How Interactivity Can Enhance the Effectiveness of Fear Appeals:

A Web-based Field Experiment of Password Security

Anthony Vance, David Eargle, Kirk Ouimet
Brigham Young University

Detmar Straub
Georgia State University

Abstract

Passwords remain the dominant authentication mechanism for information security. Unfortunately, research has shown that most passwords are highly insecure. Given the risks of using weak passwords, there is a need to effectively motivate users to select strong passwords.

In this study we examine the influence of interactivity, as well as static and interactive fear appeals, on motivating users to increase the strength of their passwords. We developed a field experiment involving the account registration process of a website in use in which we observed the strength of passwords chosen by users.

Data were collected from 354 users in 65 countries. We found that while the interactive password strength meter and static fear appeal treatments were not effective, the interactive fear appeal treatment resulted in significantly stronger passwords. Our findings suggest that interactive fear appeals are a promising means of encouraging a range of secure behaviors in end users.

1. Introduction

Passwords have been the dominant authentication mechanism in information security for more than five decades (Furnell 2011). For nearly as long, the general weakness of password security has been recognized (Morris et al. 1979). Despite this fact, many users' website

passwords are still trivially weak and can be cracked in a matter of minutes using commonly available password cracking software (Imperva 2010). Compounding the problem, large empirical studies show that the average user has 6.5 website passwords, each of which is shared among 3.9 different sites (Florencio et al. 2007), and 73 percent of users share their online banking password with at least one nonfinancial website (Trusteer 2010).

Given the threats to password security, there is a need to effectively educate and motivate users to select strong passwords. One common means used to encourage users to increase password security is the password strength meter, which interactively displays to the user the strength of the password as it is typed (Furnell 2011). However, despite its prevalence, little empirical research has examined the effectiveness of password strength meters.

The research objective of this study is to examine whether interactive fear appeals, provided during the password creation process, motivate users to enhance the security of their passwords. In doing so, we integrate principles of interactivity theory and fear appeals. Interactivity explains the psychological effects of a user being able to interact in a computer-mediated environment in real time (Steuer 1992). Fear appeals are messages designed to convey the seriousness of a threat and a user's ability to cope with it (Johnston et al. 2010a). Despite the wide use of fear appeals in a variety of media, as yet fear appeals are typically presented in static form. In this paper, we theorize that use of interactive fear appeals will be more effective in enhancing password security than either static fear appeals for interactivity (in the form of password strength meters) alone.

We test our hypotheses using a field experiment involving the account registration process for a website in actual use. We examine the effects of three experimental treatments (interactive password strength meter, static fear appeal, and interactive fear appeal) on the strength of actual

passwords chosen by new users of the website. Data were collected from 354 users in 65 countries. We found that the interactive fear appeal treatment resulted in significantly stronger passwords, as theorized. In contrast, neither the interactive password strength meter nor the static fear appeal treatments were successful in increasing password strength. Our findings suggest that interactive fear appeals are a promising means of encouraging a range of secure behaviors in end users.

The rest of this paper is organized as follows. In Section 2 we review literature relating to passwords, fear appeals, and interactivity and develop our hypotheses. In Section 3 we describe the methodology of our field experiment, and we present our analysis in Section 4. Finally, we discuss our findings and their implications in Section 5 and conclude in Section 6.

2. Literature Review and Theory

Previous behavioral research on password security has focused on usability (Adams et al. 1999) and memorability (Keith et al. 2009; Yan et al. 2004; Zhang et al. 2009; Zviran et al. 1999). In contrast, Weirich and Sasse (2001) performed an explorative qualitative study that suggested users may be amenable to persuasion to increase password security. This study breaks new ground by examining factors that motivate users to create stronger passwords.

We next review literature on fear appeals and interactivity and discuss how they relate to information security. In doing so, we also develop our hypotheses.

2.1 Fear Appeals

Fear appeals are messages that are intended to raise perceptions of a threat and one's ability to cope with it (Rogers 1983). Fear appeals have two main components: (1) statements suggesting an imminent threat, and (2) statements recommending a certain course of action,

including encouragement of one's ability or efficacy to follow the recommended course of action (Johnston et al. 2010a).

Following Witte (1992), a fear appeal consists of four basic elements within a message: (1) one's susceptibility to the threat (2) the severity of the threat, (3) clear direction for how to respond to the threat (self-efficacy), and (4) the efficacy of the response (response efficacy). Elements (1) and (2) attempt to increase perceptions of the threat, whereas (3) and (4) are designed to strengthen the perception of efficacy of the response.

Fear appeals are explained by a number of theories, the most developed of which is protection motivation theory (PMT) (Rogers 1983; Rogers 1975). PMT explains that fear appeals trigger two appraisals or assessments in connection with the message: a threat and a coping appraisal. A protective action will only occur if the threat is deemed personally relevant and potentially harmful (Johnston et al. 2010a). Failing this, no action will be taken.

While originally developed to explain protective health behaviors, PMT has been productively applied to the area of information security. For example, Vance et al. (2012) and Herath et al. (2009) used PMT to explain employee compliance with information security policies. Workman et al. (2008) applied PMT to explain specific security behaviors including updating and protecting passwords. Most relevant to this study, Johnston et al. (2010a) examined the effect of fear appeals on users' installation of anti-spyware software, finding that fear appeals were effective in motivating secure behavior.

Applying the above theory and findings to password security, we predict that a fear appeal presented to users when choosing a password will motivate users to choose stronger passwords. Accordingly, we hypothesize the following:

H1. Participants in the static (non-interactive) fear appeal treatment will select stronger passwords than those in the control group.

2.2 Interactivity

The construct of interactivity originated in the area of communications research and was subsequently applied to computer-mediated communication. Steuer (1992) defined interactivity as "the extent to which users can participate in modifying the form or content of a mediated environment in real time" (Steuer 1992). His expanded definition of interactivity includes three factors—speed, range, and mapping. Speed refers to the immediacy of response to user input, range refers to the amount of change that can be effected on the mediated environment, and mapping refers to how well human actions are connected with actions in the mediated environment.

