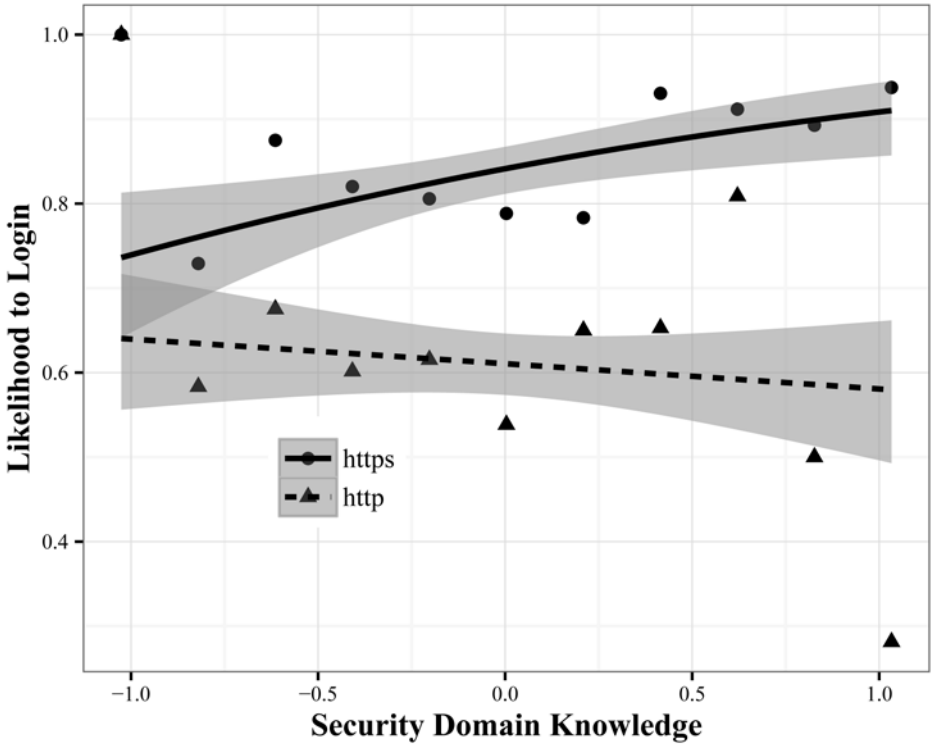


Results

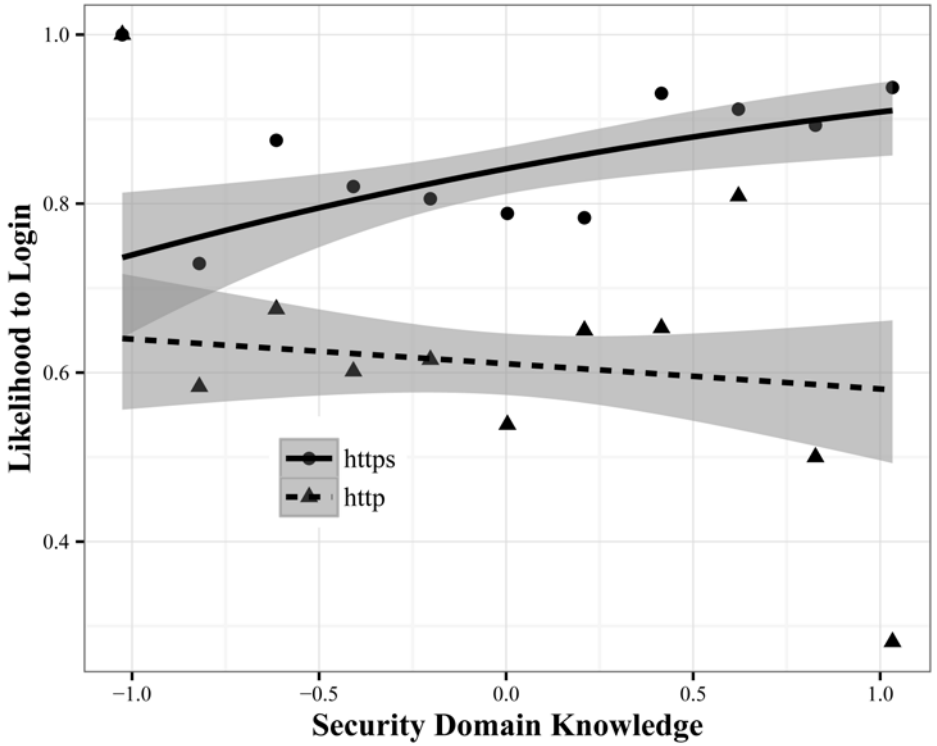
- Participants do not ignore security indicators.
  - Survey knowledge of cybersecurity is not necessarily a good predictor of risky decision-making on the web using experimental procedures

