Broken Windows, Bad Passwords: Influencing Secure User Behavior via Website Design

Completed Research Paper

G. Mark Grimes
University of Arizona
mgrimes@cmi.arizona.edu

Jim Marquardson
University of Arizona
jmarquardson@cmi.arizona.edu

Jay F. Nunamaker, Jr.
University of Arizona
jnunamaker@cmi.arizona.edu

Abstract

The broken windows theory of crime deterrence suggests that features in a community such as broken windows, graffiti, and petty crime send signals that criminal behavior is accepted as the norm. We extend the broken windows theory to information security by suggesting that poor web site design sends signals that insecure behavior is the norm. Extending the theory of planned behavior, we hypothesize that visual appeal and trust influence subjective norms such that users on a low quality web site will exhibit reduced intentions and behaviors of security. In a laboratory experiment we manipulate web site quality while participants create user accounts. Password entropy and self-reported password strength are compared for accounts created on the high and low quality sites. Our findings suggest that organizations may be able to promote secure behavior by creating systems that are high in visual appeal and trustworthiness.

Keywords

Security, Passwords, Theory of Planned Behavior

Introduction

Throughout the 1970's and 1980's, violent crime in New York City was a major and growing problem, peaking in 1990 with 1,181 incidents of violent crime per 100,000 inhabitants – over 61% higher than the national average (The Disaster Center 2013). To combat this trend, criminologist George Kelling was hired by the New York Transit Authority in 1985 to reduce violent crime in New York City's subway system. Throughout the late 1980's and early 1990's, Kelling's approach was to focus on minor crimes such as graffiti, fare-beating, and aggressive panhandling rather than directly addressing more serious or violent crimes (Gladwell 2006 pp. 140–151). This approach, known as the broken windows theory of crime deterrence, works on the premise that features such as broken windows, graffiti and petty crime send signals to individuals that criminal behavior is acceptable. By rigorously enforcing laws related to petty crimes, the signal is sent that criminal behavior is not the norm and criminals, whether opportunistic or professional, will be less likely to engage in undesirable behavior (Harcourt 1998; Wilson and Kelling 1982). We suggest that the broken windows theory applies not only to criminal behavior, but to any situation in which the environment may influence what behavior individuals deem acceptable.

In this paper, we explore the application of the broken windows theory of crime deterrence to information systems security to answer the following research question: *Does perceived web site quality influence intentions and practice of secure behavior?*

It has been suggested that elements of a web site's design send signals to users regarding the quality, credibility, and care of the site. For example, broken links on a web site may be interpreted by users as a signal that "the site has been neglected or that the site was not carefully created in the first place" (Fogg 2003 p. 723). We hypothesize that these signals influence users' subjective norms of acceptable behavior for interaction with the web site, thereby influencing their intentions of secure behavior. Web sites that send signals of low quality and credibility – analogous to broken windows in an abandoned warehouse – prime users to behave less securely. We propose that by carefully crafting the signals a web site is sending by using good design practices, users will behave more securely than when elements of good design are neglected. In this way, organizations may be able to encourage secure behavior with minimal cost and impact to users.

Users are often cited as the weakest link in information systems security (Boss et al. 2009). Persuading users to behave securely is an important issue for information systems and significant research has been conducted to identify effective ways to influence user security behavior. Security policies (Bulgurcu et al. 2010; D'Arcy et al. 2009), training (Charoen et al. 2008; Ives et al. 2004), and reminders (Jenkins and Durcikova 2013; Jenkins et al. 2013) are three methods that are commonly used for influencing secure behavior. While each of these methods positively influences secure user behavior, they also require end users to expend additional effort to carry out the secure behavior. For policies to work, users must be familiar with the policies, believe in the efficacy of the policies and consciously adhere to them (Bulgurcu et al. 2010). Security training may be time consuming and expensive for a company to implement, and users must take time from their schedule to participate in the training, often on multiple occasions. Likewise, reminders may be intrusive and may have a negative impact on the user experience or may simply be ignored by users. An ideal aide to influence secure behavior would subconsciously influence behavior and require no additional action from the user. While there are many aspects of secure user behavior, in this paper we focus on one specific aspect – the creation of strong passwords.

Building on the theory of planned behavior (TPB; Ajzen 1991), we suggest that visual and trust elements of a web site will influence the subjective norms of secure behavior for users of the site. TPB posits that changes in subjective norms, along with attitudes and perceived behavioral control, lead to a change in intentions and ultimately a change in behavior. The balance of this paper provides a review of literature relevant to creating websites high in visual appeal and trust, describes a laboratory experiment used to test our hypotheses, and discusses our results and the implications of our findings.

