ON NOT FALLING FOR PHISH: EXAMINING MULTIPLE STAGES OF PROTECTIVE BEHAVIOR OF INFORMATION SYSTEMS END-USERS

Research-in-Progress

Mary B. Burns
Augusta State University
Augusta, GA
mburns9@aug.edu

Alexandra Durcikova
The University of Oklahoma
Norman, OK
alex@ou.edu

Jeffrey L. Jenkins
The University of Arizona
Tucson, AZ
jjenkins@cmi.arizona.edu

Abstract

The adage, “old habits die hard” is especially relevant when humans learn new protective behaviors (i.e., dental flossing, IS security behaviors). The foundation that underlies many social-cognitive theories used in IS research is that intention to change predicts actual behavior change. Despite intentions to change, humans do not always change their habits due to actual or perceived obstacles, for example. In this study, user behavior, particularly with respect to vigilance over phishing attempts, will be investigated via the theoretical lens of a hybrid continuum-stage behavior change model adapted from health-related fields. The goal of this research will be to gain a better understanding of: a) whether there are distinct stages that distinguish end-users’ vigilance toward phishing attempts; b) if so, can this research study confirm three distinct stages; and, c) what characterizes these different stages. This paper describes how we will examine our research questions through a research program.

Keywords: phishing, IS security, health behavior change model, stage model, intention-behavior gap
Introduction

Estimates on worldwide losses from phishing attacks stretch from tens of millions of dollars to billions of dollars (Hong 2012). Due to the prevalence and severity of these types of attacks that can fool even expert users, there is a need to understand why both expert and novice users persist in risky IS behavior despite good intentions.

The foundation that underlies many social-cognitive theories used in IS research is that intention to change predicts actual behavior change. However, despite intention to change, humans do not always alter their habits due to actual or perceived obstacles, for example (Conner and Armitage 1998; Sheeran 2002). Although the intention-behavior gap has been examined in IT usage research (Bhattacheryee and Sanford 2009; Davis et al. 1989; Taylor and Todd 1995; Venkatesh et al. 2003) as well as in consumer marketing (Sheppard et al. 1988), it remains critical in the field of IS Security to look inside the “black box” in which users move from an intention to be more vigilant and self-protective toward phishing attempts to actual behavior change that is consistently more secure.

There are two types of behavior change models: continuum and stage (Weinstein et al. 1998). Continuum models include constructs that can influence attitudes, intentions, and/or behavior in a prediction equation to provide a snapshot of the phenomena at a given point in time. In contrast, stage models acknowledge that a myriad of natural phenomena, including user behavior, passes through different phases that allow for the passage of time. A static model on its own cannot capture the various stages toward safer behavior that a user must progress through to attain a better understanding of why behavior must change, to develop good intentions for changed behavior, to develop a corresponding action plan for countering social engineering attempts, and, finally, to adopt the new behavior consistently.

In stage models, different interventions are required to not only educate but also motivate a person to move from one stage to another (Prentice-Dunn et al. 2009). In contrast, the assumption underlying much research in IS training, for example, is that “one size fits all”, indiscriminate of the user’s stage. This type of training can help users in the short-term (Baker and Wallace 2007; Jenkins et al. 2010; Siponen 2000). Training increases knowledge but may not change behavior if the user is not at the right stage or mindset to be motivated by the training content. Interventions, on the other hand, incorporate training or life experiences tailored to users at a particular stage.

Thus, there is a gap in the IS literature with respect to how users move from a denial, or “it can’t happen to me”, stage through an intention to modify behavior stage to the final stage of changed behavior through remaining vigilant over phishing consistently. Recently, IS researchers called for the use of multi-stage models to better understand various user behaviors over time (Benbasat and Barki 2007). In response to this call for multi-stage models and to address the discrepancy in the IS Security literature for exploring the intention-behavior gap, we propose that users move through a series of preintentional motivation and postintentional volition stages as they become more vigilant toward phishing attempts.

A hybrid stage model, the Health Action Process Approach (HAPA) model (Schwarzer 1992; Schwarzer 1999; Schwarzer 2001), that incorporates both a predictive relationship among constructs and constructs that can measure progress through stages has been developed in the health-related fields. This type of hybrid model permits researchers to develop a research program that incorporates both longitudinal studies as well as continuum snapshot studies. Using the theoretical lens of the HAPA model, we developed a three-stage model that represents how the mindset of a user changes between forming an intention and subsequent behavior through action and coping planning.

