PRACTICING SAFE COMPUTING: MESSAGE FRAMING, SELF-VIEW, AND HOME COMPUTER USER SECURITY BEHAVIOR INTENTIONS

Security and Assurance

Catherine L. Anderson
University of Maryland
Canderso@rhsmith.umd.edu

Ritu Agarwal
University of Maryland
Ragarwal@rhsmith.umd.edu

Abstract

With its global reach and pervasiveness, the Internet enables individuals to be more connected through electronic linkages than ever before. In such a highly inter-dependent network, individual behaviors can have far-reaching consequences that transcend borders between people, organizations and nations. Because home computer users represent a weak link in securing cyberspace, it is critical that they be reached and motivated to consistently practice recommended security behavior so that we can continue to rely on the availability of information provided by the Internet, the capability to conduct e-Commerce transactions, and to communicate with people around the world. Drawing on the marketing and economics literatures, the purpose of this study is to examine potential message manipulations in an effort to determine which manipulations are most likely to be effective at increasing home computer users’ intentions to perform the desired security behavior. We manipulated individuals’ goal frames (promotion versus prevention goal frame) and self-views (independent versus interdependent self-view) in an experimental setting with 101 subjects and examined their independent and interactive effects on subjective and descriptive norms related to home security behaviors. We further investigated the effects of these norms on intentions to practice safe computing. The findings and implications are discussed.

Keywords: Behavioral security, home computer user, information systems security, message framing, self-view manipulation

Introduction

With its global reach and pervasiveness, the Internet enables individuals to be more connected through electronic linkages than ever before. In such a highly inter-dependent network, individual behaviors can have far-reaching consequences that transcend borders between people, organizations and nations. Not surprisingly then, there is increased interest in fostering appropriate individual security behavior both in the workplace and at home as addressed in the National Strategy to Secure Cyberspace (2003). Even as software vendors expend considerable effort to create technology to improve security, more and more attention is being focused on the role people play in security. Recently, in addition to technical approaches to developing a safe computing environment that is protected against security violations, there is recognition that a socio-technical or behavioral approach to security is warranted (Sasse et al. 2001; Stanton et al. 2005).

The risks of home computer users not practicing adequate security behaviors can be significant. They range from merely inconveniencing them in the event they contract a virus that wipes out important personal data on their computer to financially crippling retail organizations through hackers using her machine as a “bot” along with thousands of other similarly accessed machines to create denial of service attacks by overloading requests to servers (Krebs 2005). The potential risks to businesses of a security violation range from tangible losses in revenue to intangible losses due to reputation damage (Garg 2003). Additionally, violations such as identity theft can lead to a loss of confidence in consumers’ overall willingness to transact business online (Borrus 2005). These risks can be
mitigated if home users take such actions as consistently updating their antivirus software, installing and running effective firewalls and exercising care when opening emails and attachments. However, recent studies conducted both with home users and employees indicate a disconnect between individual’s perceptions of how secure they are and the reality of security level attained (Roberts 2004; Stanton et al. (in press)). Although security threats are not new, and both threats and prescribed precautionary measures have existed for years, it appears that large numbers of home computer users see themselves as invulnerable to such problems. To the extent that the behavior of one individual can have far-reaching consequences on the interconnected network, the public policy challenge is how to motivate and ensure that individuals consistently comply with security precautions.

With respect to the workplace, employers have the capability to create policies that prescribe the required security behavior of employees, to train employees in appropriate security precautions, and to monitor employee behavior and enforce policy through penalties. Unfortunately, the individual home user is not subject to employer policies, training programs or rewards/sanctions designed to increase recommended security behaviors, underscoring the need for alternative methods. The magnitude of the problem is considerable, as there is a vast population of Internet-enabled home computer users. As reported in a census study from 2003, over 54% of U.S. households have an Internet-enabled computer (Day et al. 2003). One possible solution is to attempt to increase the desired security behavior through persuasive mass media public appeals in the form of television or Internet advertisements, print or radio campaigns, and the like. The purpose of this study is to examine potential message manipulations in an effort to determine which manipulations are most likely to be effective at increasing home computer users’ intentions to perform the desired security behavior.

Recently, information systems researchers have begun to focus attention on the human aspect of security. Studies suggest that user security behavior is motivated by a variety of factors such as perceptions of severity, efficacy, controllability and optimistic bias (Rhee et al. 2005; Woon et al. 2005). Additionally, in a recent study, Anderson (Anderson 2005) found that a combination of cognitive, social and psychological factors play a role in the formation of home computer user security intentions. In the current study, we build on our understanding of user motivations and attempt to actually influence user intentions. Specifically, our goal is to determine the most effective mix of message qualities that result in an increase in home computer user security behavior intentions. We measure intentions due to the difficulty in measuring realized secure behavior, as has been noted in literature addressing security compliance in the workplace (Vroom et al. 2004). The marketing and economics literature is rich with research that explores the factors influencing decision making and choice behavior. The literature examining the positive or negative framing of messages is particularly informative along the cognitive, individual dimension. The manner in which a message is framed has been shown to influence choice behavior even when the message conveys essentially the same information. In addition, since the Anderson study found a social component to security behavior intentions, a manipulation which primes individuals to focus on different referent groups to influence the social norms invoked might prove effective at increasing intentions. One such mechanism is the manipulation of self-view to prime individuals toward an interdependent versus independent view.

