JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 1(1), 2015, 109–120
doi: 10.1093/cybsec/tyv005
Advance Access Publication Date: 6 November 2015
Research Article

Research Article

Neural correlates of gender differences and color in distinguishing security warnings and legitimate websites: a neurosecurity study

Bonnie Brinton Anderson,[1],* C. Brock Kirwan,[2] David Eargle,[3] Scott R. Jensen,[1] and Anthony Vance[1]

[1]Information Systems Department, Brigham Young University, Provo, UT 84604, USA; [2]Psychology and Neuroscience, Brigham Young University, Provo, UT 84604, USA; [3]Katz Graduate School of Business, University of Pittsburgh, Pittsburgh, PA 15260, USA

*Corresponding author: E-mail: bonnie_anderson@byu.edu

Received 31 May 2015; revised 18 September 2015; accepted 28 September 2015

Abstract

Users have long been recognized as the weakest link in security. Accordingly, researchers have applied knowledge from the fields of psychology and human–computer interaction to understand the security behaviors of users. However, many cognitive processes and responses are unconscious or obligatory and yet still have a profound effect on users' security behaviors. With this in mind, researchers have begun to apply methods and theories of neuroscience to yield greater insights into the "black box" of user cognition. The goal of this approach—termed neurosecurity—is to better understand and improve users' behaviors. This study illustrates the potential for neurosecurity by investigating how two fundamental biological factors—gender and color perception—affect users' reception of security warnings. This is important to determine because research has shown that users frequently fail to appropriately respond to security warnings. We conducted a laboratory experiment using electroencephalography, a proven method of measuring neurological activity in temporally sensitive tasks. We found that the amplitude of the P300—an event-related potential component indicative of decision-making ability—was higher for all participants when viewing malware warning screenshots relative to legitimate website shots. Additionally, we found that the P300 was greater for women than for men, indicating that women exhibit higher brain activity than men when viewing malware warnings. However, we found that there was no change in the P300 when viewing red warnings compared to grayscale warnings. Together, our results demonstrate the value of applying neurosecurity methods to the domain of cybersecurity and point to several promising avenues for future research.

Key words: neurosecurity; gender difference; security warning; color perception; user interface design.

Introduction

Users have long been recognized as the weakest link in security. Fred Cohen noted in his seminal work on computer viruses, "There are many types of information paths possible in systems, some legitimate and authorized, and others that may be covert, the most commonly ignored one being through the user" [1:22]. Today, "client-side" attacks that target end users are now a primary attack vector for hackers, making users' security behaviors increasingly important [2]. Accordingly, security researchers have applied knowledge from the fields of psychology, criminology, and human–computer interaction (HCI) to understand the security behavior of users.

Past investigations of security behavior have mainly used self-reported measures such as interview and survey data and behavioral experiments [3]. Although these approaches have substantially added to our understanding of security behaviors, many cognitive processes and responses are unconscious or obligatory and yet still have a profound effect on users decision-making and behaviors [4]. Further, emotions relevant to security behaviors, such as fear, uncertainty, and distrust, are at least partially experienced unconsciously, which makes them difficult to capture accurately [5]. With this in mind, researchers have begun to apply methods and theories of neuroscience to yield greater insights into users' security behaviors. The goal of this approach—termed *neurosecurity*—is to better understand and improve users' behaviors [6].

This study illustrates the potential for neurosecurity by investigating how two fundamental biological factors—gender and color perception—affect users' reception of security warnings. These are important to investigate because research has shown that users frequently fail to appropriately respond to security warnings for a variety of reasons [7]. Research in HCI and information systems research indicates that gender can result in differences in use and attitudes toward technology [8, 9]. However, this research does not adequately explain why these gender differences exist. An exception is the work of Riedl *et al.* [10], who used neurobiology and neuroimaging to explain why men and women differ in online trust. Additionally, the emergence of advanced electrophysiological and brain imaging methods has provided strong evidence that functional differences in brain activity may underlie gender differences in decision-making situations [11, 12]. We therefore investigate in this article how gender influences perceptions and responses to malware warnings.

In addition to examining the relationship between gender and malware warnings, we also investigate the impact that color has on a user's reception of security warnings. Several studies have shown that color has the ability to change one's perceptions regarding emotion, attitude, and even intellectual performance [13–15]. Additionally, color has been shown to influence users' perceptions of hazard levels in relation to warnings, with the color red signifying greatest severity [16]. Further, major web browsers such as Google Chrome and Firefox use the color red for their security warnings (Appendix A). Despite this, it is not known whether color is influential in capturing attention to security warnings.

To address these gaps, this study investigates the following research questions:

1. Do men and women differ in terms of brain activity when viewing security warnings?
2. Does the color of a security warning influence how they are perceived, in terms of brain activity?

We examined these research questions by conducting an electroencephalography (EEG) laboratory experiment in which participants viewed and classified screenshots of web browser malware warning screens and legitimate websites. EEG is used to measure electrical potentials on the scalp due to neural activity and has been shown to be a useful predictor of security behavior and attitudes [5, 17]. Our results show that the amplitude of the P300 was significantly higher for all participants when viewing malware warning screenshots relative to legitimate website shots. However, we found that the P300 was greater for women than for men, indicating that women exhibit higher brain activity overall when viewing malware warnings. Finally, we found no difference in the P300 between viewing monochrome and red malware warnings screens typically used in major web browsers, indicating that color did not improve the efficacy of the malware warning screen for capturing attention.

This article contributes by, first, providing neurological results of the comparative performance of men and women in performing a security task: discriminating between malware warnings and legitimate websites. While our results are preliminary in nature, discovery of gender behavior in the processing of security information could potentially be useful in designing security interfaces. Second, despite the wide use of the color red for security warnings in practice, this study is the first to empirically examine whether color influences the perception of security messages. Third, this study demonstrates the unique insights into security behavior that neuroscience can yield—insights unattainable using conventional methods.

The rest of this article is organized as follows: first, we examine relevant literature in the areas of neurosecurity; gender, IT usage, and trust; the effects of colors on perception; and the P300 measure of brain activity. Next, we present our hypotheses, followed by our methodology. Finally, we provide our results, followed by a discussion and conclusion.

Literature review

In this section, we lay a foundation for our hypotheses by reviewing literature relevant to neurosecurity, gender and trust, gender and IT usage, and the impact of color on users' perceptions of hazards. We also review the P300, a brain measure associated with attention that is captured using EEG.

Neurosecurity

There is growing evidence of the value of cognitive neuroscience for studying cybersecurity (neurosecurity). We define neuroscience methodologies to include both "neurological" methods, such as EEG and functional magnetic resonance imaging (fMRI), as well as "psychophysiological" methods, including eye tracking and mouse-cursor tracking, which can serve as objective indices of brain activity. Such tools have the potential to uncover the "black box" of subtle user reactions and behavior [e.g. 6]. Table 1 lists some of the burgeoning literature in the area of neurosecurity.

Neurosecurity studies have sought to better understand and improve users' security behaviors. For example, Anderson *et al.* [6] used fMRI to investigate the problem of attenuated attention to security messages over repeated exposure, a process termed "habituation". They developed a polymorphic security message composed of the visual variations that were most resilient to habituation. In a follow-up study, they tested the polymorphic warning in a more ecologically valid setting. They analyzed mouse-cursor movements indicative of attention as participants interacted with security messages. Users maintained higher levels of attention to the polymorphic warning over repeated exposure compared to participants in a nonpolymorphic control group [6].

In another study, Neupane *et al.* [18] conducted an fMRI experiment measuring users' security performance as well as underlying neural activity with respect to two critical security tasks: (i) distinguishing between a legitimate and a phishing website; and (ii) heeding security (malware) warnings. At a high level, they identified neural markers associated with users' performance in these tasks. They also investigated the relationship between users' personality traits and security behaviors.