Literature Review

Significant research in the area of web site design provides a basis for this work. In this section, we discuss some of the factors that have been found to influence visual appeal and trust in web sites.

Prominence-interpretation theory (Fogg 2003) suggests that people assess credibility online by noticing something (prominence) and making a judgment about it (interpretation). If one or the other does not happen, no assessment of credibility is made. Therefore, many of the elements proposed in the literature on web site quality are naturally interrelated and dependent on one another. For example, Alsudani and Casey (2009) find that dominant images (prominence) leads to higher ratings of credibility, however, as Hynes (2009), Lowery et al. (2014) and Belanger (2002) point out, the prominent symbols must have a positive interpretation to increase credibility. Table 1 presents a brief overview of some of the features that impact trust or visual appeal of web sites.

Just as broken windows and graffiti send signals to people regarding the norms for behavior in that environment, we suggest that website visual appeal and trust send signals to users regarding website behavioral norms. We expect that sites with high visual appeal and trust will trigger norms related to security best practices.

Citation	Features	Influence on Trust or Visual Appeal
Abbasi et al. 2010	Web page text, URL attributes and links	Fraudulent sites contain incorrect spelling/grammar, have more complex URLs and tend to have fewer working links
Alsudani and Casey 2009	Balance, harmony, contrast dominance and image dominance	Contrast dominance and image dominance lead to higher ratings of credibility
Bauerly and Liu 2008	Symmetry and number of elements	High complexity and low symmetry of elements leads to lower aesthetic appeal
Belanger et al. 2002	Symbols of security	Security symbols increase trustworthiness
Bonnardel et al. 2011	Color	Blue and Orange sites were considered more "usual" and received higher user appreciation than grey sites
Cyr 2008	Navigation, visual and information design	Navigation, visual and information design all positively related to trust and satisfaction
Cyr et al. 2010	Color	Increased color appeal results in greater trust and greater satisfaction
Fogg 2003	Prominence and interpretation	Highly prominent elements with positive interpretation lead to higher credibility
Fogg et al. 2003	18 elements including: design look, structure, information focus, name recognition, tone of writing and functionality	Sites with good design, organization, functionality and information rated as more credible. Name recognition and formal tone lead to higher ratings of credibility
Hynes 2009	Color and Logos	Globe logo and blue/brown associated with protection, stability and reliability
Lowry et al. 2014	Logo and website design	Consistency, stability, reassuring colors and good design increase trustworthiness
Robins and Holmes 2008	Aesthetic qualities	High aesthetics lead to higher ratings of credibility

Table 1: Site Features and impact on user perception

Research Model

We use TPB to explore why individuals carry out security behaviors. TPB suggests that three constructs influence behavioral intention: behavioral attitude, subjective norms, and perceived behavioral control (Ajzen 1991). Each of the constructs in TPB has features that are stable over time and features than may be influenced by situational factors. For example, one's overall feeling of perceived behavioral control for secure behavior may be high (high self-efficacy), however, they may feel a low level of behavioral control in certain situations (low response-efficacy). In the current study, we suggest that web site quality, operationalized here as visual appeal and trust, will not affect attitudes nor perceived behavioral control, but will have a positive relationship with subjective norms (Figure 1).