The study reported here is motivated by the need to increase the practice of safe computing by individuals in their homes. In this study, the term home computer user is intended to include individuals conducting personal (including school-related) activities on a computer that is not owned or controlled by an organization. Such individuals are not threatened by the possibility of losing a job as a result of behaving in an unsecure fashion online. The study has two broad objectives. One, we seek to apply the goal framing and self-view concepts to a critical information systems phenomenon in order to understand how the public might best be motivated to practice safe computing. Two, we examine two social mechanisms that may link these two manipulations to intentions, as called for by Aaker and Lee (Aaker et al. 2001). In the context of this study, framing of a message serves to focus the individual either on preventing the threat and associated negative outcomes of a security violation (negative or prevention frame), or on the utilization of effective coping responses in order to create a safe, reliable Internet environment (positive or promotion frame). The self-view manipulation serves to shift an individual’s frame of reference toward either an interdependent self or independent self. It is likely that such a manipulation may shift the individual’s referent group which will, in turn, influence the social norms that become salient for the individual.

Through an experiment conducted on 101 subjects using a 2 (promotion versus prevention goal frame) x 2 (independent versus interdependent self-view) factorial design, we demonstrate that home computer user security behavioral intentions can be influenced by message manipulations invoking the salience of social norms. An examination of the effectiveness of these manipulations on security intentions has practical implications which may
benefit organizational mass communication social marketing efforts. Findings are also likely to be useful for vendors desirous of creating effective advertising for security-related software and hardware. This paper contributes theoretically to the literature by further elaborating on the mechanisms which link self-view and regulatory focus to behavioral intentions.

The remainder of this paper includes a brief review of the relevant literature, including the study hypotheses. The methods are described next, followed by a discussion of the preliminary results. Finally, we conclude with a discussion of the implications of the study results.

**Theoretical Background**

**Framing and Self-Regulatory Goals**

Numerous studies, frequently based on prospect theory (Tversky et al. 1986), have been conducted to assess the influence of positively versus negatively worded messages on decision making behaviors. Tversky and Kahneman proposed prospect theory as a means of explaining circumstances where individual behavior does not conform to theories of rational choice. Prospect theory describes the process of choice as consisting of a framing and editing phase, followed by an evaluation phase. The manner in which a message is framed influences choice behavior even when the message conveys essentially the same information. During the evaluation phase, individuals evaluate alternatives partially based on their respective values in terms of whether an option is perceived to be a loss or a gain. The value function used in prospect theory indicates a response to losses that is more extreme than the response to gains, and is referred to as **loss aversion**. In simple terms, the dissatisfaction experienced as a result of a loss is stronger than the satisfaction experienced as a result of an identical gain. Thus, messages that emphasize the negative outcomes of a choice are perceived as potential losses, which individuals are likely to want to avoid more than their desire to realize a potential gain described in a message that emphasizes the positive outcomes.

In an effort to better understand the inconsistent results achieved in the various studies, Levin et al. (Levin et al. 1998) conduct a review of framing effect studies and propose a typology of framing effects. The authors categorize previous studies into three different types of framing manipulations: risky choice framing, attribute framing and goal framing. In a risky choice framing, options are presented as differing in their level of risk. Attribute framing involves describing an object or event differently. Finally, goal framing is a third type of manipulation that assumes both frames are good in that there are benefits implied in both the positive and negative frames. Goal framing involves emphasizing either the positive aspects of a behavior or the negative aspects of not performing the behavior. Levin et al (Levin et al. 1998) note that goal framing is often applied in persuasive communications. Since the focus of the current study is on determining effective communications aimed at increasing home computer users’ intentions to behave in a secure fashion online, goal framing is the most relevant type of framing.

Goal framing effects have been studied from economics, marketing, and social psychology perspectives in a variety of decision contexts such as those related to health (Dutta-Bergman 2004), social dilemmas (Brewer et al. 1986), and finances (Tversky et al. 1981). Scholars have studied the influence of message framing on numerous dependent variables including attitudes and intentions (Block et al. 1995; Maheswaran et al. 1990), perceived importance and favorability of message (Aaker et al. 2001; Lee et al. 2000), risk perceptions (Lee et al. 2004) and choices and goals (Hamilton et al. 2005). In the current study, the dependent variables of interest are social norms and intentions to take action to protect the Internet and/or one’s own computer, which are likely also influenced by self-view.

**Self-view and Social Norms**

The goal framing focus and prospect theories have a predominantly individual focus, and are largely cognitive in nature. An assumption implicit in these theories is that individuals process all available information using the self as the locus of evaluation. Thus, they do not address the social aspects that pervade certain types of decisions. Arguably, use of the Internet is inherently social in nature as individuals correspond via email, make purchases partially based on expert and consumer reviews, and share information via bulletin boards, list services, blogs and the like. The decision to practice secure online behavior has ramifications not only for an individual but also for all others accessing the shared resources of the Internet. As such, social factors are a component in the formation of
security-related intentions as demonstrated in Anderson’s study (Anderson 2005). Specifically, subjective norm, which is what an individual believes others expect him to do, and descriptive norm, which is what an individual believes others are doing, influence home computer user security intentions.

Prior literature provides evidence for the influence of the social component in message content on choice behavior. One example is in anti-smoking campaigns aimed at adolescents (Pechmann et al. 2003). Adolescent smoking decisions appear to be influenced by peer pressure and the desire to be accepted. Another example in which prospect theory is incomplete involves social dilemmas in which individuals may choose to contribute for the benefit of the common good when free-riding may hold more benefit to the individual personally (Andreoni 1995). As pointed out by Van Dijk and Wilke (Dijk et al. 1997), in a social dilemma type of situation, individuals may also weigh the benefit to others (i.e., the collective) in addition to their personal loss or gain.