Other neuroscience studies correlate neural activity with self-reported measures. Hu *et al.* [17] used EEG to examine the scalp for differences in brain region activations between individuals with high and low self-reported self-control. They took the EEG measurements as participants considered hypothetical information security policy violations. In another study, Vance *et al.* [5] measured risk perceptions using both EEG and self-reported methods. EEG measurements predicted users' security message disregard better than did self-reported measurements during a more ecologically valid

Table 1. Recent neurosecurity literature

Author(s)	Summary	Neuroscience method(s) used
Anderson *et al.* [6]	Used fMRI to identify a set of polymorphic warning variations most resilient to habituation. Corroborated MRI data with mouse cursor tracking in a more naturalistic lab study to validate the effectiveness of polymorphic warnings on decreasing susceptibility to security message habituation.	fMRI; mouse-cursor tracking
Hu *et al.* [17]	Used EEG to compare neural activity between high and low self-control individuals as they deliberated over hypothetical security policy violation scenarios.	EEG
Vance *et al.* [5]	In a multipart study, measured risk perceptions using both EEG and self-reported methods. EEG measurements predicted users' security message disregard better than did self-reported measurements during a more ecologically valid laboratory task.	EEG
Neupane *et al.* [18]	Used an fMRI study to measure users' security performance and underlying neural activity during two critical security tasks: (i) distinguishing between a legitimate and a phishing website; and (ii) heeding security malware warnings. Identifies neural markers associated with users' security-task performance, and examines the relationship between personality traits and security behavior.	fMRI
Anderson *et al.* [19]	Used fMRI to show how habituation occurs in the brain as a result of viewing security warnings. Found habituation to security messages to be more severe than habituation to screenshots of general business software.	fMRI
Anderson *et al.* [20]	Used eye tracking to show the eye movement-based memory effect (EMM effect), the phenomenon of people paying less visual attention to images similar to ones viewed previously, in the context of phishing messages. Suggests that the EMM effect is a significant contributing factor to users' susceptibility to phishing. Proposed training that could help users overcome the EEM effect and become less prone to phishing attacks.	Eye tracking

laboratory task. In the case of this study, objective neuroscience methods were used to confirm the association between risk perception and security behavior. Self-reported measures of risk perception did not indicate as strong of an association, likely due to biases that commonly plague self-reported methods [4].

Eye tracking technologies have also been used in neuroscience research. In a lab study, Anderson *et al.* [20] tracked participants' eye movements to show the impact of the eye movement-based memory effect (EMM effect) on susceptibility to falling for phishing messages. The EMM effect is a phenomenon where individuals visually attend less to images that appear similar to ones they think they have already seen.

Each of these studies (Table 1) demonstrates how neuroscience methodologies can contribute to a deeper understanding of users' unconscious security behaviors. Some (e.g. [5, 17]) also contribute to a more complete understanding of personality and perceptual components associated with security behaviors. Furthermore, others (e.g. [19, 20]) informed the design of security message interfaces and security training programs. Anderson *et al.* [6] demonstrated how neuroscience methodologies can make a practical contribution to security message design through the development and validation of their polymorphic security message artifact. Anderson *et al.* [20] gave recommendations for how to train users to overcome the EMM effect so as to be more likely to recognize a phishing message.

Gender and IT usage

Many studies have demonstrated gender differences in the behavior of IT users. These studies come from various fields, including psychology, marketing, and information systems. Riedl *et al.* [21] provided a collection of articles demonstrating gender differences in IT. We summarize some of the more relevant articles from that collection below.

Schumacher *et al.* [22] showed that women reported higher levels of computer and Internet incompetence and discomfort than men did. Jackson *et al.* [23] published related findings, showing that men use the Internet more than women do, and that women report higher levels of computer anxiety and lower levels of computer self-efficacy than men do.

Broos [24] showed that females have more negative attitudes toward computers than men do. In this study, users' general experiences with computers lessened computer anxiety for both men and women; nevertheless, such experiences were less effective at relieving the computer anxieties of women than they were for men.

Sanchez-Franco [25] tested a model to examine the effects of gender differences on the various constructs pertaining to computer usage. The results showed that attitude toward computers and perceived computer usefulness had a stronger effect for men on computer usage than for women. However, users' intention to use computers predicted actual computer usage equally powerfully for both men and women. Flow, a state of high engagement enjoyment for users [26], significantly predicted men's intention to use computers more than it did for women.

More recently, Seybert [27] found that in the European Union states, men more frequently use computers than women. Van Welsum and Montagnier [28] made the interesting observation that while differences in computer usage between gender are declining in general, men nevertheless remain more frequent users of newer technology among older users.

Additional studies on gender differences in IT behavior include Gefen and Straub [8], Gefen and Ridings [29], Venkatesh and Morris [9], and Riedl *et al.* [21]. Gefen and Straub [8] examined gender differences in the perception and use of e-mail. They found that men and women perceive e-mail technologies differently; women perceive social presence, usefulness, and ease of use to be higher. Gefen and Ridings [29] found that men and women use technologies to communicate for different purposes—women focus more on the social and emotional support aspects of technologies. Venkatesh and Morris [9] studied gender differences between men and women in the adoption and use of technology. They found that, in technology adoption decisions, men focus most on the system's usefulness, while women focus on the system's ease of use. Women were also influenced by how much they perceived that their peers and superiors wanted them to use the technology.

The percentage of women using the Internet and online stores is increasing, and is now only slightly less than men. A recent Pew Internet study has shown that among adults, Internet usage for women is now at 86%, compared to 87% for men [30]. Another Pew Internet study [31] shows that teenage girls (76%) are more likely to access the internet via mobile devices such as cell phones and tablets than their male counterparts (72%).

In addition, some recent studies have examined the differences of gender in information security, but results are mixed. For example, Crossler and Belanger [32] found that computer self-efficacy and gender significantly impacts a users' use of security tools. Herath and Rao [33] examined intrinsic and extrinsic for employee compliance and found that females have higher policy compliance intentions. However, Medlin and Cazier [34] were not able to find a gender influence on consumer password choices for ecommerce.

These general differences in IT usage between men and women suggest that researchers should be mindful of how the explanatory power of predictive theories may depend on gender. In addition, user interface design principles may need to account for the differences in how men and women will interact with and perceive the artifact. Next, we specifically review literature on differences in online trust between men and women. We do this because we predict that online trust may impact how a user engages with security messages in myriad ways.

Gender differences in online trust

The general differences in IT usage between men and women extend to differences in trust. The literature on gender differences in general trust behavior shows that, in general, men trust more than women do [35–37]. Similarly, the limited research on gender differences in online trust has indicated that women trust less in online settings as well. Most of this literature uses the context of online shopping. In one study, Rodgers *et al.* [38] indicated that women were more likely to pay attention to the more detailed aspects of a website, whereas men tended to consider the site in general. Women's higher level of scrutiny was attributed to a lack of trust, or skepticism. Additionally, women are less likely to trust a website [39] and are more influenced by the impact of trust on loyalty to e-commerce sites than men [40]. Garbarino and Strahilevitz [41] found that women perceived a higher likelihood of risk with online shopping compared to men, and that women also perceived the consequences of risk to be more severe. Gefen *et al.* [42] studied trust in online environments and also concluded that women trusted online stores less than did men.

Riedl *et al.*'s [10] study on neural gender differences in online trust used neurophysiological tools to explain differences between men and women. Using fMRI, they found that different brain regions were activated when women and men were using online retail stores, with the women's brains showing more activation from more regions than men's. These results suggest that women's brains processed the information during the decision-making process more comprehensively than men's brains did. In addition, the findings suggested that women processed the tasks more emotionally and men processed the task more cognitively.

It is interesting to note that in spite of women's lower trust in online settings, the percentage of women using the Internet and online stores is increasing, and it is now only slightly less than men, as was reviewed in the "Gender and IT usage" section. Given this, we reason that it is especially important to consider more fully the different impacts that trust can have on online interactions, such as with security messages.

Effects of color on perception

Color has a significant effect on how individuals perceive their surroundings. The color of a perceived item may affect a person's overall emotion [14], attitude toward an advertisement [13], intellectual performance [15], or may evoke a fight or flight response [43]. Elliot and coauthors performed a series of studies to determine the effects the color red has on individuals who perceive it in various contexts. They found that red has a deleterious effect on intellectual performance [14] and evokes avoidance behavior [44].

Color can also attract attention. Although there are some problems with using color as the only method of conspicuity (e.g. color blindness), it is frequently used as one of several features used to attract attention to warnings [16:54]. Color has also been shown to affect users' perceptions of the hazard. The color red has been shown to communicate a greater hazard than yellow or orange, with no significant differences found between the latter two. Other colors, such as blue and green, generally express less or no hazard [16:785]. In another study, warnings printed in red were noticed more quickly than warnings printed in black [16:138]. Similarly, Braun and Silver [45] found that red conveyed the highest level of perceived hazard, followed by orange, black, green, and blue. Additionally, hazard-related words received various levels of attention based on the color of the words. In another study conducted by Anderson *et al.* [6], researchers tested a series of warning appearance variations and found that a red security warning was one of the most resilient designs against waning attention over repeated exposure.

