Studying the Effectiveness of Security Images in Internet Banking

Joel Lee
Carnegie Mellon University
Pittsburgh, PA
jlee@cmu.edu

Lujo Bauer
Carnegie Mellon University
Pittsburgh, PA
lbauer@cmu.edu

***Abstract*—Security images are often used as part of the login process on internet banking websites, under the theory that they can help foil phishing attacks. Previous studies, however, have yielded inconsistent results about users' ability to notice that a security image is missing and their willingness to log in even when the expected security image is absent. This paper describes an online study of 482 users that attempts to clarify to what extent users notice and react to the absence of security images. We also study the contribution of various factors to the effectiveness of security images, including variations in appearance and interactivity requirements, as well as different levels of user motivation. The majority of our participants (73%) entered their password when we removed the security image and caption. We found that features that make images more noticeable do not necessarily make them more effective at preventing phishing attacks, though some appearance characteristics succeed at discouraging users from logging in when the image is absent. Interestingly, we find that habituation, the level of financial compensation, and the degree of security priming, at least as explored in our study, do not influence the effectiveness of security images.**

I. Introduction

Many of the major Internet banking websites display a security image and caption each time a user logs into the account as a security measure [1]. When a user first registers for an account, she is prompted to pick a security image from a list of security images as well as to create a caption to accompany the image. The security image and caption are shown to the user on all subsequent logins, and the user is instructed not to log in if she notices that the image or caption are missing or incorrect. This strategy is believed to help protect users from phishing attacks: During a phishing attack, a user might be attracted to a fake web site that mimics a real one in all ways except that it does not show the user's chosen security image; a vigilant user might notice the absence of the security image and refuse to log in.

Examples of well-known banks that use this technology are Bank of America, PNC Bank, and Santander Bank. Bank of America uses an image, an image title, and three challenge questions, together known as the SiteKey [2]. PNC Bank displays a user-selected personal security image and a caption created by the user [3]; Santander Bank's approach is similar [4].

Despite the almost ubiquitous use of security images on banking sites, their effectiveness at preventing phishing attacks is uncertain. Even setting aside strategies that a sophisticated attacker might use to show the correct security image on a phishing site, users' ability to notice that an expected image is missing and then refuse to log in is not well understood.

Previous studies of the effectiveness of security images have reached divergent conclusions: in one, 92% of participants proceeded to log into their bank account even when the security image was absent [5]; in another, 60% of users of an online assignment-submission system noticed missing security images and refused to log in [6]. These previous studies used different methodologies, making it difficult to reconcile their results or isolate specific reasons for their divergence. Additionally, both studies were carried out in settings sufficiently different from real-world online banking scenarios that it is difficult to generalize from their results.

With the study described in this paper, we seek to shed further light on the ability of users to notice and appropriately react to the absence of security images, and the factors that influence the effectiveness of security images. We study 482 participants in an online setting, as they interact with a simulated banking web site over a period of several days. Our simulated banking web site closely mimics a real banking web site, and over the course of the study participants are required to log in to the site two times for one condition and five times for all other conditions. We assign each participant to one of 12 conditions, which vary in the visual characteristics of the image, in the amount of interaction required to log in and the level of customization of the image; as well as in the level of habituation, compensation, and amount of security priming that participants receive.

The majority of our participants (73%) entered their password when we removed the security image and caption, substantiating previous findings that security images are not a particularly effective security measure. Interestingly, we found that features that make images more noticeable (such as requiring users to click on the security image before they are able to log in) do not necessarily make them more effective at preventing phishing attacks, though some appearance characteristics (like displaying an image that blinks) succeed at discouraging users from logging in when the image is absent. Perhaps surprisingly, we find that habituation, the level of financial compensation, and the degree of security priming—at least as explored in our study—do not influence the effectiveness of security images. In combination with previous research [5], [6], we believe these results significantly improve our understanding of the noticeability of and users' reactions to missing security images, and hence of the effectiveness of security measures as a deterrent to phishing attacks.

The rest of this paper proceeds as follows. In Section II we discuss related work. Section III describes the design of the study, and Section IV details the results. We discuss the findings further in Section V and examine some limitations of our study in Section VI. We conclude in Section VII.

II. Background and Related Work

The most relevant related work falls into three categories: visual security indicators in general, graphical passwords, and security images specifically.

A. Security Indicator Studies

A study by Wu et al. showed the ineffectiveness of security toolbars that displayed security related information which was meant to help users detect phishing attacks. Also, many users do not know about phishing attacks or realize how sophisticated the attacks can be [7]. Another study, by Sunshine et al., tried to redesign existing SSL warnings. Even though their warnings performed much better than existing warnings, they found that too many participants continued to exhibit dangerous behavior in all warning conditions. The authors of the paper suggested that the better approach might be to minimize using SSL warnings altogether by preventing users from making unsafe connections or to eliminate warnings in benign situations [8].

B. Graphical Password Studies

Much research has been done on graphical passwords and how they could act as an alternative to text passwords. Blonder coined the idea of a graphical password and patented the concept in 1996 [9]. Jermyn et al. proposed and evaluated new graphical password schemes that made use of features of graphical input displays to get better security than text based passwords. They showed that graphical passwords could be used to devise password schemes with much larger password spaces [10]. Since then, many works have proposed using graphical passwords as an alternative to using traditional text-based password systems [11]–[14]. For example, Wiedenbeck et al. developed a more secure graphical password system called PassPoints in which users created a valid password with fewer difficulties than users who created text-based passwords, but took a longer time with more invalid password inputs to do so [12]. However, despite all the research that has been done on graphical passwords, this approach has still failed to achieve mainstream deployment [15].