Interactivity is closely related to the construct of flow, as pointed out by Trevino et al. (1992). They proposed that two of interactivity's dimensions, control and intrinsic interest, are closely related to flow, and therefore, flow theory can predict the same outcomes as interactivity. Flow theory (Csikszentmihalyi 1990) describes an absorbing state that people can enter when performing a task. Of particular interest to this study, flow the theory has been convincingly applied to human-computer interactions (Jiang et al. 2007; Novak et al. 2000; Trevino et al. 1992). The flow experience with computers has been described as a state that (1) consists of a seamless sequence of responses facilitated by human-computer interactivity, (2) is enjoyable, (3) is accompanied by a loss of self-consciousness, and (4) is self-reinforcing, in that the user wants to continue performing the task for the performance's sake, rather than for any particular outcome of the task (Ghani 1995; Novak et al. 2000).

2.3 Interactivity and Information Security

A natural application for interactivity in the realm of IS security is in the area of user education of passwords. The most common example of such education is the use of password strength meters, which interactively report to the user the strength of their password as the password is typed (Furnell 2011). Password strength meters are designed to give the user a high level of control, in that the user can type whatever password they want into the meter, and a report about the password's strength will be returned to the user, with ratings such as "weak", "good", or "excellent." The meters are also designed to report immediate feedback to the user.

However, despite their prevalence, we have found no study that has empirically examined the effectiveness of password strength meters. Forget et al. (2008) examined an interactive password tool that accepted a weak password and then suggested a more complex version of the password as an alternative to the user. However, password strength was not reported to the user.

The characteristics of password strength meters correspond well to aspects of interactivity and flow: (1) they respond quickly, (2) they offer a sense of control to the user, and (3) they provide a range of relevant responses to the user (Steuer 1992). Additionally, flow and interactivity are likely to yield positive benefits relevant to password strength meters. For example, the interactivity provided via the strength meter and the resultant state of flow are likely to more fully engage the user in the process of choosing a strong password. Therefore, we predict that an interactive password strength meter will invoke the above positive benefits of interactivity, leading to the creation of stronger passwords.

H2. Participants in the interactive password strength meter treatment will select stronger passwords than those in the control group.

2.4 Fear Appeals and Interactivity

Fear appeals are essentially educational instruments designed to teach individuals new protective behaviors. This section explains how interactivity enhances learning, thereby enhancing the effectiveness of fear appeals. Both and interactivity plus flow align well with principles of learning derived from various learning theories from the fields of educational psychology and pedagogy. Championed largely by Thorndike (1932), these principles include readiness, exercise, effect, primacy, recency, intensity, freedom and requirement. Of these, *readiness*, *exercise*, and *intensity*, are most relevant to this study. We next describe how these three principles relate to interactivity, and its potential impact on fear appeals.

Readiness refers to an individual being in a physical, mental, and emotional state of preparedness for learning, or to being motivated to learn. Flow has been demonstrated to be intrinsically motivating (Ghani 1995; Novak et al. 2000), and if a fear appeal message's threat awareness component (Johnston et al. 2010a) message is effective, then the user will be motivated to learn the behavior suggested by the suggested course of action message component. The *exercise* is based on the idea that things that are practiced or repeated are best remembered (Thorndike 1932). Essential to effective practice is the idea of feedback, in order to enable continual improvement. Feedback is also a central component of interactivity (Steuer 1992). The *intensity* principle teaches that the more intensely material is taught, or the more vivid, exciting, and engaging a learning experience is, the better the learning will be retained (Thorndike 1932). Similarly, a state of Flow is intrinsically engaging, vivid, and dramatic. Thus, as explained by these learning principles, interactivity and flow have strong potential to enhance learning.

According to PMT, fear appeals will only prompt protective action if the threat is perceived to be personally relevant (Johnston et al. 2010a; Witte 1992), and the emotions

invoked by a fear appeal must be strong and vivid in order to more effectively convince an individual of the reality of a threat (Johnston et al. 2010a). Additionally, Johnston et al. (2010b) theorized that the efficacy of fear appeals can be increased if they are tailored to the individual. In this light, interactivity and flow have many effects that are relevant to individuals' reception of fear appeals. Specifically, interactivity and flow enhance user motivation, encourage exploratory behavior, and increase perceived relevance (Jiang et al. 2007; Novak et al. 2000; Trevino et al. 1992). We therefore predict that interactive fear appeals will enhance individuals' reception of the fear appeal, lead to heightened appraisals of threat and coping, and lead to greater protective action in the form of stronger passwords. By the same token, we theorize that interactive fear appeals will be more effective than interactivity alone because fear appeals provide educational and motivating information. Because interactivity and flow enhance learning (Jiang et al. 2007; Novak et al. 2000; Trevino et al. 1992), users of an interactive tool will be more receptive to the motivating message of the fear appeal. We therefore hypothesize the following:

H3. Participants in the interactive fear appeal treatment will select stronger passwords than those in the control group.

H4. Participants in the interactive fear appeal treatment will select stronger passwords than those in the static fear appeal treatment.

H5. Participants in the interactive fear appeal treatment will select stronger passwords than those in the interactive password strength meter treatment.

