Emerald Insight

Information & Computer Security

Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites

Timothy Kelley Bennett I. Bertenthal

Article information:

To cite this document:
Timothy Kelley Bennett I. Bertenthal , (2016),"Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites", Information & Computer Security, Vol. 24 Iss 2 pp. 164 - 176
Permanent link to this document:
http://dx.doi.org/10.1108/ICS-01-2016-0002

Downloaded on: 07 November 2016, At: 20:54 (PT)
References: this document contains references to 26 other documents.
To copy this document: permissions@emeraldinsight.com
The fulltext of this document has been downloaded 116 times since 2016*

Users who downloaded this article also downloaded:

(2016),"Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study", Information and Computer Security, Vol. 24 Iss 2 pp. 139-151 http://dx.doi.org/10.1108/ICS-12-2015-0048

(2016),"Assessing information security attitudes: a comparison of two studies", Information and Computer Security, Vol. 24 Iss 2 pp. 228-240 http://dx.doi.org/10.1108/ICS-01-2016-0009

Access to this document was granted through an Emerald subscription provided by emerald-srm:563821 []

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

*Related content and download information correct at time of download.

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

The current issue and full text archive of this journal is available on Emerald Insight at:
www.emeraldinsight.com/2056-4961.htm

Received 16 January 2016
Revised 16 January 2016
Accepted 9 March 2016

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

Attention and past behavior, not security knowledge, modulate users' decisions to login to insecure websites

Timothy Kelley and Bennett I. Bertenthal
Department of Psychological and Brain Sciences, Indiana University Bloomington, Bloomington, Indiana, USA

Abstract

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

Design/methodology/approach – Participants from Amazon's Mechanical Turk visited a series of secure and insecure websites and decided as quickly and as accurately as possible whether 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 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 when browsing the web. Users are being educated through daily use to ignore recommended security indicators.

Originality/value – 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.

Keywords Information security, Mechanical Turk, Browser login, Human subjects research, Security expertise

Paper type Research paper

1. Introduction

Users on the internet are regularly confronted with complex security decisions that can affect their privacy. They must decide whether it is safe to enter their username,

This 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 US Government. The US Government is authorized to reproduce and distribute reprints for government purposes notwithstanding any copyright notation here on. Additional funding was provided by the 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.

Information & Computer Security
Vol. 24 No. 2, 2016
pp. 164-176
© Emerald Group Publishing Limited
2056-4961
DOI 10.1108/ICS-01-2016-0002

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

password, credit card details and other personal information on websites with very different interfaces and only a few visual clues on whether it is safe to do so. These security indicators include the protocol used, the domain name, the secure sockets layer (SSL)/transport layer security (TLS) certificate and visual elements in the browser window. Very few users understand the technical details of these various indicators.

Not surprisingly, users often get it wrong by either ignoring security indicators completely or misunderstanding them. Many popular websites are designed in such a way that these indicators are displayed in a suboptimal way, further complicating users' decision-making process (Stebila, 2010). Moreover, these websites can appear confusing because they include no or only partial encryption, but users will treat them as secure even without security indicators if they have been previously visited (Hazim *et al.*, 2014). This confusion is due to the manner in which security information is typically deployed, that is, as communication between technical experts (Garg and Camp, 2012).

Although several studies have evaluated whether users correctly use security indicators, there has been very little work investigating whether their knowledge of these indicators will predict their behavior (Schechter *et al.*, 2007). One reason for this predicament is that it is challenging to design behavioral studies that will realistically simulate the conditions that a user would experience on the internet (Arianezhad *et al.*, 2013).

One real-world condition that is particularly difficult to replicate in an experimental environment is the experience of risk. Many studies ask participants to assume the role of someone else to avoid exposing participants to real risks (Schechter *et al.*, 2007; Sunshine *et al.*, 2009). Other studies use priming – alerting participants to the fact that the study is interested in behavior related to security – to induce secure-like behavior (Whalen and Inkpen, 2005). It is unlikely, however, that participants playing roles behave as securely as they would when they are personally at risk.