This paper describes the first two phases, a cross-sectional field study and a longitudinal field experiment, of a research program designed to investigate our model. We thereby will extend IS Security research by developing and empirically testing a theoretical model that not only represents the evolution of users’ protective behavior through stages but also includes predictive continuum-oriented constructs. The results of this research will have significant implications for cyber security job training processes.

In the next section, we review the pertinent literature from IS Security and Health Behavior and propose our research questions. We then build on health behavior change models, particularly the HAPA model, to develop a research model for examining IS protective behavior. Finally, we discuss our proposed approach for the initial testing of our model using a field survey as well as a follow-up longitudinal field experiment.
Literature Review

Given that phishing attacks are expensive to society, it is critical to understand why many people are hooked by phishing attacks when they believe that “it could not happen to them”. It is often human error or misjudgment that causes losses due to phishing. Thus, humans are considered the weakest link with respect to IS security efforts (Sasse et al. 2001; Schneier 2000). As a result, understanding user noncompliance to IS security policies and their susceptibility to phishing has been the focus of much research in both academia (e.g., Dodge Jr. et al. 2007; Parrish Jr. et al. 2009; Workman 2008; Wright and Marett 2010) and practice (e.g., Anti-Phishing Phil 2011).

In the IS literature, many studies concerning the adoption of IS technologies by end-users have been based on social-cognitive theories, such as the Technology Acceptance Model (TAM) (Davis 1989) and the Theory of Planned Behavior (TPB) (Ajzen 1988; Ajzen 1991). However, few studies have identified differences between user adoption of positive technologies (i.e., those technologies designed for users’ primary responsibilities, such as an Enterprise Resource Planning (ERP) system) and user acceptance of protective technologies, such as single sign-on password technology (Dinev and Hu 2007; Ng et al. 2009).

Recently, after Dinev and Hu (2007) “found that in the context of using protective technologies, some of the previously-established important relationships between user behavior and positive technology no longer hold” (p. 401), researchers turned to behavioral change theories from healthcare and safety in their studies of IS security (Davinson and Sillence 2010; Ng et al. 2009). Behavioral change models in health-related fields were developed to explore behaviors that protect health as well as the corresponding interventions that can encourage people to engage in safer health practices, such as practicing safe sex (the AIDS Risk Reduction Model (ARRM) developed by Catania et al. 1990) or using seat belts (the Health Belief Model (HBM) developed by Becker and Rosenstock 1987; Janz and Becker 1984; Rosenstock 1966).

Research Questions

The purpose of the initial studies in this research program is to examine the preintentional motivation and postintentional volition stages that a user goes through on the path to adhering to IS security guidelines for remaining vigilant toward phishing attempts. The results from the first phase will improve understanding of the different stages as well as inform the design of interventions for subsequent studies in our research program. Thus, our research questions for the first phase, a field survey, are:

1. Are there distinct stages that distinguish end-users’ no/low intention to actual behavior change for consistently higher vigilance toward phishing attempts?
2. If so, can this research study confirm three distinct stages?
3. What characterizes these qualitatively different stages?

Once the number of stages have been determined and characterized, the next phase, a longitudinal field experiment, of our research program will be implemented to study the following research question:

4. To what degree do stage-specific interventions help end-users to move to higher stages?

Previous Research in Phishing

Proudfoot et al. (2011) categorized the extant phishing literature, a subset of IS security research, as follows: 1) methods that phishers use in their attacks, 2) anti-phishing technologies, and 3) human factors, or the user side of phishing. The third category informs this research program. Research that concentrates on how humans interact with phishing attempts includes the following: antecedents of users’ behavior with respect to phishing attempts (Ng et al. 2009; Parrish Jr. et al. 2009; Workman 2008), how training may be used to decrease user response to phishing attempts (Dodge Jr. et al. 2007; Ferguson 2005; Kumaraguru et al. 2008; Sheng et al. 2010), and how users may detect deception in phishing attempts (Kumaraguru et al. 2010; Vishwanath et al. 2011; Wright and Marett 2010).

