Components of a Model of Cybersecurity Behavior Adoption

Cori Faklaris, *Carnegie Mellon University, cfaklari@cs.cmu.edu*

Abstract

Our research focuses on understanding how attitudes and social influences act on end users in the process of cybersecurity behavior adoption (or non-adoption). This work draws on five *expectancy-value* models and on four *stage* models that have been applied successfully in social psychology, marketing, and public health. In this talk, we will first give an overview of these models. We then will present the progress of our empirical mixed-methods research to craft a model specific to cybersecurity adoption that identifies the relevant (1) *attitudes* and (2) *social influences* acting at each step, along with (3) *tech characteristics* that are associated with sustained adoption. We will conclude with remarks on how our work can be of use to cybersecurity teams tasked with boosting awareness and/or adoption.

1. Motivation for Research

Computing systems are increasingly central to society, but many people do not understand enough about how they work or what cyber-threats to guard against [20]. McAfee cited the "lack of organization-wide understanding of cyber risks" in its estimate that the global costs of cybercrime had jumped more than 50% in 2019-20, to over $1 trillion [30]. But, fixing this problem is expensive; enterprise security training can cost around $300,000 and hundreds of staff hours [29]. To reduce costs and improve awareness and adoption, we believe that we should look outside of computer science and engineering and apply insights from social psychology, marketing, and public health.

Prior empirical studies have found that, as with mask-wearing [18] or vaccinations [16], people's *attitudes* [13] and *social contexts* [24,31] factor into the extent to which they engage in protective behaviors for cybersecurity (such as checking that their antivirus software is up-to-date or keeping their account password confidential). Further, work to create the SA-13 security-attitude inventory [3] has identified four factors -- Resistance, Concernedness, Attentiveness, and Engagement -- that weigh in a person's cybersecurity decisional balance [19]. These findings echo stage models in public health [15] such as the Transtheoretical Model [9,12,25,34] and the Precaution Adoption Process Model [37,38], each successful in promoting measures such as smoking cessation and home radon tests. Now, we seek to integrate these findings with other proven models of behavior adoption, such as Diffusion of Innovations [27] concepts of successful *tech characteristics*, and with empirical data from end users to provide insights specific to cybersecurity.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021. August 11 - 13, 2021, virtual event.

2. Prior Models of Behavior Adoption

1.1. Expectancy-Value Models

Many models of behavior adoption have followed Vroom's theory that people act as a result of expectancy (how likely an individual perceives that a desired, instrumental outcome will occur) and value (how much the individual perceives that outcome to have importance or utility) [32,33,36]. Five of the most well-known are the following:

Decisional Balance Theory [3,19] posits that people weigh the pros and cons of a decision, with action taking place once the possible benefits and self- and social-approval from the action outweigh the likely costs or disapproval.

The *Health Belief Model* [15,23] sets forth five components that lead to action: background factors, motivation, perceived risks, perceived tradeoffs, and cues to action.

The *Theory of Reasoned Action/Theory of Planned Behavior* [1,14,21] presents attitudes, norms and perceived behavioral control as key moderators of how background factors and beliefs lead to intention and action.

The *Technology Acceptance Model* [7,8,35] proposes that external variables (such as gender, age, and skills) and user appraisal (perceived ease of use, perceived usefulness, and user attitudes) lead to usage intention and to actual usage.

Protection Motivation Theory [22,28] argues that, in the presence of a threat, threat appraisal (perceived severity and vulnerability) and coping appraisal (perceived response efficacy and self-efficacy) will lead to intention and action.

Each of the above models have proven useful in human factors studies of cybersecurity. However, they lack a consideration of the progress of time and the consequent evolution of people's cognition and of social contexts for behavior.

1.2. Stage Models

The common thread in stage models is that they account for the progress of time, roughly following the *Lewin Change Model* of "unfreeze," "move," and "refreeze" [2,15]:

The *Transtheoretical Model* [12,25] proposes a cyclical process of precontemplation, contemplation/preparation,

determination to act, action, and either maintenance or relapse/termination.

The *Precaution Adoption Process Model* [37,38] breaks down inaction into four substages (unaware, unengaged, undecided, and decided not to act) and action into three substages (decided to act, action, and maintenance).

Diffusion of Innovations [27] integrates three submodels: adopter stages (innovator, early, early majority, late majority, and laggards), environmental factors (messaging channels, time, and social systems) and attractiveness of innovation (relative advantage, complexity, trialability, potential for re-invention, and observable effects).

Each has weaknesses. The Transtheoretical Model (TTM) has not been experimentally validated like the Precaution Adoption Process Model, while that model has not been as widely adopted as the TTM; neither account for social influences by stage. Diffusion of Innovations is the most complex to implement and is not suited for small-scale issues.