A different strategy is to use monetary incentives and penalties as a method for creating risky decisions. This study utilizes participants' assumed goal of maximizing payment to put pressure on the participant to act as quickly as possible by offering participants a bonus payment that decreases as the total elapsed time increases. By monetizing quick decision-making, this study investigates if, and to what extent, participants' security domain knowledge, self-reported awareness of web browser security indicators and familiarity with websites affect their willingness to login to a presented website.

2. Background

Work in usable security has attempted to address the effectiveness and understanding of the various cues, indicators and warnings available in a variety of digital environments. At the same time, these studies must be constructed in a manner that avoids placing participants at risk. To study users' ability to properly use security indicators and avoid risk, work in this area has relied on surveys, roleplaying and priming to ascertain participants' understanding of the underlying technical concepts related to digital security and their use of the available technologies.

Early studies, such as Friedman *et al.* (2002) used surveys to identify potential connections between demographic information and participants' understanding of digital security. They used survey results and participants' definitions and representations of digital security concepts to identify common misconceptions all

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

participants, not just technically naïve subjects, had when identifying secure connections. Survey data, however, do not indicate the actual usage of available cues and indicators.

Whalen and Inkpen (2005) conducted one of the first examinations of users' attention to web browser security indicators. Using eye tracking, they identified participants' gaze points within areas of interest corresponding to the location of web browser security cues while subjects performed normal browsing tasks. They then compared the gaze results with participants' self-reported use of indicators and found that none of the participants' self-reported behaviors was verified by the gaze data. Only when they explicitly primed users to pay attention to security indicators did the results show any verification of self-reported attention to indicators.

Building on the eye-tracking methodology of Whalen and Inkpen, Sobey *et al.* (2008) investigated the effects of indicators incorporating extended validation certificates. The self-reported measures of attention to security indicators they collected demonstrated a lack of certainty in participants' ability to recall their attention. When they used eye tracking, however, they found that participants who had fixations on the security indicators reported a higher willingness to conduct business transactions based on the SSL level, whereas participants who did not fixate on the security indicators had no difference in willingness to conduct business.

Drawing on Sobey *et al.*'s work, Arianezhad *et al.* (2013) attempted to explicitly examine the effects of security domain knowledge on participants' attention to security indicators. Surprisingly, they found that task context had a greater effect on participants' attention to security indicators than participants' domain knowledge. Alsharnouby *et al.* (2015) also utilized eye tracking to explore what security indicators participants might use when trying to identify phishing websites. They found that participants who had gaze points in the browser Chrome were better at identifying phishing websites. They also found, as Friedman *et al.* did, that technical knowledge did not necessarily associate with accuracy.

None of these studies, however, created an environment of risk for participants. In the eye-tracking studies, for example, participants had ample time to identify and then make their decisions. Moreover, the self-reported data from participants rarely matched the recorded output. The lack of risk, as shown by Schechter *et al.* (2007), greatly affects participants' attention. In Schechter *et al.*'s study, although they used roleplaying, priming and even allowed some participants to use their own accounts, none of the participants noticed the lack of the https indicator when presumably logging-in to a bank website. Thus, without a naturalistic environment, with potential risks, it is difficult to evaluate the effectiveness of survey data as they correspond to output measures.

One way of addressing this concern is to utilize time pressure. A recent study by Young *et al.* (2012), found that use of time pressure, in conjunction with bets, was found to increase risk-taking and reduce participants' ability to evaluate outcome utility.

3. 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. To address this question, a relatively

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

large sample with a broad distribution of knowledge concerning security indicators is needed.

3.1 Participants

The sample consisted of 173 English-speaking participants ranging in age from 18 to 76 years ($M = 32.6$, $SD = 9.58$) 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.

3.2 Stimuli

Each trial simulated websites appearing on a Firefox browser. 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 as functional websites.

3.3 Procedure

Participants were instructed to decide whether to login to a series of websites depending on whether 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 s 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 s 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, thus 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 and education level);

(2) applied security knowledge (e.g. security indicators and password behavior); and

(3) technical security knowledge (e.g. DDoS, phishing and firewalls).

3.4 Design

This study addressed two questions:

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

Q1. Do web security indicators affect participants' behavior when discerning the safety of encrypted vs unencrypted websites?