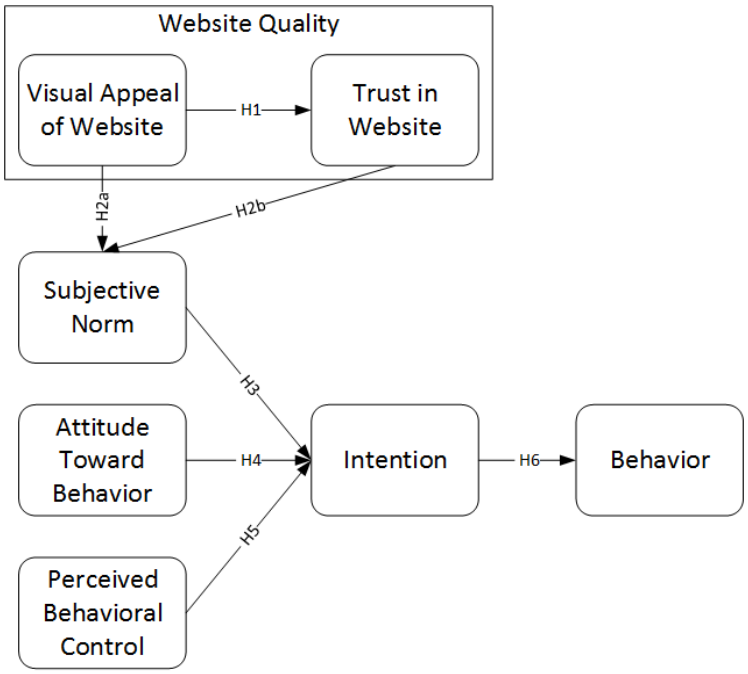

Figure 1: Proposed research model (adapted from Ajzen 1991)

We therefore propose the following hypotheses:

H1: Trust will be positively influenced by visual appeal of a web site

H2: Higher (a) visual appeal and (b) trust of a web site will positively influence subjective norms of security

H3: Subjective norms of security will be positively related to security intentions

H4: Attitudes regarding security will be positively related to security intentions

H5: Perceived behavioral control of security will be positively related to security intentions

H6: Intentions of secure behavior will be positively related to secure behavior as measured by password entropy

Methodology

A laboratory experiment was conducted at a large public university in the Southwestern United States. 189 students (100 male) from a junior level MIS class participated in exchange for class credit. Sixteen participants were removed from the sample for providing invalid survey responses, leaving 173 participants for the analysis. Upon arriving at the lab, participants were instructed to create an account on an experiment management website similar to other systems used in the college for students to register for experiments. The stated purpose of creating an account was so participants could log in at a future date (in 5-7 days) to complete the second part the experiment. The experiment following the account creation, including the second part, are unrelated to this study and are discussed in no further detail here. Since participants knew they would have to log in again in the future to complete the experiment, this incentivized them to use a password they would be able to remember rather than using a "throw away" password for the account. To discourage password reuse, a fear appeals message was used to instruct participants to not reuse a password they have used on other systems (Herath and Rao 2009; Jenkins et al. 2013; Johnston and Warkentin 2010) (Figure 2).

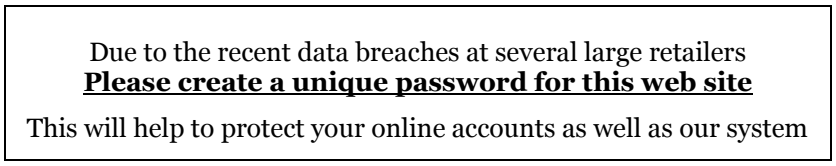

Figure 2: Unique password solicitation

While creating their account, participants were exposed to either a high quality site (Figure 3) or a low quality site (Figure 4). Several attributes suggested by the research in Table 1 were used to manipulate website quality as described in Table 2.

Feature	High Quality Manipulation	Low Quality Manipulation
Symbols of security (Belanger et al. 2002)	RSA and Verisign logos present, the word "secure" in the name of the system	No symbols of security
Quality of images (Alsudani and Casey 2009)	Visually appealing, dominant, high quality images	Antiquated web site images with warped aspect ratio
Symmetry of page (Bauerly and Liu 2008)	Appealing symmetrical layout	Amateurish asymmetric layout
Links (Abbasi et al. 2010; Lee and Kozar 2006)	Working links for help, contact and about us	Broken links for help, contact and about us, broken image link
Grammar and spelling (Abbasi et al. 2010)	Proper use of grammar and no spelling mistakes	Incorrect grammar and misspelled words
Color (Bonnardel et al. 2011; Bottomley and Doyle 2006; Cyr et al. 2010; Hynes 2009)	Use of bold, contrasting colors (red, blue and white)	Use of unappealing, low contrast colors (yellow, grey and white)
Logos (Hynes 2009; Lowry et al. 2014)	University logo a exudes an air of quality and research	Logo suggests an incomplete web site
Website URL (Abbasi et al. 2010)	Short and simple URL hosted on a university server	Long, complex URL including an IP address and cryptic words