Antecedents: Perceived susceptibility, perceived benefits, and self-efficacy were uncovered as antecedents of users’ reactions to phishing attempts (Ng et al. 2009). In a different study (Workman 2008), three threat control factors were predictive of social engineering success: threat assessment, commitment, trust,
and obedience to authority. Since obedience to authority and normative commitment can vary with personality, Parrish Jr. et al. (2009) extended social engineering research by developing a framework that incorporates the Big-Five personality traits as antecedents of Phishing Susceptibility.

Training: In a series of phishing exercises at the United States Military Academy, researchers (Dodge Jr. et al. 2007; Ferguson 2005) studied the impact of training upon the propensity of people to respond to phishing attacks. They found that training did reduce the propensity of a student to respond to phishing attacks and increase the number of students who reported that a phishing attack had occurred. Sheng et al. (2010) found that exposure to training materials lowered the tendency for users to enter information into phishing sites by 40%; however, the improved vigilance made users overly cautious and not click on non-phishing email. This study supported earlier research that found that participants who received specialized phishing training, PhishGuru, were significantly less likely to respond to mock phishing attacks one week after training (Kumaraguru et al. 2008).

Deception Detection: Phishing emails are a subset of scams, or deceptive messages designed to gain something of value from users. In general, participants with more Web experience and security awareness were less likely to be deceived by phishing attempts (Wright and Marett 2010). Because handling phishing emails is not a primary task for a user, users are often forced to make quick decisions about the email based on straightforward cues found in the email. However, cues about urgency in the email and email load may interfere with the user’s ability to detect deception (Vishwanath et al. 2011). Users who receive training about recognizing the characteristics of phishing email can leverage that knowledge on top of using advanced anti-phishing technologies to combat phishing (Kumaraguru et al. 2010).

**Adopting Behavior Change Models from Health-Related Fields**

Identifying and dealing with phishing email according to IS security training and reminders can be a complex undertaking for many users, especially as they move from a low or no intention to consistent behavior changes. Importantly, there are parallels between changing people’s intention to actual behavior that could proactively improve their health and/or safety and changing IS users’ intentions to engage in consistently protective behavior. Both types of behavior have serious consequences if not changed from intent to behavior applied on a consistent basis. Health- or safety-compromising behaviors have grave consequences, such as death. In the IS context, risky or lax behavior can result in identity theft or in computer viruses that can destroy data stored on computers. In extreme cases, identity theft can take long periods of time to resolve and recover (President’s Identity Task Force 2007).

Complying with complicated health, safety, or risk-reducing behaviors is a learned and acquired type of behavior that often progresses through several stages (e.g., ARRM, Catania et al. 1990). For example, with respect to flossing teeth as a protective health behavior, people have to learn not only the risks of not flossing properly and the costs (e.g., high dental bills) of non-compliance, but also the benefits and self-mastery (self-efficacy) of flossing. At the outset, people who first learn about dental flossing may not believe that they need to floss regularly because they have not progressed beyond an initial stage of denial. With public service messages (cues to action), a better understanding of the risks/benefits, and confidence in the ability to floss effectively, people can move to the next stage, or intention to floss. Finally, after encountering different public service messages/training, many people move to the final stage on the continuum of flossing/non-flossing in which they actually took the action to floss on a regular basis. However, even though people acknowledge the benefits of flossing, they may regress to not flossing when distracted by life events or breaks in routine.

An email user who has not advanced through all stages to engage in protective behavior consistently would agree that becoming a phishing victim is not good, but he may not remain vigilant at all times. As a result, he may click on a link that looks legitimate because it appears to link to a web site with low perceived risk, such as his bank. Phishing research (e.g., Vishwanath et al. 2011; Workman 2008) has been conducted under the assumption that all users are in the final stage of understanding and acceptance of how they need to be vigilant against phishing attempts but that research does not consider to which stage a user has progressed. A user in an earlier stage may not have absorbed the training, had the right type of experiences to understand the severity and consequences of the problem, nor gained the tools to cope with phishing attempts in the same way that a user who has moved forward to the final stage of the continuum of non-protective/protective behavior. Thus, using stage models to research phishing and IS
security offers a promising theoretical base. Recently, Myyry et al. (2009) examined compliance with IS security policies using Kohlburg’s six-stage theory of moral cognitive development. In summary, the use of health behavior change models, empirically tested as successful in moving respondents from intention to behavior (Lippke et al. 2007; Velicer et al. 2007; Weinstein et al. 1998), is appropriate for our context of examining how IS users move from intention to protective behavior.