3. Methodology

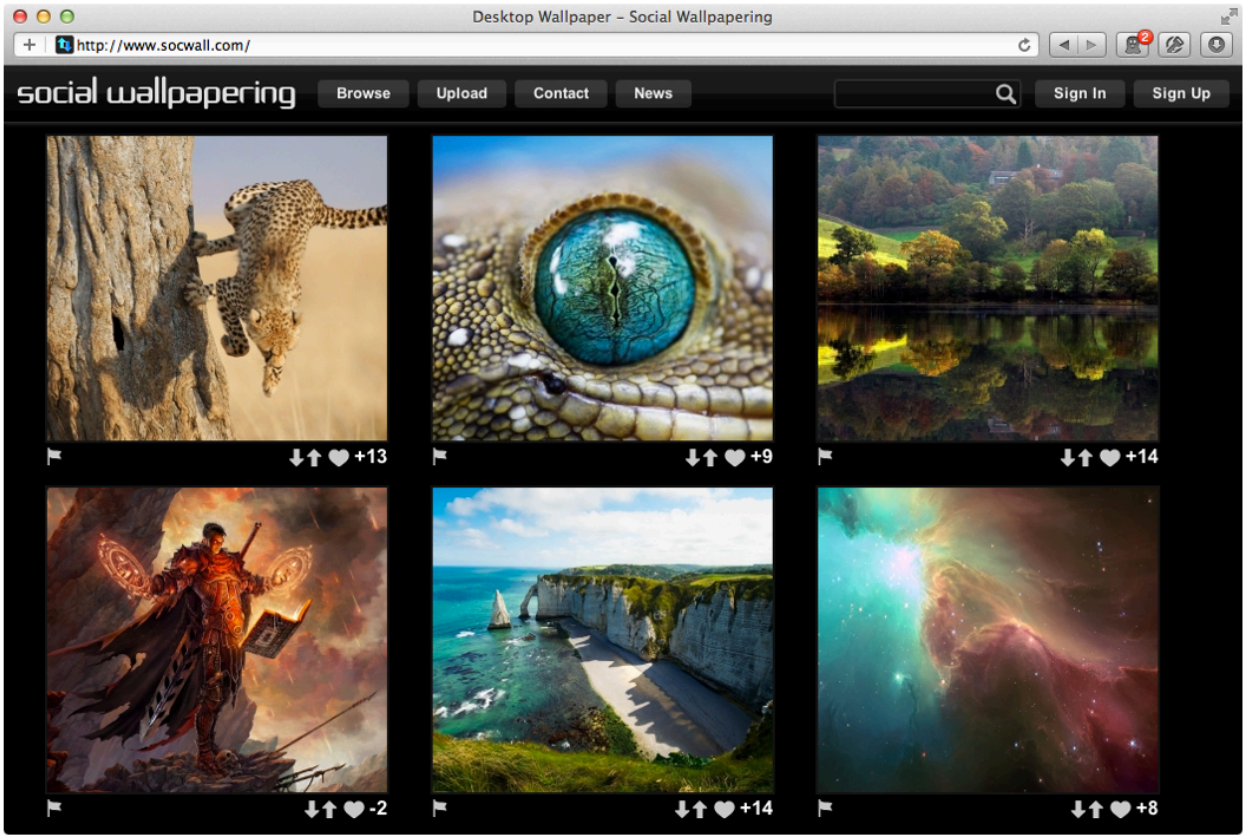
To test our hypotheses, we employed a field experiment involving a website in actual use with a global user base. This choice was made for two related reasons. First, field experiments have the advantage of increased generalizability and realism because they are situated in naturally occurring systems in which dependent and independent variables more closely assume real-world values (Bouchard 1976; Boudreau et al. 2001; Straub et al. 1993). By adopting the field experiment method, we were able to examine the effectiveness of fear appeals and interactivity in influencing users' selection of actual passwords.

Second, we chose the field experiment method to complement previous IS studies on password security that used controlled experiments with university students as subjects (Keith et al. 2009; Zhang et al. 2009). Controlled experiments have the advantage of greater precision and internal validity relative to other research methods, but have the disadvantage of weaker external validity (Dennis et al. 2001; McGrath 1981). Similarly, homogenous samples are useful for falsifying theory, but again come at the cost of external validity (Calder et al. 1981). Our work responds to Zhang et al. (2009), who called for password studies "in field settings which are embedded with richer realism and provide a deeper understanding of the participants involved" (Zhang et al. 2009, p. 174). Thus, we compliment previous work by employing a field experiment involving an actual website in use with a global user base.

We collaborated with Socwall.com, a popular socially driven repository for computer desktop wallpaper that allows users to download, rate, and upload desktop wallpaper images (see Figure 1). Launched in 2006, Socwall.com now receives approximately 10,000 visitors a day, with each visitor viewing an average of 10 pages. This equates to an average of 3 million page views each month, or 30 terabytes of bandwidth. Additionally, Socwall.com is highly ranked in

popular search engines for various terms related to computer desktop wallpapers. In late 2011, Socwall.com began requiring users to create a user account in order to rate submitted wallpaper images. In approximately six months, 3,874 accounts were created for users in 203 countries around the world.

Figure 1. Socwall.com



As part of the Socwall.com account creation process, users were informed of the experimental study and consented to participate, in addition to agreeing to the terms and services of Socwall.com. In doing so, users consented to allow the researchers to analyze their anonymized passwords in plaintext (unencrypted) form. Although users were given the option of signing up without participating in the study, no user chose to do so. Thus, during the

experimental period, the researchers were provided with anonymized passwords for each user account.

3.1 Dependent Variable

The dependent variable for the experiment was the estimated time required for an attacker to guess the password, hereafter referred to as *estimated time to crack* (ETC). Since we had access to the user's plaintext password, we were able to calculate ETC for the actual password submitted when the Socwall.com user account was created. Thus ETC was an objective measure of observed behavior. The following section describes how this variable was derived.

Password strength, in terms of resistance to a brute force guessing attack, is a function of length, composition, and membership in known password dictionaries (Herley 2009). Length and composition determine the size of the search space, which can be calculated as n^L, where n is the size of the character set used to create the password, and L is the length of the password (Keith et al. 2009). For example, if a user's password consists of only of lowercase letters and a length of six characters, the search space would be 27^6 possible passwords, or 387,420,489. If we assume each password in the search space is equally likely (i.e., the distribution of possible passwords is uniform), then on average, the number of guesses required to crack the password is one half of the search space (Keith et al. 2009).

However, password strength is also a function of membership in known password dictionaries. We combined several publically available password dictionaries to determine whether substrings of a password occurred in our password dictionaries. For example, let's assume the password in the above example was "monkey," a password that commonly appears in the top 20 of most frequently observed passwords in real-world datasets (Burnett et al. 2006;

Vance 2010). If an attacker used a password dictionary sorted by frequency of occurrence, then this password would be cracked in less than 20 attempts.

With this background, we calculated ETC using the following steps:

1. Find the number of attempts required to guess dictionary words contained in the password. This was calculated by recursively searching substrings of the password to find the combination of the fewest dictionary words that resulted in the fewest number of unmatched characters left over. If one dictionary word was found in the optimal solution, the number of attempts required to guess the word was its rank in the dictionary based on frequency. If multiple dictionary words were found in the optimal solution, the number of attempts to guess the words was the product of the rank of each word in the dictionary.
2. Calculate the search space of the part of the password not found in the dictionary, calculated as n^L, (Keith et al. 2009).
3. Calculate the number of possible ways that all of the dictionary words could be inserted into the remaining non-matching portion of the password to form the final password. Each word that is "inserted" can be inserted at any position in the non-matching portion, therefore the number of possibilities is (length of non-matching portion)$^{(\text{number of dictionary words})}$.
4. Multiply the results of steps 1–3.

