Full text available at: http://dx.doi.org/10.1561/3300000026

The Security & Privacy Acceptance Framework (SPAF)

Other titles in Foundations and Trends® in Privacy and Security

Assured Autonomy Survey
Christopher Rouff and Lanier Watkins
ISBN: 978-1-63828-038-5

Hardware Platform Security for Mobile Devices
Lachlan J. Gunn, N. Asokan, Jan-Erik Ekberg, Hans Liljestrand, Vijayanand Nayani and Thomas Nyman
ISBN: 978-1-68083-976-0

Cloud Computing Security: Foundations and Research Directions
Anrin Chakraborti, Reza Curtmola, Jonathan Katz, Jason Nieh, Ahmad-Reza Sadeghi, Radu Sion and Yinqian Zhang
ISBN: 978-1-68083-958-6

Expressing Information Flow Properties
Elisavet Kozyri, Stephen Chong and Andrew C. Myers
ISBN: 978-1-68083-936-4

Accountability in Computing: Concepts and Mechanisms
Joan Feigenbaum, Aaron D. Jaggard and Rebecca N. Wright
ISBN: 978-1-68083-784-1

The Security & Privacy Acceptance Framework (SPAF)

Sauvik Das
Carnegie Mellon University
sauvik@cmu.edu

Cori Faklaris
University of North Carolina
cfaklari@uncc.edu

Jason I. Hong
Carnegie Mellon University
jasonh@cs.cmu.edu

Laura A. Dabbish
Carnegie Mellon University
dabbish@cs.cmu.edu

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

S. Das *et al.*. *The Security & Privacy Acceptance Framework (SPAF)*. Foundations and Trends® in Privacy and Security, vol. 5, no. 1-2, pp. 1–143, 2022.

ISBN: 978-1-63828-119-1

Contents

The Security & Privacy Acceptance Framework (SPAF)

Sauvik Das[1], Cori Faklaris[2], Jason I. Hong[1] and Laura A. Dabbish[1]

[1] *Carnegie Mellon University, USA; sauvik@cmu.edu, jasonh@cs.cmu.edu, dabbish@cs.cmu.edu*

[2] *University of North Carolina, Charlotte, USA; cori@corifaklaris.com*

ABSTRACT

How can we encourage end-user acceptance of expert recommended cybersecurity and privacy (S&P) behaviors? We review prior art in human-centered S&P and identified three barriers to end-user acceptance of expert recommendations: (1) awareness: i.e., people may not know of relevant security threats and appropriate mitigation measures; (2) motivation: i.e., people may be unwilling to enact S&P behaviors because, e.g., the perceived costs are too high, and (3) ability; i.e., people may not know when, why, and how to effectively implement S&P behaviors. These three barriers make up what we call the "Security & Privacy Acceptance Framework" (SPAF). We then review and critically analyze prior work that has explored mitigating one or more of the barriers that make up the SPAF. Finally, using the SPAF as a lens, we discuss how the human-centered S&P community might re-orient to encourage widespread end-user acceptance of pro-S&P behaviors by employing integrative approaches that address each one of the awareness, motivation, and ability barriers.

Sauvik Das, Cori Faklaris, Jason I. Hong and Laura A. Dabbish (2022), "The Security & Privacy Acceptance Framework (SPAF)", Foundations and Trends® in Privacy and Security: Vol. 5, No. 1-2, pp 1–143. DOI: 10.1561/3300000026.

1

Introduction

Cybersecurity and privacy (S&P[1]) unlock the full potential of computing. Use of encryption, authentication, and access control, for example, allows employees to correspond with professional colleagues via email with reduced fear of leaking confidential data to competitors or cybercriminals, parents to share photos of children with remote loved ones over the Internet with reduced fear of this data reaching the hands of unknown strangers, and anonymous whistleblowers to share information about problematic practices in the workplace with reduced fear of being outed. Conversely, failure to employ appropriate S&P measures can leave people and organizations vulnerable to a broad range of threats.

In short, the security and privacy decisions we make on a day-to-day basis determine whether the data we share, manipulate, and store online is protected from theft, surveillance, and exploitation. It is unsurprising, therefore, that the compromising of weak security and privacy practices remains the central tenet for a professional cybercrime industry which —

[1]We use the term cybersecurity and privacy to encapsulate the broad concept of protecting digital resources and data from intruders. Cybersecurity is commonly abbreviated to just "security", and so throughout this document we use S&P as shorthand for "cybersecurity and privacy." We use this short-hand in various ways, typically as a descriptor: e.g., S&P threats, S&P behaviors, and S&P tools.