**Previous Research in Health Behavioral Change Models**

Continuum and stage theory behavioral change models in health-related fields have been developed to explore behaviors that protect health as well as the corresponding interventions that can encourage people to engage in safer health practices by moving from intention through behavior change. Continuum models include: the Theory of Reasoned Action (TRA) (Ajzen and Fishbein 1980; Fishbein and Ajzen 1975), TPB (Ajzen 1988; Ajzen 1991), HBM (Becker and Rosenstock 1987; Janz and Becker 1984; Rosenstock 1966), and the Protection Motivation Theory (PMT) (Maddux and Rogers 1983; Rogers 1975). In continuum models, there is an assumption that when people form the intention to change behavior, they will make the shift to actual behavior change. The intention predicts the behavior change in a static model. However, in a static model, it is difficult to capture the “if”, “how”, “when”, and “reasons why” a person moves from intention to actual behavior changes. This is referred to as the “intention-behavior gap,” or black box, that is difficult to study (Sheeran 2002). Therefore, a serious limitation of continuum models is that they provide a better explanation for changes in intention than for changes in behavior because they cannot account adequately for the shift from intention to behavior. Obstacles or distractions can derail the intention-behavior translation. Also, continuum models assume that interventions can occur in any order to move a person from denial to intention to behavior change (Schwarzer 2008).

In contrast, ARRM (Catania et al. 1990), the Transtheoretical Model (TTM) (Prochaska et al. 1992), and the Precaution Adoption Process Model (PAPM) (Weinstein 1988) are examples of stage theory models. “The term stage may be best understood as implying an important marker in the change process” (Catania et al. 1990). A stage theory includes four defining properties: 1) a way to classify and define the stages, 2) a sequence for the stages, 3) common hurdles to overcome before moving to the next stage, and 4) different hurdles to overcome at each stage. In most stage theories, people have the opportunity to move from an initial stage, in which they do not plan to change their behavior because they do not see a problem with it, to later stages in which they are taking action toward safer behavior.

One problem with stage theory models is that it can be difficult to delineate different qualitative stages: How many are needed? What are the differences between stages? Can a person regress from one stage to another? Is there a requisite length of time to move from one stage to another? In view of these types of questions, researchers point out that people may not move through stages but rather they may occupy points along a continuous process (Sutton 2000; Sutton 2005; Weinstein et al. 1998). Due to their inherent time-dependent sequence of phases, stage models can be challenging to assess. Nevertheless, recent empirical studies using stage models have provided support that intention to active protective behavior does change through stages (Lippke et al. 2007; Velicer et al. 2007; Weinstein et al. 1998).

**Health Action Process Approach (HAPA) Model**

To overcome the disadvantages of both types of models, a hybrid continuum-stage model, the Health Action Process Approach (HAPA) Model (Schwarzer 1992; Schwarzer 1999; Schwarzer 2001), was developed by building on: Social Cognitive Theory (SCT) (Bandura 1986), TPB (Ajzen 1988; Ajzen 1991), and the Stages of Change (SOC) Theory (Prochaska et al. 1992). HAPA resembles a continuum model except that it contains two phases: motivational (pre-intentional) and volitional (post-intentional). The two phases are comprised of three stages; the pre-intentional phase contains Stage 0 and the post-intentional phase contains Stages 1 and 2. Stage 0 includes those people, called Low Intenders, who have not formed even the intention to make behavioral changes. The post-intention phase is comprised of people in two distinct stages: Intenders (Stage 1), who have formed the intention to make behavioral changes and Actors (Stage 2), who have crossed the intention-behavior gap. A key strength of this model is in its simplicity of three stages, common to other health behavior stage models (e.g., the Model of Action Phases (MAP) (Heckhausen and Gollwitzer 1987), the Integrated Change (I-change) Model (de Vries et al. 2005;
People in a pre-intentional phase are concerned with the continuum-oriented constructs including: Outcome Expectancies, Action Self-Efficacy, and Risk Perception. In contrast, the post-intentional participants can be influenced by the “how to” constructs, Planning and Recovery Self-Efficacy for behavior maintenance and recovery in case of a relapse. The HAPA model is depicted in Figure 1.