For example, the password "monkey&2d!" would require 2,072,843,136 guesses to crack, given that "monkey" has a rank of 14 in the password dictionary, and the search space of the unmatched part is 37,015,056 (78 characters raised to 4, the length of the unmatched part), and the number of possible ways the unmatched characters could be inserted is 4^1.

Since the goal of a fear appeal is to cause a person to internalize the threat (Witte 1992), and because large numbers can quickly become abstract to people, we presented the number of

attempts to guess in terms of the time required for an attacker to successfully crack the password. To determine the rate of password guessing, we assumed the scenario of an online attack in which the rate of password guessing is limited, since this is the attack that users of Socwall.com would most likely be susceptible. In our testing of open source password cracking tools such as Hydra (http://thc.org/thc-hydra), we were able to consistently able to guess approximately 200 passwords a second for web-based user accounts. We therefore used this rate in our ETC estimation. Thus, ETC for the password "monkey&2d!" is 6.7 seconds (1,330/200), while the ETC for the password "iron&2d!monkey" is 1.6 days (26,884,620/200 seconds).

3.2 Experimental Design

The field experiment consisted of four experimental treatments, which are summarized as a matrix in Table 1. When participants visited the Socwall.com account registration page, the web server randomly assigned one of four experimental treatments: control, password strength meter, static fear appeal, or interactive fear appeal. These four treatments corresponded to whether a treatment involved a fear appeal, interactivity, or both a fear appeal and interactivity. Importantly, for all treatments, no password requirements were imposed (i.e., there was no minimum length or character requirement)—users were free to choose any password they wished.

Table 1. Experimental Design

		Fear Appeal	
		No	Yes
Interactivity	No	Control	Static Fear Appeal
	Yes	Password Strength Meter	Interactive Fear appeal

In the control group (upper-left of the matrix), users received no feedback in creating their password. This is typical of the majority of web site account registrations (Furnell 2007). In the password strength meter treatment (lower-left of the matrix), participants received a password strength meter that interactively measured the strength of the password based on ETC (see Figure 1). This is a best practice of major websites (Furnell 2011).

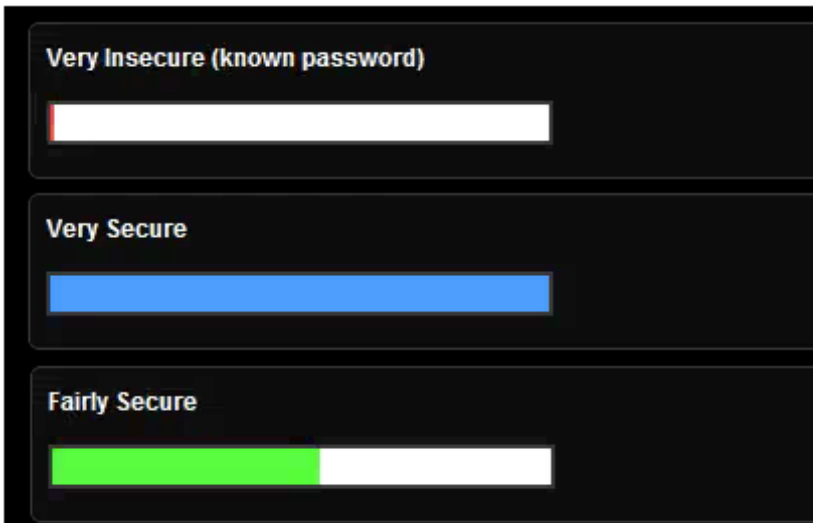


Figure 1. Password strength meter examples

In the static fear appeal treatment (upper-right of the matrix), users were given a fear appeal about password security, similar to those of existing fear appeal studies (Johnston et al. 2010a; Johnston et al. 2010b). Additionally, most major websites provide written guidance for what constitutes a strong password (Furnell 2011). As is typical in both cases, the fear appeal was static—it did not change based on the user's input. The static fear appeal treatment is depicted in Figure 2.

Following Witte (1992), a fear appeal consists of four basic elements within a message: (1) one's susceptibility to the threat (2) the severity of the threat, (3) clear direction for how respond to the threat (self-efficacy), (4) the efficacy of the response (response efficacy). Elements (1) and

(2) attempt to increase perceptions of the threat, whereas (3) and (4) are designed to strengthen the perception of efficacy of the response. Accordingly, we designed our fear appeal to incorporate each of these four elements. In developing our fear appeal, we consulted an expert IS security and fear appeal research.

Finally, in the interactive fear appeal treatment (lower-right of the matrix in Table 1), users received an interactive fear appeal, which changed based on the characters the user entered in the password input field (see Figure 3). The interactive fear appeal was similar to that of the static fear appeal treatment in content and appearance. For example, the severity element of the message ("having your password guessed means a hacker would be able to access other accounts that use a similar password") remained constant regardless of what the user typed. This is because the severity of having one's password compromised is independent of the password selection of the user. However, the three remaining elements of the fear appeal—susceptibility, self-efficacy, and response efficacy—were interactively updated based on the user's input. This was accomplished by recording keystrokes dynamically as typed into the password input field using asynchronous JavaScript and XML (AJAX) techniques (see Figure 3).

First, susceptibility was updated to show the estimated time to track based on the ETC measure described previously. Two seconds after the final keystroke was entered, the server recalculated ETC and updated the user with a new estimate. Thus, the susceptibility component of the message was interactively changed based on the user's response.

Second, the self-efficacy portion of the message, which suggested tips on how to strengthen the password, was updated in a similar manner. The same password recommendations were given as per the static fear appeal treatment. However, the interactive fear appeal showed which

suggestions were met by the user's current password via green checkmarks, and which suggestions were not yet incorporated via red X marks.