On the other hand, security images have been widely used by internet banking websites as a security feature. Unlike graphical passwords, the use of security images is not to authenticate the user, but for the user to verify that the website that she is accessing is legitimate. Despite its widespread use, we found that the amount of academic literature on internet security images has been relatively sparse.

C. Studies of Security Images

To date, there have been to our knowledge two main user studies on security images, which have produced divergent results.

1) Study by Schechter, Dhamija, Ozment and Fischer: Schechter, Dhamija, Ozment and Fischer performed a study to evaluate website authentication measures that are meant to protect users from man-in-the-middle, phishing, and other site forgery attacks. The study had 67 bank customers conduct common online banking tasks and each time they presented increasingly alarming clues about their insecure connection. First, the HTTPS indicators were removed; next the participant's security image was removed; and then the bank's password-entry page was replaced with a warning page. The study found the security images to be ineffective, since all 18 participants in the role playing group, all 17 participants in the security primed group and 23 of the 25 participants who made use of their own accounts entered their passwords [5].

The methodology of this study has attracted some criticism, including that the results were biased in over-estimating the real-world rates at which the security indicators will be ignored [16]. The criticism was that participants were recruited around a university campus, 68% of participants were 18–25 with 91% of them being university students. Also, 21 people were recruited but chose not to participate in the study, 3 of these people refused to sign the consent form, and 5 people stated that they could not remember their login information, which might be because they had concerns with using their personal banking information for the study. Moreover, the research setting took place in a classroom building and participants were given a set of tasks to complete and could not proceed to the next task till they completed the current. Participants were told that the experimenters would not answer questions about the study tasks or to provide assistance. Since participants were given tasks to complete, they might have taken the tasks very seriously and be highly motivated to complete them. Participants might feel that they are being tested and wanted to complete the task and thus did not refuse to log in to the bank's site. Another reason could be because research participants were willing to obey authority figures in a research environment and thus put their financial information at risk under the influence of an authority figure in the study.

2) Study by Herzberg and Margulies: Herzberg and Margulies performed a long-term user study of site-based login mechanisms which forced users to log in safely. For their study, they used an online exercise submission system used by most courses at the computer science department of a university. Students used the system to submit their exercises and receive emails about their new grades; most users logged in to the system up to hundreds of times throughout the study. Several phishing attacks were simulated on the system and results were collected over three semesters. There were two variants of the experiment being conducted. In the first experiment, up to 5 bonus points were announced at the beginning of the study for one of the courses of their choice for correctly detecting attacks. At the end of 2 semesters, the authors found that 26% of the students did not cooperate with the experiment by trying to detect attacks and removed the results of those users. In the third semester, the authors provided extra incentives for students to cooperate with the experiment by displaying an instructions page that shortly described phishing, the authors' goals as well as the experiment details during the user's first login. In addition, students were told that they would lose bonus points based on classification mistakes.

Each user was randomly assigned to one out of the five conditions upon registration. In the first condition, an interactive custom image was shown and users had to click on the image before they could submit their password and log in. Different attack scenarios were carried out. In the classic phishing attack, a spoofed email that had the link to the spoofed login page was sent to the user. In that spoofed page, the interactive custom image was not displayed. Detailed statistics for each attack scenario were not available, but, overall, 59.84% of users detected the phished website when only the security images were used [6]. As such, the results of this study significantly differ from the results presented by the study in the previous sub-section. The authors attributed this to the interactive security images—users had to click on the custom image before they were allowed to log in, whereas the images were non-interactive in the previous study.

However, differences in results from the previous study could also be due to other differences in methodology. Participants in this study were students taking courses at the computer science department. As such, they would likely have above-average knowledge of information security. Also, participants were given explicit incentives to detect attacks. They were given up to 5 bonus points for correctly detecting attacks, which might have been a significant incentive for students who wanted to do well in the course. In addition, participants were specifically warned that an attack could happen. This could have made them more security conscious and caused them to pay greater attention to the security indicators in order to ensure that they would not be susceptible to an attack. Finally, the authors of the paper specifically removed 26% of users from the study who did not cooperate with the experiment by trying to detect attacks. This could cause a bias in the study results leading to higher detection rates.

III. Study Methodology

A. Goals and Overview

The focus of our study was not just to measure whether security images were effective, but also to examine what makes them effective. For example, we explore the influence of factors such as the size, appearance, and customizability of security images. Also, we wanted to find out whether changes to the way the study was conducted—such as by making participants more security conscious, paying them more for the study, etc.—would cause them to pay more attention to the security images. Several of these variations were motivated by the desire to shed light on the divergent results obtained by previous studies. Since the security images were typically displayed on internet banking websites and because we want to examine how users react in a high-value website, we decided to simulate a real-life internet banking scenario. Our study was approved by our institution's institutional review board (IRB).

B. Study Procedure

We built an internet banking website that had a similar look and feel as an actual internet banking website. The main website is shown in Figure 1.