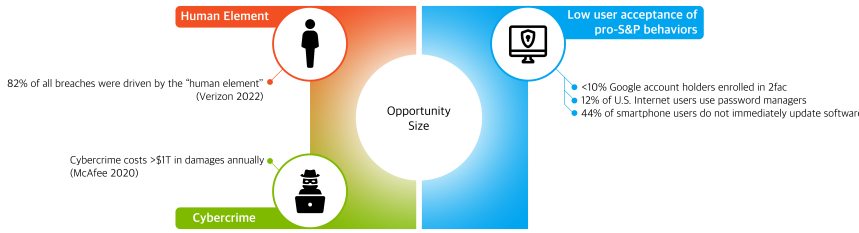

Figure 1.1: Cybercrime is estimated to cause over $1 trillion USD in damages to the global economy, and much of it is enabled by human error. Yet, user acceptance and adoption of expert-recommended security and privacy behaviors remains low. There remains an immense opportunity for impact by improving end-user acceptance and adoption of expert-recommended security and privacy behaviors.

by some estimates — causes upwards of $1 trillion in damages annually to the global economy (Smith and Lostri, 2020).

Many of the data breaches that are responsible for these damages involve human error or manipulation — i.e., improperly configured security settings, the accidental divulsion of key account credentials, or the unwitting installation of destructive malware. Moreover, as an increasing share of economic and social activity is conducted partially or exclusively online, the ramifications of these breaches have never been more significant. In 2021, for example, a ransomware attack crippled the Colonial Pipeline company, causing gas outages all over the eastern seaboard of the United States, resulting in outages, panic and predatory price inflation — and all because the company's private VPN was accessible without multi-factor authentication (Kerner, 2022). The Colonial Pipeline company incident is not an isolated incident. In early 2013, the Associated Press's Twitter account was compromised through a password phishing scheme, and erroneously tweeted that President Obama was injured in a bombing (Moore and Roberts, 2013). In response, stock prices plummeted, adversely affecting thousands. The cause? The AP's Twitter account credentials were phished, and the account was not protected with two-factor authentication. More generally, in 2020, Verizon published an analysis of 3950 security incidents, showing that the most common "actions" that led to breaches were social attacks that prey on human fallibilities (accounting for 22% of all breaches).

Moreover, the authors of that report observed that "the only action type that is consistently increasing year to year in frequency is [human] error." (Verizon, 2020). The 2022 version of that report estimated that the "human element" drove 82% of the 5212 breaches studied (Verizon, 2022). Unsurprisingly, prior work has found that the S&P behaviors that experts recommend only thinly overlap with the behaviors that people find important and adopt (Ion *et al.*, 2015; Busse *et al.*, 2019).

The upshot: if enough people employed basic, expert-recommended best practices — e.g., keeping one's software up-to-date, using multi-factor authentication on important accounts, using a password manager to ensure the reliable use of strong, random passwords unique for each individual account — the cybercrime industry would be hamstrung. The costs of these attacks would be substantially increased, shifting economic incentives, and would likely reduce the prevalence of all but the most sophisticated, targeted attacks. Yet, despite decades of improvements to the usability of S&P systems, end-users still struggle with adopting expert-recommended S&P advice. Indeed, as of early 2018, fewer than 10% of Google account holders had enrolled in two-factor authentication, and at least 17% of Google users reused their account passwords (Milka, 2018). Recent Pew surveys found that only 12% of Internet users in the U.S. use password managers and only 44% immediately update the operating system on their mobile phones (Olmstead and Smith, 2017).

This discrepancy — between the massive damages caused by the exploitation of weak security behaviors, and the existence of security technologies that can significantly reduce these damages, as summarized in Figure 1.1 — begs the question: "How can we encourage end-users to heed the advice of S&P experts?" Put another way, we might ask: "What inhibits acceptance of pro-S&P behaviors among end-users, and how can we overcome those inhibitors?"

In this monograph, we conducted an extensive review of prior literature to answer these questions. We covered a broad range of interdisciplinary perspectives — those from computer science, cognitive, behavioral and social psychology, human-computer interaction, design and behavioral economics. We start with a comprehensive review of extant models of human behavior and technology adoption and use those models as a lens to contextualize prior findings in human-centered

S&P that help explain why end-users accept or reject pro-S&P behaviors (see Section 2).