Q2. Do web security indicators affect participants' ability to discern between spoof vs no-spoof 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 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 the other four corresponded to insecure websites (http/spoof). For the https/http manipulation, each secure website included one of the three valid levels of encryption information (EV, FE or PE), whereas each insecure website included only the NE indicator. For the spoof/no-spoof manipulation, four secure and four insecure trials each corresponded to one of the four encryption information levels. The secure and insecure websites were counterbalanced between participants, and the presentation order of the websites was randomized.

3.5 Metrics and data reduction

Applied security knowledge was computed from the number of correct and incorrect security indicators identified in the survey $\#correct\ indicators + 1 / \#incorrect\ indicators + 1$, resulting in an indicator score ranging from 0.2 to 4.0 with a log-normal distribution of $\log N(M = 0.14, SD = 0.58)$. This score was then centered to place the values on a similar scale as the dichotomous predictors (Gelman and Hill, 2007). References to indicator score refer to the final, centered value.

Technical security knowledge was scored from 1 to 5 depending on the number of survey questions answered correctly (0-20 per cent = 1, 21-40 per cent = 2 […]). Participants scoring greater than 60 per cent ($N = 50$) were identified as "High Technical Security Knowledge" (Hi-Knowledge), and participants scoring 60 per cent or less ($N = 123$) were identified as "Low Technical Security Knowledge" (Lo-Knowledge).

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

Familiarity of the websites was rated on a five-point Likert scale. The mean rating was 2.90, and it ranged from a low of 1.00 to a high of 5.00 (Figure 1). Familiarity was centered in the manner described above for the indicator score. References to familiarity refer to the final value.

3.6 Statistical analysis

A hierarchical general logistic mixed-effects model was used to analyze both manipulations (https/http and no-spoof/spoof) separately. Likelihood to login was the predicted variable with manipulation and participants' security domain knowledge as the predictor variables. Participants' familiarity with a presented website (familiarity) and their self-reported use of security indicators (indicator score) were included as covariate predictors. Lock presence (lock vs no-lock) was included as a predictor in the no-spoof/spoof manipulations because of a balanced design but was analyzed as a *post hoc* test to evaluate potential effects of lock within the https condition in the https/http manipulation.

The login model utilized the maximal random effects structure justified by the data as described by Barr *et al.* (2013). Models were analyzed in *R* by using the arm, lme4, lsmeans, car, phia and psych packages (Fox and Weisberg, 2011; Bates *et al.*, 2015; R Core Team, 2014; Gelman and Su, 2015; Lenth, 2016; Revelle, 2015). The ggplot2 package was used for plotting (Wickham, 2009), and data manipulation was assisted by the plyr package (Wickham, 2011).

Tukey's honest significant difference test was used for *post hoc* analysis of multiple comparisons between categorical predictors (Tukey, 1949), and Bayesian estimation was used in place of standard *t*-tests (Kruschke, 2013). Covariate predictors were centered to improve analysis (Gelman and Hill, 2007), and the *p*-values for model coefficients were calculated using Type III Wald Chi-square tests.

4. Results

The primary question concerned how frequently participants would login to insecure websites. Overall, they were more likely to login to encrypted than to unencrypted websites (M_{diff} = 0.23, *95 per cent HDI* = 0.17, 0.28) and to non-spoofed than to spoofed websites (M_{diff} = 0.21, *95 per cent HDI* = 0.15, 0.27). Critically, the results revealed a strong response bias to login regardless of available security indicators (Figure 2). Participants' lack of sensitivity to the available stimuli was reflected in the relatively low *d*'s in both the https/http manipulation (M = 0.41, 95 per cent *HDI* = −0.67, 1.35) and the no-spoof/spoof manipulation (M = 0.34, *95 per cent HDI* = −0.67, 1.35).