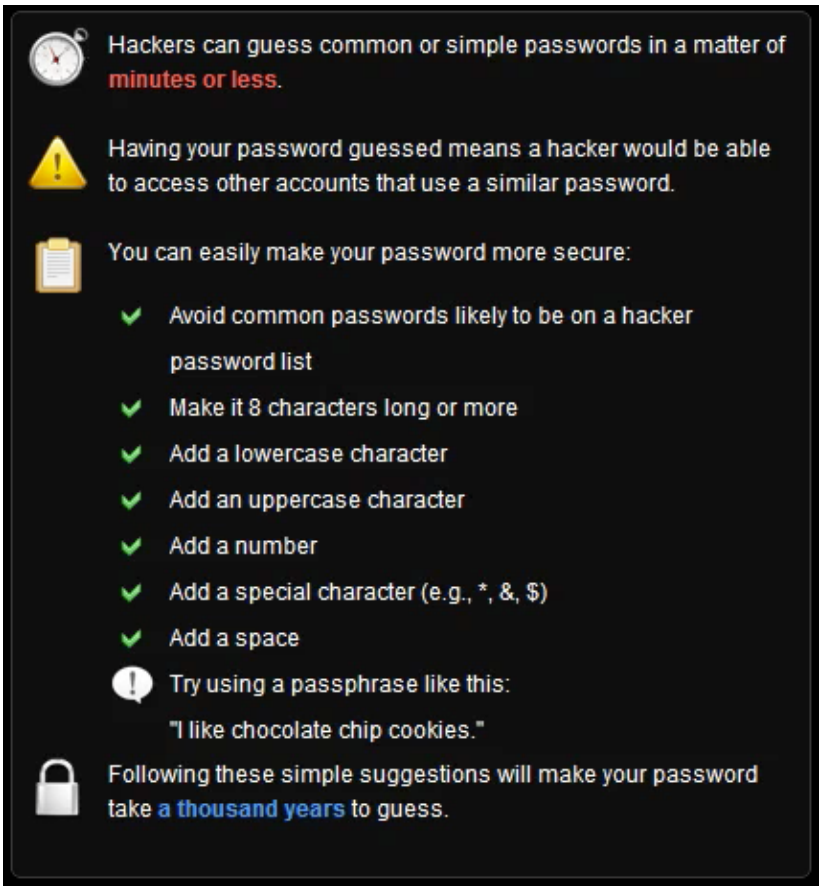


Figure 2. Static fear appeal text

Third, the response efficacy portion of the message calculated the ETC for the user's password if the outstanding suggestions were also applied. This provided the user with an indication of the efficacy of their response if all of the suggestions were followed.

For example, a user's password might include upper and lowercase letters and numbers, but no symbols. In this case, the response efficacy portion of the message would show the estimated time to crack if a symbol were also added to the password. Thus, susceptibility, self-efficacy, and

response efficacy were all interactively updated based on keystrokes the user entered into the password field.

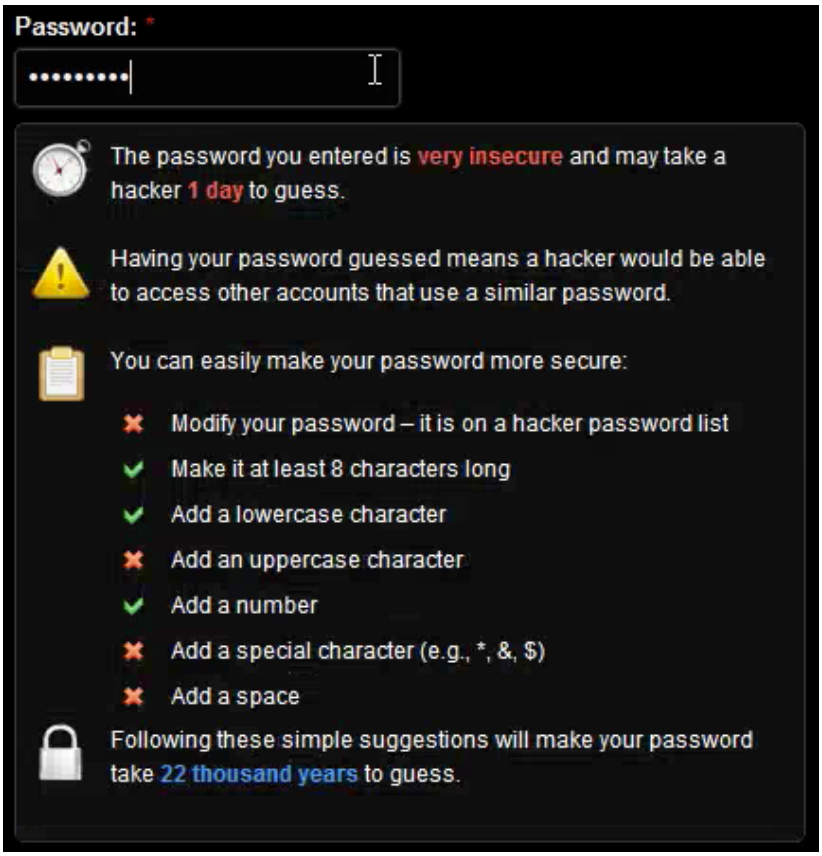


Figure 3. Interactive fear appeal treatment

3.2 Posttest Survey

After the participant selected a password and clicked the "next" button on the registration form, the participant was asked a battery of 21 survey questions for the purpose of statistical controls. These items included demographics (age and gender), as well a question asking the number of security incidents the participant has experienced in the past and his/her general concern with password security. We also asked items to measure perceived severity, perceived susceptibility, self-efficacy, response efficacy, social influence, and response cost (Johnston et al.

2010a). Finally, we measured how interactive the participant perceived the password creation page to be (Jiang et al. 2007). Please refer to Appendix 2 for the items of the posttest survey.

Additionally, after selecting a password and clicking the "Next" button, participants assigned to an experimental treatment were asked a manipulation check question, "Did you notice the password suggestion tip on the previous page?" The manipulation check question ensured that participants in the experimental groups perceived the treatments (Straub et al. 2004).

3.3 Pilot Test Data Collection

We performed a pilot test involving 285 participants to ensure our treatments were functioning correctly and that the manipulations were recognized. Further, the instrument was further clarified and refined. Reliabilities of the survey items were calculated and items were modified or dropped from the instrument as needed.

3.4 Primary Data Collection

Our primary sample consisted of 427 participants. Of these, 73 participants answered the manipulation check question incorrectly (i.e., they didn't notice the password tip suggestion). Thus our final sample N was 354. 71 percent of the sample was male, 14.7 percent female, and 14.4 percent declined to report their gender. In terms of age, 21 percent were age 20 or younger, 33 percent were between 21 and 25, 22 percent were between 26 and 35, and 8 percent were 35 or older. 16 percent declined to report their age. The average number of security incidents experienced was 4.36 (standard deviation of 6.75), and the average level of concern about password security was 3.85 (on a scale from 1–very unconcerned to 7–very unconcerned; standard deviation 1.89). Finally, participants were drawn from 65 different countries, with the highest proportion coming from the US (18 percent); the People's Republic of China (11

percent); and France, Italy, and India (with 4.5 percent each) (see Appendix 1 for a frequency of participants by country).