In the continuum part of the model, Outcome Expectancies are the personal consequences that can arise from adopting new health-promoting behaviors (Bandura 1997). Antecedents (not explicitly depicted in the model) of Outcome Expectancies include: Threat (Perceived Susceptibility x Perceived Severity) and Threat Appraisal overlap with other health behavior models, such as PMT and HBM (Armitage and Conner 2000). Risk Perception is what an individual perceives is the risk of not performing the new behaviors. Intention represents an individual’s goals. Action/Coping Planning involve detailed plans to deal with moving from intention to action and dealing with barriers that could obstruct progress to less risky behavior. Outcome Expectancies and Risk Perception, along with Action Self-Efficacy, predict whether people can form good intentions toward behavior changes.

HAPA shares the Self-Efficacy construct with several continuum theories: SCT (Bandura 1986), the revised version of TPB (which uses a similar construct of perceived behavioral control) (Ajzen 1991), and PMT (Maddux and Rogers 1983). A key difference is that HAPA breaks Self-Efficacy (Bandura 1997) into three parts, each of which corresponds to a stage in the model: Action Self-Efficacy, Maintenance Self-Efficacy, and Recovery Self-Efficacy. Action Self-Efficacy (aka Pre-action Self-Efficacy, Motivational Self-Efficacy, or Task Self-Efficacy), a construct of the pre-intention stage, refers to the ability of the individual to envision either success or failure at changing to less risky behavior. With high Action Self-Efficacy, the individual is more likely to move to the next stages because she believes that she has the ability not only to perform a specific behavior but also that she can control changing her behavior (Luszczynska and Schwarzer 2003). To move to the post-intention phase, a person needs not only high Action Self-Efficacy but also confidence in her ability to maintain the new behaviors when confronted by obstacles through high Maintenance (or Coping) Self-Efficacy. Thus, Maintenance Self-Efficacy predicts behavior change and is critical during the stage in which an individual moves from pre-intention to an intention to change behaviors. Finally, the ability to recover in case of a setback in the adoption of the new behaviors is a key factor in moving to the Action phase. High Recovery Self-Efficacy, in addition to high Action Self-Efficacy and high Maintenance Self-Efficacy, is essential in getting beyond a relapse via an action plan to continue the health-promoting behaviors.
The mediator, Planning, between intention and behavior permits an individual to cross the intention-behavior gap. Planning makes sense only when one has formed an intention (Sheeran et al. 2005). Failure in translating intention into action occurs when a person does not know what to do in what sequence or how to deal with obstacles when adopting new behaviors. Planning is comprised of Action Planning and Coping Planning. Action Planning deals with what sequence of actions need to be used in what situations for the new behaviors. If a person spots a phishing attempt, he needs to know to whom to report it. Coping Planning permits an individual to prepare for inevitable problems in the way of new behaviors or routines. For example, a user needs to know what to do if he does get hooked by a phishing attempt. Planning predicts successful adoption of new behaviors.

The stages in this model can be adapted to fit the phishing context: a user moves from an initial or baseline stage in which a person does not acknowledge that there is a problem, to recognition of risky IS behavior with intention to reduce high-risk user behavior, and, ultimately, to the final stage of taking action. The continuum part of the model will be adapted from HAPA and will incorporate individual and environmental characteristics as control variables.

**Research Model for Examining IS Protective Behavior**

Next, we introduce our proposed 3-stage research model (see Figure 2), the Security Action Stage Model (SASM), adapted from HAPA:

**Stage 0 (Low Intender):** At this stage, individuals may not exhibit protective behavior (e.g., not clicking on a link in an email) because their perception of being vulnerable to phishing attempts is low; thus, their intention to change behavior is non-existent or low. Although they may or may not have received training about phishing attempts, they do not intend to behave securely because they think that the probability of falling for a phishing attempt is close to zero.

**Stage 1 (Intender):** Individuals who reach this stage will realize that they are indeed vulnerable to phishing attempts. Thus, the individual has a higher level of intention to make behavioral changes, such as actively learning about and being attentive to cues typically contained in phishing emails. However, he may not apply the behavior consistently nor know how to cope with a successful phishing attempt.

**Stage 2 (Actor):** At this stage, individuals take active steps to prevent any future phishing attempts and have moved to consistent behavior. These steps include developing an action or coping plan in case they click on a phishing attempt, taking an active role in learning about phishing precautions, using the recommendations from anti-phishing software, and remaining vigilant for potential phishing attempts.
Movement from stage to stage: An external motivator, such as an intervention that explains how to cope in case a person has been hooked by a phishing attempt, is needed for an individual to move to the next stage. Different interventions will lead to different movement along stages. If the same intervention would lead to movement from one stage to another, irrespective of a user’s stage, then we could design one intervention that would be applicable to all users in all stages, and stages would be unnecessary (Weinstein et al. 1998). However, researchers in health-related fields have documented that different interventions are indeed required to move people to one stage to the next (Weinstein and Sandman 1992).

Proposed Research Methodology

First phase: In the first study in our research program, we will administer online survey questions and a short phishing quiz to participants in a cross-sectional study to examine the stages and predictive constructs in our model. The survey instrument will contain constructs/items identified by a literature review and will include established, reliable, and validated scales designed to measure the seven SASM variables (Outcome Expectancies, Risk Perception, Action Self-Efficacy, Intention, Coping Self-Efficacy, Action/Coping Planning, Coping Self-Efficacy, and Recovery Self-Efficacy) as well as questions related to experiential and individual control variables, such as previous phishing experience in Web and email contexts. In this particular study, behavior (IS Secure Behavior) will not be captured because the intent is to classify respondents into stages according to the seven SASM variables. The short phishing quiz, adapted from OnGuardOnline.gov, tests knowledge about phishing in Web and email contexts.

Our goal is to include both students and non-students in an overall data sample that represents the population who encounter phishing attempts. While our subjects will be drawn mainly from the student population of a large university, the study will be open to the general public via the Internet using a snowball sampling plan. Undergraduate business students enrolled in an MIS class will be the initial contacts asked to participate in this survey. These participants will be asked to recruit 0-5 friends who are not enrolled in the same class to fill out the survey. Extra credit will be offered for participation and for referring snowball participants who complete the survey successfully. No identifying information will be collected from the subjects. The expected time to take the Likert-style survey will be a maximum of 45 minutes.

Because we plan to collect data from approximately 400 participants, we will have a sample size which should be large enough to analyze the data in a statistical manner. To rule out potential bias and to ensure that the groups’ data can be combined for analyses, we will conduct ANOVA comparisons to confirm that there were no differences between subject groups. The data will be analyzed in SPSS using ANOVA, factor analysis, and exploratory cluster analysis. Standard tests of reliability, internal and external validity, and factor analyses for each scale and sub-scale will be conducted. After administration of the scales, descriptive statistics regarding size of sample, response ranges, and standard deviations for each scale will be provided. Following previous studies of HAPA (e.g., Schüz et al. 2009) and from the IS literature (Sabherwal and King 1995), exploratory cluster analysis techniques (hierarchical followed by K-means) will be used to analyze the SASM model to determine the number of discrete stages and what characterizes those stages. First, an agglomerative hierarchical cluster analysis using within-groups method of average linkage and Euclidean distance measures will be performed on the model’s constructs. The number of clusters identified by this analysis will be the optimal number to be used in the subsequent K-means cluster analysis. Finally, after conducting analyses for stability and validity for the cluster solution, we will compare the means of the model’s constructs to develop profiles for the distinct stages.