However, the strengths of each of these models is that they account for progress of time and the consequent evolution of people's cognition and of social contexts for behavior. This helps practitioners to better match their messaging to their target audience's receptiveness, and to avoid "one size fits all" tools or training that will be ignored or resented by a portion of those users for whom it is not suited.

3. Research in Progress

We seek to create an integrated model of behavior adoption that is specific to cybersecurity. Such a model will explicitly account for how either real or imagined threats impact people's thinking, along with their general attitudes toward cybersecurity and the influences of peers, authorities and/or media. It also will compare how the tech characteristics of specific security tools and practices impact each stage.

To create this cybersecurity adoption model, we are conducting two user research studies in Spring and Summer 2021. The first, a remote interview study with 12-16 participants, is being used to identify the stages of cybersecurity behavior adoption and the social influences [4,6,11,26] that are particularly relevant at each stage, along with participants' mental states [5,10], prior experiences of security breaches [13], and internet know-how [20]. A pre-interview screener scored participants by their attitudes toward cybersecurity [3,13] and by their awareness and adoption of practices in four general areas [10,17]: keeping software up-to-date, maintaining good password hygiene, staying alert for phishing, scammers and "fake news", and securing devices and networks.

The results are informing the design of the second study, an online survey deployed to 250 adults chosen at random across the U.S. This survey will give us data that can be generalized to the U.S. adult population, which we will use to assess the validity of the model created in the first study.

The resulting socio-cognitive model will help to move the field of usable security away from "one size fits all" strategies, paving the way for a classification algorithm to direct resources and match "interventions" (such as security tips or interface nudges) to those most likely to benefit.

Ultimately, we hope this model will boost the sensitivity of enterprise security applications that assess an organization's cybersecurity risks and inform the work of industry researchers on adoption of an array of solutions in their product-service systems, driving business value and improving the effectiveness of dollars spent.

Acknowledgements

For their helpful comments, thanks go to Jason I. Hong, Laura Dabbish, and Geoff Kaufman of the Human-Computer Interaction Institute, as well as the anonymous reviewers of this submission. This work was supported by the U.S. National Science Foundation, grant no. CNS-1704087. The author also has received fellowship support from the CyLab Security and Privacy Institute and the Center for Informed Democracy and Social Cybersecurity (IDeaS), both at Carnegie Mellon University.

References

[1] Icek Ajzen. 1991. The theory of planned behavior. *Organ. Behav. Hum. Decis. Process.* 50, 2 (December 1991), 179–211. DOI:https://doi.org/10.1016/0749-5978(91)90020-T

[2] Bernard Burnes and David Bargal. 2017. Kurt Lewin: 70 Years on. *J. Change Manag.* 17, 2 (April 2017), 91–100. DOI:https://doi.org/10.1080/14697017.2017.1299371

[3] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2021. SA-13, the 13-item security attitude scale. Retrieved from https://socialcybersecurity.org/files/SA13handout.pdf

[4] Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association Berkeley, CA. Retrieved August 28, 2019 from https://www.usenix.org/conference/soups2019/presentation/das

[5] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The effect of social influence on security sensitivity. In *Proceedings of the Symposium on Usable Privacy and Security*,

USENIX Association Berkeley, CA. Retrieved from https://www.usenix.org/system/files/conference/soups2014/ soups14-paper- das.pdf

[6] 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), ACM, New York, NY, USA, 1416–1426. DOI:https://doi.org/10.1145/2675133.2675225

[7] 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

[8] Fred D. Davis. 1993. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *Int. J. Man-Mach. Stud.* 38, 3 (March 1993), 475–487. DOI:https://doi.org/10.1006/imms.1993.1022

[9] Carlo C. DiClemente, James O. Prochaska, Scott K. Fairhurst, Wayne F. Velicer, Mary M. Velasquez, and Joseph S. Rossi. 1991. The process of smoking cessation: An analysis of precontemplation, contemplation, and preparation stages of change. *J. Consult. Clin. Psychol.* 59, 2 (1991), 295–304. DOI:https://doi.org/10.1037/0022-006X.59.2.295

[10] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (CHI '15), ACM, New York, NY, USA, 2873–2882. DOI:https://doi.org/10.1145/2702123.2702249

[11] M. Fagan and M. M. Khan. 2018. To Follow or Not to Follow: A Study of User Motivations around Cybersecurity Advice. *IEEE Internet Computing 22*, 25–34. Retrieved October 9, 2018 from doi.ieeecomputersociety.org/10.1109/MIC.2017.3301619

[12] Cori Faklaris, Laura Dabbish, and Jason Hong. 2018. Adapting the Transtheoretical Model for the Design of Security Interventions. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, Md., USA. Retrieved December 4, 2019 from https://doi.org/10.13140/RG.2.2.15447.57760

[13] Cori Faklaris, Laura Dabbish, and Jason I Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, USENIX Association Berkeley, CA, Santa Clara, CA, 18. Retrieved from https://www.usenix.org/system/files/soups2019-faklaris.pdf

[14] Martin Fishbein and Icek Ajzen. 2010. *Predicting and changing behavior: The reasoned action approach*. Psychology Press, New York, NY, US.