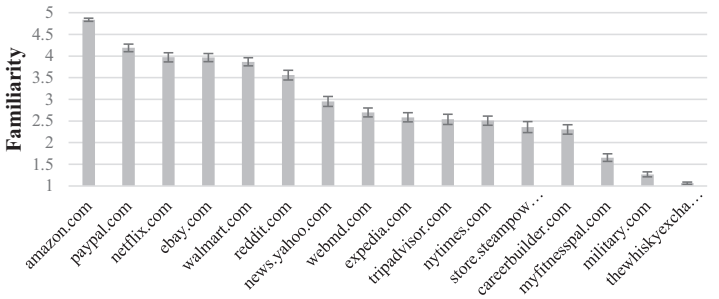

Figure 1.
Mean familiarity for each website used in this study

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

4.1 Survey data

Surprisingly, most of the various demographic data collected were not predictive of participants' likelihood to login. There was no linear correlation between participants' age and their likelihood to login, $r(171) = 0.01, p = 0.89$. More interestingly, none of the various applied security or general computer use results were related to likelihood to login (e.g. number of hours spent on the internet – $\chi^2(44) = 37.99, p = 0.75$ – or years of practical security experience – $\chi^2(44) = 38.23, p = 0.72$). Even participants' self-reported use of security indicators were not linearly related to participants' likelihood to login, $r(171) = -0.09, p = 0.24$. Participants' accuracy in defining technical concepts from digital security was also not found to be correlated with likelihood to login, $r(171) = -0.13, p = 0.07$. Participants' familiarity, however, was also found to be correlated with their likelihood to login, $r(171) = 0.11, p < 0.01$.

4.2 Http/https manipulation

Participants' performance on the http/https websites was analyzed by assessing the per cent of logins as a function of technical security knowledge (Lo vs Hi), security manipulation (http vs https), familiarity and indicator score. A likelihood ratio test for nested models showed the omnibus analysis of the hierarchical general logistic mixed-effects model to be more predictive than the null model, $\chi^2(4) = 124.99, p < 0.0001$. The omnibus analysis revealed significant main effects for security manipulation, technical security knowledge and familiarity (Table I).

Figure 3 shows that participants were more likely to login in the https condition than the http condition ($M_{diff} = 0.23$, *95 per cent HDI* = 0.17, 0.29, $p < 0.0001$), and Hi-Knowledge participants were more likely to login than Lo-Knowledge participants ($M_{diff} = 0.07$, *95 per cent HDI* = 0.003, 0.13, $p < 0.01$). Surprisingly, participants' self-reported use of indicator scores was not found to have a significant effect on participants' likelihood to login.

A significant interaction between manipulation and technical security knowledge was revealed by a more detailed model – as determined by a likelihood ratio test ($\chi^2(19) = 49.67, p < 0.001$) – including interactions between the predictors (Table II). As

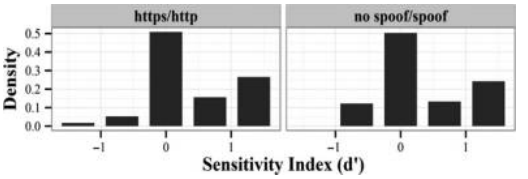

Figure 2.
Participants' response bias toward login

Table I.
Results of https/http omnibus analysis with coefficient estimates (β), standard errors, Wald-III χ^2 degrees of freedom, p-values and odd ratios

Parameter	Estimate (β)	Standard error	χ^2	df	$p(>\chi^2)$	Odd ratio
(Intercept)	1.35	0.116	135.03	1	<0.0001	3.85
http → https	0.67	0.07	87.93	1	<0.0001	1.95
Lo-Knowledge → Hi-Knowledge	0.41	0.16	6.74	1	<0.01	1.51
Familiarity	0.6	0.14	17.54	1	<0.0001	1.83
Indicator score	−0.25	0.2	1.57	1	0.21	0.78

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

shown in Figure 3, Hi-Knowledge participants were more likely to login than Lo-Knowledge participants in the https condition ($M_{diff} = 0.11$, *95 per cent HDI* = 0.06, 0.17, $p < 0.001$), but technical security knowledge had no effect in the http condition ($M_{diff} = -0.02$, *95 per cent HDI* = −0.10, 0.14, $p > 0.72$).

In a separate analysis of encryption information in the https condition, encryption was found to have a main effect (Table II) but was not involved in any interactions. As can be seen in Figure 3, participants were more likely to login when a lock was present (FE and EV) than when no lock was present (PE) in the https condition ($M_{diff} = 0.12$, *95 per cent HDI* = 0.06, 0.18, $p < 0.001$). Participants' likelihood to login was also shown to increase with an increase in the familiarity with the presented website (Table II).