We did not inform participants about the true purpose of the study since that might have caused participants to pay more attention to the security image than they would in a real

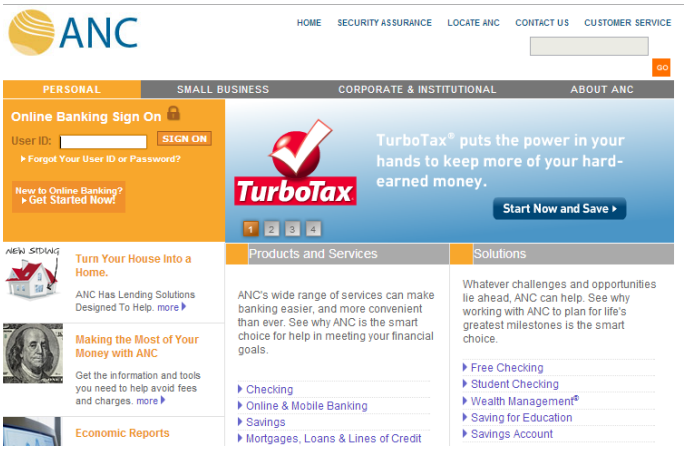

Fig. 1. Fictitious bank website used in study, designed to closely mimic a real banking website.

setting. Instead, participants were told that they were to test out the website on its direct deposit functionality. Participants had to report five deposits over a minimum period of five days in order to complete the study, except in one condition in which we shortened the study to two deposits over a minimum period of two days. 24 hours after participants registered for the account or after the last deposit report, an email would be sent with the following message.

> Hi [user],
>
> A deposit has been made to your ANC Bank Account.
>
> Please log on to your account by clicking on the link below. Once you are logged on, click on the "Report Deposit Value" button to report the last deposit that has been credited to your account.
>
> http://www.ancbank.com?id=15213
>
> Thank You!

Once participants clicked on the link, their browser stores a session cookie. Participants could later access the website simply by entering the ancbank.com URL in their web browser. We required participants to report five deposits over a minimum period of five days in order to habituate participants to seeing the security images and captions, as would occur in real online banking. Additionally, participants would receive as compensation the total amount that was "deposited" into their account if they completed the study. This was to make the study more realistic, since the amount in their account was the amount they received for the study. Each time they logged in, participants were shown the following message: "If you do not recognize your Personal Security Image & Caption then DO NOT enter your password and email us immediately at [email address]." This message was similar to that displayed at an actual internet banking website. The login screen with the security image, caption and the message is shown in Figure 2.

When the participant has to log in to the account to report the amount for the last time, the security image and caption was not displayed and was replaced with an "under maintenance" image. The security image and caption were again present on any log-in attempt five minutes or later from then. This simulates a real-life scenario when the user does not

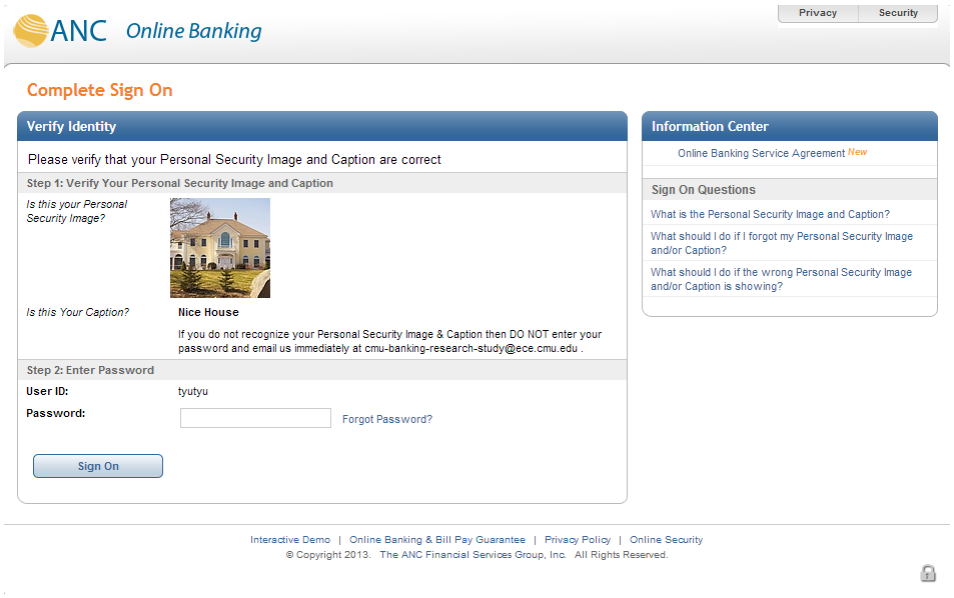

Fig. 2. Login screen with security image and caption as shown in the control condition.

see the security image upon accessing a phished website. In the real-life context, the user might choose to wait a while before trying again, to try accessing the website on a different device, or to call the bank to notify them about the problem. Likewise, in the study participants might choose to wait a while, try a different device or to email to notify us about the problem. There were a number of participants who emailed to alert us about the "under maintenance" image. When participants emailed us, we would tell them to wait for a few minutes before trying again. We recorded whether each participant entered her password in the five-minute period during which the security image and caption were not displayed. After the participant reported the last amount that was deposited into their account, they were then led to an exit survey where we asked several questions about security images and their demographics.

C. Exit Survey

The exit survey asked participants to indicate how much they agree or disagree with the following five statements about the security image that they saw each time they logged in.

1) Using a security image as part of the login process was annoying.
2) Using a security image as part of the login process was fun.
3) I wish that my bank's website used a similar security image.
4) I did not look at the security image before I entered my password.
5) Using a security image as part of the login process helps to improve online security.

Participants were asked to indicate their agreement with each statement on a Likert scale with the following five choices: Strongly disagree, Disagree, Neutral, Agree, Strongly agree.

We also asked participants six demographics questions about their age group; gender; country; whether they are majoring in or do they have a degree or job in computer science, computer engineering, information technology or a related field; their highest level of education; and if they have done one or more of the following:

- deleted browser cookies,
- cleared their web browser cache,
- changed their web browser cookie policy,
- refused to give information to a website, or
- supplied false or fictitious information to a website when asked to register.