4. Analysis

We analyzed our control variable data using regression and our hypotheses testing using analysis of covariance (ANCOVA). Both methods require that residuals be normally distributed. However, password strength data is by nature exponential, and therefore the data was highly skewed. For example, adding a single lowercase character to the end of "kscncy" increases the strength of the password 26 times (the character set, or base of the formula n^L). For this reason, we transformed our data by taking the natural log of ETC (hereafter lnETC), which resulted in data that was approximately normal.

4.1 Control Variable Testing

We captured a variety of variables to control for their influence on the dependent variable. In addition to the items collected in the posttest, we also captured objective data for use as control variables. First, as noted previously we recorded the country from which participants accessed Socwall.com to create their account, based on a geographic look-up of each participant's the internet protocol (IP) address, as recorded in Socwall.com's web server access logs. One-way ANOVA analyses showed no significant difference in lnETC either across countries, or for those inside versus outside the United States.

We also measured the amount of time participants took to create their password, as measured by the time between the first entered keystroke and the time when the password was selected using the submit button. This was accomplished by recording keystrokes dynamically as typed using asynchronous JavaScript and XML (AJAX) techniques. Additionally, since participants

likely would iteratively increase the strength of their password based on the feedback they received from their experimental treatment, we captured the number of passwords for the account creation session, which represented the number of passwords participants entered before selecting their final password. For this measure, a "password" was operationalized as the set of characters typed before at least a two-second pause. This captured the commonly observed behavior of a participant entering a password, pausing to read feedback, and then revising the password to incorporate the feedback.

To determine which of these control variables influenced lnETC, we first summed the posttest items (reliability analysis showed that all items exhibited Cronbach's α scores of over .80) to create control variables for our analysis. We then entered all 13 of the above variables (excepting country of origin, since this was already found to be insignificant) into a stepwise regression analysis, with lnETC as the dependent variable. The best resulting regression model included response cost, response efficacy, concern, and number of passwords for session. Together, these variables explained 11 percent of the variance of lnETC. These four variables were subsequently used as control variables for our hypothesis tests.

4.2 Hypotheses Testing

Our hypothesis testing is summarized in Table 2. We used analysis of covariance (ANCOVA) to evaluate our hypotheses so we could control for the effects of the control variables identified in the pervious section. Given the directional nature of our hypothesis, one-tailed tests were used. Although the *F*-statistic generated by the ANOVA family of tests is always one-tailed (i.e., the *F*-statistic is always greater than zero), the test itself is nondirectional (Rutherford 2011). Accordingly, when directional hypothesis tests are appropriate, the *p*-value for the *F*-statistic should be halved, as per an independent samples *t*-test (McNeil et al. 1996).

Contrary to our hypotheses, the static fear appeal treatment did not result in stronger passwords in terms of lnETC as compared with the control group ($F = .819$; $p = .367$). Thus H1 was not supported. Similarly, H2, the password strength meter treatment, was also unsupported ($F = .969$; $p = .765$). Thus, contrary to conventional wisdom, the commonly used password strength meter did not result in stronger passwords.

In contrast, the hypotheses relating to the interactive fear appeal were all strongly supported. Supporting H3, the interactive fear appeal treatment resulted in a substantially higher lnETC measure than the control treatment ($F = 6.707$; $p < .01$). Similarly, the interactive fear appeal treatment resulted in higher time-to-crack than the static fear appeal treatment ($F = 5.946$; $p < .01$) and the password strength meter treatment ($F = 2.734$; $p < .05$), supporting H4 and H5 respectively.

In terms of effect size, the ANCOVA analysis showed that partial eta^2, a measure of explained variance, explained between 1.5 and 3.8 percent of the variance in lnETC for the supported hypotheses. According to Cohen (1988), eta^2 scores of 1, 6, and 14 constitute small, medium, and large effects, respectively. Thus, our observed effect sizes ranged between small

and medium. However, because our lnETC measure is the natural logarithm of the time in seconds to crack, small effect sizes nevertheless indicate a very large practical difference. For example, the smallest effect size observed was for H5, which tested the difference between the interactive and static fear appeal treatments (eta^2 = .015). The mean difference in lnETC between the treatment and control group was 3.1. To put this result in perspective, the median untransformed time-in-seconds difference between groups was 1,560,788,196 seconds, or 49.5 years. Thus, even though partial eta^2 indicated small effect sizes, the practical effects were substantial.

Table 2: Summary of Hypotheses Testing

Between-group Hypotheses	Mean difference	*F*	Supported?
H1. Participants in the static (non-interactive) fear appeal treatment will select stronger passwords than those in the control group.	2.363	.819 n.s.	No
H2. Participants in the interactive password strength meter treatment will select stronger passwords than those in the control group.	.969	.090 n.s.	No
H3. Participants in the interactive fear appeal treatment will select stronger passwords than those in the control group.	5.506	6.707**	Yes
H4. Participants in the interactive fear appeal treatment will select stronger passwords than those in the static fear appeal treatment.	4.537	5.946**	Yes
H5. Participants in the interactive fear appeal treatment will select stronger passwords than those in the interactive password strength meter treatment.	3.139	2.734*	Yes
* $p < .05$; ** $p < .01$; n.s. = not significant.			

5. Discussion

Our results make several important contributions. First, we found that the interactive fear appeal treatment significantly increased password strength by 16–33 percent over the control, static fear appeal, and interactive password meter treatments. This finding is more impressive in

view of the difference in password strength for the untransformed data, in which the smallest advantage for the interactive fear appeal treatment was still an average of 49.5 years of increased password security (H5).

This finding provides strong evidence that interactivity can enhance the efficacy of fear appeals. This is highlighted in the fact that the static and interactive fear appeal treatments had the same appearance and made the same arguments relative to (1) perceived severity, (2) perceived susceptibility, (3) response efficacy, and (4) self-efficacy. The only difference was that the interactive fear appeal customized elements 2–4 based on interaction with the user. This result has implications for a range of applications for fear appeals in IS security domain. For example, it is easy to conceive how fear appeals relating to the threats of malware, phishing, and backup failures could be made more effective by providing interactive messages to the user. Further, because interactivity adds an element of playfulness and learning to the warning (Novak et al. 2000), interactive fear appeals gain an element of enjoyment and knowledge discovery.

