

Security Usability Studies: Risk, Roles and Ethics

Position Paper for CHI 2007 Workshop on Security User Studies

Rachna Dhamija
Harvard University
rachna@deas.harvard.edu

We conducted a study to evaluate website authentication measures that are designed to protect users from man-in-the-middle, ‘phishing’, and other site forgery attacks [1]. We also investigated how a study’s design affects participant behavior: we asked some participants to play a role and others to use their own accounts and passwords. We also presented some participants with security-focused instructions.

In the workshop, I propose to share the design and results of the study in order to encourage discussion of the following questions:

- Do participants behave less securely when playing a role than when the risk is their own?
- Do participants behave more securely when they are informed that security is a focus of the study?
- Can we ethically replicate the experience of a real attack in a usability study?

Study Overview

We asked 67 bank customers to conduct common online banking tasks. Each time they logged in, we presented increasingly alarming clues that their connection was insecure. First, we removed HTTPS indicators. Next, we removed the participant’s site-authentication image—a customer-selected image that users are required to verify before entering their passwords. Finally, we replaced the bank’s password-entry page with a warning page. After each clue, we measured whether participants entered their passwords or withheld them.

In designing our study of website authentication indicators, we tried to realistically simulate the conditions that a user would experience during an attack. One real-world condition that is difficult to replicate in an experimental environment is the experience of risk. Most studies ask participants to assume the role of someone else to avoid exposing participants to real risks. In these role-playing scenarios, the consequences of behaving insecurely are borne by the fictional role, not by the participants themselves. Until now, no studies have tested whether participants playing roles behave as securely as they do when they are personally at risk.

Participants in a usability study may not behave realistically if they are told, or can infer, that security is the focus of the study. However, it is often difficult to conceal the focus of the study. Researchers may need to provide participants with the training or knowledge required to behave securely, especially if new security features are being tested.

Researchers are also obligated to inform participants of risks and obtain their informed consent prior to the study. Some researchers argue that informed consent requirements should be waived in order to obtain valid participant responses to phishing attacks [2]. Thus, there is a tension between the requirement to obtain informed consent from participants and the desire for participants to perceive realistic risk.

Study Design

We used a between-subjects design, where the participants were divided into three groups; 19 participants were required to play a role and to login using the credentials of that role. 20 participants used the same role-playing scenario and were also given additional instructions to behave securely. 28 participants were required to complete tasks by logging into their own bank accounts.

Ethical guidelines are of particular concern in this study, because we ask participants to perform tasks using their own account information. Our study protocol was jointly reviewed and approved by the institutional review boards of Harvard University and MIT. One strict rule was at the core of our study design: participants must only be deceived in ways that cause them to believe they are less secure than they actually are. While we provided attack clues that indicated it was unsafe for participants to enter their passwords, we secretly made sure that the necessary security measures were in place. In addition, we took the following steps to ensure that participants were aware of risks and that these risks could be minimized.

- Our consent form notified participants that their actions could be observed. (We informed participants that the study was about bank website usability, not that we were studying security.)
- Our observation system did not record user IDs, passcodes, or other private information.
- We did not introduce risks to participants beyond those inherent to accessing their bank from a university-managed computer.
- At the end of the study, we provided participants with an in-person, private debriefing that explained the purpose of the study, the attack clues that we had presented, the precautions we had taken, and how participants could protect themselves from real site-forgery attacks in the future.

Participants in Group 1, the role playing group, were instructed to assume the role of a named individual and to conduct tasks on behalf of that role. These participants used test accounts that we created for the study. They received the following instructions, with no indication that security was a focus of our study.

Imagine that you are [role name], a medical doctor who has an account at [bank name]. You often use this account to transfer money to your retirement plan. You are at home on a Sunday afternoon and decide to tackle a number of banking errands. All of your bank branches are closed, so you decide to access [bank name] online banking web site.

Participants in Group 2, the security primed group, were also instructed to play a role. The instructions provided to this group were identical to those in the first group, with one exception: an extra paragraph indicated that they were playing the role of someone who was concerned about the security of his password.

As [role name], you chose [bank name] because it advertises additional security features. Control over your account is protected by a passcode (also known as a password), and you want to ensure that this passcode doesn't fall into the wrong hands.

Participants assigned to Group 3, the personal risk group, were asked to perform tasks using their own bank account. These participants, like those in the first group, were given no indication that security was a factor in the study. Instead, their incentive to behave securely was that their own account information, including their username and password, would appear to be at risk. Their instructions simply began:

We will now ask you to perform five online banking tasks at the [bank name] web site.

Results

Our study confirms prior findings that users ignore HTTPS indicators: no participants withheld their passwords when these indicators were removed. Our results also show that site-authentication indicators are ineffective: even when removed, 23 of the 25 (92%) participants who used their own accounts, and all other participants, entered their passwords. Furthermore, we discovered that site-authentication indicators may cause users to disregard other important security indicators.

The effect of role playing

Participants who used their own accounts in our study behaved more securely than those who were assigned to play roles. While we did not see a statistical difference when we compared the role playing group (Group 1) to the personal account group (Group 3), we did find a significant difference when comparing the personal account group (Group 3) to the security primed group (Group 2) and to the union of all role-playing groups.

Our results should give pause to researchers designing studies that rely on role playing. Participants who may be vigilant in securing themselves from real-life risks may be less

motivated to behave securely when when playing a role—especially if the risks are perceived as fictional.

It is possible that better study designs, with more compelling scenarios, could increase the security-vigilance of role playing participants to the levels exhibited by those exposed to more realistic risk. However, even if a scenario successfully approximates real-world conditions in one study, it may not be equally effective when experimental conditions change (e.g., when a different system is being tested, a different population is used, or when the context of use differs).

Our results do not discount the usefulness of role-playing scenarios. In some cases, artificial scenarios may be the only way to simulate attack responses in an ethical manner. For example, role playing may be a useful device in qualitative studies where researchers want to closely observe participants without compromising their privacy. Role playing may also be useful to study the comparative efficacy of security approaches, where each group uses an identical role-playing scenario to test a different approach.

The effect of security priming

Though the result was not statistically significant, we were surprised to find that participants assigned to the security primed group behaved less securely than those in the role playing group, who had no security-priming. Because the difference is not significant, it may likely be due to chance.

One alternative explanation is that the security-priming instructions were too subtle: we had wanted to test if simply mentioning security would affect behavior. Participants may have behaved more securely if we had been more specific about how they should protect their password. It is also possible that the role-playing effect was actually stronger in the security primed group than the role playing group (Group 1): we informed participants that security was important in the context of their role, which significantly increased the length of the instructions devoted to role playing.

While our methodology and sample sizes did not produce a measurable effect of security-priming on security behavior, such an effect may still exist. Measuring the conditions under which priming affects security behavior is an area for future work. For example, future studies might focus specifically on the effects of security training or the effects of providing monetary incentives to behave securely.

References

1. The Emperor's New Security Indicators, Stuart Schechter, Rachna Dhamija, Andy Ozment and Ian Fischer, To appear in the Proceedings of the 2007 IEEE Symposium on Security and Privacy, May 2007
2. Markus P. Finn and M. Jakobsson. "Designing and Conducting Phishing Experiments" To appear in IEEE Technology and Society Magazine, Special Issue on Usability and Security