4.3 No-spoof/spoof manipulation

Including predictors in the hierarchical generalized logistic mixed-effects model for the no-spoof/spoof manipulation was found to explain more deviance than the null model, $\chi^2(5) = 126.17$, $p < 0.0001$. An omnibus analysis of the logistic model revealed main effects for manipulation (no-spoof vs spoof), encryption information (lock vs no-lock), technical security knowledge (Hi vs Lo) and familiarity (Table III). Participants' self-reported use of indicators was not found to be a main effect.

Figure 4 reveals that participants are more likely to login in the no-spoof condition than in the spoof condition ($M_{diff} = 0.20$, *95 per cent HDI* = 0.15, 0.26, $p < 0.0001$) and more when a lock is present than when it is not present ($M_{diff} = 0.14$, *95 per cent HDI* = 0.08, 0.19, $p < 0.0001$).

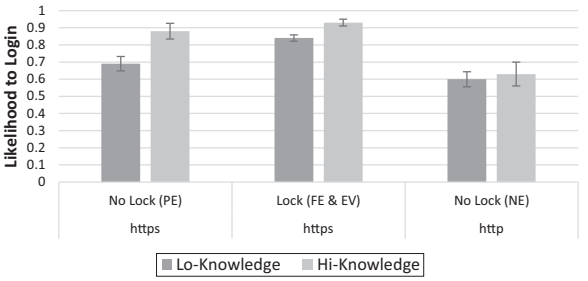

Figure 3. Participants' observed likelihood to login to the https/http manipulation by encryption information (no-lock/lock) and technical security knowledge

Parameter	Estimate (β)	Standard error	χ^2	df	$p(>\chi^2)$	Odds ratio
(Intercept)	1.41	0.15	82.86	1	<0.0001	4.09
http → https	0.74	0.12	35.41	1	<0.0001	2.09
Lo-Knowledge → Hi-Knowledge	0.65	0.21	9.25	1	<0.01	1.91
Familiarity	0.98	0.27	13.49	1	<0.001	2.67
Indicator score	−0.27	0.31	0.75	1	0.39	0.77
https/http × Lo-Knowledge/ Hi-Knowledge	−0.36	0.17	4.16	1	<0.05	1.43
$\text{https}_{\text{no-lock} \rightarrow \text{lock}}$	0.78	0.31	6.38	1	<0.05	2.18

Table II. Coefficient estimates for main effects and significant interactions for the https/http manipulation. *Post hoc* coefficient estimate for lock presence is also included

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

Unlike in the https/http manipulation, Hi-Knowledge participants are shown to login less than Lo-Knowledge participants ($M_{diff} = -0.09$, *95 per cent HDI* $= -0.15, -0.03$, $p < 0.01$). As in the https/http manipulation, self-reported use of security cues was not a significant indicator of participants' likelihood to login, and increased familiarity was also shown to increase participants' likelihood to login.

The more complete model with interactions ($\chi^2(26) = 86.32$, $p < 0.0001$) showed main effects for manipulation (no-spoof/spoof), encryption information (lock/no-lock) and familiarity. Neither technical security knowledge nor participants' self-reported use of security indicators were found to be significant (Table IV). The more complete model further reveals three two-way interactions between manipulation and familiarity; encryption information and indicator score; and manipulation and technical security knowledge (Table IV).

Figure 4 shows that Hi-Knowledge participants and Lo-Knowledge participants have roughly the same likelihood to login to "no-spoof" websites ($M_{diff} = 0.04$, *95 per cent HDI* $= -0.03, 0.10$, $p = 0.07$), but Hi-Knowledge participants are less likely to login to "spoof" websites than Lo-Knowledge participants ($M_{diff} = -0.26$, *95 per cent HDI* $= -0.37, -0.15$, $p < 0.0001$).

Manipulation (no-spoof/spoof) was also shown to interact with participants' familiarity with the displayed website (Table IV). In the "no-spoof" condition, the likelihood to login increased with an increase in participants' familiarity with the website ($\beta_{\text{no-spoof} \times \text{familiarity}} = 1.44$, *95 per cent CI* $= 0.59, 2.3$, $p < 0.001$). In the "spoof" condition, however, familiarity is not a significant predictor of participants' likelihood to login ($\beta_{\text{spoof} \times \text{familiarity}} = -0.23$, *95 per cent CI* $= -0.66, 0.21$, $p = 0.31$). Thus, as shown in Figure 5, familiarity leads to a greater likelihood to login in "no-spoof" than in the

Table III.
Results of no-spoof/spoof omnibus analysis with coefficient estimates (β), standard errors, Wald-III χ^2 degrees of freedom, p-values and odd ratios.