Second, we found that interactivity alone, in the form of an interactive password strength meter, does not significantly increase password security. This finding is surprising given the prevalence of password strength meters in actual use (Furnell 2011). This finding suggests that interactivity should be coupled with information about the severity and susceptibility of threats, as well as the efficacy of the user's response. Without this information, interactivity provides flash without much supporting substance. Our results suggest that elements of fear appeals should be incorporated into interactive content, such as password strength meters, in order to help users to better understand the implications of their actions.

Third, our interactive fear appeal treatment essentially tests a prototype of a more effective password strength meter that makes use of fear appeals to add weight to the interactive feedback provided to the user. Our findings suggest that by making relatively minor changes to existing password creation forms, practitioners may encourage their users to substantially increase the strength of their passwords.

5.1 Limitations

Our results need to be considered in light of the following limitations. First, whereas field experiments provide greater external validity due to their situation in real-world contexts, this comes at the expense of greater precision and control (McGrath 1981). Similarly, our heterogeneous global sample likely increased error variance making significant effects more difficult to detect. It may be that in a laboratory setting, the effects for the fear appeal and interactive password meter treatments would be significant.

Second, although our experiment involved an actual website in use, the risk of having one's password cracked was low given that Socwall.com didn't store sensitive information about the user. This was reflected in participants' average reported concern for the security of their password of 3.85 (on a scale from 1–very unconcerned to 7–very unconcerned; standard deviation 1.89). Results may likely be different for an online bank site for which high value information is protected by passwords. However, the fact that participants were neutral in their concern for password security does not invalidate our results. On the contrary, the finding that participants in the interactive fear appeal group significantly increased the security of their passwords is even more compelling, given participants' moderate concern.

6. Conclusions

Fear appeals are a venerable form of user education and have been scientifically studied for over 60 years (Hovland et al. 1953). However, the content fear appeals—whether in text, audio, or video form—has largely remained static. This research contributes by showing that interactivity, afforded by computer-mediated communication, can significantly enhance the effectiveness of fear appeals. We conducted a field experiment involving an active website in actual use, 354 participants in 65 countries. The results showed that the interactive fear appeal treatment substantially increased password security by at least 49.5 years on average, over the control, static fear appeal, and interactive password strength meter treatments. These findings have broad implications for the use of fear appeals in information security.

7. References

Adams, A., and Sasse, M. A. "Users are not the enemy," *Communications of the ACM* (42) 1999, pp 40-46.

Bouchard, T. "Field research methods: Interviewing, questionnaires, participant observation, systematic observation, unobtrusive measures," *Handbook of industrial and organizational psychology*) 1976, pp 363-413.

Boudreau, M.-C., Gefen, D., and Straub, D. W. "Validation in Information Systems Research: A State-of-the-Art Assessment," *MIS Quarterly* (25) 2001, pp 1-16.

Brown, A. L. "The Advancement of Learning," *Educational Researcher* (23:8) 1994, pp 4-12.

Burnett, M., and Kleiman, D. "Perfect Passwords: Selection, Protection, Authentication,") 2006, pp 53-59.

Calder, B., Phillips, L., and Tybout, A. M. "Designing research for application," *Journal of Consumer Research* (8) 1981, pp 197-207.

Csikszentmihalyi, M. *Flow: The psychology of optimal experience*, (First ed.) Harper Perennial, 1990.

Dennis, A. R., and Valacich, J. S. "Conducting Experimental Research in Information Systems," *Communications of the Association for Information Systems* (7) 2001, pp 1-41.

Florencio, D., and Herley, C. "A large-scale study of web password habits," in: *Proceedings of the 16th international conference on World Wide Web - WWW '07*, ACM Press, New York, New York, USA, 2007, p. 657.

Forget, A., Chiasson, S., van Oorschot, P., and Biddle, R. "Persuasion for Stronger Passwords: Motivation and Pilot Study," H. Oinas-Kukkonen, P. Hasle, M. Harjumaa, K. Segerståhl and P. Øhrstrøm (eds.), Springer Berlin / Heidelberg, 2008, pp. 140-150.

Furnell, S. "An assessment of website password practices," *Computers & Security* (26) 2007, pp 445-451.

Furnell, S. "Assessing password guidance and enforcement on leading websites," *Computer Fraud & Security* (2011) 2011, pp 10-18.

Ghani, J. "Flow in human-computer interactions: test of a model," Human Factors in Information Systems, Ablex Publishing Copr., Norwood, NJ, USA, 1995, pp. 291 - 311.