D. Reasons for Using Mechanical Turk

We recruited participants on Amazon's Mechanical Turk to perform our study. We decided to make use of Mechanical Turk rather than a lab study due to several advantages: First, making use of Mechanical Turk allowed us to recruit participants from a much wider demographics group. We were able to reach out to participants from varied age groups, education level, profession, etc. This made our results less biased to a particular demographics group. A typical lab study done on campus would have only allowed us to recruit students with similar backgrounds which might then cause biases in our data.

Second, Mechanical Turk allowed us to carry out our study that lasted five days and required participants to perform tasks during that entire period. A lab study would have made it difficult to accomplish that since participants would have had to report to the lab six times (the first time to register for the account and the next five times to report the deposit amount) to complete the study, incurring significant inconvenience.

Third, carrying out the study on Mechanical Turk allows participants to perform the study in an environment that is similar to how they would access their actual internet banking website, by accessing the website from the comfort of their own home or office. Unlike a lab study, participants would not be under direct observation by the experimenter and hence

there is less risk that such observation (or other effects of accessing a bank account in a lab setting) would cause them to behave particularly self-consciously to strive to please the experimenter. This addresses a criticism of some previous studies that participants were biased as they might behave in a way that would conform to the experimenter's expectations [16].

Researchers who have examined Mechanical Turk have found participants to be significantly more diverse than in typical samples from American colleges (previously the usual source of study participants), and have confirmed that data obtained through well-designed studies on Mechanical Turk can be of high quality and at least as reliable as that collected by more traditional methods [17], [18].

E. Participant Recruitment

We recruited participants on Mechanical Turk by advertising a study "to test a new internet banking website on its direct deposit functionality." Participants were given a brief description of what they had to do for the study—to register for an account and to report each deposit that comes in. Also, they were told to act as if the bank account belonged to them and to take the necessary security measures to safeguard their account, as they would when logging in to any other internet banking website. We also provided an email address to contact should participants have any security-related concerns.

F. Study Conditions

Our 12 conditions fall into seven main categories. The first category consists of our control condition. Each of the other categories consisted of conditions designed to explore a specific factor that could influence the effectiveness of security images: the appearance of security images; the interactivity of security images; the ability of participants to customize security images; the lack of a caption; and methodological variations to explore the effects of motivation and habituation. In addition, one category explored the effects of varying multiple factors at the same time. The study had a between-subjects design. Participants were assigned randomly to one of the first nine conditions. Conditions 10–12 tested variations in study methodology; participants for these were solicited separately (in parallel with soliciting participants for the other conditions) because the methodological variations being tested included changes to the compensation and the length of the study, which required small changes to the study advertisement.

Control Condition.

1) *Control.* Our control condition closely mimics the PNC Bank's implementation of security images. The security image that participants have previously chosen is shown at 100 pixels high and 100 pixels wide. This size and other aspects of the login process are similar to those on an actual internet banking website.

Conditions Differing in Appearance. Using these conditions, we seek to explore whether security images with different appearance features make it more likely that a participant will notice that a security image is missing.

2) *Large image.* The chosen security image would be increased in size to 300 pixels high and 300 pixels wide, so as to be 9 times larger than the base condition. This was to find out if a larger security image would result in greater noticeability by users.
3) *Blinking image.* The image would be the same as the base condition, but it would be made to blink repeatedly using JavaScript in order to be more obvious to the user. We wanted to find out if a security image that draws attention through a blinking feature increases the chance that participants would pay attention to it.

Conditions Differing in Interaction. These conditions test whether requiring participants to interact with the security image makes it more likely that they will refuse to log in when the security image is missing.

4) *Interactive image.* Participants have to click on the security image before they can enter in their password to log in to the account.
5) *Copy random word.* Participants have to copy a random word that is placed in the security image before they can enter in their password to log in to the account.
6) *Copy caption.* Participants have to copy the caption that is displayed with the security image before they can submit the password.

Condition Differing in Customization. This condition tests whether allowing users to customize their security image increases its effectiveness.

7) *Custom image.* Participants will upload an image of their choice and then type in a caption that matches the image. This will be the security image and caption for the account.

Condition Differing in Customization, Appearance, and Interactivity. This condition tests whether the simultaneous presence of features present individually in other conditions improves the effectiveness of security images.

8) *Multi-feature.* Participants will upload an image of their choice and type in a caption that matches the image. This will be the security image and caption for the account. The image will be made to blink continuously using JavaScript. Participants have to click on the image before they are allowed to log in to the account.

Condition Without Security Caption. Security images are commonly accompanied by a caption. However, we wanted to decouple the effect of the security image from the effect of the caption.

9) *No caption.* Participants will not be asked to create a caption when they register for an account. Also, they will not be shown a security caption each time they log in to the account.

Conditions Differing in Study Methodology. These conditions are designed to test the effects of study duration (and habituation) and monetary and other incentives.

10) *Two logins.* Participants log in to the account twice, instead of five times, as in other conditions. The second time that they log in, the security image would be removed.
11) *More pay.* Participants would be paid twice the amount of money as the base condition.

12) *More security conscious.* In the consent form and in the instructions page, we put in the following message: "Recently, internet banking websites have been under attack. If your account is compromised, you will not receive payment for the study. It is important for you to take the necessary security measures, such as to choose a hard to guess password." A debriefing at the end of the study explained to participants that the message was fictitious and its purpose. The purpose of including this message was to make participants more security conscious, which we expected would make them more likely to notice the absence of a security image.