We found that there are three key inhibitory barriers to pro-S&P behaviors: awareness, motivation, and ability (see Section 3). First, many consumers are unaware of S&P threats that may be pertinent to a given situation, nor the techniques and tools that can be used to counteract these threats. Second, many consumers are unwilling to employ the techniques and tools that are available to protect against common threats. Third, many consumers are unable to correctly use the techniques and tools that are available to protect against common threats. Taken together, this triplet of inhibitory barriers make up what we call the "Security and Privacy Acceptance Framework" (SPAF). Efforts to address one or more of these inhibitory barriers can be said to increase acceptance of expert-recommended (pro-)S&P behaviors; efforts that — intentionally or not — exacerbate these barriers can be said to decrease acceptance of pro-S&P behaviors.

We next reviewed the existing body of work in human-centered S&P aimed at increasing end-user acceptance of pro-S&P behaviors (see Section 4) — particularly in the usable privacy and security, behavioral economics, human-computer interaction, and social psychology domains. Using the SPAF as a lens, we then critically analyzed why, despite decades of improvements to the usability of end-user S&P systems, widespread acceptance of pro-S&P behaviors remains relatively low (see Section 5). Specifically, we argue that while many existing interventions have been shown to be effective at addressing one or more of the barriers in the SPAF, there are relatively few interventions that target all barriers at once. Integrative approaches that target awareness, motivation, and ability at once are likely to be more effective at driving end-user acceptance and adoption of pro-S&P behaviors. We conclude by synthesizing promising trends and directions for future work (also Section 5).

A final note: in this monograph, we primarily focus on encouraging S&P behaviors that protect users against third-party and interpersonal threats, often making the assumption that a first-party service provider can be trusted. We acknowledge that security and privacy enhancing technologies can also be used to protect oneself against first-party and

institutional threats, but argue that protection against these threats is less straightforward from the perspective of end-user action — indeed, placing the onus strictly on end-users is a problematic approach. For these situations, there may be a stronger need for regulation of bad-faith corporate and intelligence agency practices, rather than targeted design interventions and behavioral improvements on the part of end-users.

References

Aas, J., R. Barnes, B. Case, Z. Durumeric, P. Eckersley, A. Flores-López, J. A. Halderman, J. Hoffman-Andrews, J. Kasten, E. Rescorla, *et al.* (2019). "Let's Encrypt: an automated certificate authority to encrypt the entire web". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2473–2487.

Acar, Y., S. Fahl, and M. L. Mazurek. (2016). "You are not your developer, either: A research agenda for usable security and privacy research beyond end users". *2016 IEEE Cybersecurity Development (SecDev)*: 3–8.

Ackerman, M. S. (2000). "The intellectual challenge of CSCW: the gap between social requirements and technical feasibility". *Human–Computer Interaction*. 15(2-3): 179–203.

Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, *et al.* (2017). "Nudges for privacy and security: Understanding and assisting users' choices online". *ACM Computing Surveys (CSUR)*. 50(3): 1–41.

Acquisti, A., L. Brandimarte, and G. Loewenstein. (2015). "Privacy and human behavior in the age of information". *Science*. 347(6221): 509–514.

Acquisti, A. and J. Grossklags. (2005). "Privacy and rationality in individual decision making". *IEEE security & privacy*. 3(1): 26–33.

Adams, A. and M. A. Sasse. (1999). "Users are not the enemy". *Communications of the ACM (CACM)*. 42(12): 40–46. DOI: 10.1145/322796.322806.

Addae, J. H., M. Brown, X. Sun, D. Towey, and M. Radenkovic. (2017). "Measuring attitude towards personal data for adaptive cybersecurity". *Information & Computer Security*.

Ajzen, I. (1991). "The theory of planned behavior". *Organizational behavior and human decision processes*. 50(2): 179–211.

Akhawe, D. and A. P. Felt. (2013). "Alice in warningland: a large-scale field study of browser security warning effectiveness". In: *Proc. USENIX Sec'13*. 257–272.

Akter, M., A. J. Godfrey, J. Kropczynski, H. R. Lipford, and P. J. Wisniewski. (2022). "From Parental Control to Joint Family Oversight: Can Parents and Teens Manage Mobile Online Safety and Privacy as Equals?" *Proceedings of the ACM on Human-Computer Interaction*. 6(CSCW1): 1–28.

Almuhimedi, H., F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal. (2015). "Your location has been shared 5,398 times! A field study on mobile app privacy nudging". In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 787–796.

Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. (2016). "A review of using gaming technology for cyber-security awareness". *Int. J. Inf. Secur. Res.(IJISR)*. 6(2): 660–666.

Alotaibi, F., S. Furnell, I. Stengel, and M. Papadaki. (2017). "Enhancing cyber security awareness with mobile games". In: *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE. 129–134.

Alqahtani, H. and M. Kavakli-Thorne. (2020). "Design and evaluation of an augmented reality game for cybersecurity awareness (cybar)". *Information*. 11(2): 121.

Alsulaiman, F. A. and A. El Saddik. (2006). "A novel 3D graphical password schema". In: *2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems*. IEEE. 125–128.

Alsulaiman, F. A. and A. El Saddik. (2008). "Three-dimensional password for more secure authentication". *IEEE Transactions on Instrumentation and measurement*. 57(9): 1929–1938.

Anderson, B. B., C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance. (2015). "How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study". In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2883–2892.

Assal, H. and S. Chiasson. (2019). "'Think secure from the beginning' A Survey with Software Developers". In: *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–13.

Auxier, B., L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner. (2019). "Americans and privacy: Concerned, confused and feeling lack of control over their personal information". *Pew Research Center: Internet, Science & Tech (blog). November*. 15: 2019.

Azenkot, S., K. Rector, R. Ladner, and J. Wobbrock. (2012). "PassChords: secure multi-touch authentication for blind people". In: *Proceedings of the 14th international ACM SIGACCESS conference on Computers and accessibility*. 159–166.

Bada, M., A. M. Sasse, and J. R. Nurse. (2019). "Cyber security awareness campaigns: Why do they fail to change behaviour?" *arXiv preprint arXiv:1901.02672*.

Bai, W., D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek. (2017). "Balancing security and usability in encrypted email". *IEEE Internet Computing*. 21(3): 30–38.

Barbosa, N. M., J. Hayes, and Y. Wang. (2016). "UniPass: design and evaluation of a smart device-based password manager for visually impaired users". In: *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 49–60.

Bauer, L., L. F. Cranor, M. K. Reiter, and K. Vaniea. (2007). "Lessons learned from the deployment of a smartphone-based access-control system". In: *Proceedings of the 3rd Symposium on Usable Privacy and Security*. 64–75.

Beautement, A., M. A. Sasse, and M. Wonham. (2008). "The Compliance Budget: Managing Security Behavior in Organisations". In: *Proceedings of the 2008 workshop on New security paradigms - NSPW '08*. New York, New York, USA: ACM Press. 47. DOI: 10.1145/1595676.1595684.

Benet, J. (2014). "Ipfs-content addressed, versioned, p2p file system". *arXiv preprint arXiv:1407.3561*.

Beydoun, K. A. (2022). "The New State of Surveillance: Societies of Subjugation". *Wash. & Lee L. Rev.* 79: 769.

Bhagavatula, R., B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides. (2015). "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption".

Biddle, R., S. Chiasson, and P. C. Van Oorschot. (2012). "Graphical passwords: Learning from the first twelve years". *ACM Computing Surveys (CSUR)*. 44(4): 1–41.

Bigham, J. P. and A. C. Cavender. (2009). "Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 1829–1838.

Blocki, J., S. Komanduri, L. Cranor, and A. Datta. (2014). "Spaced repetition and mnemonics enable recall of multiple strong passwords". *arXiv preprint arXiv:1410.1490*.

Bonneau, J., J. Anderson, and L. Church. (2009). "Privacy suites: shared privacy for social networks." In: *SOUPS*. Vol. 9. 1–2.

Bonneau, J., C. Herley, P. C. Van Oorschot, and F. Stajano. (2012). "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes". In: *2012 IEEE symposium on security and privacy*. IEEE. 553–567.

Bonneau, J. and S. Schechter. (2014). "Towards reliable storage of 56-bit secrets in human memory". In: *23rd USENIX Security Symposium (USENIX Security 14)*. 607–623.

Brainard, J., A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. (2006). "Fourth-factor authentication: somebody you know". In: *Proceedings of the 13th ACM conference on Computer and communications security*. 168–178.

Bravo-Lillo, C., L. F. Cranor, J. Downs, S. Komanduri, R. W. Reeder, S. Schechter, and M. Sleeper. (2013). "Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore". In: *Proc. SOUPS'13*.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Buchanan, T., C. Paine, A. N. Joinson, and U.-D. Reips. (2007). "Development of measures of online privacy concern and protection for use on the Internet". *Journal of the American society for information science and technology*. 58(2): 157–165.

Buolamwini, J. and T. Gebru. (2018). "Gender shades: Intersectional accuracy disparities in commercial gender classification". In: *Conference on fairness, accountability and transparency*. PMLR. 77–91.

Busse, K., J. Schäfer, and M. Smith. (2019). "Replication: no one can hack my mind revisiting a study on expert and non-expert security practices and advice". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*.

Cai, C. J., S. Winter, D. Steiner, L. Wilcox, and M. Terry. (2019). "Hello AI: uncovering the onboarding needs of medical practitioners for human-AI collaborative decision-making". *Proceedings of the ACM on Human-computer Interaction*. 3(CSCW): 1–24.

Carre, J. R., S. R. Curtis, and D. N. Jones. (2018). "Ascribing responsibility for online security and data breaches". *Managerial Auditing Journal*.

Chandrasekaran, V., C. Gao, B. Tang, K. Fawaz, S. Jha, and S. Banerjee. (2020). "Face-off: Adversarial face obfuscation". *arXiv preprint arXiv:2003.08861*.

Chatterjee, R., P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy, and T. Ristenpart. (2018). "The spyware used in intimate partner violence". In: *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE. 441–458.

Chen, T., M. Stewart, Z. Bai, E. Chen, L. Dabbish, and J. Hammer. (2020). "Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game". In: *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. 1737–1749.

Cherepanova, V., M. Goldblum, H. Foley, S. Duan, J. Dickerson, G. Taylor, and T. Goldstein. (2021). "LowKey: leveraging adversarial attacks to protect social media users from facial recognition". *arXiv preprint arXiv:2101.07922*.

Chesney, B. and D. Citron. (2019). "Deep fakes: A looming challenge for privacy, democracy, and national security". *Calif. L. Rev.* 107: 1753.

Chouhan, C., C. M. LaPerriere, Z. Aljallad, J. Kropczynski, H. Lipford, and P. J. Wisniewski. (2019). "Co-designing for community oversight: Helping people make privacy and security decisions together". *Proceedings of the ACM on Human-Computer Interaction*. 3(CSCW): 1–31.

Cialdini, R. B. (1987). *Influence*. Vol. 3. A. Michel Port Harcourt.

CJ, G., S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Lodha. (2018). "Phishy-a serious game to train enterprise users on phishing awareness". In: *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts*. 169–181.

Costanza-Chock, S. (2018). "Design justice: Towards an intersectional feminist framework for design theory and practice". *Proceedings of the Design Research Society*.

Cranor, L. F. (2008). "A framework for reasoning about the human in the loop".

Cranor, L. F. (2003). "P3P: Making privacy policies more useful". *IEEE Security & Privacy*. 1(6): 50–55.

Dabrowski, A., M. Kammerstetter, E. Thamm, E. Weippl, and W. Kastner. (2015). "Leveraging competitive gamification for sustainable fun and profit in security education". In: *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Das, A., M. Degeling, D. Smullen, and N. Sadeh. (2018a). "Personalized privacy assistants for the internet of things: Providing users with notice and choice". *IEEE Pervasive Computing*. 17(3): 35–46.

Das, S. (2016). "Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity". *it-Information Technology*. 58(5): 237–245.

Das, S. (2017). "Social Cybersecurity: Reshaping Security Through An Empirical Understanding of Human Social Behavior". *PhD thesis*. Carnegie Mellon University.

Das, S., L. A. Dabbish, and J. I. Hong. (2019a). "A Typology of Perceived Triggers for End-User Security and Privacy Behaviors". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 97–115.

Das, S., E. Hayashi, and J. I. Hong. (2013). "Exploring capturable everyday memory for autobiographical authentication". In: *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. 211–220.

Das, S., J. Hong, and S. Schechter. (2016). "Testing Computer-Aided Mnemonics and Feedback for Fast Memorization of High-Value Secrets". In: *2016 Usable Security (USEC) Workshop*.

Das, S., T. H.-J. Kim, L. A. Dabbish, and J. I. Hong. (2014a). "The effect of social influence on security sensitivity". In: *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. 143–157.

Das, S., A. D. Kramer, L. A. Dabbish, and J. I. Hong. (2014b). "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)*. New York, New York, USA: ACM Press. 739–749. DOI: 10.1145/2660267.2660271.