Self-view manipulations involve priming an individual to either think of herself as distinct and separate from others (independent), or to think of herself as part of a larger group (interdependent). By manipulating the self-view, an individual’s referent group is modified. Theories from social psychology such as the theory of reasoned action (Ajzen et al. 1980) and the theory of planned behavior (Ajzen 1988) suggest that social influences in the form of subjective norms are important predictors of individual behavior. Drawing upon these theories, a robust literature in information systems has identified subjective norms as salient to technology adoption and use decisions (e.g. Venkatesh et al. 2003)). For example, Taylor and Todd note that an individual’s referent group and the associated norms invoked are context dependent/external (Taylor et al. 1995). Taylor and Todd’s study examined factors influencing an individual’s adoption of technology and is particularly relevant to the current study because technology provides the interface to security software. A manipulation priming an interdependent self-view may shift the relative importance of various social norms in the decision/choice situation and modify the resultant outcome. Therefore, we expect differences in the level of subjective norm reported by subjects, depending on whether they are primed with an interdependent or independent self-view which will, in turn, influence security behavior intentions.

The Internet provides an infrastructure in which individuals can communicate and share information. Individuals did not pay to establish the Internet infrastructure nor do they pay to maintain it, however, the Internet can be conceived of as a public good in that it is a non-exclusive resource that can be accessed for free. Asking home computer users to practice secure online behavior in order to increase cyber security can be viewed as a contribution of time and effort (to learn the appropriate steps to take and to purchase the appropriate software) with not only personal benefits, but also benefits to all Internet users. Economics research on choice behavior in social dilemmas has demonstrated an influence of group and organization affiliation (Frey et al. 2004; Keser et al. 2000) on pro-social behavior, as well as a fully mediated influence of social responsibility on choices to voluntarily contribute toward a collective’s interest (Dijk et al. 1997). In social dilemma settings, there appears to be an element of conditional cooperation which invokes a descriptive norm. Descriptive norm captures what an individual believes others are doing. Individuals tend to be more inclined to contribute in social dilemmas when they believe others are doing the same. For the current study, these findings lead to an expectation that priming an interdependent self-view will focus individuals on a larger referent group and cause more weight to be placed on descriptive norm which will, in turn, influence security behavior intentions.

**Self-View and Goal Frame Interaction**

As described earlier, self-view and goal frame manipulations are likely to influence social norms and intentions to perform a particular behavior. In order to hypothesize the influence of these two manipulations in combination, we draw upon prior research which has investigated the interaction of self-view and goal frame on intentions. Studies have found that subjects primed with an independent self-view are more attuned toward promotion focused messages and subjects primed with an interdependent self-view attend and respond more to prevention focused messages (Aaker et al. 2001; Lee et al. 2000). An independent self-view may prime an individual to place more value on individuating factors when making a decision or forming an intention. This leads us to propose the following hypotheses:

**H1:** Self-view and goal frame manipulations will interact to influence subjective norm. Specifically, subjects primed with an independent (interdependent) self-view will report a higher level of

---

**Security and Assurance**

1546 Twenty-Seventh International Conference on Information Systems, Milwaukee 2006
subjective norm when receiving a promotion-focused (prevention-focused) goal frame than subjects primed with a prevention-focused goal frame. 

H2: Self-view and goal frame manipulations will interact to influence descriptive norm. Specifically, subjects primed with an independent (interdependent) self-view will report a higher level of descriptive norm when receiving a promotion-focused (prevention-focused) goal frame than subjects primed with a prevention-focused goal frame.

The link between subjective and descriptive norms and security behavioral intentions is based on prior research (Anderson 2005), where these relationships were examined based on survey results. In the current study, we seek to confirm the relationship between norms and security behavioral intentions in a controlled, experimental environment. An individual’s desire to take action to protect his own computer may differ from the individual’s desire to protect the Internet as a whole. To isolate these effects, we examine the influence of norms on intentions to protect one’s own computer separately from one’s intentions to protect the Internet.

H3a: Subjective norm is positively related to security behavioral intentions to protect the Internet.
H3b: Subjective norm is positively related to security behavioral intentions to protect one’s own computer
H4a: Descriptive norm is positively related to security behavioral intentions to protect the Internet.
H4b: Descriptive norm is positively related to security behavioral intentions to protect one’s own computer

Methodology

To test the research hypotheses, we conducted an experiment in a laboratory setting. As explained below, message framing and self-view of the message were manipulated via asking the subjects to review a Web site. Because the target population is any user of an Internet-enabled computer who is not subject to job-related consequences as the result of acting in an unsecure fashion online, the sample consists of undergraduate students from a large university enrolled in a required marketing course. Our sample is similar to the U.S. Internet user population in terms of gender breakdown and education level. Over half of the sample, 52%, was male and 57% of the U.S. Internet population was male according to the 2003 census (Day et al. 2003). In 2003, the majority of U.S. Internet user population fell into the same education category as our sample. Specifically, all of our sample and 55% of U.S. Internet users possess a high school diploma or some college education. To ensure subject involvement in the experimental task, student participants received extra credit for participation in lab experiments.

Message Framing Manipulation

Subjects were randomly asked to review a Web site containing a security message that is positively (promotion focused goal) or negatively (prevention focused goal) worded. The positively worded message focuses on the “benefits” of performing security precautions such as reliability, stability, peace-of-mind for both individuals and organizations. The negatively worded message stresses the consequences of not taking security precautions, thus focusing on the severity and probability of threats.