[15] Karen Glanz, Barbara K. Rimer, and K. Viswanath. 2008. *Health Behavior and Health Education: Theory, Research, and Practice*. John Wiley & Sons.

[16] Helge G. Hollmeyer, Frederick Hayden, Gregory Poland, and Udo Buchholz. 2009. Influenza vaccination of health care workers in hospitals—A review of studies on attitudes and predictors. *Vaccine* 27, 30 (June 2009), 3935–3944. DOI:https://doi.org/10.1016/j.vaccine.2009.03.056

[17] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. 327–346. Retrieved March 27, 2020 from https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[18] James R Mahalik, Michael Di Bianca, and Michael P Harris. 2021. Men's attitudes toward mask-wearing during COVID-19: Understanding the complexities of mask-ulinity. *J. Health Psychol.* (February 2021). DOI:https://doi.org/10.1177/1359105321990793

[19] Irving L. Janis and Leon Mann. 1977. *Decision making: A psychological analysis of conflict, choice, and commitment*. Free Press, New York, NY, US.

[20] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Symposium on Usable Privacy and Security (SOUPS)*, USENIX Association Berkeley, CA, 39–52. Retrieved from https://www.usenix.org/conference/soups2015/proceedings/presentation/kang

[21] Thomas J. Madden, Pamela Scholder Ellen, and Icek Ajzen. 1992. A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. *Pers. Soc. Psychol. Bull.* 18, 1 (February 1992), 3–9. DOI:https://doi.org/10.1177/0146167292181001

[22] James E Maddux and Ronald W Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *J. Exp. Soc. Psychol.* 19, 5 (September 1983), 469–479.

DOI:https://doi.org/10.1016/0022-1031(83)90023-9

[23] Boon-Yuen Ng, Atreyi Kankanhalli, and Yunjie (Calvin) Xu. 2009. Studying users' computer security behavior: A health belief perspective. *Decis. Support Syst.* 46, 4 (March 2009), 815–825. DOI:https://doi.org/10.1016/j.dss.2008.11.010

[24] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, USENIX Association Berkeley, CA, Baltimore, Md., USA, 83–102. Retrieved February 26, 2019 from https://www.usenix.org/conference/soups2018/presentation/park

[25] 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.

[26] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (CCS '16), ACM, New York, NY, USA, 666–677. DOI:https://doi.org/10.1145/2976749.2978307

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

[28] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *J. Psychol.* 91, 1 (September 1975), 93–114. DOI:https://doi.org/10.1080/00223980.1975.9915803

[29] Tara Seals. 2017. Cost of User Security Training Tops $290K Per Year. *Infosecurity Magazine*. Retrieved January 20, 2021 from https://www.infosecurity-magazine.com:443/news/cost-of-user-security-training/

[30] Zhanna Malekos Smith, Eugenia Lostri, and James A Lewis. 2020. *The Hidden Costs of Cybercrime*. McAfee.

[31] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. 2019. Normal and Easy: Account Sharing Practices in the Workplace. *Proc ACM Hum-Comput Interact* 3, CSCW (November 2019), 83:1-83:25. DOI:https://doi.org/10.1145/3359185

[32] B. Studer and S. Knecht. 2016. Chapter 2 - A benefit–cost framework of motivation for a specific activity. In *Progress in Brain Research*, Bettina Studer and Stefan Knecht (eds.). Elsevier, 25–47. DOI:https://doi.org/10.1016/bs.pbr.2016.06.014

[33] Wendelien Van Eerde and Henk Thierry. 1996. Vroom's expectancy models and work-related criteria: A meta-analysis. *J. Appl. Psychol.* 81, 5 (1996), 575–586. DOI:https://doi.org/10.1037/0021-9010.81.5.575

[34] 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.

[35] 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.

[36] V.H. Vroom. 1964. *Work and motivation*. Wiley, Oxford, England.

[37] Neil D Weinstein, Judith E Lyon, and Peter M Sandman. 1998. Experimental Evidence for Stages of Health Behavior Change: The Precaution Adoption Process Model Applied to Home Radon Testing. *Health Psychol.* 17, 5 (1998), 445–453. DOI:https://doi.org/10.1037/0278-6133.17.5.445

[38] Neil D. Weinstein and Peter M. Sandman. 1992. A model of the precaution adoption process: Evidence from home radon testing. *Health Psychol.* 11, 3 (1992), 170–180. DOI:https://doi.org/10.1037/0278-6133.11.3.170