Wogalter [16] noted that the color of a warning should be distinctive in the environment in which it is placed. For example, a yellow warning in a mostly yellow environment will have a weaker effect on conspicuity than a red warning in a mostly yellow environment. Braun and Silver [45] found support for this notion—in this study, a common household cleaning product labeled "WARNING: SEVERE EYE IRRITANT. HARMFUL IF SWALLLOWED" colored in blue received less attention than when the warning was printed in red.

Based on our review of this stream, more research is needed to discover differences in the processing of warning message of various colors. Specific to a security message context, it remains to be tested whether colors such as red are equally effective at drawing attention to hazards when used in security warnings.

EEG measures

The neurophysiological measure we used in this study is the P300 component of an event-related potential (ERP) measured with EEG. The P300 is a positive-going component that peaks between 250 and 500 milliseconds after stimulus onset and has been observed in tasks that require stimulus discrimination [46]. Passive stimulus processing generally produces smaller P300 amplitudes than active tasks; when task conditions are undemanding, the P300 amplitude is smaller. It has been proposed that the P300 reflects processes related to updating mental representations of the task structure [47, 48]. According to the "context-updating theory", incoming stimuli are compared against stimuli previously held in working memory. If the new stimulus matches the previous stimuli, no updating is required and no P300 is generated. If, however, the new stimulus produces a mismatch with the stimuli held in working memory, the context for that stimulus is updated and a P300 is generated. It is believed that because infrequent, low-probability stimuli can be biologically important, it is adaptive to inhibit unrelated activity to promote processing efficiency and thereby yield large P300 amplitudes [46].

EEG has been used in broader information systems research as well. In one study, researchers first used an eye-tracking device to capture eye fixations and then used EEG to measure changes in P300 levels once the eye fixations began [49]. This method allows researchers to precisely capture users' neural activity at the exact time at which they start to cognitively process a stimulus (e.g. an event on the screen). In a neurosecurity study conducted by Vance *et al.* [5], researchers used EEG to measure people's risk perceptions. They found that the EEG measure of risk perception was a better predictor of users' subsequent security behaviors than their own stated risk perceptions. This study emphasizes the point that while users commonly state that they are concerned about security, their actions frequently do not match their stated perceptions. This highlights the need for more objective measures of user perception of security, such as those that can be obtained using neuroscience methodologies like EEG.

Hypotheses

Our experiment falls into what is termed an "oddball paradigm" [50] because our subjects will see one of the targets (the malware warning) relatively infrequently. Passive stimulus processing generally produces smaller P300 amplitudes than active tasks. In other words, when task conditions are undemanding, P300 amplitude is smaller. Since infrequent, low probability stimuli can be biologically important, it is adaptive to inhibit unrelated activity to promote processing efficiency, thereby yielding large P300 amplitudes [11]. Because the malware warning could be a very important (although infrequent) event, we would expect the respective P300 to be higher relative to the legitimate website. Therefore we hypothesize:

> *H1. P300 will be higher for all participants when viewing malware warning screenshots than when viewing legitimate website screenshots.*

The relationship between gender and P300 has been controversial as some studies see no gender bias or larger amplitudes in males [12]. However, Kolb and Whishaw [51] demonstrated that ERPs are sensitive to gender. Using both auditory and visual oddball tasks, Steffensen *et al.* [11] reported that females have a larger P300 component than do males. Additionally, Guillem and Mograss [52] showed that females had a greater P300 response to an ERP for the relevant stimulus than did males.

Papanicolaou *et al.* [53] and Polich [54] proposed that hemispheric asymmetry might give rise to greater P300 amplitudes in females than in males. Because the brains of men are typically more lateralized (asymmetrical) than those of women [55], women should evince more symmetrical processing of visual stimuli. This difference in symmetry may lead to differences between the measures of P300 at the Cz (central) and Pz (parietal) sites. Females show a larger anteroposterior amplitude gradient, meaning the front part the brain plays a more critical role in females [e.g. 56–58].

It has been suggested that stimulus "intensity" may be an important variable in determining P300 amplitude [59]. Fjell and Walhovd [60] reported that a larger P300 amplitude was elicited by viewing unpleasant scenes rather than pleasant scenes presented on slides. Paired with the general distrust shown by women in online environments [61, 62], we hypothesize that the P300 amplitude will be higher for women than for men, subject to brain topography:

> *H2. P300 will be higher for women than for men when viewing malware warning screenshots.*

Individual differences for P300 latency are correlated with mental function speed, such that shorter latencies are related to superior cognitive performance [63]. While there has been research on latency and children [64], aging [14], and dementia and brain disease [13], there have not been any conclusive studies about gender and P300 latencies. Consequently, there is no precedent for gender differences in latency, so we cannot predict whether or not there will be a difference. Nonetheless, we offer an exploratory hypothesis to examine whether one group or the other has an additional process or a slower process in classifying the malware screen:

> *H3. P300 will be slower for women or men.*

In the set of experiments conducted by Elliot *et al.* [14], participants' reactions were measured using EEG. Although this measurement focused on the differences between the brain's right and left prefrontal cortexes, it sets a precedent for using EEG to measure individuals' reactions to color and demonstrates the need to determine what those reactions are. As our experiment focuses on P300 interpretation, and because P300 is a measurement of stimulus discrimination, we craft our hypothesis with respect to the P300. Additionally, we take into consideration the findings of Elliot and colleagues regarding the color red.

Although our experiment does not present an achievement context as Elliot and Maier define in their several studies, we hypothesize the following based on the discrimination measurement of the P300:

> *H4a. P300 will be higher for all participants when viewing red malware warning screenshots than when viewing grayscale malware warning screenshots.*

> *H4b. P300 will be higher for all participants when viewing red legitimate website screenshots than when viewing non-red legitimate website screenshots.*

Method

Participants and materials

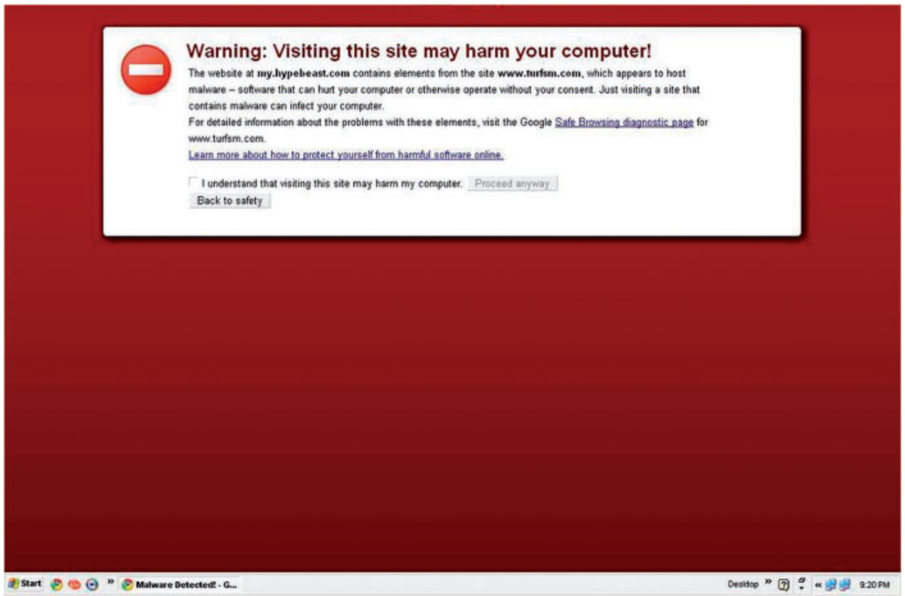
A total of 61 healthy volunteers (32 females, 29 males) were recruited from a large private university to participate. Participants gave written informed consent before participation and received $10 for their participation. Participants had normal color vision and were free from head injuries, neurological insults, and major psychiatric disorders. The mean age for participants was 22.44 (SD = 2.35); females: 21.69 (2.62); males: 23.28 (1.69). The stimuli consisted of 20 screen shots of popular websites (e.g. amazon.com, netflix.com) as well as a full color and grayscale version of Google Chrome's web browser warning screen (Fig. 1).

Procedures

Participants were instructed that this was a target-detection task in which they would be shown images of common websites and browser warning screens. Participants were familiarized prior to the experiment with the warning screen and instructed to press one button with the index finger of their right hand for "safe" websites and another button with the middle finger of their right hand for warning screens. Stimuli were presented in an electrically shielded testing room on a 17-inch LCD computer monitor, and responses were recorded with an EEG-compatible keypad. Each trial of the experiment began with a central fixation screen for 2000 ms, followed by a safe website or warning screen stimulus. Each safe website was presented five times for a total of 100 safe websites. The colorized warning screen was presented eight times, and the grayscale warning screen was presented twice. Stimulus order was randomized. Stimuli were presented for 3000 ms, during which time participants were instructed to press a button in order to classify the stimulus. Stimulus presentation was followed by a "blink" screen for 1500 ms, during which participants were instructed to blink.

Electrophysiological data recording and processing

The EEG was recorded from 128 scalp sites using a HydroCel Geodesic Sensor Net and an Electrical Geodesics Inc (EGI; Eugene, Oregon, USA; Fig. 2) amplification system (amplification 20K, nominal bandpass 0.10–100 Hz). The EEG was referenced to the vertex electrode and digitized at 250 Hz. Impedances were maintained below 50 kΩ. EEG data were processed off-line beginning with a



Warning: Visiting this site may harm your computer!

The website at **my.hypebeast.com** contains elements from the site **www.turfsm.com**, which appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that contains malware can infect your computer.

For detailed information about the problems with these elements, visit the Google Safe Browsing diagnostic page for www.turfsm.com.

Learn more about how to protect yourself from harmful software online.

□ I understand that visiting this site may harm my computer. Proceed anyway

Back to safety

Figure 1. Color screenshot of Google Chrome malware warning screen shown to participants.

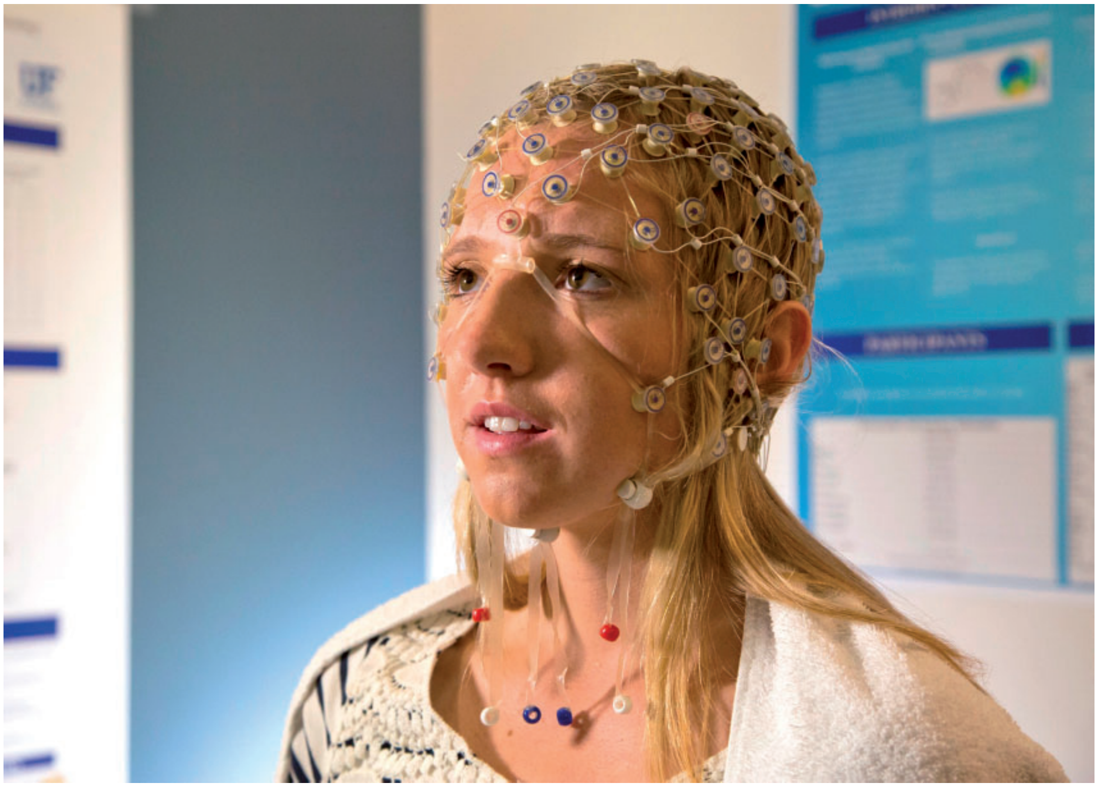


Figure 2. The 128-node HydroCel Geodesic Sensor Net used for recording the EEG.

0.1-Hz first-order highpass filter and 30 Hz lowpass filter. Stimulus-locked ERP averages were derived spanning 200 ms pre-stimulus to 1000 ms poststimulus, and they were segmented based on trial type criteria (safe websites, warning screens). Eye blinks were removed from the segmented waveforms using ICA in the ERP PCA Toolkit [65]. The ICA components that correlated at 0.9 with the scalp topography of a blink template generated based on the current data were removed from the data [35–37]. Artifacts in the EEG data due to saccades and motion were removed from the segmented waveforms using PCA in the ERP PCA Toolkit [38]. Channels were marked bad if the fast average amplitude exceeded 100 mV or if the differential average amplitude exceeded 50 mV. Data from three participants (1 female, 2 males) were excluded from ERP analyses due to low trial counts or excess bad channels. Data from the remaining participants were average re-referenced, and waveforms were baseline corrected using a 200-ms window prior to stimulus presentation.

Analysis

The P300 amplitudes were extracted as the mean amplitude within the 300–600 ms poststimulus window [60]. Latencies were calculated as the 50% area latency [61, 62] for the 300–600 ms poststimulus window. Amplitudes and latencies were analyzed for the Cz and Pz electrodes using repeated measures ANOVAs.

Results

Behavioral performance

As a group, participants correctly identified 96.9% (SD = 7.9%) of safe websites and 99.3% (2.6%) of warning screens. Because of the disproportionate number of safe trials (100 out of 110), participants could have responded "safe" regardless of the stimulus and still obtained a 91% correct score. Accordingly, we calculated a discriminability measure (d') that takes into account hit rates as well as false alarm rates. The mean d' measure was well above chance: mean $d' = 4.66$ (0.60) ($t[57] = 58.74$, $p < 0.0001$). Discriminability did not differ across gender: male mean $d' = 4.58$ (0.68); female mean $d' = 4.73$ (0.53) ($t[56] = 0.94$, $p = 0.35$). Likewise, reaction times (RTs) did not differ across gender: male mean RT = 952.3 (322.3) ms; female mean RT = 847.4 (275.9) ms ($t[56] = 1.34$, $p = 0.19$). Taken together, these results indicate that men and women performed approximately equally on the behavioral task.

The P300 ERP

Investigation of the topographical activation maps confirmed a centrally distributed positivity at 300 ms poststimulus onset (Fig. 3). Figure 4 depicts the grand average waveforms for the Cz and Pz electrode sites. The P300 amplitude was analyzed during the 300–600 ms poststimulus period (shaded).

For our hypothesis testing, we first examined whether P300 was higher for all participants when viewing malware warning screenshots than when viewing legitimate website screenshots (H1). At the Cz electrode site, an ANOVA on the mean amplitude revealed a main effect of screen type (safe sites versus warning screens) ($F[1,56] = 34.23$, $p < 0.0001$). Similarly, at the Pz electrode site, an ANOVA revealed a main effect of screen type ($F[1,56] = 23.35$, $p < 0.0001$). Thus, H1 was supported.

We next examined whether P300 will be higher for women than for men when viewing malware warning screenshots (H2). At the Cz electrode site, an ANOVA demonstrated a main effect of gender ($F[1,56] = 4.63$, $p < 0.05$; Table 2). At the Pz electrode site, no main effect of gender was found ($F[1,56] = 0.12$, $p = 0.73$). Thus, the amplitude of P300 was greater for women than for men at the Cz electrode overall, but not at the more posterior Pz electrode site. Therefore, H2 was supported, albeit only for the Cz electrode site.

Interestingly, although we observed the expected P300 enhancement for warning screens relative to legitimate websites at both electrode sites, the gender by screen type interaction was not significant (cZ: $F[1,56] = 0.15$, $p = 0.70$); pZ: $F[1,56] = 0.01$, $p = 0.95$). This indicates that while women do exhibit higher P300 than do men when viewing malware warning screens, the size of the enhancement or "boost" to P300 when viewing malware warning screens was not greater for women than for men at either electrode site. In other words, for both women and men, P300 increased by approximately the same amount when viewing the malware warning (Fig. 3).

We also examined the P300 latency at both electrode sites. Because P300 is dependent on stimulus classification, its latency has often been used as an indication of stimulus classification processes [e.g. 66]. Latency was defined as the 50% area latency [65] for the 300–600 ms poststimulus window. Latencies at the Cz and Pz electrodes are listed in Table 3. At the Cz electrode, a 2 × 2 (screen type × gender) ANOVA revealed no significant main effects or interactions ($p > 0.05$). Similarly, at the Pz electrode, the ANOVA revealed no significant main effects or interactions ($p > 0.05$). Thus, H3 was not supported. These results indicate that men and women relied on similar cognitive processes in the initial categorization of the safe websites and the warning screens.

Finally, we examined whether P300 will be higher for all participants when viewing red malware warning screenshots than when viewing grayscale malware warning screenshots (H4a), as well as when viewing red legitimate website screenshots compared to non-red legitimate website screenshots (H4b). To test these hypotheses, we randomly presented a subset of the warning screens as grayscale images. Also, a subset of the safe websites were predominately red as was the warning screen. We examined ERP amplitudes for these four stimulus categories (safe sites, red safe sites, grayscale warning screens, and red warning screens) separately at the Cz and Pz electrode sites. Twenty-four men and 25 women had sufficient trials for this more restricted ERP analysis. An ANOVA on the Cz amplitude data revealed a main effect of screen type ($F[1,47] = 59.02$, $p < 0.001$) but no main effect of color and no interactions between color and gender or color and screen type ($p > 0.05$). At the Pz electrode site, an ANOVA revealed a main effect of screen type ($F[1,47] = 4.86$, $p < 0.05$) and a main effect of color ($F[1,47] = 4.92$, $p < 0.05$) but no color by gender or color by screen type interactions ($p > 0.05$). Taken together, these results indicate that the stimulus color did not differentially impact cognitive processing, as indexed by the P300 amplitude. Thus H4a and H4b were not supported.

Discussion

We next discuss our results, which are summarized in Table 4, as well as implications for further research and practice.

First, the amplitude of the P300 for all subjects increased when viewing the malware warning screenshot regardless of gender, supporting H1. This finding indicates that malware warnings do elicit a response in the brain, even for screenshots in our simulated laboratory setting. Although users may be habituated to security warnings [6], this finding at least shows that the malware warnings succeeded in gaining participants' attention and prompting a cognitive decision process.

Second, we found that women exhibited higher P300 when viewing malware warning screens than did men for electrodes in

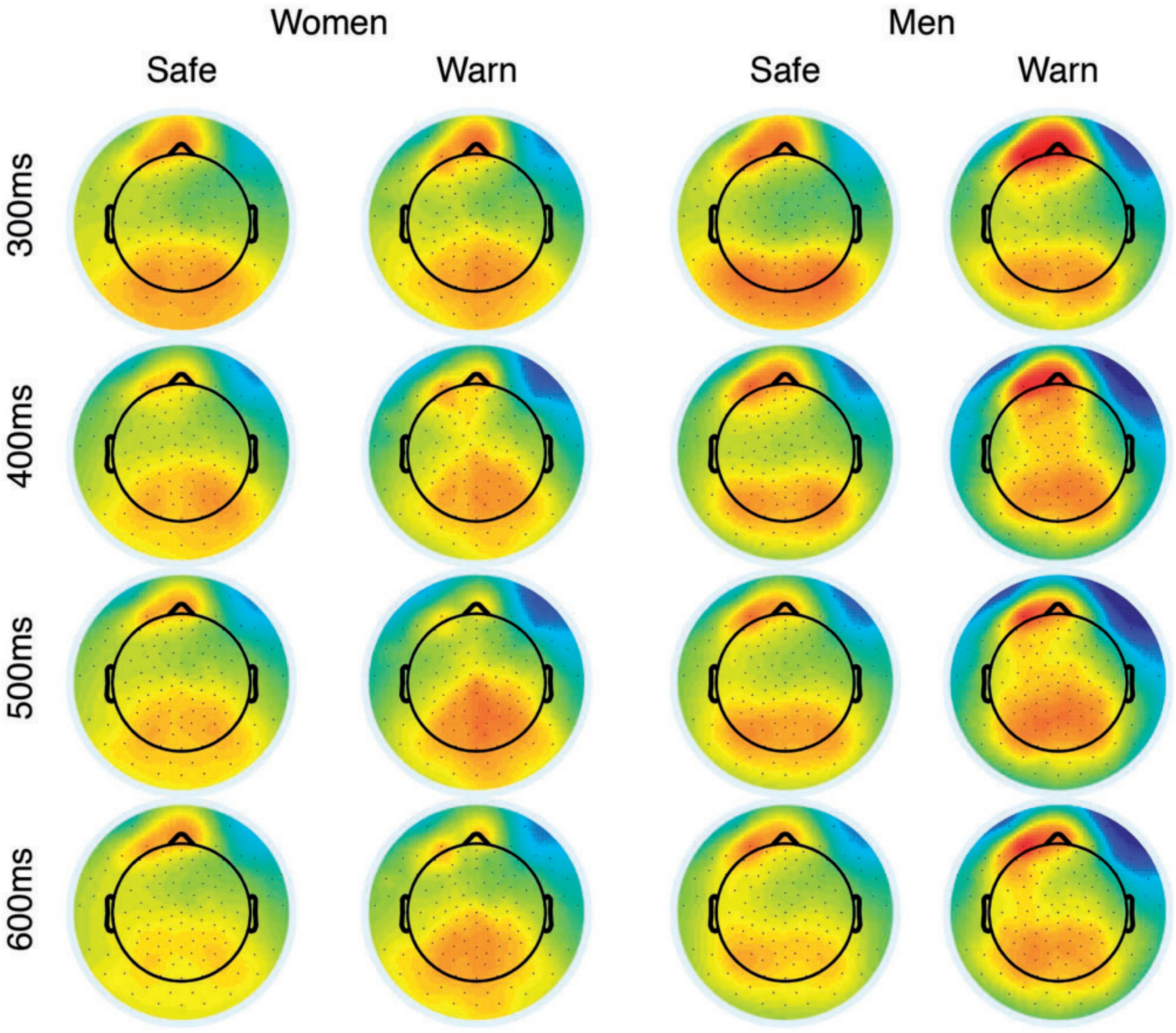


Figure 3. Topographical distribution of ERPs for the 300–600 ms poststimulus periods. There was a centrally distributed positivity at 300 ms poststimulus onset.

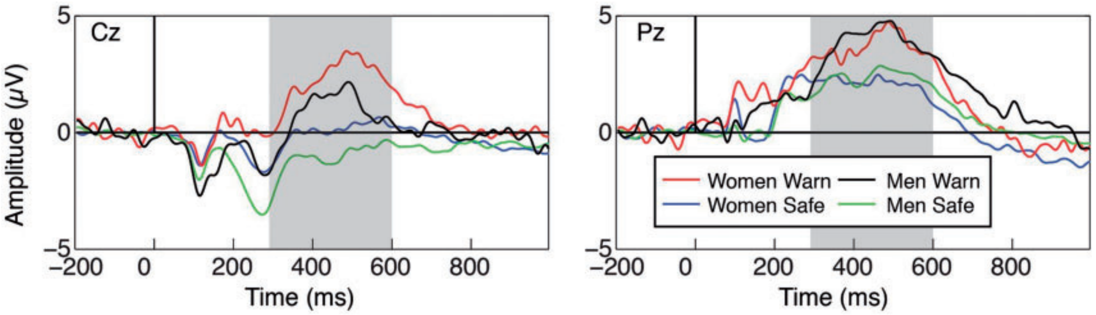


Figure 4. Grand average ERP waveforms at the Cz and Pz electrode sites. At the Cz electrode site, women had greater amplitudes for the P300 for both safe websites and the warning screen. The P300 amplitude was enhanced for the warning screen across genders at both electrode sites.

the Cz region. However, we found no support for a difference in gender in the more posterior Pz region. Thus, H2 is supported, albeit only for the Cz region. This finding corresponds to previous findings in trust research, which showed that women are generally less trusting of online sites than are men [35–37]. For example, Rodgers and Harris [38] found that women were more likely than men to pay attention to detailed characteristics of a website when forming impressions of initial trust. This finding is consistent with the higher levels of P300 that we observed in our experiment.

Third, in an exploratory hypothesis, we examined whether the P300 was elicited more quickly for one gender. We found no difference in gender in terms of how quickly the P300 is elicited, failing to support H3. This result is consistent with previous neurobiological work, which has failed to demonstrate that P300 is elicited more quickly based on gender [13]. Finally, we tested color differences between red and grayscale malware warnings and between predominantly red screenshots (including malware warning screens) and non-red screenshots. Our results found no difference in the P300 based on the color of the screenshot received. Therefore, H4a and H4b were not supported. This finding is contrary to practice, as popular web browsers such as Chrome and Firefox use the color red in the display of malware warnings (Appendix A).

This study makes three primary contributions. First, it provides empirical evidence that men and women's brains process malware warnings differently. Although preliminary in nature, our findings indicate that significant differences exist in the brain based on gender. These findings could potentially be useful in designing security interfaces that adapt to the user based on a profile that includes gender.

Second, our findings in relation to the effects of color on brain activity when viewing security warnings highlight an interesting phenomenon: research relying on self-purported measures indicate that color should increase brain activity while our research using EEG showed no additional activity when viewing predominantly red screens versus grayscale screens. As noted above, these findings are contrary to prior research and practice in this area and should be investigated further.

Table 2. Mean amplitude (and standard deviation) of the P300 ERP component as measured during the 300–600 ms poststimulus period

	Cz		Pz	
	Females	Males	Females	Males
Safe	0.07 (1.73)	−1.02 (1.89)	2.11 (1.99)	2.36 (2.32)
Warning	2.30 (3.34)	0.94 (2.85)	3.70 (3.58)	3.92 (3.29)

Table 3. Mean 50% area latency (and standard deviation) of the P300 ERP component for the 300–600 ms poststimulus period

	Cz		Pz	
	Females	Males	Females	Males
Safe	431.7 (30.8)	427.0 (25.0)	453.9 (26.1)	445.6 (30.7)
Warning	434.1 (27.5)	438.7 (26.5)	446.1 (27.5)	443.7 (26.5)

Finally, this study demonstrates the benefit of using neuroscience methods to study cybersecurity behaviors. Neurosecurity allows researchers to open the "black box" of the brain to better understand fundamental cognitive factors that may be difficult or impossible to investigate using conventional methods. Because automatic or unconscious mental processes underlie much of human cognition and decision-making, they likely play an important role in a number of other security behaviors, such as security education, training, and awareness (SETA) programs, password use, and information security policy compliance. Additionally, neuroscience methods have the potential to lead to the development of more complete behavioral security theories and guide the design of more effective security interventions. For example, rather than creating security interventions and expecting users to change their behavior in response, researchers and developers may instead use neurosecurity techniques to design security interfaces that are more compatible with users' biology and natural tendencies.

Limitations and future research

Our research is subject to a number of limitations. First, we employed a laboratory experiment that showed simulated screenshots to participants. Laboratory experiments have the advantage of greater precision and control, but they come with the cost of weak generalizability to real-world situations [67]. The realism and generalizability of our study could be strengthened in future research by employing a free simulation experiment, in which treatment levels are allowed to range freely in accordance with how participants interact naturally with the simulation [68, 69]. For example, experimental participants could use a web service such as StumbleUpon (http://stumbleupon.com) in which at the press of a button they will be taken to a random website. On 10% of the sites, participants would receive a warning screen and be given a choice to continue or go back. Not only would such a design provide greater realism in the experimental task by providing a level of user control beyond the recognition task in our current study, it would also reveal differences in behavior and timing.

Second, and related to the previous point, our subjects consisted of a homogenous sample of university undergraduates. Homogenous samples are useful for falsifying theory due to more stringent statistical tests of hypotheses due to decreased error in the sample, but they come at the cost of external validity [70]. Further research is needed to test the effects of gender on security behavior in other settings.

Third, our sample consisted of 61 participants. While more data are generally better, Dimoka [71] points out that although sample sizes tend to be smaller for neuroscience studies due to the expense and time commitment required per subject, neuroscience methods generally provide many data points per subject. In our case, we

Table 4. Hypotheses and outcomes

Hypothesis		Supported?
H1	P300 will be higher for all participants when viewing malware warning screenshots than when viewing legitimate website screenshots.	Yes
H2	P300 will be higher for women than for men when viewing malware warning screenshots.	Yes, for the Cz region
H3	P300 will be slower for women or men.	No
H4a	P300 will be higher for all participants when viewing red malware warning screenshots than when viewing grayscale malware warning screenshots.	No
H4b	P300 will be higher for all participants when viewing red legitimate website screenshots than when viewing non-red legitimate website screenshots.	No

collected over 300 behavioral observations per participant while recording EEGs at 250 Hz. Thus, the amount of data captured and used in our analysis was actually much greater than a sample size of 61 would suggest.

Fourth, our results are based upon a single research method. While multi-method approaches can be beneficial to research generally [72], additional methods are especially useful for neurosecurity studies, which are largely exploratory and can therefore benefit most from corroborating evidence provided by additional data collection methods [73]. For example, eye-tracking equipment could be used to measure eye movement to observe which aspects of malware warnings are most salient or persuasive to participants. Similarly, whereas EEG excels in inferring temporal ordering of brain activity, fMRI can demonstrate which areas, and therefore, which functions of the brain are activated by responding to malware warnings [71]. Thus, additional and complimentary neurosecurity methods may together yield results that are difficult or impossible to obtain with a single research method alone.

Fifth, this study examined one aspect of security warnings: whether perceptions of malware warnings differ by gender. Other factors are known to influence users' reception of security warnings, including habituation [6], lack of comprehension [74], and conscious decisions to ignore security messages [75]. These and similar questions are ripe for examination by neurosecurity methods that, to an increasing extent, open the "black box" of user behavior.

Finally, our study only used the color red to compare against grayscale versions of screenshot warnings and webpages. As previously discussed, "The color red has been shown to express greater hazard than yellow or orange, which between them are not substantially different from each other. Other colors, such as blue and green, generally express less or no hazard," and "dynamic warnings designed to reflect the current status of the situation could change: from yellow or orange for lower hazards to red for higher hazards" [16:785]. With this insight, further research should be done to investigate whether different colors in security messages elicit greater brain activity over the color red.

In summary, we call for future research to use neuroscience methods to investigate individual differences such as gender and design factors such as color, and to incorporate findings into comprehensive behavioral security theories. Such theories can be used as foundations to inform the experimental designs and hypotheses of future behavioral security research, and to inform the design of security messages in practice.

Conclusion

Although there is growing evidence of the value of cognitive neuroscience in studying information security (neurosecurity), as yet there has been limited work applied to this domain. We contribute by conducting a neurosecurity study of the comparative performance of men and women in performing a security task: discriminating between web browser malware warnings and legitimate websites. We found support for the position that mental processing of malware warnings differs depending on gender; women display higher brain activity when viewing malware warnings than do men. While our results are preliminary in nature, the discovery of gender differences in the processing of security information can potentially be useful in designing more effective security warning interfaces. Further, our findings illustrate the kind of unique insights that can be provided via neurosecurity methods and point the way to several promising avenues for future research.

Funding

This work was supported by the National Science Foundation (DGE-1247842) and by the David Berg Center for Ethics and Leadership at the Joseph M. Katz Graduate School of Business and College of Business Administration at the University of Pittsburgh through a grant from the BNY Mellon Foundation of Western PA.