The four Web site conditions are included in Appendix C. The content of the Web sites is based on examples of descriptions of risks and benefits to practicing secure behavior across non-profit Web sites such as the Department of Homeland Security, National Cyber Security Alliance (NCSA) and EDUCAUSE. In addition, we reviewed relevant Web sites hosted by security-related software vendors such as Symantec/Norton, Microsoft and McAfee. The Web site manipulations represent an effort to consolidate common themes to create strong positive and negative content. To control any possible decision making biases due to length, the messages are of comparable length in terms of number of words and paragraphs.

Self-view Manipulation

The messages on the Web sites are worded in such a way as to focus either on the individual (e.g. yourself, your data, your personal productivity, etc) or on the individual as part of the Internet Community (e.g. All inter-connected users of the Internet, the community, etc.). Graphics/ pictures are also used to reinforce the individual versus interdependent view.
Main Study Design and Variable Operationalization

A 2 X 2 (message framing x self-view) factorial design was employed to test the research questions. Participants were isolated from each other and completed the experiment independently as part of a set of unrelated experiments. Subjects participated in computer labs equipped with computers that enable them to access the experimental scenarios, which are assigned at random, and respond to the post-questionnaire electronically. The laboratory setting ensured an environment that was consistent across all participants and free of distraction.

The participants were asked to take their time reviewing the Web site and then proceed to the questionnaire portion of the study. After each participant read the Web site, s/he completed an online questionnaire including multi-item scales measuring the dependent variables (Anderson 2005; Culnan et al. 2004) including subjective norm, descriptive norm, and security intentions (see Appendix A for the measures). Where necessary, terms such as security violation and security measures were explicitly defined (see Appendix A) so that each respondent had a common understanding of each term. The security intentions were measured separately for the Internet and the subject’s own computer as an individual may hold differing intentions for the two targets.

Since this study involved individual-level perceptions, we collected demographic information such as gender, age, education, years of computer and Internet experience. In addition, the subjects were asked to indicate how much they heard or read about computer security recently in order to assess any influence of prior media exposure.

Results

A total of 101 subjects participated in the experiment. Random assignment of subjects to conditions resulted in a 25 subjects for conditions 1 (independent/prevention), 3 (independent/promotion) and 4 (interdependent/promotion) and 26 subjects in condition 2 (interdependent/prevention). Although we did not directly measure subjects’ prior exposure to security related information, random assignment ensured that, on average, subjects in all four conditions had the same level of previous exposure to messages about security and the risks of not practicing secure computing.

Manipulation Checks

As a manipulation check, subjects completed several questions regarding their thoughts immediately after reviewing the Web site(s). The questions focused on determining the extent to which the subject was thinking about the benefits or consequences of security violations and the extent to which the subject was thinking about him or herself as compared to thoughts about others (see Appendix A). A repeated measures ANOVA shows the anticipated effect of goal frame on thoughts about consequences versus benefits (F=11.225, p=.001).

The repeated measures ANOVA on the self-view condition indicated that the subjects’ levels of thoughts about themselves and thoughts about others was significantly different (F=4.74, p=.032). However, the interaction between these thoughts and self-view was not significant (F=0, p=.983). Although the self-view manipulation check failed, it can be seen based on the ANOVA results described below to test the hypotheses, that self-view did significantly influence some of the study’s proposed mediating and dependent variables. Since self-view does appear to influence the dependent variables, it may be that the self-view manipulation is more subtle than could be assessed by the manipulation check questions. Perhaps, the wording of the self-view manipulation questions misled or were somehow confusing to the subjects. According to Sigall & Mills (Sigall et al. 1998), the questions we use constitute an independent variable check and not a treatment check. A treatment check would have asked the respondents if they noticed that the Web site referred to an individual and his/her actions versus groups of people and their collective actions and may have served to sensitize respondents to our experimental treatments. An independent variable check is intended to assess the conceptual independent variable (in our case, self-view) and is harder to obtain as it is more subtle. Sigall & Mills note it would be inappropriate to exclude participants based on responses to an independent variable check, and that differences on mediating and/or dependent variables can be taken as evidence that the treatment was noticed.

Psychometric Properties of Scales

We first assessed the convergent and discriminant validity of the multi-item scales using principal components factor analysis with varimax rotation (See Appendix B). The items all loaded on their predicted factors, indicating
that the measures are valid. We further assessed the reliability of the scales: Table 1 shows that each of the questionnaire scales exceeds the generally accepted Cronbach’s alpha level of .7. We created indices for all of the dependent and independent measures for further analysis. Table 2 provides means for the key dependent measures across the self-view and goal frame conditions. The independent self-view condition is coded 1 (interdependent is 2) and the promotion focused goal frame condition is coded 1 (the prevention focused goal frame is 2).

