Toward a Socio-Cognitive Stage Model of Cybersecurity Behavior Adoption

My research looks at how to apply insights from social psychology, marketing, and public health to reduce the costs of cybercrime and improve adoption of security practices. The central problem that I am addressing is what McAfee termed the "lack of organization-wide understanding of cyber risks" [24], which they estimate led to a jump of more than 50% in the global costs of cybercrime in 2019-20, to over $1 trillion [24]. But, fixing this problem is expensive; enterprise security training can cost around $300,000 and hundreds of staff hours per organization [36]. While many good solutions exist (such as using password managers or Virtual Private Networks), people have been slow to become fully aware of what they do and to use them regularly [14,26]. To address the problem, we should look to insights from social psychology, marketing, and public health that behavior change unfolds as a process in time that is influenced by relevant contacts at each stage. This rejects a "one size fits all" approach by splitting the target audience into segments, then using what is known about each segment to design and direct an intervention (such as awareness messaging or nudges to act) to those who are most likely to benefit.

No one has yet fully described the behavior adoption process for cybersecurity in a way that identifies stages of adoption and the social and cognitive factors that differentiate each stage. We do know that cybersecurity practices oblige people to interact with technology that they find scary, confusing or dull [2,10,14]; they afford abstract and non-absolute protections against specific threats [11,15,21]; and they provide solutions to collective problems that the potential adopter may not see as affecting them personally [21,25,28,30]. Fear appeals are important [1,12,22] but not sufficient to spark adoption [29]; people need awareness, motivation, and knowledge of how to use these practices to protect against threats, a framework known as "security sensitivity" [5,12,22]. Security sensitivity, in turn, is driven by social influences, such as whether a trusted family member or authority figure gives advice about which security practices to use [19,20], whether people hear stories that teach them about security practices [16–18,27], or whether they observe others engaging in secure behaviors [4–6]. My work [3,7–9,13,25] has found that social contexts influence whether people choose to keep their account credentials confidential, and that security attitudes are significantly associated with experiences of security breaches, security behavior intention, and recalled security actions. Now, I seek to answer this research question:

- ***RQ:*** *What stages do people go through in adoption of cybersecurity behaviors?*

To pursue answers, I propose a research project in three phases. Phase 1, a **remote interview study** with 17 participants, is already under way. We will elicit participants' experiences and thinking about the adoption process, along with the relevant social influences, for security practices in four general areas: keeping software up to date, maintaining good password hygiene, staying alert for phishing, scammers and "fake news", and securing devices and networks. Phase 2, an **online survey** deployed to 1000 people, will assess the distribution of these stages among a U.S.-representative randomized sample who are asked their awareness and adoption of using either a computational tool (password managers) or a knowledge practice (evaluating whether a website is legitimate). Phase 3 will produce materials on how to put into practice this **stage model of security behavior adoption**.

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. Future work will experimentally investigate the degree to which stage-matched interventions are associated with adoption of either a tool or a knowledge-based practice, versus interventions that are not stage-matched, and the degree to which participants are likely to maintain these security practices within one year.

[1] Scott Boss, Dennis Galletta, Paul Benjamin Lowry, Gregory D. Moody, and Peter Polak. 2015. *What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors*. Social Science Research Network, Rochester, NY. Retrieved July 18, 2018 from https://papers.ssrn.com/abstract=2607190

[2] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), ACM, New York, NY, USA, 456:1-456:11. DOI:https://doi.org/10.1145/3173574.3174030

[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] Cori Faklaris. 2021. Components of a Model of Cybersecurity Behavior Adoption. In *7th Workshop on Security Information Workers (WSIW 2021)*, USENIX Association Berkeley, CA, Virtual event. Retrieved from https://corifaklaris.com/files/Faklaris_WSIW2021_stagemodels.pdf

[8] 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

[9] 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

[10] Julie M Haney and Wayne G Lutters. 2018. "It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Proceedings of the Fourteenth Symposium on Usable Privacy and Security*, USENIX Association Berkeley, CA, Baltimore, Maryland, USA, 16.

[11] Daniel Kahneman and Amos Tversky. 1979. Prospect Theory: An Analysis of Decision Making Under Risk. *Econometrica* 47, 2 (March 1979), 262–292. Retrieved July 19, 2021 from http://links.jstor.org/sici?sici=0012-9682%28197903%2947%3A2%3C263%3APTAAOD%3E2.0.CO%3B2-3

[12] 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

[13] 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

[14] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. 319–338. Retrieved July 15, 2021 from https://www.usenix.org/conference/soups2019/presentation/pearman

[15] Leilei Qu, Cheng Wang, Ruojin Xiao, Jianwei Hou, Wenchang Shi, and Bin Liang. 2019. Towards Better Security Decisions: Applying Prospect Theory to Cybersecurity. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI EA '19), ACM, New York, NY, USA, LBW2613:1-LBW2613:6. DOI:https://doi.org/10.1145/3290607.3312782

[16] Christina A. Rader, Richard P. Larrick, and Jack B. Soll. 2017. Advice as a form of social influence: Informational motives and the consequences for accuracy. *Soc. Personal. Psychol. Compass* 11, 8 (August 2017), n/a-n/a. DOI:https://doi.org/10.1111/spc3.12329

[17] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *J. Cybersecurity* 1, 1 (September 2015), 121–144. DOI:https://doi.org/10.1093/cybsec/tyv008

[18] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS '12)*, USENIX Association Berkeley, CA, 1. DOI:https://doi.org/10.1145/2335356.2335364

[19] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *2016 IEEE Symposium on Security and Privacy (SP)*, 272–288. DOI:https://doi.org/10.1109/SP.2016.24

[20] 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

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

[22] 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

[23] 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/

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

[25] 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

[26] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proc. Priv. Enhancing Technol.* 2021, 3 (July 2021), 308–333. DOI:https://doi.org/10.2478/popets-2021-0049

[27] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), ACM, New York, NY, USA, 11:1-11:16. DOI:https://doi.org/10.1145/1837110.1837125

[28] Neil D. Weinstein. 1989. Effects of personal experience on self-protective behavior. *Psychol. Bull.* 105, 1 (1989), 31–50. DOI:https://doi.org/10.1037/0033-2909.105.1.31

[29] Dirk Weirich and Martina Angela Sasse. 2001. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms* (NSPW '01), Association for Computing Machinery, New York, NY, USA, 137–143. DOI:https://doi.org/10.1145/508171.508195

[30] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ACM, Honolulu HI USA, 1–15. DOI:https://doi.org/10.1145/3313831.3376570