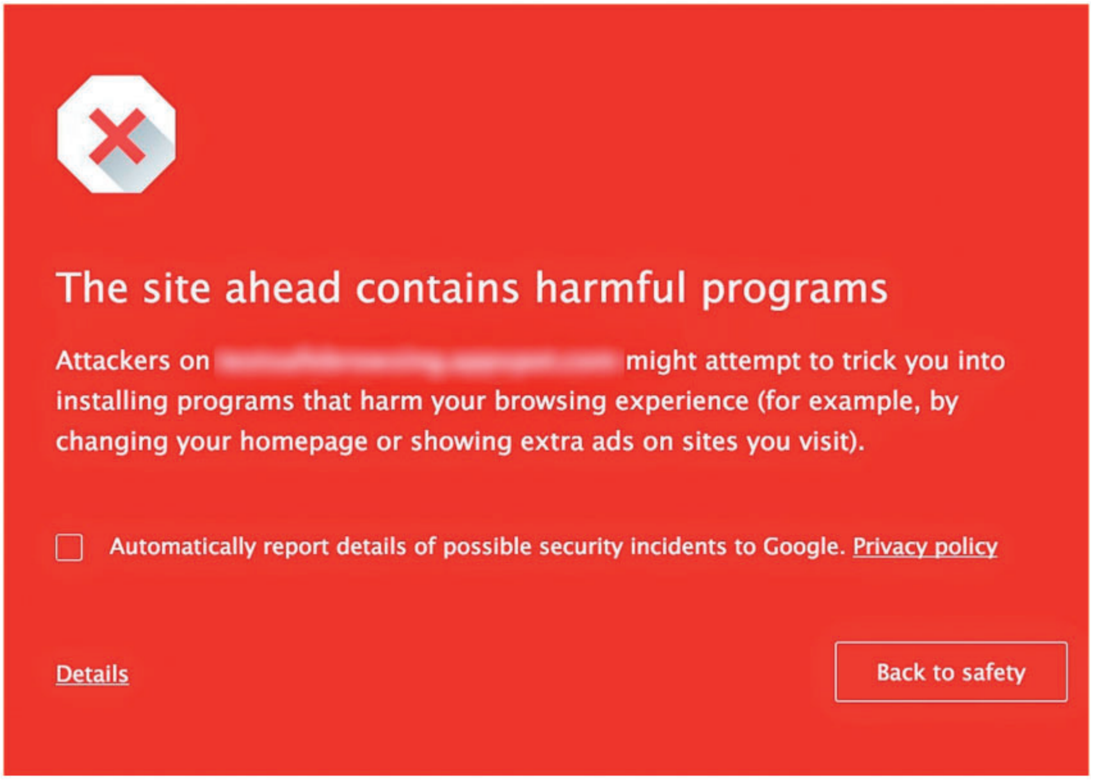
Conflict of interest statement. None declared.

References

1. Cohen F. Computer viruses: theory and experiments. *Computers Security* 1987;**6**: 22–35.
2. Oriyano S-P, Shimonski R. Chapter 1 - Client-side attacks defined. In Oriyano S-P and Shimonski R (eds.), *Client-side Attacks and Defense*. Boston: Syngress, 2012, 1-24.
3. Crossler RE, Johnston AC, Lowry PB *et al*. Future directions for behavioral information security research. *Computers Security* 2013;**32**:90–101.
4. Dimoka A, Pavlou PA, Davis FD. Research commentary-NeuroIS: the potential of cognitive neuroscience for information systems research. *Inf Syst Res* 2011; **22**:687–702.
5. Vance A, Anderson BB, Kirwan CB *et al*. Using measures of risk perception to predict information security behavior: insights from electroencephalography (EEG). *J Assoc Inf Syst* 2014; **15**:679–722.
6. Anderson B, Kirwan B, Eargle D *et al*. How polymorphic warnings reduce habituation in the brain: insights from an fMRI study. In: *Proceedings of CHI '15*, ACM, 2015.
7. Bravo-Lillo C, Cranor LF, Downs J *et al*. Improving computer security dialogs. In: *Proceedings of INTERACT 2011*. Springer, 2011, 18–35.
8. Gefen D, Straub DW. Gender differences in the perception and use of e-mail: an extension to the technology acceptance model. *MIS Quart* 1997; **21**:389–400.
9. Venkatesh V, Morris MG. Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quart* 2000; **24**:115–39.
10. Riedl R, Hubert M, Kenning P. Are there neural gender differences in online trust? An fMRI study on the perceived trustworthiness of ebay offers. *MIS Quart* 2010; **34**:397–428.
11. Steffensen SC, Ohran AJ, Shipp DN *et al*. Gender-selective effects of the p300 and n400 components of the visual evoked potential. *Vision Res* 2008; **48**:917–25.
12. Roalf D, Lowery N, Turetsky BI. Behavioral and physiological findings of gender differences in global-local visual processing. *Brain Cogn* 2006; **60**:32–42.
13. Elliot AJ, Maier MA, Binser MJ *et al*. The effect of red on avoidance behavior in achievement contexts. *Pers Soc Psychol Bull* 2009; **35**:365–75.
14. Elliot AJ, Maier MA, Moller AC *et al*. Color and psychological functioning: the effect of red on performance attainment. *J Exp Psychol Gen* 2007; **136**:154–68.
15. Elliot AJ, Niesta D. Romantic red: red enhances men's attraction to women. *J Pers Soc Psychol* 2008; **95**:1150–64.
16. Wogalter M. *Handbook of Warnings*. Mahwah, NJ: Lawrence Erlbaum Associates, 2006.
17. Hu Q, West R, Smarandescu L. The role of self-control in information security violations: insights from a cognitive neuroscience perspective. *J Manag Informat Syst* 2015; **31**:6–48.
18. Neupane A, Saxena N, Kuruvilla K *et al*. Neural signatures of user-centered security: an fMRI study of phishing, and malware warnings. In: *Proceedings of NDSS*, 2014, 1–16.
19. Anderson B, Vance A, Kirwan B *et al*. Users aren't (necessarily) lazy: using neurois to explain habituation to security warnings. In: *Proceedings of ICIS 2014*, AIS, 2014.
20. Anderson B, Vance A, Eargle D *et al*. Your memory is working against you: How eye tracking and memory explain susceptibility to phishing. In: *Proc. IFIP WG8.11/WG11.13*, 2013, paper 18.