Parameter	Estimate (β)	Standard error	χ^2	df	$p(>\chi^2)$	Odds ratio
(Intercept)	0.99	0.09	110.95	1	<0.0001	2.68
Spoof → no-spoof	0.58	0.07	73.55	1	<0.0001	1.78
No-lock → lock	0.59	0.09	38.41	1	<0.0001	1.51
Lo-Knowledge → Hi-Knowledge	−0.34	0.13	6.49	1	<0.05	0.71
Familiarity	0.36	0.14	6.73	1	<0.01	1.43
Indicator score	−0.07	0.17	1.67	1	0.68	0.93

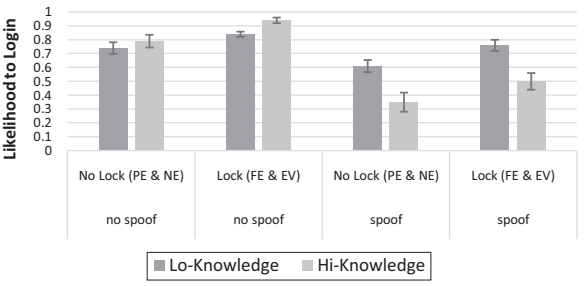

Figure 4.
Participants' observed likelihood to login to the no-spoof/spoof manipulation by encryption information (no-lock/lock) and technical security knowledge

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

"spoof" condition ($\beta_{(\text{no-spoof} - \text{spoof}) \times \text{familiarity}} = 1.67$, *95 per cent CI* = 1.15, 2.19, $p < 0.0001$).

Indicator score was also found to interact with lock presence (no-lock/lock). As shown in Figure 6, participants login significantly more when there is no lock present, and their indicator score is low ($\beta_{(\text{no lock} - \text{lock}) \times \text{indicator score}} = -1.25$, *95 per cent CI* = –2.47, –0.03, $p < 0.05$).

5. Discussion

Although these results suggest that security knowledge is related to a decrease in risky behavior, it would be a gross exaggeration to suggest that security knowledge is sufficient to ensure secure and safe behavior on the web. Limiting the analysis to just those participants who scored correctly on at least 80 per cent of the technical security questions ($n = 32$), the results show that they logged-in to 88 per cent of secure logins and 41 per cent of the insecure logins across both studies.

These results clearly reveal that there is no simple relationship between security knowledge and the likelihood of logging-in to insecure websites. Although this result might have been predicted for non-experts, it was expected that experts would show a lower likelihood of logging-in to insecure websites. Given that this study was designed to increase both risk-taking and stress by motivating participants to respond as quickly as possible to maximize their payoff, it is possible that either factor or both inflated the

Parameter	Estimate (β)	Standard error	χ^2	df	$p(>\chi^2)$	Odds ratio
(Intercept)	1.51	0.15	61.40	1	<0.0001	4.53
Spoof → no-spoof	0.97	0.13	54.17	1	<0.0001	2.64
No-lock → lock	0.80	0.19	18.82	1	<0.0001	2.23
Lo-Knowledge → Hi-Knowledge	−0.10	0.21	0.23	1	0.63	0.90
Familiarity	0.61	0.24	6.20	1	<0.05	1.84
Indicator score	0.22	0.33	0.44	1	0.51	1.25
Spoof/no-spoof × familiarity	0.83	0.24	11.63	1	<0.001	2.29
No-lock/lock × indicator score	0.88	0.42	4.24	1	<0.05	2.41
Spoof/no-spoof × Lo-knowledge/ Hi-Knowledge	0.82	0.19	19.41	1	<0.0001	2.27

Table IV. Coefficient estimates for main effects and significant interactions for the no-spoof/spoof manipulation

