**Purpose:** Modern browsers are designed to inform users as to whether or not it is secure to login to a website, but most users are not aware of this information and even those that are sometimes ignore it. This study seeks to assess users’ knowledge of security warnings communicated via browser indicators and the likelihood that their online decision making adheres to this knowledge.

**Methodology:** Participants from Amazon’s Mechanical Turk visited a series of secure and insecure websites, and decided as quickly and as accurately as possible whether or not it was safe to login. An online survey was then used to assess their knowledge of information security.

**Findings:** Knowledge of information security was not necessarily a good predictor of decisions regarding whether or not to sign-in to a website. Moreover, these decisions were modulated by attention to security indicators, familiarity of the website, and psychosocial stress induced by bonus payments determined by response times and accuracy.

**Practical Implications:** Even individuals with security knowledge are unable to draw the necessary conclusions about digital risks while browsing the web. Users are being educated through daily use to ignore recommended security indicators.

**Originality:** This study represents a new way to entice participants into risky behavior by monetizing both speed and accuracy. This approach could be broadly useful as a way to study risky environments without placing participants at risk.

Timothy Kelley <kelleyt@umail.iu.edu> is a visiting research fellow at the Developmental Cognitive Neuroscience Lab in the Department of Psychological and Brain Sciences at Indiana University. He has also worked as a postdoctoral research fellow for the American Society for Engineering Education at NSWC Crane, IN. He studies cognitive processes and real-time decision-making in the digital realm, focusing primarily on cyber security. He completed his PhD at the School of Informatics and Computing and in the Department of Psychological and Brain Sciences at the Indiana University. Prior to studying decision-making, Tim completed a master's degree in Computer Science and Information Assurance from James Madison University, and a master's degree in Bioinformatics from Indiana University, Bloomington. He completed his bachelor's degree in Computer Science from Calvin College.

# Methodology

Introducing a performance bonus based on both speed and accuracy in completing the task was done to increase the motivation and risk taking behavior of participants (Petzold *et al.* 2010). The primary question was whether users would ignore or simply miss security indicators when pressed for time. In order to address this question, a relatively large sample with a broad distribution of knowledge concerning security indicators was needed.

## Participants

The sample consisted of 173 English-speaking participants ranging in age from 18- to 76-years-old *(M* = 32.6, *SD* = 9.58*)* recruited from Amazon’s Mechanical Turk (AMT). Studies have shown that AMT provides more diverse study populations and robust findings in numerous psychological paradigms (Buhrmester *et al.* 2011, Crump *et al.* 2013). There were 100 males and 73 females, primarily Caucasian. Most participants listed Firefox *(N* = 84*)* or Google Chrome *(N* = 81*)* as their primary browser.

## Stimuli

Each trial simulated websites appearing on a Firefox browser. In order to standardize all websites, logins always appeared on the second page of the website. All stimuli were presented to participants in a popup window with disabled user interface chrome to minimize confusion between the proxy websites’ chrome and their actual browser chrome. This also prevented participants from manipulating the experiment by reloading pages or navigating back and forward outside of the simulated website user interface. Presented websites were manipulated in a graphical editing program to appear a functional websites.

## Procedure

Participants were instructed to decide whether or not to login to a series of websites depending on whether or not they were judged to be secure. The goal was to visit all the websites as quickly as possible, and the pay for completing this task was contingent on how quickly it was completed. If a participant clicked to login to a secure website, the screen advanced to the next one. If a participant did not click to login to a secure website and instead pressed the back button, a penalty screen was displayed for 20 sec and that time was added to their cumulative time. If a participant pressed the back button and the website was insecure, the screen advanced to the next website. If, however, a participant clicked to login to an insecure website, the penalty screen was displayed for 10 sec and that time was added to their cumulative time. The difference in penalty times for incorrect backs and logins were chosen to correct for the fact that participants demonstrated faster response times with back response than with login responses, presumably because the back button was always in the same location making it easier for participants to find and click on it.

An online survey assessing participants’ knowledge concerning security indicators was administered after the experimental task so as not to bias participants’ performance. There were three categories of questions: 1) Demographic information (e.g., age, gender, education level), 2) Applied security knowledge (e.g., security indicators, password behavior), and 3) Technical security knowledge (e.g., DDoS, Phishing, Firewalls).

## Design

This study addressed two questions: 1) Do web security indicators affect participants’ behavior when discerning the safety of encrypted vs. unencrypted websites, and 2) Do web security indicators affect participants’ ability to discern between spoofed vs. not spoofed websites. The first question was tested by manipulating whether the security indicators included http or https (https/http manipulation). The second question was tested by manipulating whether or not the website was spoofed with an incorrect domain name (no-spoof/spoof manipulation). There are four different levels of encryption information displayed by web security indicators:

1. Extended Validation (EV) – green lock and https – full encryption; Extended vetting by certificate authority
2. Full Encryption (FE) – grey lock and https – full encryption; domain validation only
3. Partial Encryption (PE) – triangle with exclamation mark; some (unknown) elements of website encrypted
4. No Encryption (NE) – globe; no encryption of the displayed page

All four levels were included for both spoof and no-spoof websites in the no spoof/spoof manipulation, but this was not possible for the https/http manipulation because unencrypted websites (http) only display a globe (NE), whereas the encrypted websites (https) display the three other security symbols listed above (1-3). Thus the https/http and no-spoof/spoof manipulations were analyzed separately in this study.

Each participant was presented with 16 trials, 8 corresponding to each security manipulation condition (https/http vs. no spoof/spoof). Four trials corresponded to secure websites (https/no spoof) and 4 corresponded to insecure websites (http/spoof). For the https/http manipulation, each secure website included 1 of the 3 valid levels of encryption information (EV, FE, or PE), whereas each insecure website included only the NE indicator. For the spoof/no spoof manipulation, the 4 secure and 4 insecure trials each corresponded to one of the 4 encryption information levels. The secure and insecure websites were counterbalanced between participants and the presentation order of the websites was randomized.

# Acknowledgements

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. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on. Additional funding provided by NSWC Crane. The authors would also like to acknowledge the following people for their assistance: L. Jean Camp, Prashanth Rajivan, Rachel Huss, and Tom Denning.

# References

Buhrmester, M., Kwang, T., and Gosling, S.D., 2011. Amazon’s Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science*, 6 (1), 3–5.

Crump, M.J.C., McDonnell, J. V., and Gureckis, T.M., 2013. Evaluating Amazon’s Mechanical Turk as a Tool for Experimental Behavioral Research. *PLoS ONE*, 8 (3), e57410.

Petzold, A., Plessow, F., Goschke, T., and Kirschbaum, C., 2010. Stress reduces use of negative feedback in a feedback-based learning task. *Behavioral neuroscience*, 124 (2), 248–255.