21. Benbasat I, Dimoka A, Pavlou PA *et al*. Incorporating social presence in the design of the anthropomorphic interface of recommendation agents: Insights from an fMRI study. In: *Proceedings of ICIS 2010*, AIS, 2010.
22. Schumacher P, Morahan-Martin J. Gender, internet and computer attitudes and experiences. *Comput Hum Behav* 2001; **17**:95–110.
23. Jackson LA, Ervin KS, Gardner PD *et al*. Gender and the internet: women communicating and men searching. *Sex Roles* 2001; **44**:363–379.
24. Broos A. Gender and information and communication technologies (ict) anxiety: male self-assurance and female hesitation. *CyberPsychol Behav* 2005; **8**:21–31.
25. Sanchez-Franco MJ. Exploring the influence of gender on the web usage via partial least squares. *Behav Informat Technol* 2006; **25**:19–36.
26. Csikszentmihalyi M. *Finding Flow: the Psychology of Engagement with Everyday Life*. New York, NY: Basic Books, 1997.
27. Seybert H. Gender differences in the use of computers and the internet. *Eurostat Stat Focus Populat Soc Cond* 2007; **119**:1–7.
28. Dodge R, Jr, Carver C, Ferguson AJ. Phishing for user security awareness. *Computers Security* 2007; **26**:73–80.
29. Gefen D, Ridings CM. If you spoke as she does, sir, instead of the way you do: a sociolinguistics perspective of gender differences in virtual communities. *SIGMIS Database* 2005; **36**:78–92.
30. Pew. *Internet User in 2014*. http://www.pewinternet.org/data-trend/internet-use/latest-stats/ (19 October 2015, date last accessed).
31. Pew. *Teen Internet Access Demographics*. http://www.pewinternet.org/data-trend/teens/internet-user-demographics/ (19 October 2015, date last accessed).
32. Crossler RE, Bélanger F. The effects of security education training and awareness programs and individual characteristics on end user security tool usage. *J Informat Syst Security* 2009; **5**:3–22.
33. Herath T, Rao HR. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decision Support Syst* 2009; **47**:154–65.
34. Medlin BD, Cazier JA. An investigative study: consumers password choices on an e-commerce site. *J Informat Privacy Security* 2005; **1**:33–52.
35. Alesina A, La Ferrara E. Who trusts others? *Journal of Public Economics* 2002; **85**:207–34.
36. Glaeser EL, Laibson DI, Scheinkman JA *et al*. Measuring trust. *Quart J Economics* 2000; **115**:811–46.
37. Terrell F, Barrett RK. Interpersonal trust among college students as a function of race, sex, and socioeconomic class. *Percept Motor Skills* 1979; **48**:1194.
38. Rodgers S, Harris MA. Gender and e-commerce: an exploratory study. *J Advert Res* 2003; **43**:322–29.
39. Cyr D, Bonanni C. Gender and website design in e-business. *Int J Electronic Bus* 2005; **3**:565–82.
40. Cyr D, Hassanein K, Head M *et al*. The role of social presence in establishing loyalty in e-service environments. *Interact Computers* 2007; **19**:43–56.
41. Garbarino E, Strahilevitz M. Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *J Bus Res* 2004; **57**:768–75.
42. Gefen D, Benbasat I, Pavlou PA. A research agenda for trust in online environments. *J Manag Informat Syst* 2008; **24**:275–86.
43. Elliot AJ, Niesta Kayser D, Greitemeyer T *et al*. Red, rank, and romance in women viewing men. *J Exp Psychol Gen* 2010; **139**:399–417.
44. Dien J, Michelson CA, Franklin MS. Separating the visual sentence n400 effect from the p400 sequential expectancy effect: Cognitive and neuroanatomical implications. *Brain Res* 2010; **1355**:126–40.
45. Braun CC, Silver NC. Interaction of signal word and colour on warning labels: differences in perceived hazard and behavioural compliance. *Ergonomics* 1995; **38**:2207–20.
46. Polich J. Updating p300: an integrative theory of p3a and p3b. *Clin Neurophysiol* 2007; **118**:2128–48.
47. Donchin E. Surprise! … surprise? *Psychophysiology* 1981; **18**:493–513.
48. Donchin E, Coles MG. Is the p300 component a manifestation of context updating? *Behav Brain Sci* 1988; **11**:357–74.
49. Léger P-M, Sénecal S, Courtemanche F *et al*. Precision is in the eye of the beholder: application of eye fixation-related potentials to information systems research. *J Assoc Inf Syst* 2014; **15**:651–78.
50. Polich J, Margala C. P300 and probability: comparison of oddball and single-stimulus paradigms. *Int J Psychophysiol* 1997; **25**:169–76.
51. Kolb B, Whishaw IQ. *Fundamentals of Human Neuropsychology*. New York, NY: W H Freeman/Times Books/Henry Holt & Co, 1990.
52. Guillem F, Mograss M. Gender differences in memory processing: evidence from event-related potentials to faces. *Brain Cogn* 2005; **57**:84–92.
53. Papanicolaou AC, Loring DW, Raz N *et al*. Relationship between stimulus intensity and the p300. *Psychophysiology* 1985; **22**:326–9.
54. Polich J. Frequency, intensity, and duration as determinants of p300 from auditory stimuli. *J Clin Neurophysiol* 1989; **6**:277–86.
55. Yee CM, Miller GA. Affective valence and information processing. *Electroencephalogr Clin Neurophysiol Suppl* 1987; **40**:300–7.
56. Emmerson RY, Dustman RE, Shearer DE *et al*. P3 latency and symbol digit performance correlations in aging. *Exp Aging Res* 1989; **15**:151–9.
57. Johnson R, Pfefferbaum A, Kopell BS. P300 and long-term memory: latency predicts recognition performance. *Psychophysiology* 1985; **22**:497–507.
58. Pelosi L, Holly M, Slade T *et al*. Event-related potential (erp) correlates of performance of intelligence tests. *Electroencephalogr Clin Neurophysiol* 1992; **84**:515–20.
59. Howard L, Polich J. P300 latency and memory span development. *Dev Psychol* 1985; **21**:283–9.
60. Fjell A, Walhovd K. P300 and neuropsychological tests as measures of aging: scalp topography and cognitive changes. *Brain Topogr* 2001; **14**:25–40.
61. Polich J, Corey-Bloom J. Alzheimer's disease and p300: review and evaluation of task and modality. *Curr Alzheimer Res* 2005; **2**:515–25.
62. Bashore TR, Ridderinkhof KR. Older age, traumatic brain injury, and cognitive slowing: Some convergent and divergent findings. *Psychol Bull* 2002; **128**:151–98.
63. Jacobs KW, Suess JF. Effects of four psychological primary colors on anxiety state. *Percept Mot Skills* 1975; **41**:207–10.
64. Lichtlé M-C. The effect of an advertisement's colour on emotions evoked by an ad and attitude towards the ad. *Int J Advert* 2007; **26**:37–62.
65. Luck SJ. *An Introduction to the Event-Related Potential Technique*. Cambridge, MA: MIT Press, 2005.
66. Kutas M, McCarthy G, Donchin E. Augmenting mental chronometry: the p300 as a measure of stimulus evaluation time. *Science* 1977; **197**:792–5.
67. McGrath JE. Dilemmatics: the study of research choices and dilemmas. *Am Behav Scientist* 1981; **25**:179–210.
68. Vance A, Elie-dit-cosaque C, Straub D. Examining trust in IT artifacts: the effects of system quality and culture on trust. *J Manag Informat Syst* 2008; **24**:73–100.
69. Fromkin, Streufert, Dunnette B. Laboratory experimentation. *Handbook Indus Organ Psychol* 1976:415–65.
70. Calder B, Phillips L, Tybout AM. Designing research for application. *J Consum Res* 1981; 8:197–207.
71. Dimoka A. How to conduct a functional magnetic resonance (fMRI) study in social science research. *MIS Quart* 2012; **36**:811–40.
72. Straub D, Boudreau M-C, Gefen D. Validation guidelines for IS positivist research. *CAIS* 2004; **13**:380–427.
73. Dimoka A, Banker RD, Benbasat I *et al*. On the use of neurophysiological tools in IS research: Developing a research agenda for NeuroIS. *MIS Quart* 2012; **36**:679–702.
74. Felt AP, Ainslie A, Reeder RW *et al*. Improving SSL warnings: comprehension and adherence. In: *Proc. CHI '15*, ACM, 2015.
75. Egelman S, Schechter S. The importance of being earnest [in security warnings]. In Sadeghis A-R (ed.), *Financial Cryptography and Data Security*. Springer, 2013, 52–59.

Appendix A—browser security warning examples

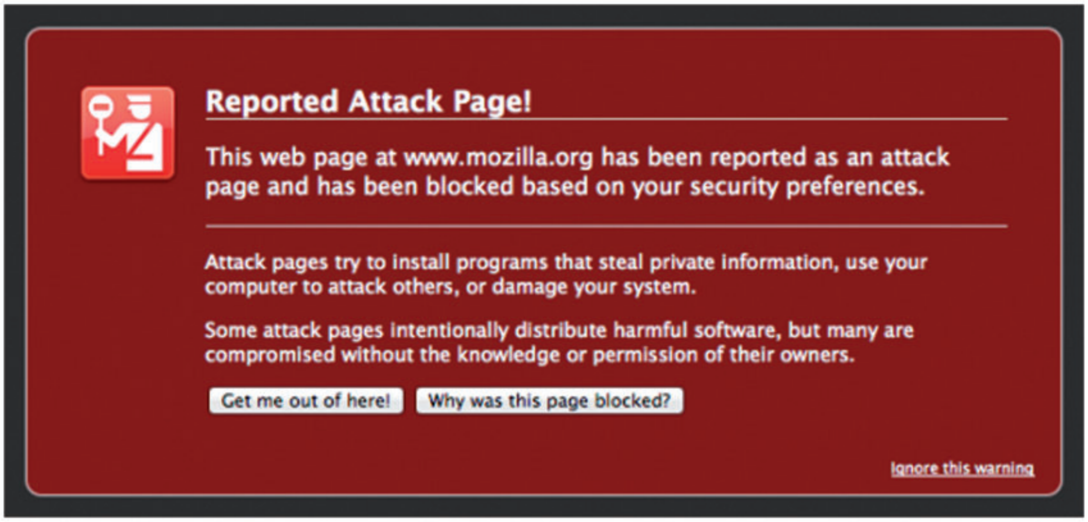


The site ahead contains harmful programs

Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

□ Automatically report details of possible security incidents to Google. Privacy policy

Figure A1. Google Chrome browser malware warning, build 43.0.2357.81 m.



Reported Attack Page!

This web page at www.mozilla.org has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Figure A2. Mozilla Firefox browser malware warning, build 38.0.1.