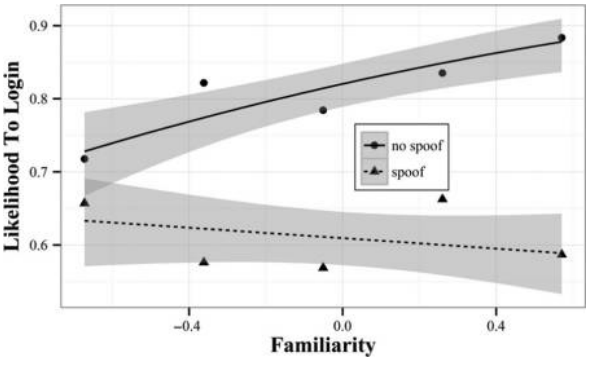

Figure 5. Effect of manipulation and familiarity on participants' likelihood to login to the no-spoof/spoof condition

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

number of errors that were shown by experts. Familiarity of the websites may have also contributed to participants being less likely to check security indicators because they were more likely to revert to the habitual behavior of logging-in to familiar websites. In theory, this should have made all participants more vulnerable to the no-spoof/spoof manipulation, but the performance of experts, in particular, was more complex than expected.

Experts are better than non-experts at detecting spoofed websites but no better at detecting sites without encryption information. One possible explanation for this phenomenon is that experts primarily use the domain name highlighting feature available in modern browsers when identifying insecure websites, whereas non-experts do not. Assuming that spoofed uniform resource locators (URLs) are not particularly clever, the modest familiarity of an authentic URL – but not user interface – should expose a fraudulent website if one is aware of domain highlighting. This hypothesis would help explain why experts are good at identifying fraudulent websites but no better than non-experts when it comes to logging-in to websites with no encryption. Experts' choices rely on more than familiarity. The presence of security indicators appears to diminish their accuracy when detecting spoofed websites. This suggests that experts find that security cues obscure the presence of an inauthentic URL, leading to a reduction in accuracy when dealing with spoofed websites with encryption information present.

These results clearly suggest that education alone will not be sufficient to change risky behaviors on the web. Just like in this study, a typical internet user will often be asked to make security decisions against best-practice recommendations on security indicators. In essence, users are being educated through daily use to ignore recommended security indicators. These indicators are also used in an inconsistent fashion, where it is often necessary to have some familiarity with the website to know whether a partial or no encryption indicator is tantamount to commerce on an insecure site. Some of this confusion could be reduced if website designers conformed to the same set of conventions regarding security indicators. This would at the very least give users a better chance to identify insecure and spoof websites where their credentials and financial information can be hijacked.

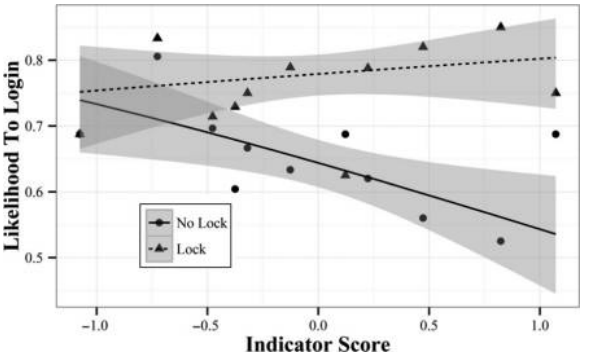

Figure 6.
Effects of encryption information and indicator score on participants' likelihood to login to the no-spoof/spoof condition

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

References

Alsharnouby, M., Alaca, F. and Chiasson, S. (2015), "Why phishing still works: user strategies for combating phishing attacks", *International Journal of Human-Computer Studies*, Vol. 82, pp. 69-82.

Arianezhad, M., Camp, L.J., Kelley, T. and Stebila, D. (2013), "Comparative eye tracking of experts and novices in web single sign-on", *Proceedings of the third ACM Conference on Data and Application Security and Privacy – CODASPY '13*, *ACM Press, New York, NY*, p. 105.

Barr, D.J., Levy, R., Scheepers, C. and Tily, H.J. (2013), "Random effects structure for confirmatory hypothesis testing: keep it maximal", *Journal of Memory and Language*, Vol. 68 No. 3, pp. 255-278.

Bates, D., Mächler, M., Bolker, B., et al. (2015), "Fitting linear mixed-effects models using {lme4}", *Journal of Statistical Software*, Vol. 67 No. 1, pp. 1-48.