IV. Results

The study was conducted in April and May 2013. 569 participants completed part 1 of our study by signing up for an account on our website. Out of the 569 participants, 482 participants (85%) completed the entire study by reporting five deposit amounts over five days (or two deposit amounts over two days for users in the two-logins condition). For the remainder of this paper, we focus on those 482 participants.

A. Demographics

Our participants spanned a range of age groups. 152 (31.6%) participants reported themselves to be in the 18–25 age range, 200 (41.6%) in the 26–35 range, 70 (14.6%) in the 36–45 range, 33 (6.9%) 46–55, 21 (4.4%) 56–65, and 5 (1.0%) in the 65 and up range. 269 (55.9%) participants reported that they were male and 212 (44.1%) female.

The vast majority of our participants (99.2%) were from the United States (based on IP address), which is consistent with the stipulation in the study advertisement that participants should be in the USA. The remaining four participants were from Vietnam, Taiwan, India, and Georgia.

The majority of participants reported that their degree, major, or job was not in computer science, computer engineering, information technology or related field. 98 participants (20.4%) reported that it was.

All participants reported at least finishing high school. 181 (37.6%) participants reported high school as their highest level of education; 247 (51.4%) participants reported obtaining a college degree; and 51 (10.6%) reported receiving a graduate degree.

Despite a majority not reporting a major or occupation in information technology or a related field, the majority of participants were technically savvy, with between 70.8% and 73.2% reporting that they had at some point deleted browser cookies, cleared the browser cache, changed the cookie policy, and modified information they provided to a website in order to preserve their privacy.

B. Security Image Effectiveness

The purpose of our study was to examine if participants logged into their account when their security image and caption were not present.

Across all conditions, 352 of 482 (73.0%) participants entered their passwords when their security image and caption was not displayed. The remaining 130 (27.0%) participants did not do so. Results by condition are shown in Table I. We received numerous emails from participants about the "under maintenance" security image, asking us whether or not to log in in the absence of their security image and caption. We replied such email messages by telling participants not to log in, to try again after a few minutes and to only log in when their correct security image and caption appears.

Condition	% entered password	# entered pwd / # participants	p-value
control (1)	75.00%	30/40	
large (2)	86.84%	33/38	0.092
***blinking (3)**	**57.14%**	**24/42**	**0.044**
interactive (4)	74.36%	29/39	0.474
copy-random-word (5)	63.64%	21/33	0.146
copy-caption (6)	69.77%	30/43	0.297
custom-image (7)	82.50%	33/40	0.206
multi-feature (8)	74.36%	29/39	0.474
no-caption (9)	78.05%	32/41	0.373
two-logins (10)	68.42%	26/38	0.259
more-pay (11)	77.78%	35/45	0.382
more-sec-conscious (12)	68.18%	30/44	0.245
Total	73.03%	352/482	

TABLE I. Percentage and count of participants who entered their password without the security image. * indicates statistically significant difference from base condition. Shading groups conditions that belong to the same category.

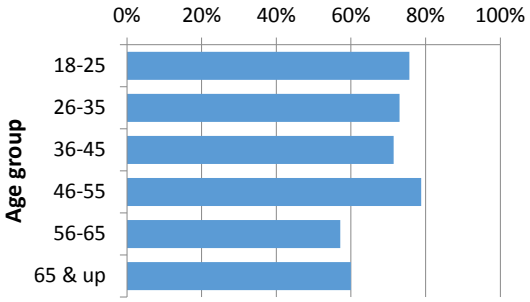

Fig. 3. Percentage of participants who logged in without a security image showing, by age group.

We used a one-tailed Chi-square test in order to compare the 11 experimental conditions to the control condition for statistical significance at α = 0.05.

We found no statistically significant difference in the effectiveness of security images based on participants' gender, country, major/degree/job, level of education, or security experience.

We did find, however, that participants in the 56–65 age group were less likely to enter a password in the absence of a security image than participants in the 46–55 (p=0.045) and 18–25 (p=0.036) age groups. 57.1% of participants in the 56–65 age group entered their password, compared to 75.7% participants in the 18–25 group and 78.8% participants in the 46–55 group. (See Figure 3.)

C. Sentiment Toward Security Images

At the end of the study, we asked participants to rate how much they agree or disagree with five statements on a

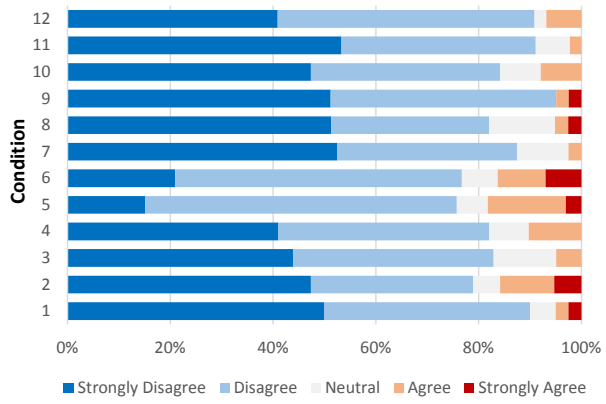

Fig. 4. Participants' responses to the statement that using a security image as part of the login process is annoying.