Table 2: Manipulations of site quality

Figure 3: High quality site

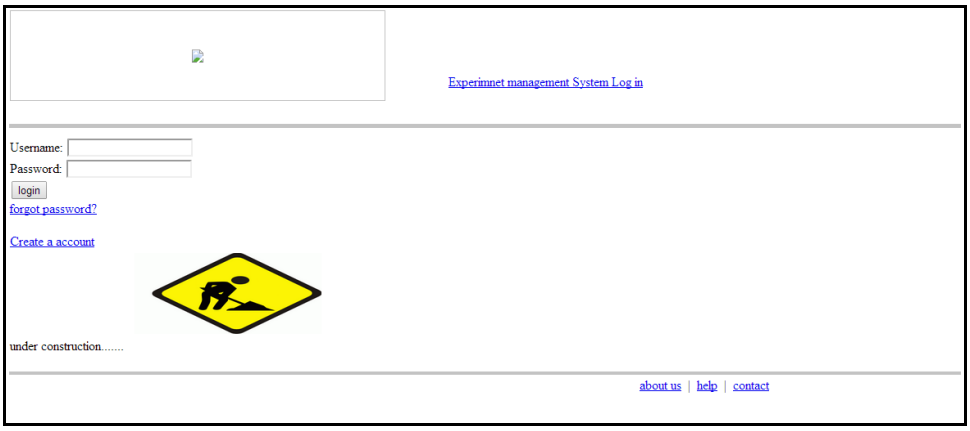

Figure 4: Low quality site

Password entropy was used to operationalize secure behavior. Entropy is defined as the amount of randomness a secret contains based on the length and potential character set and is usually stated in bits (Burr et al. 2011). While bits of entropy is a statistical measure of randomness formally stated for random strings as $Log_2(b^n)$ where b is the size of the character set and n is the length of the string, calculating entropy for passwords created by humans is significantly more complex as people typically generate passwords that roughly conform to rules of word composition (Burr et al. 2011). Therefore, the effective entropy of human generated passwords is significantly lower than for random strings (Shannon 1948). For these reasons, calculations of entropy for user-generated passwords are approximate at best and may follow a wide range of criteria. To calculate the effective password entropy of the participant generated passwords, an open source JavaScript software called passchk was used to estimate the entropy of each password (Akins 2014).

During the account creation process, the participant's password was encrypted with SHA-256 encryption and associated with the user account to enable them to log in again in the future. A clear text version of the password was temporarily stored in a separate database in order to calculate the password entropy,

however, the clear text password was not directly associated with the user. Only the password entropy value was associated with the participant. At no time were clear text passwords associated with any personally identifiable information of the participants and all passwords were deleted from the system as soon as practical.

Results

Survey items for subjective norms, attitudes, perceived behavioral self-efficacy, and intentions were adapted from Anderson and Agarwal (2010). Items for website visual appeal and website trust were taken from Loiacono et al. (2002). An exploratory factor analysis was used to verify the measurement model. Structural equation modelling (SEM) was used to test the research hypotheses. R version 3.0.2 and the lavaan package were used to conduct the analysis (Rosseel 2012).

We assessed the constructs for convergent validity, reliability, and discriminant validity. One perceived behavioral control item was dropped because it loaded significantly poorer than the remaining four items. All of the remaining items loaded above the recommended 0.60 level (Bagozzi and Yi 1988). See Table 3 for the detailed loadings and reliability. Scales are typically regarded as reliable if the Cronbach's alpha is above 0.70 and the AVE is above 0.50 (Bagozzi and Yi 1988; Straub et al. 2004). All latent factors met the criteria for reliability. Discriminant validity can be observed in Table 3 and Table 4. Discriminant validity is demonstrated in part when items load on a single construct and no other constructs. No item loads on an unrelated factor more than 0.20. In addition, the square root of AVE of the constructs should be higher than the inter-construct correlations. All latent constructs satisfy these criteria for discriminant validity. Having established the validity and reliability of our model, we proceeded with the analysis.