<table>
<thead>
<tr>
<th>Construct</th>
<th>Reliability(number of items)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective Norm</td>
<td>.80(3)</td>
</tr>
<tr>
<td>Descriptive norm</td>
<td>.76(2)</td>
</tr>
<tr>
<td>Security intentions toward Internet</td>
<td>.96(4)</td>
</tr>
<tr>
<td>Security intentions toward own computer</td>
<td>.91(4)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2. Variable Measures Across Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-view</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
**ANOVA Results**

A two-way ANOVA (self-view x goal frame) showed that self-view significantly influenced subjective norm ($F=3.90$, $p=.05$). Subjects primed with the independent self-view indicated a higher (M=5.193) level of subjective norm than those primed with an interdependent self-view (M=4.692). The ANOVA results also indicate a marginal influence of the interaction of self-view and goal frame ($F=3.467$, $p=.066$). Figure 1 depicts this interaction. Follow up contrasts show that subjects primed with the independent self-view experience significantly different levels of subjective norm based on the goal frame. Specifically, subjects primed with the independent self-view and promotion focused goal report a significantly higher subjective norm (M=5.64) when compared to subject’s primed with the independent self-view and prevention focused goal (M=5.75, $p=.017$) which provides partial support for hypothesis 1. Subjects primed with the interdependent self-view indicate no significant differences in subjective norm based on goal frame.

![Figure 1. Interaction of Self-View and Frame on Subjective Norm](image)

A similar analysis showed that the interaction of self-view and goal frame significantly influenced descriptive norm ($F=4.30$, $p=.04$). As hypothesized, Figure 2 shows the interaction graph which indicates that subjects primed with an independent self-view combined with the promotion focused message indicated a higher level of descriptive norm and subjects primed with an interdependent self-view combined with the prevention focused message indicated a higher level of descriptive norm. Follow up contrasts show that subjects primed with an independent self-view indicate marginally higher levels of descriptive norm when presented with the promotion focused goal frame compared to the prevention focused goal frame (M=5.72 and 5.08, respectively, t=1.862, $p=.069$). Subjects primed with the interdependent self-view indicate no significant differences in descriptive norm based on goal frame. These results provide partial support for hypothesis 2.
OLS regressions of intentions to protect the Internet and intentions to protect one’s own computer on subjective and descriptive norm support hypotheses 3a, 3b, and 4b and are displayed in Table 3. A summary of the study results by hypothesis is provided in Table 4. Multicollinearity, as indicated by the variance inflation factors, was acceptably low. Subjective norm was found to be significant and positive in predicting intentions to protect the Internet (β = .40, p=.001) and intentions to protect one’s own computer (β = .25, p=.001). Similarly, descriptive norm was significant in predicting intentions to protect the Internet (β = -.34, p=.007) and intentions to protect one’s own computer (β = .19, p=.013). Variance explained in the two intentions ranged from 11 to 21%. The sign of the coefficient for descriptive norm on intentions to protect the Internet is negative which is opposite to the positive hypothesized relationship, thus, hypothesis 4a is not supported. One potential explanation for why this negative relationship is opposite to that found by Anderson is the relatively homogenous experimental sample. All of the experimental subjects are young and may feel less responsibility or be differentially influenced by what they think others are doing. It may be that if an individual believes others are taking action to secure their home computers, the individual will feel less inclined to take action personally. Generally, these results provide support for Anderson’s home computer user security intention model as we replicate the findings in an experimental context with a sample consisting exclusively of students aged 18-21. The prior study’s results were based on a survey and sample the majority of which consisted of subjects aged 35-54 with high level of computer and Internet experience.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Intentions to Protect One’s Own Computer</th>
<th>Intentions to Protect the Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standardized Beta p-value</td>
<td>Standardized Beta p-value</td>
</tr>
<tr>
<td>Intercept</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subjective Norm</td>
<td>.33***</td>
<td>.34***</td>
</tr>
<tr>
<td></td>
<td>.001</td>
<td>.001</td>
</tr>
<tr>
<td>Descriptive Norm</td>
<td>.24***</td>
<td>-.28***</td>
</tr>
<tr>
<td></td>
<td>.013</td>
<td>.007</td>
</tr>
<tr>
<td>R squared</td>
<td>.227</td>
<td>.126</td>
</tr>
<tr>
<td>Adjusted R-squared</td>
<td>.211</td>
<td>.108</td>
</tr>
<tr>
<td>Max VIF</td>
<td>1.147</td>
<td>1.147</td>
</tr>
</tbody>
</table>

***p<.01
Table 4. Summary of Results by Hypothesis

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: Self-view*Goal Frame → Subjective Norm</td>
<td>Partially Supported</td>
</tr>
<tr>
<td>H2: Self-view*Goal Frame → Descriptive Norm</td>
<td>Partially Supported</td>
</tr>
<tr>
<td>H3a: Subjective Norm → Intentions to protect Internet</td>
<td>Supported</td>
</tr>
<tr>
<td>H3b: Subjective Norm → Intentions to protect own computer</td>
<td>Supported</td>
</tr>
<tr>
<td>H4a: Descriptive Norm → Intentions to protect Internet</td>
<td>Not Supported</td>
</tr>
<tr>
<td>H4b: Descriptive Norm → Intentions to protect own computer</td>
<td>Supported</td>
</tr>
</tbody>
</table>

A post hoc analysis to examine potential direct effects of self-view and goal frame on security behavior intentions reveals a direct effect of goal frame on intentions to protect the Internet \(F=3.97, \ p=.049\) and a goal-frame/self-view interaction on intentions to protect one’s own computer \(F=5.92, \ p=.017\). Subjects primed with a promotion focused goal showed higher intentions to protect the Internet \(M=4.75\) than did subjects primed with a prevention focused goal \(M=4.145\). Contrasts on the interaction of goal frame and self-view on intentions to protect one’s own computer show that the means are only significantly different for the independent self-view with a higher mean in the promotion focused frame \(M=6.59\) and \(5.89\), respectively, \(t=2.914, \ p=.005\).

**Demographic Control Variables**

Gender, media exposure, prior experience with a security violation, computer and Internet experience were all found to have no significant influence on the attitude or intention measures. As a result, we dropped these controls from the regression analysis.