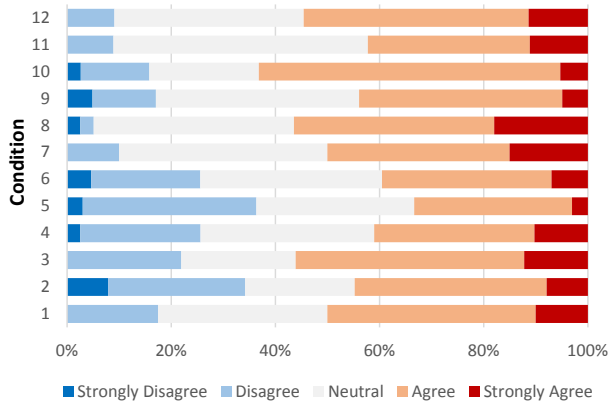

Fig. 5. Participants' responses to the statement that using a security image as part of the login process is fun.

5-point Likert scale about the security image that they saw each time they logged in. This was to obtain an evaluation of their attitudes toward the security images. For analysis, we binned the responses into two groups—"agreed" and "disagreed". Participants who responded to the five statements with "strongly disagree," "disagree," and "neutral" were assigned to the "disagreed" bin and those who answered "agree" and "strongly agree" were assigned to be "agreed" bin. We then ran a 1-tailed Chi-square test to determine if there was any difference in participants' sentiment towards security images based on the condition they were in.

The statements that we asked about were as follows:

1) "Using a security image as part of the login process was annoying": Of the participants in the control condition, 5% agreed that using the security image was annoying. Across the experimental conditions, agreement varied from 2.2% and 18.2% of participants. Participants' responses are shown in Figure 4. Statistically significantly different from the control condition were the *copy-random-word* condition (p=0.036) at 18.2% and the *copy-caption* condition (p=0.049) at 16.3%. Condition *copy-random-word* required the user to type in a random word placed in the image while the *copy-caption* condition required the user to type in the security caption shown beneath the image each time they log in to the account. This additional step requires additional effort and slows down the login process, and so it was consistent with our expectations that sentiment was negatively affected.

2) "Using a security image as part of the login process was fun": Exactly half of the participants in the control condition, and between 33.3% (*copy-random-word* condition) and 63.2% (*two-logins* condition) participants in experimental conditions agreed that the security image was "fun." However, we found no statistically significant differences by condition. Results are shown in Figure 5.

3) "I wish that my bank's website used a similar security image": Participants were also relatively evenly split on whether they wished their own bank adopted a login process similar to the condition they were in: 42.5% of participants in the control condition agreed, and agreement in experimental conditions ranged from 42.4% (*copy-random-word* condition) to 71.8% (*multi-feature* condition). The only statistically significant result was in the *multi-feature* condition (p=0.004), in which 71.8% of participants wished their bank used a similar login process. This may have been due to a combination of noticeability and convenience: the image was supplied by the participant, blinked, and had to be clicked on before a participant could log in; but the amount of effort required during the login process was minimal (an extra click).

4) "I did not look at the security image before I entered my password": The vast majority of participants reported paying attention to the security image: 92.5% in the control condition, and between 84.2% (*large* condition) and 100.0% (*multi-feature* condition) in experimental conditions. As for the previous statement, the only statistically significant difference from the control condition was for the *multi-feature* condition (p=0.040)—the multiple additional features might have made more participants look at the security image before they entered their password.

5) "Using a security image as part of the login process helps to improve online security": A majority of participants (73.0% overall) felt that using a security image as part of the login process helped to improve online security. Agreement with this statement ranged from 66.7% to 82.2%, with no statistically significant difference between experimental conditions and the control.

V. Discussion

A. Effectiveness of Security Images

We found that 27.0% of participants did not enter their password when their security image and caption were not shown in the control condition. This result differs from a prior study which found that 8% of participants who used their own internet banking accounts did not do so, using a similar login process but in a lab setting [5]. For the condition which participants had to click on the security image before they could log in, we equivalently found that 25.6% of participants did not enter in their password when their security image and caption were not shown. This result also differs from another prior study that had a similar interactive component to the login process, which found that 59.8% of users detected the phished website [6].

B. Blinking Security Image

Our study found significantly more participants did not log in to the account when the security image was not present in the *blinking* condition (p=0.044). We believe that a blinking security image might have drawn participants' attention to it each time they log in to the account. When the "under maintenance" image was displayed, it could have aroused participants' suspicion greater, since their blinking security image was not displayed but instead replaced with a static "under maintenance" image. Since a blinking image is easily implementable (either using JavaScript or to use an animated GIF), it could be a cost-effective method for websites to improve the effectiveness of the security images by making them blink.

C. Large Security Image

We expected to find more participants to not enter in their password in the absence of the security image and caption in the *large* condition when the image was displayed at 9 times the size as the image in the control condition. However, we found the converse to be true. 13.2% did not enter in their password when their security image and caption was not shown, compared to 25% in the base condition, though the result was not statistically significant (p=0.092).

D. Conditions Differing in Interaction

Even though participants had to click on the security image before they could enter their password for the *interactive* condition, this did not significantly affect the effectiveness of the security image. This result suggests that an interactive image does not lead to significantly better results than a static image, which is a finding that is different from Herzberg and Margulies [6]. Participants might have clicked on the image without noticing if the image was correct; when the "under maintenance" image was displayed, they could have just clicked on it and entered their password.

In the *copy-random-word* condition, where participants had to copy a random word placed in an image before they could enter their password, and the *copy-caption* condition, where participants had to copy the security caption, security images were not more effective than in the control condition. At the same time, significantly more users in these conditions stated that using a security image as part of the login process was more annoying than the control condition, indicating an increased awareness of the security image. The inconvenience which users had to go through each time they logged in could have made them glad that they did not have to do so when the website was "under maintenance," leading them to just enter the password.