Constructs/items		Loadings					
		1	2	3	4	5	6
Subjective Norm	SN1	**0.82**	0.04	-0.08	0.03	-0.10	0.04
Alpha=0.82	SN2	**0.71**	0.06	0.03	0.02	-0.01	-0.01
AVE=0.65	SN3	**0.82**	-0.05	0.00	-0.04	0.10	-0.01
Perceived Behavioral Control	PBC1	0.01	**0.70**	0.10	0.06	-0.01	0.01
Alpha=0.82	PBC2	0.00	**0.67**	0.19	-0.02	0.03	0.06
AVE=0.69	PBC3	0.04	**0.74**	-0.04	-0.04	-0.07	-0.03
	PBC4	-0.01	**0.77**	-0.13	0.00	0.06	-0.06
Attitude	ATT1	-0.10	0.06	**0.84**	-0.01	-0.01	0.01
Alpha=0.79	ATT2	0.00	0.08	**0.70**	-0.01	0.06	0.05
AVE=0.67	ATT3	0.12	-0.10	**0.65**	0.10	-0.06	-0.07
Intention	INT1	-0.02	0.01	0.05	**0.90**	-0.06	0.02
Alpha=0.81	INT2	-0.10	0.09	-0.10	**0.69**	-0.01	0.03
AVE=0.55	INT3	0.14	-0.08	0.07	**0.69**	0.12	-0.05
Website Trust	WTR1	-0.03	0.02	-0.01	0.02	**0.72**	0.05
Alpha=0.84	WTR2	0.02	0.03	-0.03	-0.01	**0.80**	0.04
AVE=0.65	WTR3	0.00	-0.03	0.03	-0.02	**0.86**	-0.07
Website Visual Appeal	WVA1	-0.06	-0.04	0.05	0.04	-0.04	**0.98**
Alpha=0.96	WVA2	0.02	0.06	-0.06	0.05	-0.01	**0.94**
AVE=0.93	WVA3	0.08	-0.04	0.02	-0.08	0.08	**0.89**

Table 3: Latent factor loadings, Cronbach's Alpha and AVE of measurement instrument

	Mean	SD	1	2	3	4	5	6	7
1. Attitude	6.09	0.78	*0.82*						
2. Website Trust	4.98	1.18	0.08	*0.80*					
3. Website Visual Appeal	4.12	1.46	0.15	0.52	*0.97*				
4. Subjective Norms	4.89	1.18	0.50	0.17	0.38	*0.81*			
5. Secure Behavior Intentions	5.62	0.92	0.58	0.36	.020	0.46	*0.74*		
6. Perceived Behavioral Control	5.79	0.80	0.42	0.10	0.18	0.23	0.38	*0.83*	
7. Password Entropy	34.79	13.19	-0.02	-0.01	-0.01	-0.02	-0.04	-0.02	NA
Notes: Diagonal elements are the square root of the AVE values; off-diagonal elements are correlations									

Table 4: Descriptive statistics, correlation matrix, and AVE

Hypothesis Testing Results

A manipulation check was performed to validate that the experimental treatment had the intended effect. As expected, participants reported on average significantly greater website visual appeal in the high quality condition (M=4.94, SE=0.11) than in the low quality condition (M=3.32, SE=0.15), t(163.07)=−8.80, p<0.001). Likewise, participants reported higher trust in the high quality site (M=5.36, SE=0.11), than in the low quality site (M=4.61, SE=0.13), t(163.42)=−4.38, p<0.001).

Initial model testing showed that some improvements to the model were necessary. Modification indices suggested a path from website trust to security intentions, a path from website visual appeal to intention, and residual covariances between select items for perceived behavioral control, attitudes, website visual appearance, and intentions. Four indices were used to estimate goodness of fit: chi-square (χ^2), relative chi-square (χ^2/df), comparative fit index (CFI), normed fit index (NFI), and root mean square error of approximation (RMSEA) (Holbert and Stephenson 2002). To demonstrate good fit, the χ^2 statistic should be nonsignificant at the 0.05 level, CFI and NFI should be greater than or equal to 0.95, and RMSEA should be .05 or less (Hooper et al. 2008). It has been noted that NFI tends to report poorer fit even for good fitting models for sample sizes less than 200, which is the case in this study (Bentler 1990). The final model achieved a good fit (χ^2=181.18, df=152, p>0.05, χ^2/df=1.19, *CFI*=0.98, *NFI*=0.91, *RMSEA*=0.03).

As illustrated in Figure 5, our model explains 27 percent of the variance in website trust, 15 percent of the variance in subjective norms, 49 percent of the variance in intention to create secure passwords and 0 percent of the variance in actual behavior as measured by password entropy.

As proposed in H1, a significant positive relationship was found between visual appeal and trust. Visual appeal was found to have a significant positive effect on subjective norms, thus supporting H2a. Contrary to our hypothesis, however, trust did not have a statistically significant relationship with subjective norms, but rather influenced intentions directly. Therefore, H2b was not supported. As expected from the TPB model, subjective norms, attitudes and perceived behavioral control were found to have statistically significant relationships with intentions, supporting H3, H4 and H5. Finally, the relationship between intentions and observed behavior (H6) was not found to be significant. These results are summarized in Table 5. Though not originally hypothesized, the path from website trust to intention was significant (β=0.42, SE=0.113, p<0.001). The added path from website visual appeal to intention was not significant (β=-0.221, SE=0.122, p>0.05).