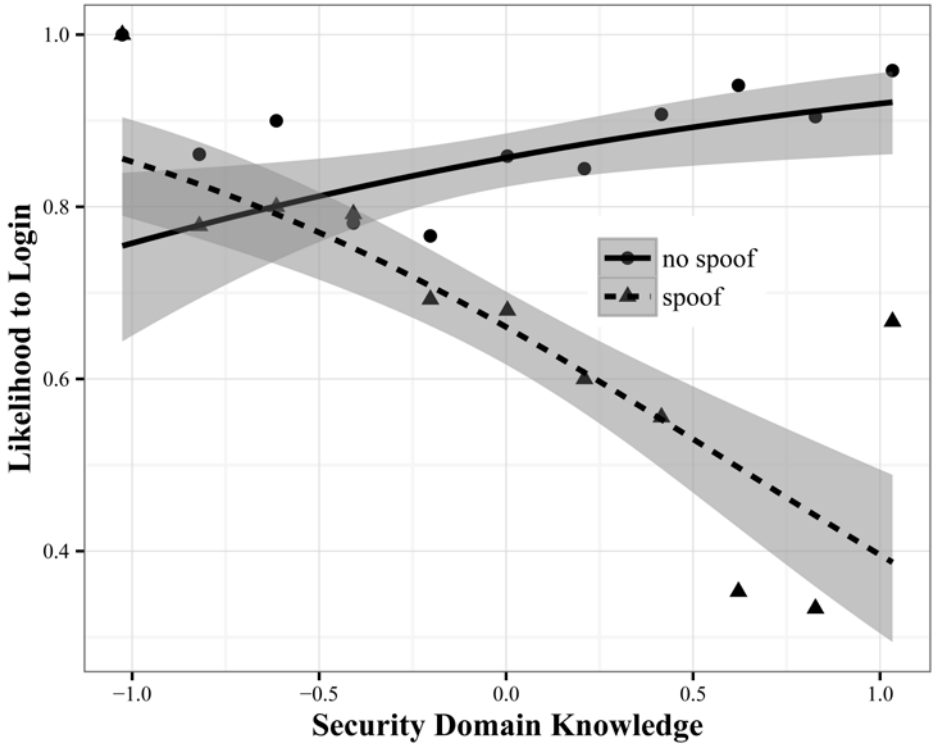
Results

- Survey knowledge of cybersecurity is not necessarily a good predictor of risky decision-making on the web using experimental procedures



Results


1.0
0.8
0.6
0.4
Likelihood to Login
https
http
−1.0
−0.5
0.0
0.5
1.0
Security Domain Knowledge