E. Condition Differing in Customization

In the *custom-image* condition, in which participants uploaded a personal security image, there was no significant increase in the effectiveness of security images. Based on this result, websites should continue their current practice of asking users to choose a security image from a pool of images rather than to upload a customized version. Allowing users to upload a customized security image leads to several problems: it creates additional work for users to find images to upload, there is a need to restrict users from using photos with explicit content, and websites face the risk of a virus-infected image file being uploaded.

F. Condition Differing in Customization, Appearance, and Interaction

Interestingly, the *multi-feature* condition, where participants defined the security image, the image blinked, and participants had to click on the image, proved no more effective than conditions with much subtler image effects and fewer attention-grabbing features. The addition of multiple security features might have led participants to believe that there was a greater possibility of the security image being incorrectly displayed, and thus they could have believed that the webpage really was under maintenance when the security image was missing. This is despite the fact that significantly more participants in the *multi-image* condition stated that they looked at the security images before they entered in the password compared to the control condition.

G. Conditions Without Security Caption

The *no-caption* condition, where no security caption was shown, was as effective as the control condition, which did include a security caption. This suggests that a security image alone might just be as effective as the combination of a security image and a caption.

H. Conditions Differing in Study Methodology

The *two-logins* condition, in which participants participated in a shorter study, did not show significant changes in the effectiveness of security images. This contradicts our hypothesis that habituation might affect the effectiveness of security images.

The *more-pay* condition, in which participants were paid twice the amount as in other conditions, also did not lead to significant increases in security image effectiveness. This suggests that the amount that we paid participants did not affect how they responded to security images. This finding is in line with that of Buhrmester et al., which showed that differences in compensation rates received by Mechanical Turk participants do not appear to affect data quality [17]. As such, we have a stronger reason to believe that participants might behave in the same way when dealing with even larger amounts of money in their actual internet banking account.

The *more-security-conscious* condition, in which participants were security primed, also did not show a significant difference in the effectiveness of security images. This could be because participants might be unsure of the security measures which they had to take to safeguard their account. They could also have believed that the website was really under maintenance and hence chose to enter their password despite not being shown their security image and caption.

VI. Limitations

As with other studies, the study described in this paper has a number of limitations, which we discuss in this section.

A. Fake Internet Banking Accounts

While we took great care to ensure the ecological validity of our study by making the website as realistic as possible, there were limits to what could be done. The internet banking website that we created existed only within the study and participants were not creating real internet banking accounts. As such, participants might not have been as motivated to pay attention to the security image and caption as when accessing an actual internet banking web site. Additionally, even if they noticed that a security image was missing, participants may have felt that they needed to log in to complete the study even in the absence of the security image. For example, a participant wrote that "maybe the study wanted to see if I would proceed with login...I would never do so with my actual bank account." Another participant wrote that "had this been my actual bank account I would have exited and tried again later." Only a handful of participants reported such motivations, however.

We tried to isolate the effect of motivation by creating a separate condition which paid participants twice as much as the other conditions and a condition which made participants more security conscious—we informed participants that internet banking websites have been under attack and they would not receive money for the study should their account get compromised. These conditions produced nearly the same results as the base condition, and had no significant statistical differences.

B. Habituation

Another potential limitation is due to habituation, which is the decrease in the response to a stimulus after repeated exposure to it. In a real-world setting, internet banking users would likely have logged into their internet banking website a larger number of times.

We attempted to isolate the effect of habituation by including a condition in which only two deposits were required, rather than the usual five. Slightly fewer participants (68.4% to 75.0%) entered their passwords when the security image was missing in the two-day condition compared to the control condition. The difference was not statistically significant. The effect of habituation in a real-world setting would likely be much stronger. However, this might be mitigated by participants using their actual Internet banking accounts rather than a fake account.

C. Money as Motivating Factor

It is believed that money is the main motivating factor for Mechanical Turk workers [19], and some workers try to game the system to achieve maximal financial advantage [20]. As such, participants might have just wanted to complete the study as quickly as possible, without paying much attention to the security indicators. However, the incidence of participants leaving thoughtful optional comments on our study was sufficiently high to suggest that this may not have been the case.

D. Under Maintenance Image and Attack Vectors

In this study, we decided to simulate a phishing attack on the banking website by replacing the real security image and caption with an "under maintenance" image. Actual attacks could take a number of other forms, including not displaying a security image and caption at all with a plausible explanation provided, displaying an incorrect security image with the same security features such as a blinking image or requiring interactivity, or showing a redesigned web page with an incorrect security image and caption. In the absence of a definitive understanding of the most effective way to trick users, we chose to use the "under maintenance" image as a reasonable approximation of what might happen in a real attack scenario; other attack scenarios may be more effective.

Beyond the appearance of the site, real attacks could differ according to the attack vector. For example, an attack might be mounted by sending users a phishing email with a link to a malicious web site that impersonated their bank. We did not examine the effects of using different attack vectors, instead focusing purely on the effect of removing security images and captions.

E. SSL Certificate

Due to problems with obtaining the SSL certificate for the domain name that we used for the study, we were unable to display a HTTPS secure connection indication in the browser, which is typically a standard feature on an internet banking website. While research has found that such security indicators are generally not effective [21], some users might have realized that the webpage they were accessing was not via a HTTPS connection and could have behaved differently. For example, one participant asked: "The login page is not an https secure connection, which is what I'd normally expect. Is this ok?"