Second phase: Once we have determined the number of stages in the first study, we will proceed to the next phase, a longitudinal field experiment, of our research program. The purpose of the role-playing email phishing experiment patterned after earlier phishing experiments (e.g., Kumaraguru 2009; Sheng 2009) will be to examine over time the effects of stage-appropriate interventions designed to move users from one stage of the SASM model to a higher stage. Assuming that three clusters emerge from the first study, the two interventions designed for this particular experiment are separate single-page informative messages that use cartoon characters to convey simple messages. These interventions are re-fabrications of the landing page that was carefully created through several iterations with focus groups by Kumaraguru (2009) and that is now incorporated at the Anti-Phishing Working Group (APWG) web site. The current landing page at APWG contains a ‘one-size-fits-all’ approach that had to be modified for research about
interventions for stages. Thus, the first intervention is designed to move IS end-users in the Low Intender stage to Intender; the second intervention has been reworked to move Intenders to Actors.

To determine what stage a person is in before and after a treatment, we will administer pre- and post-experiment survey questions, including scales to measure the seven SASM constructs, to participants. The on-line survey instruments will be a subset of the survey used in initial research study that focuses on phishing in an email context only. The pre-survey and experiment participation will be separated by a time of at least two weeks to avoid priming and/or recency biases. To avoid any form of education or training in the pre-experiment survey, the phishing quiz will not be included in the pre-experiment survey. The post-survey, administered one week after the experiment, will include: self-reported stage membership, the same seven SASM variables as in the pre-experiment survey, and the phishing quiz used in the first study. The one-week delay between the experiment and the post-survey is an attempt to capture stage changes that may not occur immediately after the experiment. One major drawback of splitting apart the pre-experiment survey, experiment, and post-experiment across several weeks is attrition of the participants; however, participants will be cautioned in the recruiting and disclosure material that they will not receive any incentives (e.g., extra credit) unless they complete the pre-experiment survey, experiment, and post-experiment survey.

In the online experiment, we will manipulate participants in a 3x3 experiment crossing stage membership (Stage 0, Stage 1, Stage 2) with intervention type (No intervention; Intervention #1; Intervention #2) design. Subjects will be randomly assigned to a treatment group. We will capture IS Secure Behavior before and after the treatment through respondents’ actions (e.g., choosing to click on a link or ignore email) in the role-play experiment in which respondent have to process pre-treatment emails and post-treatment emails (e.g., legitimate email without links, spam email with links, phishing email) set up in a counter-balanced design patterned after previous experiments (Kumaraguru 2009; Sheng 2009). Because we plan to collect data from approximately 600 participants, we will have a sample size with adequate statistical power. The goal of the data analyses will be to show that movement to higher stages occurs only when the appropriate intervention was administered. This will be demonstrated by running an ANOVA for a 3x3 experiment crossing stage membership (Stage 0, Stage 1, Stage 2) with intervention type (No intervention, Intervention #1, Intervention #2). The change in stage membership will be calculated based on centroid values for each stage. Kruskal-Wallis will be used to test for significance of effects by intervention type.

Next steps: Future phases of the research program will include different and larger sample groups, longer-term longitudinal studies that capture actual user behavior and how it relates to the stage a user is in, and a focus on other Information Security behavior, such as compliance with password policies.

**Conclusion**

Before discussing the potential contributions of this research, we need to focus on limitations of these preliminary studies. First, limitations stem from the nature of the proposed model, a stage theory model. Our current model proposes three stages through which the user moves. It may be possible that there are more or fewer than three stages. Future studies need to investigate if there are a different number of stages for this type of behavioral change. Next, our samples are not going to be a random sample but rather convenience samples comprised mainly of student subjects. Future research should examine this model with users in different settings, such as employees of different types of organizations. Finally, the behavior data from a role-playing field experiment may differ from actual user behavior.

This proposed research will contribute to the existing research stream on IS security and social engineering, specifically focused on phishing. First, the proposed model is a hybrid continuum-stage model adapted from health-behavior change models and applied to the phishing context. A key strength of this type of model closes the intention-behavior gap. Second, the longitudinal nature of the model will permit us in future studies to empirically test causal relationships that previously were only implied by cross-sectional research. Third, exploring and characterizing the various stages along which a user must progress toward secure IS behavior will help researchers identify to which stage a user has evolved. Studying vigilance or susceptibility with respect to phishing may not be relevant until a user reaches the final stage. Finally, the longitudinal design proposed for the second study of this research plan will permit researchers to track movement through stages over period of time; thus, causality can be established.
References


Anti-Phishing Phil. 2011. from http://cups.cs.cmu.edu/antiphishing_phil/