**Discussion and Conclusion**

The overall goal of this study was to better understand how individuals can be motivated to practice safe computing at home – i.e., perform the behaviors necessary to protect their own computer and the Internet. The potential impacts of an individual’s online behavior are not isolated to that individual. Other Internet users and organizations stand to suffer if the stability of the network becomes questionable due to security violations leading to a loss of confidence in conducting business and personal transactions over the Internet. To the extent home computer users can be reached and their security behaviors improved, every user of the Internet stands to benefit. Drawing upon research from information systems, economics, marketing, and social psychology, we argued that it is possible to influence security behavioral intentions of home computer users with self-view and goal frame message manipulations through the social norms made salient to the user. This experiment contributes to a nascent stream of information systems literature that examines user security behavior and its antecedents. It represents a logical next step which takes the understanding of what motivates a user to behave in a secure fashion and uses it to frame a message aimed at amplifying the incidence of the desired behavior.

Before discussing any specific findings or suggestions for practice, the limitations of this study must be noted. This study was conducted on undergraduate students and, as a result, care should be taken in generalizing these findings to other groups. It is possible that different demographic groups may find different types of messages persuasive. Arguably, however, it is important to understand how to reach college students as they represent a significant portion of the Internet user population who are highly connected, and have a tendency to engage in risky behaviors. We assessed intentions rather than actual behavior in this study. In our experimental setup it is not feasible to examine actual behavior as may be, for example, in a survey. However, as noted before, in the security context actual behaviors are difficult to study, even through surveys. Furthermore, the relationship between intentions and actual behavior has been shown to be reasonably strong and consistent (Venkatesh et al. 2003). Nonetheless, future studies should endeavor to assess users’ actions with respect to security. Finally, we used regression analysis to test for the effects of norms on intentions. While our scales displayed adequate psychometric properties and we have a single stage theoretical model for which regression analysis is appropriate, an alternative analysis technique such as structural equation modeling would allow for a test of the measurement model and structural relationships simultaneously.

Although most messages targeted at improving individual online security behaviors tend to emphasize the potential negative consequences of not acting in a secure fashion which would be consistent with a loss aversion approach, a striking finding of our study is that messages focused on the positive consequences (promotion focused goal frame)
of performing the behavior may actually be more persuasive in the context of online security behavioral intentions. Particularly if that message is conveyed in combination with an individual self-view. While this study examined intentions to protect one’s own computer separate from intentions to protect the Internet in order to better understand individual motivations, the net effect to the security of the Internet is virtually the same. That is, by taking such individual measures as keeping anti-virus software current, installing firewalls and selectively viewing emails/attachments, every user of the Internet benefits by the improved security of each node in the network. Messages targeted at increasing intentions to protect one’s own computer or to protect the Internet as a whole are both beneficial to the Internet community.

In conclusion, the Internet is a critical component of infrastructure that sustains individuals, companies and nations and must be protected by the combined efforts of all Internet users. Even short outages in the network can lead to significant productivity and financial losses. As home computer users represent a weak link in securing cyberspace, it is critical that they be reached and motivated to consistently practice recommended security behavior so that we can continue to rely on the availability of information provided by the Internet, the capability to conduct e-Commerce transactions, and to communicate with people around the world. Clearly, more research is warranted to examine potential ways of reaching home computer users in a wide range of demographic groups. Several opportunities for fruitful future research remain. Perhaps an examination of source credibility in messages would yield interesting results. Alternatively, researchers could study the specific content of messages (as opposed to their overall framing) that are more potent in influencing security behavior intentions. Finally, to the extent that individuals may be exposed to the importance of security through training and awareness programs in the workplace, it would be useful to study how much “transference” of this knowledge occurs when the individual moves from the office to the home environment.

References


Appendix A – Survey Items

Manipulation Checks – Self-view
For the following questions, the term “security violations” is meant to indicate threats such as virus attacks and/or unauthorized access to data by hackers.

While you were reviewing the Web site about the security issue and becoming a conscientious cybercitizen, please describe the extent to which:

You thought about yourself
- Not at all 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 A lot
You thoughts about the security issue were focused on just yourself
- Not at all 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 A lot
Your thoughts were focused on just you
- Not at all 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 A lot
You thought about other users of the Internet
- Not at all 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 A lot
Your thoughts about the security issue were focused on other users of the Internet
- Not at all 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 A lot
Your thoughts were focused on other users of the Internet
- Not at all 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 A lot

Manipulation Checks – Goal Frame
While you were reviewing the Web site about the security issue and becoming a conscientious cybercitizen, please describe the extent to which you agree or disagree with the following statements:

The Web site made me think about the benefits of following recommended security behaviors
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree
The Web site made me think about the benefits of a secure Internet environment
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree
The Web site made me think about the consequences of security violations
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree
The Web site made me think about the consequences of not performing the recommended security behaviors
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree

Subjective Norm
For the following questions, security measures are individual actions such as running and updating antivirus software, keeping passwords secure, running a firewall when necessary, etc. Indicate the degree to which you agree or disagree with the following statements:

Friends who influence my behavior would think that I should take measures to secure my primary home computer
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree
Significant others who are important to me would think that I should take measures to secure my primary home computer
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree
My peers would think that I should take security measures on my primary home computer to help secure the Internet
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree

Descriptive Norm
Indicate the degree to which you agree or disagree with the following statements:

I believe other people implement security measures on their primary home computers.
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree
I am convinced other people take security measures on their primary home computers.
- Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree
Intentions to protect own computer
Thinking of your future actions, please answer the following questions regarding implementing security measures to protect YOUR COMPUTER from an attack by hackers
The probability that I will take security measures to protect my home computer is…
Not Probable 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Probable
The probability that I would consider taking security measures to protect my home computer is…
Not Probable 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Probable
The likelihood that I would take security measures to protect my home computer is…
Not Likely 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Likely
My willingness to take security precautions to protect my home computer is…
Not Willing 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Willing

Intentions to protect the Internet
Thinking of your future actions, please answer the following questions regarding implementing security measures to protect THE INTERNET from an attack by hackers
The probability that I will take security measures on my home computer to protect the Internet is…
Not Probable 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Probable
The probability that I would consider taking security measures on my home computer to protect the Internet is…
Not Probable 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Probable
The likelihood that I would take security measures on my home computer to protect the Internet is…
Not Likely 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Likely
My willingness to take security precautions on my home computer to protect the Internet is…
Not Willing 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Highly Willing

Previous exposure to a security violation
Indicate the frequency with which you have been exposed to the following events:
How frequently have you personally been affected by a security violation?
Very Infrequently 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Very Frequently
How frequently have you known someone who has been affected by a security violation?
Very Infrequently 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Very Frequently

Media Exposure
I have heard or read a lot about the potential threats to computers and the Internet this past year
Strongly Disagree 1 --- 2 --- 3 --- 4 --- 5 --- 6 --- 7 Strongly Agree

Demographics
Indicate your level of Internet experience:
< 1 year 1-5 years 6-10 years 11-15 years >15 years
Indicate your level of computer experience:
< 1 year 1-5 years 6-10 years 11-15 years >15 years
What is your age?
What is your gender? M F
Appendix B – Correlations and Factor Analysis Results

<table>
<thead>
<tr>
<th>Rotated Component Matrix</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Comp Intent1</td>
<td>.027</td>
</tr>
<tr>
<td>Comp Intent2</td>
<td>.047</td>
</tr>
<tr>
<td>Comp Intent3</td>
<td>.158</td>
</tr>
<tr>
<td>Comp Intent4</td>
<td>.097</td>
</tr>
<tr>
<td>Internet Intent1</td>
<td>.928</td>
</tr>
<tr>
<td>Internet Intent2</td>
<td>.964</td>
</tr>
<tr>
<td>Internet Intent3</td>
<td>.938</td>
</tr>
<tr>
<td>Internet Intent4</td>
<td>.909</td>
</tr>
<tr>
<td>Subj Norm1</td>
<td>-.004</td>
</tr>
<tr>
<td>Subj Norm2</td>
<td>-.020</td>
</tr>
<tr>
<td>Subj Norm3</td>
<td>.443</td>
</tr>
<tr>
<td>Desc Norm1</td>
<td>-.098</td>
</tr>
<tr>
<td>Desc Norm2</td>
<td>-.117</td>
</tr>
</tbody>
</table>

Extraction Method: Principal Component Analysis.  Rotation Method: Varimax with Kaiser Normalization

<table>
<thead>
<tr>
<th>Correlations</th>
<th>Subjective Norm</th>
<th>Descriptive Norm</th>
<th>Intentions to protect own computer</th>
<th>Intentions to protect Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subjective Norm</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Descriptive Norm</td>
<td>.358**</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intentions to protect own computer</td>
<td>.420**</td>
<td>.360**</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Intentions to protect Internet</td>
<td>.239*</td>
<td>-.159</td>
<td>.173</td>
<td>1</td>
</tr>
</tbody>
</table>

** Correlation is significant at the .01 level (2-tailed)
* Correlation is significant at the .05 level (2-tailed)
Appendix C - Manipulations

Prevention/Independent Condition (1)

How You Can Become a Conscientious Cybercitizen

The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses or government agencies. With the U.S. Census reporting in 2001 that over half of U.S. households contain a computer with Internet access, the American population has unprecedented access to the resources of this global network from their own homes. Your behavior and habits can impact the security and privacy of your own personal data and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. You must be aware of the security issue and practice appropriate security behavior on your home computers.

<table>
<thead>
<tr>
<th>What Can You Do</th>
<th>Personal Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use &quot;anti-virus software&quot; and keep it up to date.</td>
<td>Lost personal information on home PC</td>
</tr>
<tr>
<td>Don’t open emails or attachments from unknown sources.</td>
<td>Unauthorized access to your personal information (identity theft)</td>
</tr>
<tr>
<td>Protect your computer from Internet intruders - use &quot;firewalls.&quot;</td>
<td>Use of your computer to send spam or spread viruses to friends and family</td>
</tr>
<tr>
<td>Regularly download security updates and &quot;patches&quot; for your operating systems and other software.</td>
<td>Use of your computer as a bot to send or download viruses with requests (Denial of Service attacks)</td>
</tr>
<tr>
<td>Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.</td>
<td>Unavailability of Internet resources for conducting personal research and business transactions</td>
</tr>
<tr>
<td>Don’t share access to your computers with strangers.</td>
<td></td>
</tr>
<tr>
<td>Disconnect from the Internet when not in use.</td>
<td></td>
</tr>
</tbody>
</table>

Avoid the personal consequences of security violations -
Protect yourself by following these suggested secure online behaviors:

You must do your part in the effort to secure this vital, global network for your future.
Prevention / Interdependent Condition (2)

How All Inter-Connected Users of the Internet Can Become Conscientious Cybercitzens

The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses or government agencies. With the U.S. Census reporting in 2001 that over half of U.S. households contain a computer with Internet access, the American population has unprecedented access to the shared resources of this global network from their own homes. The behavior and habits of each inter-connected user of the Internet can impact the security and privacy of the the data of all Internet users and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. All members of the Internet community must be aware of the security issues and practice appropriate security behavior on their home computers.