F. Significant Results Around p=0.05 Threshold

Several results that we report were statistically significant at the p=0.05 threshold but had relatively large p-values. Future studies would benefit from a larger sample size or an experimental design with fewer conditions.

VII. Conclusion

Building on previous studies of security images, we designed a study that sought to shed more light on the ability of users to notice missing security images and react appropriately. Our conclusions include the following.

A. Security images are generally not very effective

In our control condition, 75.0% of participants entered their password even in the absence of a security image. This is less than in a previous study, in which 92% of participants logging into their own bank account using a similar login process failed to notice the absence of a security image [5]. These differences can be at least partly attributed to the fact that our study was carried out online, not in the lab, and in that way perhaps provided a more realistic simulation of the environment in which online banking transactions usually take place.

At the same time, in the condition in which users were required to click on an image before they could log in, 74.4% of participants continued to enter in their password when the security image was not present. In a previous study that also required participants to click on the image, only 40.2% of

participants did not detect it when their personalized security image was not present [6]. In that prior work, participants were particularly alert to phishing attacks. We believe our study, particularly including the condition in which participants received additional security priming, is in this way more consistent with the amount of priming users would receive in practice.

Overall, we conclude that security images are generally not very effective, especially when compared to other more secure albeit expensive methods, such as using a security token for two-factor authentication. However, improvements could be made at a low cost in the way that the security images are displayed which could result in greater effectiveness.

B. Having a blinking image results in significantly greater effectiveness

When participants are shown a blinking image each time they log in, they are significantly less likely to log in in the absence of the image, compared to the control condition where they are shown a non-blinking image. Internet banking websites may want to explore blinking or other visual effects beyond what we studied, particularly since these can be simple to implement.

C. Performing additional tasks to log in does not lead to significantly greater effectiveness but leads to significantly greater annoyance

Surprisingly, participants who had to type in a word that appeared in the image or type in the security caption before they could enter their password were not more successful at evading simulated phishing attacks. These participants did, on the other hand, experience significantly greater levels of annoyance with the login process, suggesting that adding non-trivial complications or tasks to the login process is not a fruitful avenue for improving the effectiveness of security images and other similar security measures.

D. Customized security images did not lead to significantly greater effectiveness

Also surprisingly, participants who uploaded their own images to use as their security image—instead of choosing from a list of images provided by the website—were not significantly more effective at noticing the absence of a security image.

E. Habituation, level of motivation, and security priming have minimal effect

To the extent that these factors were exposed by our study, habituation, the financial compensation to participants, and the amount of security priming participants received did not significantly affect participants' ability to notice and effectively react to missing security images.

ACKNOWLEDGMENTS

This work was supported in part by NSF award CNS-1018211. The authors would like to thank Cristian Bravo-Lillo, Limin Jia, and Blase Ur for their input and help in various phases of the research.

REFERENCES

[1] J. Kirk, "Study: Users ignore bank security features," *Computerworld*, Feb. 2007, http://www.computerworld.com/s/article/9010283/Study_Users_ignore_bank_security_features_.

[2] Bank of America, "SiteKey FAQs," https://www.bankofamerica.com/privacy/faq/sitekey-faq.go, 2013.

[3] PNC, "Online security information," https://www.pnc.com/webapp/unsec/Solutions.do?siteArea=/pnccorp/PNC/Security+Information/Security+Information, 2013.

[4] Santander Bank, "SSA makes online banking even more secure," https://www.santanderbank.com/us/personal/banking/online-and-mobile-banking/security-center/ssa-learn-more, 2014.

[5] S. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies," in *Proceedings of the 28th IEEE Symposium on Security and Privacy*, 2007.

[6] A. Herzberg and R. Margulies, "Forcing Johnny to login safely," in *Proceedings of the 16th European Symposium on Research in Computer Security*, 2011.

[7] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?" in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010.

[8] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying wolf: An empirical study of SSL warning effectiveness," in *Proceedings of the 18th USENIX Security Symposium*, 2009.

[9] "U.S. patent number 5,559,961," 1996.

[10] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

[11] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Proceedings of the 1st Symposium on Usable Privacy and Security*, 2005.

[12] ——, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies – Special issue: HCI research in privacy and security is critical now*, vol. 63, no. 1–2, pp. 102–127, 2005.

[13] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Proceedings of the 12th European Symposium on Research in Computer Security*, 2007.

[14] D. Hong, S. Man, B. Hawes, and M. Matthews, "A graphical password scheme strongly resistant to spyware," in *Proceedings of the International Conference on Security and Management*, 2004.

[15] C. Herley and P. C. van Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE Security and Privacy Magazine*, vol. 11, no. 1, pp. 28–36, 2012.

[16] A. Patrick, "Commentary on research on new security indicators," http://www.andrewpatrick.ca/essays/commentary-on-research-on-new-security-indicators, 2007.

[17] M. Buhrmester, T. Kwang, and S. D. Gosling, "Amazon's Mechanical Turk – A new source of inexpensive, yet high-quality, data?" *Perspective on Psychological Science*, vol. 6, no. 1, pp. 3–5, 2011.

[18] G. Paolacci, J. Chandler, and P. G. Ipeirotis, "Running experiments on Amazon Mechanical Turk," *Judgment and Decision Making*, vol. 5, no. 5, pp. 411–419, 2010.

[19] P. G. Ipeirotis, "Demographics of Mechanical Turk," NYU Working Paper No. CEDER-10-01, 2001.

[20] K. S. Downs, M. B. Holbrook, S. Sheng, and L. F. Cranor, "Are your participants gaming the system? Screening Mechanical Turk workers," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010.

[21] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing*