Adapting the Transtheoretical Model for the Design of Security Interventions

Cori Faklaris
Carnegie Mellon University
Pittsburgh, PA 15213, USA
cfaklari@cs.cmu.edu

Laura Dabbish
Carnegie Mellon University
Pittsburgh, PA 15213, USA
dabbish@cs.cmu.edu

Jason Hong
Carnegie Mellon University
Pittsburgh, PA 15213, USA
jasonh@cs.cmu.edu

Abstract
The continued susceptibility of end users to cybersecurity attacks suggests an incomplete understanding of why some people ignore security advice and neglect to use best practices and tools to prevent threats. A more detailed and nuanced approach can help more accurately target security interventions for end users according to their stage of intentional security behavior change. In this paper, we adapt the Transtheoretical Model of Behavior Change for use in a cybersecurity design context. We provide a visual diagram of our model as adapted from public health and cybersecurity literature. We then contribute advice for designers' use of our model in the context of human-computer interaction and the specific domain of usable privacy and security, such as for encouraging timely software updates, voluntary use of two-factor authentication and attention to password hygiene.

Author Keywords
Theoretical models; usable privacy and security; social cybersecurity; collaborative systems; design theory; user experience design; interaction design.

ACM Classification Keywords
H.1.2. [MODELS AND PRINCIPLES]: User/Machine Systems - Human factors.

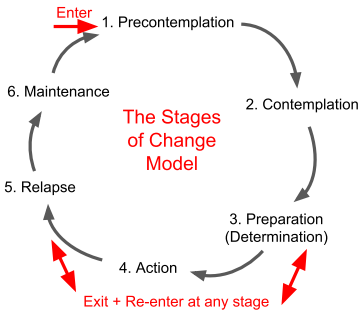

Figure 1: The Transtheoretical Model of Behavior Change. A person might enter the process of change at Precontemplation; progress to Contemplation and to Preparation (also called Determination), before arriving at Maintenance. Relapse can lead to any stage. A person may enter or exit at any point.

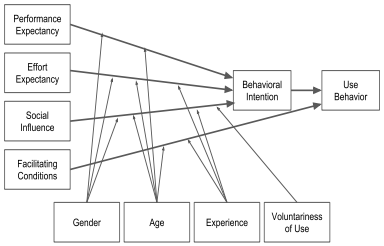

Figure 2: The Unified Theory of Use and Acceptance of Technology, which shows Performance Expectancy, Effort Expectancy, Social Influence and Facilitating Conditions as direct causes of Behavior Intention and Use Behavior, with Gender, Age, Experience, and Voluntariness of Use as moderating factors.

Introduction

A 2017 Pew Research Center study [13] contained sobering statistics on general attitudes and behaviors in the U.S. around cybersecurity issues. The survey found that 64% of Americans had personally experienced a major data breach and that 49% felt that their personal data was less secure than five years previously. Yet, many failed to follow best practices recommended by experts. For instance, 84% rely on memorization or pen and paper to keep track of online passwords rather than using an encrypted file, saving them in a browser or using a password management program.

This data underline the significance and broader impact that could result from use of a tool to design more effective interventions for security behavior change in end users. To this end, we have adapted Prochaska and DiClemente's *Transtheoretical Model of Behavior Change* [14,20]. This model has already been identified as useful for privacy and security research [1,2,9,16]. It posits that "behavior change is a process that unfolds over time through a sequence of stages" and that individuals need planned interventions matched to their stages of change in order to move them toward and maintain desired actions [14].

Our contributions in this paper are the following:

- A visual diagram and chart of each stage's associated intervention strategy, as adapted from medical and wellness and HCI literature.
- Advice for designers' use of our model in the context of human-computer interaction and the usable privacy and security, such as for encouraging timely software updates, voluntary use of two-factor authentication and attention to password hygiene.

Background and Related Work

Security sensitivity is defined by Das as "the awareness of, motivation to use, and knowledge of how to use security tools" [3]. Das and collaborators based this construct on prior findings that many people believe themselves in no danger of falling victim to a security breach and are unaware of the existence of tools to protect them against those threats; they perceive the inconvenience and cost to their time and attention as outweighing the harm of experiencing a security breach, and they think they are too difficult to use or lack the knowledge to use them effectively [3–5]. This conception builds in turn on work from Davis et al. [6,7] on user perceptions of usefulness and ease of use, from Egelman et al. [10]'s adaptation of the Communication-Human Information Processing cognitive model to end-user security, and from Rogers' Diffusion of Innovations theory [15] of how messages spread in a social network about a "new ideal."

Our search for a model that better encapsulates shifts in end-user security decisions over time led us to Prochaska and DiClemente's *Transtheoretical Model of Behavior Change* [8,14,21]. This model has been identified in the literature as a useful framework for privacy and security research [1,2,9,16]. It seems to be a good candidate to further extend the Technology Acceptance Model (TAM) and Unified Theory of Use and Acceptance of Technology [7,18,19] for addressing social-behavioral issues in human-computer interaction.

The TTM marks a shift from thinking of behavior change as occurring in a single, decisive moment to that of a longer-term, cyclical process in which people balance pros and cons along with self-efficacy (belief in their ability to achieve goals) and temptation (desire for

Evidence of End Users' Stages of Change

What users will communicate in words or behaviors that marks their current stage of security behavior change:

Precontemplation: *"I don't need to use / have time to use security practices … "*

Contemplation: *"I worry I don't use / I may want to use security practices … "*

Preparation (Determination): *"I want to change / I need to change my security practices …"*

Action and Maintenance: *"I intend to use / I know why to use / I am already using / I value security practices … "*

short-term enjoyment at the expense of long-term goals) in their decision making. A key assumption that drives TTM theory, research and practice is that, unlike with stages of physical and psychological development, people do not possess any "inherent motivation to progress through the stages of intentional change"; and thus, individuals need planned interventions matched to their stages of change in order to move them toward desired actions and maintenance of their new behaviors [37]. In medicine and public health, the TTM has been used for interventions to encourage exercise [11], smoking cessation [8,17] and sobriety [12].

Cyclical Model of Security Behavior Change

As shown in Figure 3, our model situates the TTM Stages of Change with Goals or Tasks for interventions that enable transition to the next stage. Creating *awareness* and interest in security practices will move end users from Precontemplation to Contemplation; *motivating* users and changing their values will move them further to Preparation (or Determination); and giving users the specific *knowledge* of practices is key to moving them into *Action.* Creating *reinforcement* conditions for these actions will help users move into the Maintenance stage. It is very likely that *resistance* sometimes will arise in users, moving them into Relapse. If this resistance solidifies into *denial* of the need to use security tools and practices*,* however, the end user falls back into the Precontemplation stage.

A person moves through the stages as they are impacted by either a negative or positive balance of pros and cons (the factors of Performance Expectancy, Effort Expectancy, Social Influence and Facilitating Conditions) along with Self-Efficacy and Temptation. These situational and social factors are drawn from

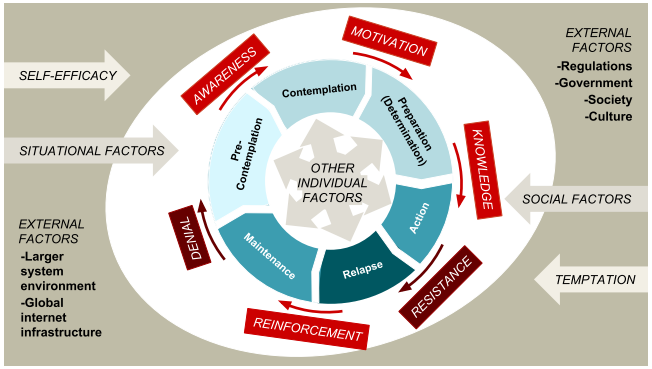

Figure 3: The Cyclical Model of Security Behavior Change incorporates the TTM Stages of Change with Goals or Tasks for interventions that enable transition to the next stage. A person moves through the stages as they weigh pros and cons comprised of situational and social factors (Performance Expectancy, Effort Expectancy, Social Influence and Facilitating Conditions), along with Self-Efficacy and Temptation. As in other user acceptance models, these are moderated by individual factors of Gender, Age, Experience and Voluntariness of Use.

theories of technology acceptance and use by Davis et al. [7,18,19] and Venkatesh et al. [25,26] and from TTM theory [9,28]. These also are moderated by four individual factors as drawn from Venkatesh et al. [ibid]: Gender, Age, Experience and Voluntariness of Use. The change cycle is situated in a larger system of social, cultural, political and environmental contexts of use.

How Designers Can Use the Model

Designers can and should make use of insights into how change occurs from the TTM literature, as summarized in in the following, when ideating, prototyping and testing interventions for security behavior change.

Examples of Successful Results for Each Stage

What users will communicate in words or behaviors that documents a successful intervention, by stage:

Precontemplation: *"It may be a good idea to use security practices … "*

Contemplation: *"I will regret it if I do not start using security practices … "*

Preparation (Determination*): "I feel better for committing to my chosen security practices …"*

Action and Maintenance: *"I ask for help with using / I get help with using / I am successful with / I keep improving my security practices … "*

Individuals in the Precontemplation stage are described as resistant or unmotivated to change their high-risk behaviors, which in our research and the work of Das et al.[3,5] corresponds to statements from people such as "I am too busy" or "It is a lost cause" to use recommended security tools and advice, even "It is a sign of paranoia" to use recommended tools and "There are good reasons" why to not use them. For these individuals, the processes of change thought in the TTM framework to be most effective are *Consciousness-raising, Dramatic relief* and *Environmental re-evaluation,* to increase their awareness, emotional response and empathy for how their behaviors affect themselves and others [14].

These processes of change can also be effective for those in the Contemplation stage, who are beginning to doubt their negative attitude toward change (corresponding to a statement such as "I worry about the impact of my lax security behaviors"), but the focus shifts to *Self re-evaluation,* combining cognitive and affective assessments of how unhealthy habits affect their self-image and confidence; followed by *Self liberation* and *Social liberation* for the Preparation/Determination stage ("I want to change" or "I need to change" statements from end users). In the latter stage, a public commitment to behavior change can be particularly effective [14], which echoes Das et al.'s findings that social influence techniques such as observable adoption of security behaviors can drive secure behavior adoption by social ties [4].

Under the TTM framework, it is the individuals already in the Action and Maintenance stage who are the ones who benefit most from the interventions that are probably the most common in end-user security today: *Contingency management*, or the application of positive sanctions and punishments to drive behavior; *Helping relationships,* such as buddy systems and coaching sessions; *Counterconditioning,* the learning of desired behaviors to substitute for problem behaviors; and *Stimulus control,* such as interface or systems re-engineering to reduce cues that lead to problematic behaviors and to add prompts for the desired behaviors. The Action and Maintenance stages are signified by statements from end users such as "I am extremely knowledgeable" and "I diligently follow a routine" about cybersecurity (keeping in mind that the user's self-perceived state of knowledge or actions may not accurately reflect actual knowledge or actions).

Conclusion and Future Work

In this work, we adapted the *Transtheoretical Model of Behavior Change* for use in a cybersecurity design context. We provided a visual diagram of each stage's associated intervention strategy as adapted from medical and wellness literature. We then contributed advice for designers' use of our model in the context of human-computer interaction and the specific domain of usable privacy and security, such as for encouraging timely software updates, voluntary use of two-factor authentication and attention to password hygiene.

Our next steps will be to validate this design model through research into the model's effectiveness for guiding the design and implementation of interventions for security behavior change among everyday computing users. We hope these studies will create lasting and usable knowledge of why some people ignore security advice and neglect to use best practices and tools to prevent threats.

References

[1] P. Briggs, D. Jeske, and L. Coventry. 2017. Chapter 6 - Behavior Change Interventions for Cybersecurity. In *Behavior Change Research and Theory*, Linda Little, Elizabeth Sillence and Adam Joinson (eds.). Academic Press, San Diego, 115–136. DOI:https://doi.org/10.1016/B978-0-12-802690-8.00004-9

[2] S. Charney. 2012. Collective Defense: Applying the Public-Health Model to the Internet. *IEEE Secur. Priv.* 10, 2 (March 2012), 54–59. DOI:https://doi.org/10.1109/MSP.2011.152

[3] Sauvik Das. 2017. Social Cybersecurity: Reshaping Security Through An Empirical Understanding of Human Social Behavior. *Dissertations* (May 2017). Retrieved from http://repository.cmu.edu/dissertations/982

[4] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (CCS '14), 739–749. DOI:https://doi.org/10.1145/2660267.2660271

[5] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15), 1416–1426. DOI:https://doi.org/10.1145/2675133.2675225

[6] Fred D. Davis. 1989. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q.* 13, 3 (1989), 319–340. DOI:https://doi.org/10.2307/249008

[7] Fred D. Davis, Richard P. Bagozzi, and Paul R. Warshaw. 1989. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Manag. Sci.* 35, 8 (August 1989), 982–1003. DOI:https://doi.org/10.1287/mnsc.35.8.982

[8] Carlo C. DiClemente, James O. Prochaska, and Michael Gibertini. 1985. Self-efficacy and the stages of self-change of smoking. *Cogn. Ther. Res.* 9, 2 (April 1985), 181–200. DOI:https://doi.org/10.1007/BF01204849

[9] Ersin Dincelli and Shobha Chengalur-Smith. 2017. Applying the Transtheoretical Model of Behavior Change to Online Self-Disclosure. *ICIS 2017 Proc.* (December 2017). Retrieved from http://aisel.aisnet.org/icis2017/Security/Presentations/21

[10] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You'Ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '08), 1065–1074. DOI:https://doi.org/10.1145/1357054.1357219

[11] C. Lee. 1993. Attitudes, knowledge, and stages of change: a survey of exercise patterns in older Australian women. *Health Psychol. Off. J. Div. Health Psychol. Am. Psychol. Assoc.* 12, 6 (November 1993), 476–480.

[12] Robert J. Meyers, Hendrik G. Roozen, and Jane Ellen Smith. 2011. The Community Reinforcement Approach. *Alcohol Res. Health* 33, 4 (2011), 380–388.

[13] Kenneth Olmstead and Aaron Smith. 2017. Americans and Cybersecurity. *Pew Research Center: Internet, Science & Tech*. Retrieved November 7, 2017 from

http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[14] J. O. Prochaska and W. F. Velicer. 1997. The transtheoretical model of health behavior change. *Am. J. Health Promot. AJHP* 12, 1 (October 1997), 38–48.

[15] Everett M. Rogers. 2010. *Diffusion of Innovations, 4th Edition*. Simon and Schuster.

[16] Pei-Ju Lucy Ting. 2006. The Transtheoretical Model, Stages of Change and Decisional Balance as Predictors of Behavioural Change in Internet Privacy and Security. University of Manchester. Retrieved February 9, 2018 from http://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.603434

[17] Wayne F. Velicer, Carlo C. DiClemente, James O. Prochaska, and Nancy Brandenburg. 1985. Decisional balance measure for assessing and predicting smoking status. *J. Pers. Soc. Psychol.* 48, 5 (1985), 1279.

[18] Viswanath Venkatesh and Fred D. Davis. 2000. A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Manag. Sci.* 46, 2 (2000), 186–204.

[19] Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. User Acceptance of Information Technology: Toward a Unified View. *Manag. Inf. Syst. Q.* 27, 3 (2003), 5.

[20] G. L. Zimmerman, C. G. Olsen, and M. F. Bosworth. 2000. A "stages of change" approach to helping patients change behavior. *Am. Fam. Physician* 61, 5 (March 2000), 1409–1416.

[21] The Transtheoretical Model (Stages of Change). Retrieved October 23, 2017 from http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories6.html