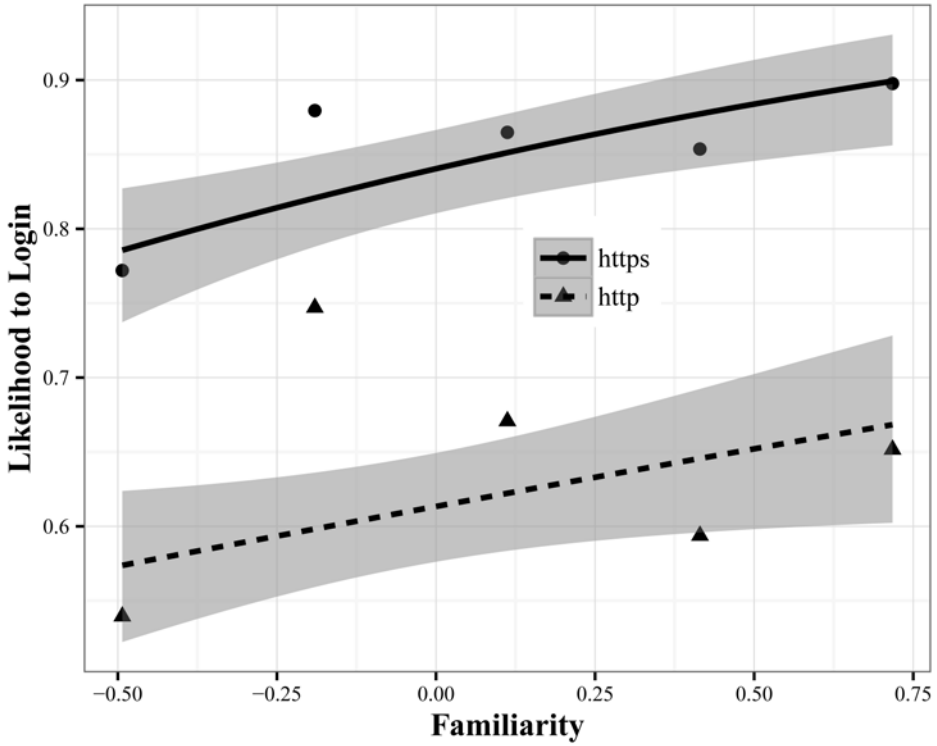

1.0
0.8
0.6
0.4
Likelihood to Login
no spoof
spoof
−1.0
−0.5
0.0
0.5
1.0
Security Domain Knowledge

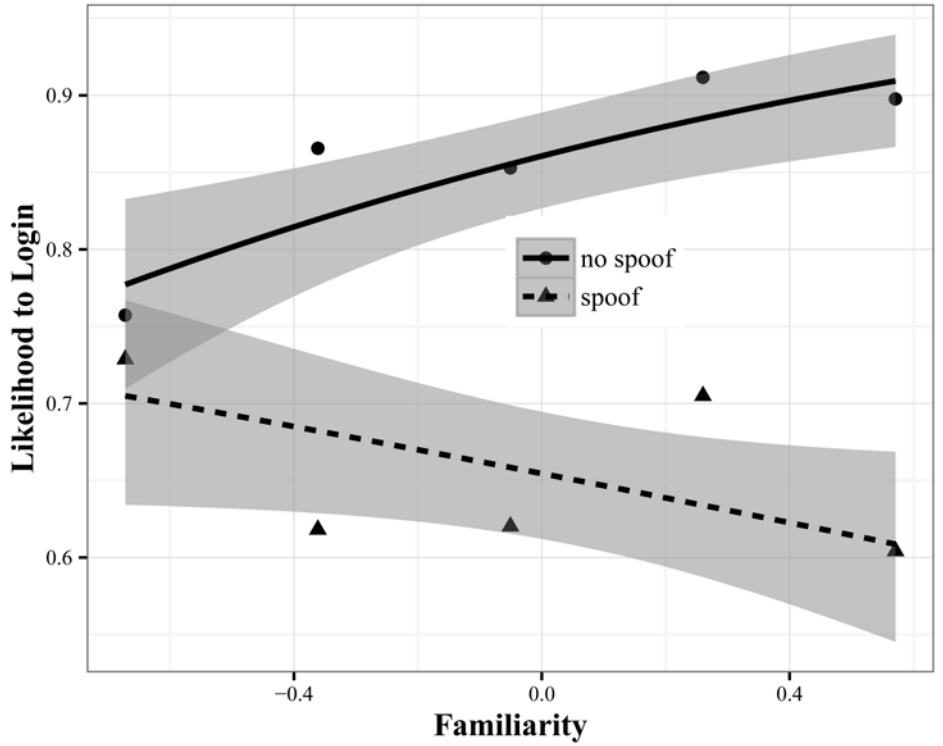
Results

- Participants do not ignore security indicators.
  - Survey knowledge of cybersecurity is not necessarily a good predictor of risky decision-making on the web using experimental procedures
  - Familiarity is an important aspect of logging-in.

Results

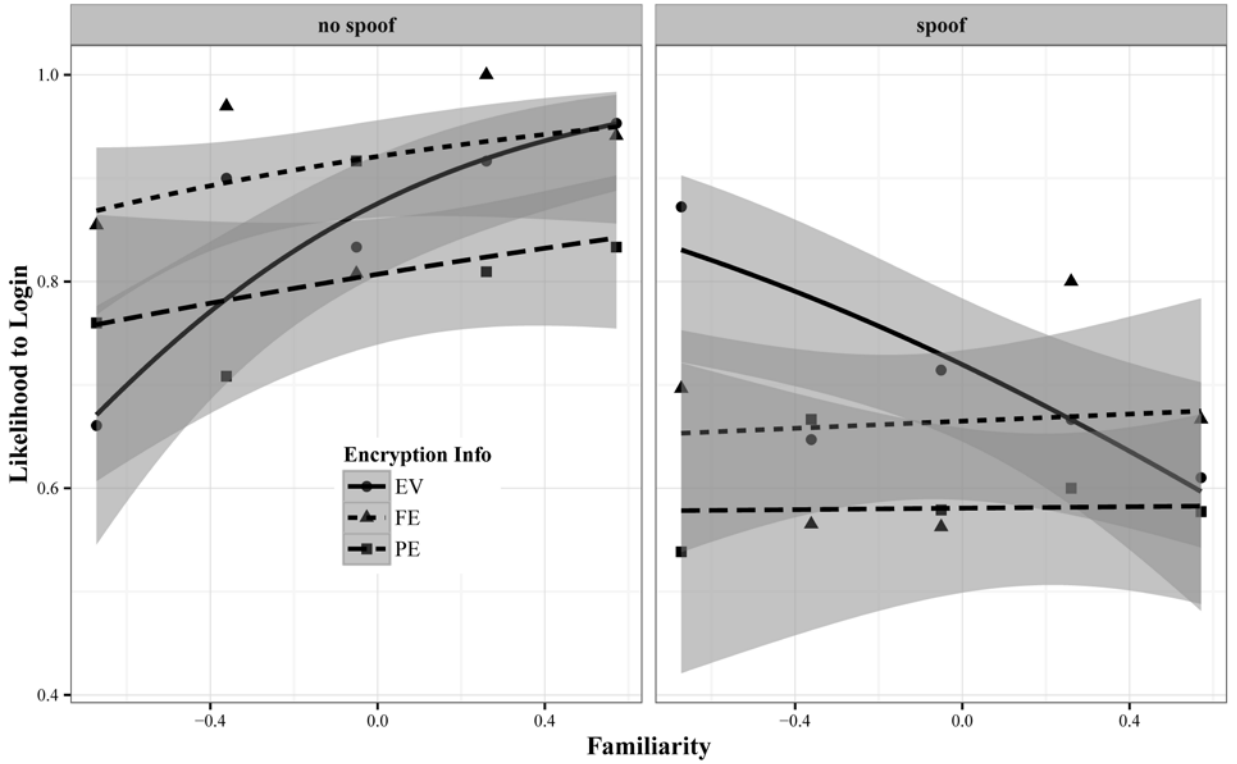
- Familiarity is an important aspect of logging-in.





Results

- Participants do not ignore security indicators
  - Familiarity is an important aspect of logging-in

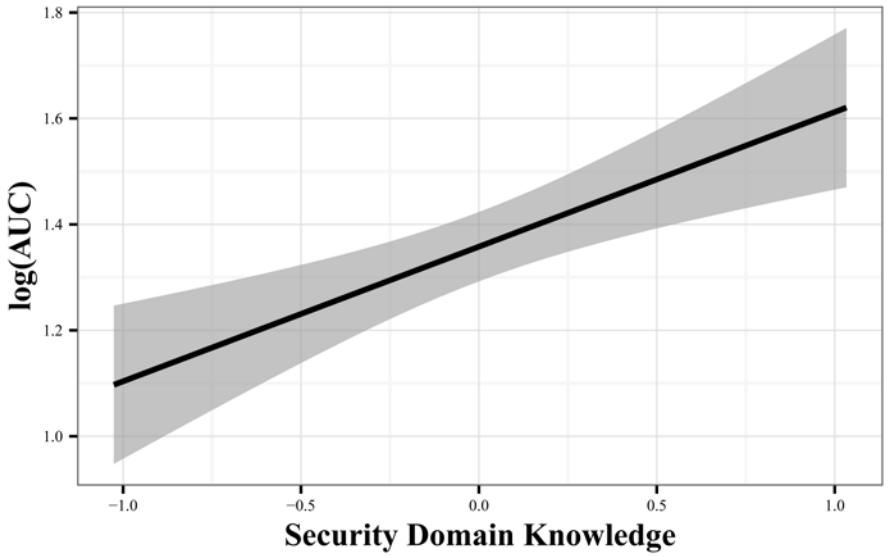


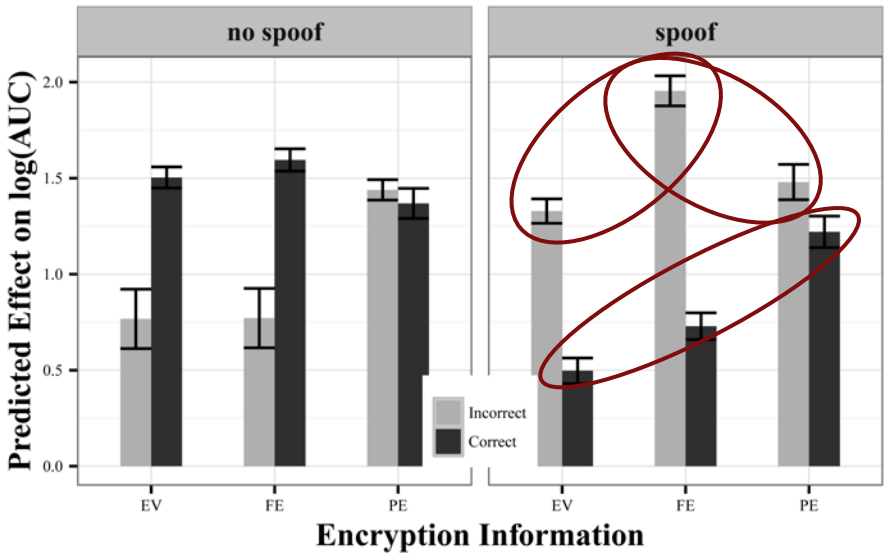
Results

- Participants do not ignore security indicators.
  - Survey knowledge of cybersecurity is not necessarily a good predictor of risky decision-making on the web using experimental procedures
  - Familiarity is an important aspect of logging-in.
- Mouse tracking clarifies the decision making process

Results

- Participants do not ignore security indicators.
- Mouse tracking clarifies the decision making process