A follow-up survey of participants was conducted to investigate a) whether the participants reused a password they have used on other web sites and b) their perception of the strength of their password. We suggest that perception of strength may be a more appropriate measure of behavior than password entropy, since participants may have thought they were creating a strong password but did not have the skills to do so (Furnell 2007). In total, 172 participants responded to the follow up survey. Of those that

responded only 39 (18 in the high quality condition) indicated that they created a unique password for the experimental web site. Of those that created a unique password for the site, participants in the high quality condition rated their passwords using a ten point scale as significantly stronger (M=5.44, SD=2.19) than those in the low quality condition (M=3.83, SD=1.84), (t(33.37)=2.40, p=0.011). This effect suggests that a) participants that reused a password may have simply reused a password out of habit with no regard to their security intentions and b) for many participants their perceived strength of the password they created was not reflected in the actual strength of their password.

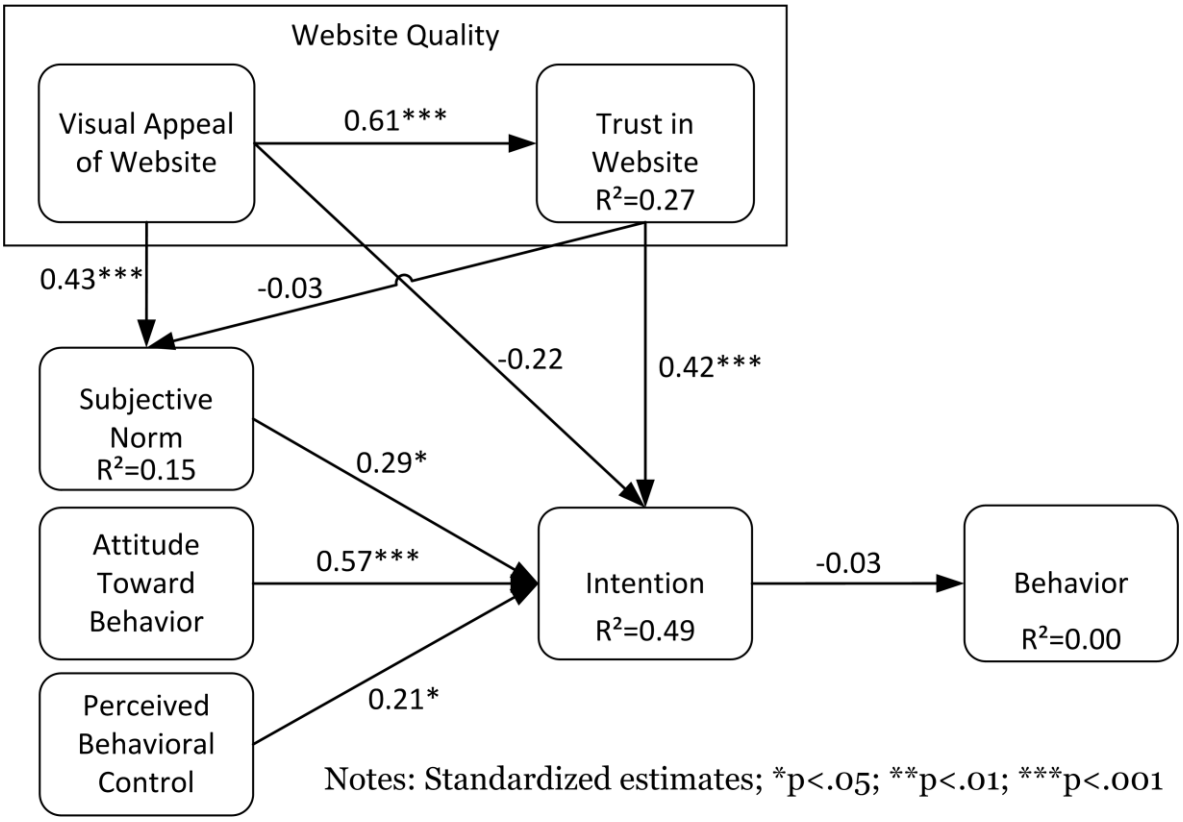

Figure 5: Model results

Hypothesis	Supported?	Path Coefficient	Standard Error	p-value
H1: Website Visual Appeal → Website Trust	Yes	0.614	0.101	<0.001
H2a: Website Visual Appeal → Subjective Norms	Yes	0.433	0.106	<0.001
H2b: Website Trust → Subjective Norms	No	-0.034	0.088	0.697
H3: Subjective Norms → Intention	Yes	0.285	0.128	0.026
H4: Attitude Toward Behavior → Intention	Yes	0.566	0.148	<0.001
H5: Perceived Behavioral Control → Intention	Yes	0.207	0.097	0.032
H6: Intention → Behavior	No	-0.029	0.059	0.617

Table 5: Summary of hypothesis testing results

Discussion

The data support the overarching idea that signals of quality presented by a website influence how users intend to interact with the site, however, the precise operationalization of these changes deviated slightly from the hypothesized relationships. While we predicted both visual appeal and trust would influence subjective norms, we found that only visual appeal directly influence subjective norms, while trust directly influenced intentions.

Although intention did not have a significant effect on password entropy, we suggest there are two main reason for this. First, the majority of participants neglected the instructions to create a unique password for this website, thus diminishing the impact of the website quality manipulation. Password reuse is a major problem in information systems security, as it can lead to a "domino effect" – i.e. if a user's password is compromised on a single web site with poor security, that password could be used to compromise their account across multiple systems (Ives et al. 2004). To combat password reuse, administrators of websites might consider implementing means to identify and deter password reuse (see Jenkins et al. 2013) in addition to manipulations such as the ones presented in this paper to encourage users to create strong passwords. Second, using password entropy as an operationalization of behavior may not have been representative of the behavior participants believed they were engaging in. Participants that intended to engage in secure behavior may have genuinely thought they were constructing a secure password (engaging in secure behavior), despite their password having low entropy. Training in how to create secure passwords might be used to improve this disparity, and future research should consider exploring the relationship between how secure users believe their passwords are and how secure they actually are.

Conclusion

Encouraging secure behavior in users is an important, but difficult, task. While many methods such as training, reminders and security policies are currently used with varying levels of success, traditional methods of influencing secure behavior places additional load on the user. Furthermore, since behaving securely is rarely, if ever, the primary goal of users when interacting with a computer system or web site, secure behavior is likely to be one of the first goals neglected by users when exposed to additional stressors. This study does not suggest that priming secure user behavior is a substitute for policies, training, or reminders, but rather it should be considered a supplement to these methods to increase the protection afforded by passwords. This study demonstrates that subtle cognitive priming via website quality may be used to generate more secure user behavior without placing additional load or requirements on the user.

While creating quality web sites is already a focus of many practitioners, this study helps to illustrate the importance of good design and may provide additional incentive for companies to design high quality web sites. By exerting a modest amount of extra effort into designing sites to exude symbols of trust and visual appeal, firms may be able to increase secure behavior with minimal cost and impact to users.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Nunamaker Jr, J. F. 2010. "Detecting fake websites: the contribution of statistical learning theory," *MIS Quarterly* (34:3), pp. 435–461.

Ajzen, I. 1991. "The theory of planned behavior," *Organizational behavior and human decision processes* (50:2), pp. 179–211.

Akins, T. 2014, February 17. "Strength Test," http://rumkin.com/tools/password/passchk.php.

Alsudani, F., and Casey, M. 2009. "The Effect of Aesthetics on Web Credibility," in *Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, BCS-HCI '09, Swinton, UK, UK, pp. 512–519.

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613–A15.

Bagozzi, R. P., and Yi, Y. 1988. "On the evaluation of structural equation models," *Journal of the academy of marketing science* (16:1), pp. 74–94.

Bauerly, M., and Liu, Y. 2008. "Effects of symmetry and number of compositional elements on interface and design aesthetics," *Intl. Journal of Human–Computer Interaction* (24:3), pp. 275–287.

Belanger, F., Hiller, J. S., and Smith, W. J. 2002. "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems* (11:3), pp. 245–270.

Bentler, P. M. 1990. "Comparative fit indexes in structural models," *Psychological bulletin* (107:2), p. 238.

Bonnardel, N., Piolat, A., and Le Bigot, L. 2011. "The impact of colour on Website appeal and users' cognitive processes," *Displays* (32:2), pp. 69–80.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. 2009. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security," *European Journal of Information Systems* (18:2), pp. 151–164.

Bottomley, P. A., and Doyle, J. R. 2006. "The interactive effects of colors and products on perceptions of brand logo appropriateness," *Marketing Theory* (6:1), pp. 63–83.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly* (34:3), pp. 523–548.