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*, Vol. 6 No. 1, pp. 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*, Vol. 8 No. 3, p. e57410.

Fox, J. and Weisberg, S. (2011), *An {R} Companion to Applied Regression*, 2nd edn., Sage, Thousand Oaks, CA.

Friedman, B., Hurley, D., Howe, D.C., Felten, E. and Nissenbaum, H. (2002), "Users' conceptions of web security", *CHI '02 Extended Abstracts on Human Factors in Computing Systems – CHI '02*, ACM Press, New York, NY, p. 746.

Garg, V. and Camp, J. (2012), "End user perception of online risk under uncertainty", *2012 45th Hawaii International Conference on System Sciences*, IEEE, Maui, HI, pp. 3278-3287.

Gelman, A. and Hill, J. (2007), "Data analysis using regression and multilevel/hierarchical models", *Data Analysis Using Regression and Multilevel/Hierarchical Models*, Cambridge University Press, New York, NY.

Gelman, A. and Su, Y.-S. (2015), *is Using Regression and Multilevel/Hierarchical Models*, available at: http://cran.r-project.org/package=arm

Hazim, A., Felt, A.P. and Reeder, R.W. (2014), "Your reputation precedes you: history, reputation, and the chrome malware warning", in *Symposium on Usable Privacy and Security (SOUPS)*, available at: www.adrienneporterfelt.com/chromemalwarewarning-soups.pdf (accessed 12 December 2014).

Kruschke, J.K. (2013), "Bayesian estimation supersedes the t test", *Journal of Experimental Psychology*, Vol. 142 No. 2, pp. 573-603.

Lenth, R.V. (2016), "Least-squares means: the {R} package {lsmeans}", *Journal of Statistical Software*, Vol. 69 No. 1, pp. 1-33.

Petzold, A., Plessow, F., Goschke, T. and Kirschbaum, C. (2010), "Stress reduces use of negative feedback in a feedback-based learning task", *Behavioral neuroscience*, Vol. 124 No. 2, pp. 248-255.

R Core Team (2014), *R: A Language and Environment for Statistical Computing*, R Core Team.

Revelle, W. (2015), *psych: Procedures for Psychological, Psychometric, and Personality Research*, Evanston, Illinois, available at: http://cran.r-project.org/package=psych

Schechter, S.E., Dhamija, R., Ozment, A. and Fischer, I. (2007), "The emperor's new security indicators an evaluation of website authentication and the effect of role playing on usability

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 20:54 07 November 2016 (PT)

studies", *Proceedings – IEEE Symposium on Security and Privacy, IEEE, Oakland/Berkley, CA*, pp. 51-65.

Sobey, J., Biddle, R., van Oorschot, P. and Patrick, A.S. (2008), "Exploring user reactions to new browser cues for extended validation certificates", in Jajodia, S. and Lopez, J. (Eds), *Proceeding 13th European Symposium on Research in Computer Security (ESORICS) 2008*, *Springer*, pp. 411-427.

Stebila, D. (2010), "Reinforcing bad behaviour", *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction – OZCHI '10*, *ACM Press*, *New York, NY*, p. 248.

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. and Cranor, L.F. (2009), "Crying wolf: an empirical study of SSL warning effectiveness", *Proceedings 18th USENIX Security Symposium*, *Berkeley, CA*.

Tukey, J.W. (1949), "Comparing individual means in the analysis of variance", *Biometrics*, Vol. 5 No. 2, pp. 99-114.

Whalen, T. and Inkpen, K.M. (2005), "Gathering evidence: use of visual security cues in web browsers", *Proceedings of Graphics Interface*, *Waterloo, ON*, pp. 137-144.

Wickham, H. (2009), *ggplot2: Elegant Graphics for Data Analysis*, Springer, New York, NY.

Wickham, H. (2011), "The split-apply-combine strategy for data analysis", *Journal of Statistical Software*, Vol. 40 No. 1, pp. 1-29.

Young, D.L., Goodie, A.S., Hall, D.B. and Wu, E. (2012), "Decision making under time pressure, modeled in a prospect theory framework", *Organizational Behavior and Human Decision Processes*, Vol. 118 No. 2, pp. 179-188.

Corresponding author
Timothy Kelley can be contacted at: kelleyt@indiana.edu

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**