<table>
<thead>
<tr>
<th>What Can All Interconnected-Users Do?</th>
<th>Internet Community Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use “anti-virus software” and keep it up to date</td>
<td>• Lost information on Internet connected PCs</td>
</tr>
<tr>
<td>• Don’t open emails or attachments from unknown sources</td>
<td>• Unauthorized access to information (identity theft)</td>
</tr>
<tr>
<td>• Protect each computer from Internet intruders – use “firewalls.”</td>
<td>• Use of connected computers to send spam or spread viruses to other</td>
</tr>
<tr>
<td>• Regularly download security updates and “patches” for operating</td>
<td>Internet users</td>
</tr>
<tr>
<td>systems and other software.</td>
<td>• Use of connected computers as bots to overload servers with requests</td>
</tr>
<tr>
<td>• Use hard-to-guess passwords, both upper case, lower case, numbers, or</td>
<td>(Denial of Service attack)</td>
</tr>
<tr>
<td>other characters not easy to find in a dictionary; and make sure they</td>
<td>• Decreased confidence in using the Internet to conduct research and</td>
</tr>
<tr>
<td>are at least eight characters long</td>
<td>business transactions (e.g. providing information to trusted sources)</td>
</tr>
<tr>
<td>• Don’t share access to computers with strangers.</td>
<td>• Unavailability of Internet resources for conducting research and</td>
</tr>
<tr>
<td>• Disconnect from the Internet when not in use.</td>
<td>business transactions</td>
</tr>
</tbody>
</table>

Avoid the consequences to the community of Internet users from security violations – Protect your community by following these suggested secure online behaviors:

We all must do our part in the effort to secure this vital, global network for the future.
How You Can Become a Conscientious Cybercitizen

The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses, or government agencies. With the U.S. Census reporting in 2001 that over half of U.S. households contain a computer with Internet access, the American population has unprecedented access to the shared resources of this global network from their own homes. Your behavior and habits can impact the security and privacy of your own personal data and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. You must be aware of the security issue and practice appropriate security behavior on your home computer.

<table>
<thead>
<tr>
<th>What Can You Do?</th>
<th>Personal Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use “anti-virus software” and keep it up to date.</td>
<td>Increased confidence in storing your personal information on home PCs</td>
</tr>
<tr>
<td>Don’t open emails or attachments from unknown sources.</td>
<td>Increased privacy - Only authorized access to your personal information</td>
</tr>
<tr>
<td>Protect your computer from Internet intruders - use “firewalls.”</td>
<td>Confidence that your computer will not be unwittingly used to participate in the spread of spam or viruses to Internet users</td>
</tr>
<tr>
<td>Regularly download security updates and “patches” for your operating systems and other software.</td>
<td>Confidence that your computer will not be unwittingly used as a bot to overload servers with requests (Denial of Service attacks)</td>
</tr>
<tr>
<td>Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long.</td>
<td>Increased trust in using the internet to conduct personal research and business transactions</td>
</tr>
<tr>
<td>Don’t share access to your computer with strangers.</td>
<td>Access to Internet resources for conducting personal research and business transactions</td>
</tr>
<tr>
<td>Disconnect from the Internet when not in use.</td>
<td><strong>Enjoy the confidence of knowing you are doing your part to secure cyberspace</strong> - Reap the benefits by following these suggested secure online behaviors:</td>
</tr>
<tr>
<td></td>
<td><em>Your action is needed to gain the full benefit of this vital, global network for the future.</em></td>
</tr>
</tbody>
</table>
### How All Inter-Connected Users of the Internet Can Become Conscientious Cybercitizens

The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses or government agencies. With the U.S. Census reporting in 2001 that over half of U.S. households contain a computer with Internet access, the American population has unprecedented access to the shared resources of this global network: from their own homes. The behavior and habits of each inter-connected user of the Internet can impact the security and privacy of the data of all Internet users and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. The members of the Internet community must be aware of the security issue and practice appropriate security behavior on their home computers.

#### What Can All Inter-Connected Users Do?

- Use "anti-virus software" and keep it up-to-date.
- Don’t open emails or attachments from unknown sources.
- Protect each computer from Internet intruders – use “firewalls.”
- Regularly download security updates and “patches” for operating systems and software.
- Use hard-to-guess passwords that consist of a mix of upper case, lower case, numbers, or other characters not easily found in a dictionary, and make sure they are at least eight characters long.
- Don’t share access to computers with strangers.
- Disconnect from the Internet when not in use.

#### Internet Community Benefits

- Increased confidence in storing information on Internet-connected PCs.
- Increased privacy – only authorized access to information on the Internet.
- Confidence that computers will not be unwittingly used to participate in the spread of spam or viruses to Internet users.
- Confidence that connected computers will not be unwittingly used as bots to overload servers with requests (Denial of Service attacks).
- Increased trust in using the Internet to conduct research and business transactions.
- Access to a wealth of Internet resources for conducting research and business transactions.

---

Enjoy the confidence of knowing we are all doing our part to secure cyberspace - Reap the benefits by following these suggested secure online behaviors!

*We all must do our part to gain the full benefits of this vital, global network for the future.*