Burr, W. E., Dodson, D. F., and Polk, W. T. 2011. *Electronic Authentication Guideline*, (1.0.2 ed.) .

Charoen, D., Raman, M., and Olfman, L. 2008. "Improving end user behaviour in password utilization: An action research initiative," *Systemic Practice and Action Research* (21:1), pp. 55–72.

Cyr, D. 2008. "Modeling web site design across cultures: relationships to trust, satisfaction, and e-loyalty," *Journal of Management Information Systems* (24:4), pp. 47–72.

Cyr, D., Head, M., and Larios, H. 2010. "Colour appeal in website design within and across cultures: A multi-method evaluation," *International Journal of Human-Computer Studies* (68:1), pp. 1–21.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach," *Information Systems Research* (20:1), pp. 79–98.

Fogg, B. J. 2003. "Prominence-interpretation theory: explaining how people assess credibility online," in *CHI'03 extended abstracts on human factors in computing systems*, , pp. 722–723.

Fogg, B. J., Soohoo, C., Danielson, D. R., Marable, L., Stanford, J., and Tauber, E. R. 2003. "How do users evaluate the credibility of Web sites?: a study with over 2,500 participants," in *Proceedings of the 2003 conference on Designing for user experiences*, , pp. 1–15.

Furnell, S. 2007. "An assessment of website password practices," *Computers & Security* (26:7), pp. 445–451.

Gladwell, M. 2006. *The tipping point: How little things can make a big difference*, Hachette Digital.

Harcourt, B. E. 1998. "Reflecting on the Subject: A Critique of the Social Influence Conception of Deterrence, the Broken Windows Theory, and Order-Maintenance Policing New York Style," *Michigan Law Review* (97:2), p. 291.

Herath, T., and Rao, H. R. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems* (18:2), pp. 106–125.

Holbert, R. L., and Stephenson, M. T. 2002. "Structural equation modeling in the communication sciences, 1995–2000," *Human Communication Research* (28:4), pp. 531–551.

Hooper, D., Coughlan, J., and Mullen, M. 2008. "Structural Equation Modelling: Guidelines for Determining Model Fit," *Electronic Journal of Business Research Methods* (6:1), pp. 53–60.

Hynes, N. 2009. "Colour and meaning in corporate logos: An empirical study," *Journal of Brand Management* (16:8), pp. 545–555.

Ives, B., Walsh, K. R., and Schneider, H. 2004. "The domino effect of password reuse," *Communications of the ACM* (47:4), pp. 75–78.

Jenkins, J., and Durcikova, A. 2013. "What, I Shouldn't Have Done That? : The Influence of Training and Just-in-Time Reminders on Secure Behavior," *ICIS 2013 Proceedings* .

Jenkins, J. L., Grimes, M., Proudfoot, J. G., and Lowry, P. B. 2013. "Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals," *Information Technology for Development* , pp. 1–18.

Johnston, A. C., and Warkentin, M. 2010. "Fear appeals and information security behaviors: an empirical study," *MIS quarterly* (34:3), pp. 549–566.

Lee, Y., and Kozar, K. A. 2006. "Investigating the effect of website quality on e-business success: an analytic hierarchy process (AHP) approach," *Decision support systems* (42:3), pp. 1383–1401.

Loiacono, E. T., Watson, R. T., and Goodhue, D. L. 2002. "WebQual: A measure of website quality," *Marketing theory and applications* (13:3), pp. 432–438.

Lowry, P. B., Wilson, D. W., and Haig, W. L. 2014. "A Picture is Worth a Thousand Words: Source Credibility Theory Applied to Logo and Website Design for Heightened Credibility and Consumer Trust," *International Journal of Human-Computer Interaction* (30:1), pp. 63–93.

Robins, D., and Holmes, J. 2008. "Aesthetics and credibility in web site design," *Information Processing & Management* (44:1), pp. 386–399.

Rosseel, Y. 2012. "lavaan: An R package for structural equation modeling," *Journal of Statistical* .

Shannon, C. E. 1948. "A mathematical theory of communication," *Bell Systems Technical Journal* (27).

Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation guidelines for IS positivist research," *Communications of the Association for Information Systems* (13:24), pp. 380–427.

The Disaster Center. 2013. *Uniform Crime Report – State Statistics from 1960-2012*.

Wilson, J. Q., and Kelling, G. L. 1982. "Broken windows," *Atlantic monthly* (249:3), pp. 29–38.