Herath, T., and Rao, H. R. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information* (18) 2009, pp 106-125.
Herley, C. "So long, and no thanks for the externalities: the rational rejection of security advice by users," *Proceedings of the 2009 workshop on New security*) 2009.
Hovland, C., and Janis, I. "Communication and persuasion; psychological studies of opinion change.,") 1953.
Imperva "Consumer Password Worst Practices," Imperva Application Defense Center, 2010, pp. 1-5.
Jiang, Z., and Benbasat, I. "Research Note Investigating the Influence of the Functional Mechanisms of Online Product Presentations," *Information Systems Research* (18) 2007, pp 454-470.
Johnston, A. C., and Warkentin, M. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34) 2010a, pp 549-566.
Johnston, A. C., and Warkentin, M. "Persuasive Communication Strategies: Assessing the Fit Between Organizational Identification and Fear Appeal Message Orientation," The Dewald Roode Information Security Workshop, IFIP WG 8.11/11.13, 2010b, pp. 128-154.
Keith, M., Shao, B., and Steinbart, P. "A Behavioral Analysis of Passphrase Design and Effectiveness," *Journal of the Association for Information Systems* (10) 2009.
McGrath, J. E. "Dilemmatics: The Study of Research Choices and Dilemmas," *American Behavioral Scientist* (25) 1981, pp 179-210.
McKeachie, W. J. "The Decline and Fall of the Laws of Learning," *Educational Researcher* (3:3) 1974, pp 7-11.
McNeil, K. A., Newman, I., and Kelly, F. J. "Testing Research Hypotheses With the General Linear Model,") 1996, p 372.
Morris, R., and Thompson, K. "Password security: A case history," *Communications of the ACM* (22) 1979, pp 594-597.
Novak, T., Hoffman, D., and Yung, Y. "Measuring the Flow Construct in Online Environments: A Structural Modeling Approach," *Marketing Science* (19) 2000, pp 22 - 44.
Rogers, R. "{Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation}," *Social psychophysiology*) 1983, pp 153 - 176.
Rogers, R. W. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* (91) 1975, pp 93-114.
Rutherford, A. "Anova and Ancova: A Glm Approach,") 2011, p 360.
Steuer, J. "Defining Virtual Reality: Dimensions Determining Telepresence," *Journal of Communication* (42) 1992, pp 73-93.
Straub, D., Boudreau, M.-C., and Gefen, D. "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems* (13) 2004, pp 380-427.
Straub, D., Carlson, P., and Jones, E. "Deterring cheating by student programmers: A field experiment in computer security," *Journal of Management Systems* (5) 1993, pp 33-48.
Thorndike, E. L. "The fundamentals of learning," Teachers college, Columbia university, New York, 1932, pp. 1 online resource (xvii, 638 p.).
Trevino, L. K., and Webster, J. "Flow in Computer-Mediated Communication: Electronic Mail and Voice Mail Evaluation and Impacts," *Communication Research* (19) 1992, pp 539-573.
Trusteer "Reused Login Credentials," Trusteer, New York, New York, USA, 2010.
Vance, A. "If Your Password is 123456, Just Make It HackMe," in: *New York Times*, 2010.
Vance, A., Siponen, M., and Pahnila, S. "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49) 2012, pp 190-198.
Weirich, D., and Sasse, M. A. "Pretty good persuasion," in: *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*, ACM Press, New York, New York, USA, 2001, p. 137.
Witte, K. "Putting the fear back into fear appeals: The extended parallel process model," *Communications Monographs*) 1992.

Workman, M., Bommer, W., and Straub, D. "Security lapses and the omission of information security measures: A threat control model and empirical test," *Computers in Human Behavior* (24) 2008, pp 2799-2816.

Yan, J., Blackwell, A., Anderson, R., and Grant, A. "Password memorability and security: empirical results," *IEEE Security & Privacy Magazine* (2) 2004, pp 25-31.

Zhang, J., Luo, X., Akkaladevi, S., and Ziegelmayer, J. "Improving multiple-password recall: an empirical study," *European Journal of Information Systems* (18) 2009, pp 165-176.

Zviran, M., and Haga, W. J. "Password security: an empirical study," *Journal of Management Information Systems* (15) 1999, pp 161-185.

Appendix 1. Frequency of Experimental Participants by Country

Country	# of Participants	Country	# of Participants
United States	71	Hong Kong	2
China	47	New Zealand	2
France	22	Switzerland	2
India	19	Ukraine	2
Germany	18	Åland Islands	1
Italy	18	Algeria	1
Brazil	17	Austria	1
Canada	16	Bangladesh	1
Taiwan	16	Bosnia-Herzegovina	1
Mexico	15	Costa Rica	1
Great Britain	11	Czech Republic	1
Argentina	8	Egypt	1
Indonesia	7	El Salvador	1
Spain	7	Finland	1
Russian Federation	6	Greece	1
Australia	5	Guernsey	1
Iran	5	Hungary	1
Serbia	5	Iceland	1
Belgium	4	Israel	1
Colombia	4	Kazakhstan	1
Romania	4	Lithuania	1
Ecuador	3	Macedonia	1
Japan	3	Mauritius	1
Malaysia	3	Myanmar	1
Netherlands	3	Norway	1
Pakistan	3	Peru	1
Philippines	3	Portugal	1
Poland	3	Puerto Rico	1
Saudi Arabia	3	Singapore	1
Albania	2	South Africa	1
Asia/Pacific Region	2	Sri Lanka	1
Belarus	2	Tanzania	1
Chile	2	Uganda	1
Croatia	2	Venezuela	1
Denmark	2	Vietnam	1

Appendix 2. Posttest Instrument

Construct	Item	Item Text	Source
Severity	severity1	If my password was stolen, the consequences would be severe	Allen and Warkentin 2010b
	severity2	If my password was stolen, the consequences would be serious	Allen and Warkentin 2010b
	severity3	If my password was stolen, the consequences would be significant	Allen and Warkentin 2010b
Susceptibility	suscept1	My password is at risk of being stolen	Allen and Warkentin 2010b
	suscept2	It is likely that my password will be stolen	Allen and Warkentin 2010b
	suscept3	It is possible that my password will be stolen	Allen and Warkentin 2010b
Self-efficacy	selfeff1	Using a hard-to-guess password is easy to do	Allen and Warkentin 2010b
	selfeff2	Using a hard-to-guess password is convenient to do	Allen and Warkentin 2010b
	selfeff3	I am able to use a hard-to-guess without much effort	Allen and Warkentin 2010b
Response efficacy	responseeff1	Using a hard-to-guess password works for protection	Allen and Warkentin 2010b
	responseeff2	Using a hard-to-guess password is effective for protection	Allen and Warkentin 2010b
	responseeff3	By using a hard-to-guess password, my password is more likely to be protected	Allen and Warkentin 2010b
Social Influence	social1	People who influence my behavior think that I should use a hard-to-guess password	Allen and Warkentin 2010b
	social2	People who are important to me think that I should use a hard-to-guess password	Allen and Warkentin 2010b
Response Cost	responsecost1	Using a hard-to-guess password would be time consuming	Allen and Warkentin 2010b
	responsecost2	Using a hard-to-guess password would make my life more difficult	Allen and Warkentin 2010b
	responsecost3	Using a hard-to-guess inconveniences my life	Allen and Warkentin 2010b
Interactivity	interact1	I am able to interact with Socwall's password creation web page.	Jiang and Benbasat (2007)
	interact2	Socwall's password creation web page interactively responds to my input.	Jiang and Benbasat (2007)
	interact3	Socwall's password creation web page is interactive	New item
Concern	concern	To what extent have you been concerned with password security in the past?	New item
Past incidents	incidents	Roughly how many security incidents have you experienced? For example, hackers sending you viruses or someone accessing your online accounts (e.g., Yahoo Mail or Facebook) without your permission).	New item