Conclusions

- Participants do not ignore security indicators

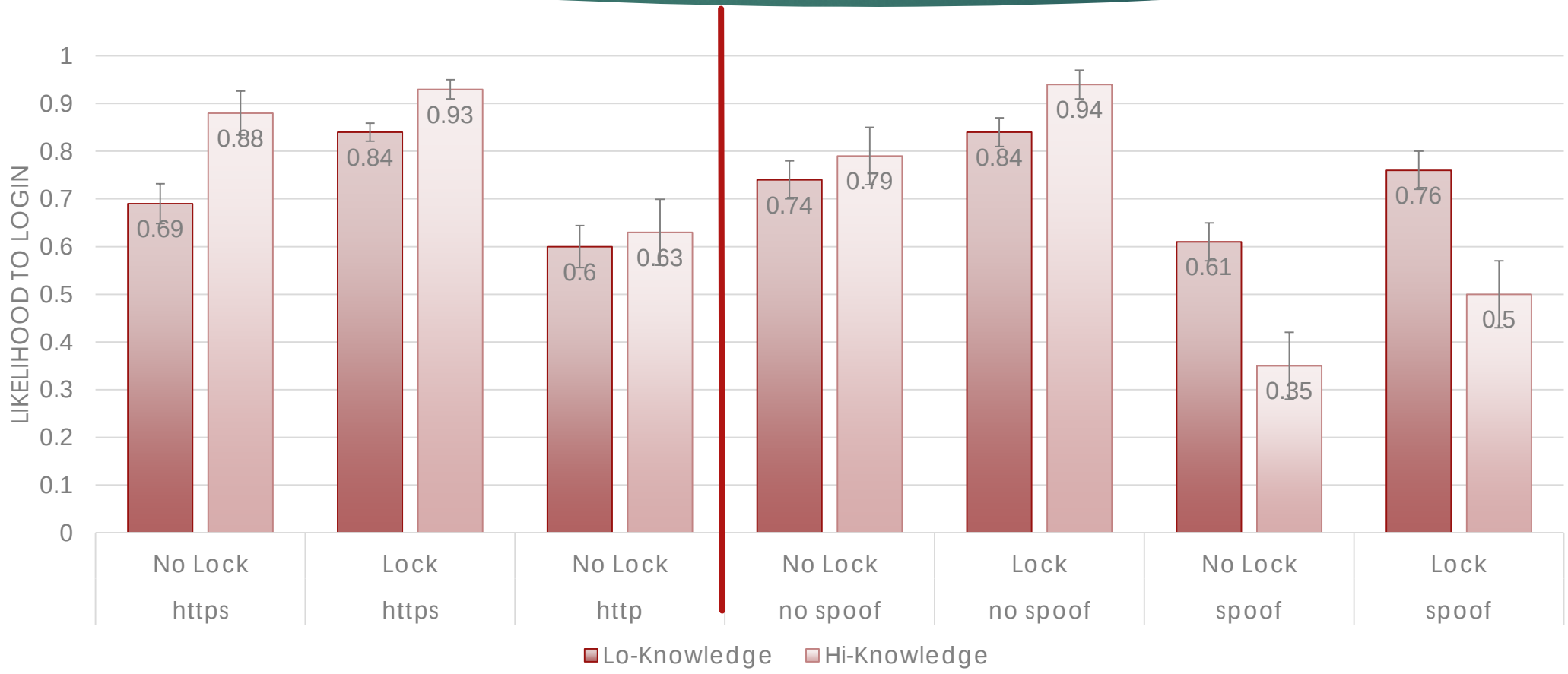
Conclusions

- Participants do not ignore security indicators
  - Security Indicators Increase Likelihood to Login!

Conclusions

- Participants do not ignore security indicators
  - Security Indicators Increase Likelihood to Login!
  - Survey-based measures of knowledge are limited as predictors of behavior

Conclusions



Conclusions

- Participants do not ignore security indicators
  - Security Indicators Increase Likelihood To Login!
  - Survey-based measures of knowledge are limited as predictors of behavior
  - Heuristics and biases play an important role in risky actions in digital environments

Conclusions

- Participants do not ignore security indicators
  - Security Indicators Increase Likelihood to Login!
  - Survey-based measures of knowledge are limited as predictors of behavior
  - Heuristics and biases play an important role in risky actions in digital environments
- Mouse tracking reveals the dynamics of perception
  - And shows that participants are not guessing

Discussion

- Why do participants fail to interpret available security cues correctly?
  - In this experiment, may be due to time pressure
  - More generally:
    - What is up with HTTP?
    - Confusion between encryption and authentication?

Acknowledgements

Advice and assistance from the HATS lab: L. Jean Camp, Prashanth Rajivan, Rachel Huss, and Tom Denning.

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.