Das, S., A. D. Kramer, L. A. Dabbish, and J. 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*. 1416–1426.

Das, S., G. Laput, C. Harrison, and J. I. Hong. (2017). "Thumprint: Socially-inclusive local group authentication through shared secret knocks". In: *Proceedings of the 2017 chi conference on human factors in computing systems*. 3764–3774.

Das, S., J. Lo, L. Dabbish, and J. I. Hong. (2018b). "Breaking! A Typology of Security and Privacy News and How It's Shared". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*. New York, New York, USA: ACM Press. 1–12. DOI: 10.1145/3173574.3173575.

Das, S., D. Lu, T. Lee, J. Lo, and J. I. Hong. (2019b). "The memory palace: Exploring visual-spatial paths for strong, memorable, infrequent authentication". In: *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology*. 1109–1121.

Davis, F. D. (1989). "Perceived usefulness, perceived ease of use, and user acceptance of information technology". *MIS quarterly*: 319–340.

Denning, T., A. Lerner, A. Shostack, and T. Kohno. (2013). "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education". In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 915–928.

Dhamija, R., J. D. Tygar, and M. Hearst. (2006). "Why phishing works". In: *Proc. CHI '06*. No. April. New York, New York, USA: ACM Press. 581–590. DOI: 10.1145/1124772.1124861.

DiGioia, P. and P. Dourish. (2005). "Social navigation as a model for usable security". In: *Proc. SOUPS '05*. New York, New York, USA: ACM Press. 101–108. DOI: 10.1145/1073001.1073011.

Distler, V., G. Lenzini, C. Lallemand, and V. Koenig. (2020). "The framework of security-enhancing friction: How UX can help users behave more securely". In: *New security paradigms workshop 2020*. 45–58.

Do, Y., L. T. Hoang, J. W. Park, G. D. Abowd, and S. Das. (2021a). "Spidey Sense: Designing Wrist-Mounted Affective Haptics for Communicating Cybersecurity Warnings". In: *Designing Interactive Systems Conference 2021*. 125–137.

Do, Y., J. W. Park, Y. Wu, A. Basu, D. Zhang, G. D. Abowd, and S. Das. (2021b). "Smart Webcam Cover: Exploring the Design of an Intelligent Webcam Cover to Improve Usability and Trust". *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 5(4): 1–21.

Do, Y., S. Singh, Z. Li, S. R. Craig, P. J. Welch, C. Shi, T. Starner, G. D. Abowd, and S. Das. (2021c). "Bit Whisperer: Improving Access Control over Ad-hoc, Short-range, Wireless Communications via Surface-bound Acoustics". In: *Proceedings of the 34th ACM User Interface Software and Technology Symposium (UIST)*.

Dodge Jr, R. C., C. Carver, and A. J. Ferguson. (2007). "Phishing for user security awareness". *computers & security*. 26(1): 73–80.

Dourish, P. and K. Anderson. (2006). "Collective information practice: Exploring privacy and security as social and cultural phenomena". *Human-computer interaction*. 21(3): 319–342.

Dourish, P., R. E. Grinter, J. Delgado de la Flor, and M. Joseph. (2004). "Security in the wild: user strategies for managing security as an everyday, practical problem". *Personal and Ubiquitous Computing*. 8(6): 391–401. DOI: 10.1007/s00779-004-0308-5.

Dupuis, M. and F. Khan. (2018). "Effects of peer feedback on password strength". In: *2018 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE. 1–9.

Edwards, W. K., E. S. Poole, and J. Stoll. (2008). "Security automation considered harmful?" In: *Proceedings of the 2007 Workshop on New Security Paradigms*. 33–42.

Egelman, S., A. B. Brush, and K. M. Inkpen. (2008a). "Family accounts: A new paradigm for user accounts within the home environment". In: *Proceedings of the 2008 ACM conference on Computer supported cooperative work*. 669–678.

Egelman, S., L. F. Cranor, and J. Hong. (2008b). "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*. 1065–1074.

Egelman, S., D. Molnar, N. Christin, A. Acquisti, C. Herley, and S. Krishnamurthi. (2010). "Please Continue to Hold: An empirical study on user tolerance of security delays". In: *Proc. WEIS'10*. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.167.5560.

Egelman, S. and E. Peer. (2015a). "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*. 2873–2882.

Egelman, S. and E. Peer. (2015b). "The myth of the average user: Improving privacy and security systems through individualization". In: *Proceedings of the 2015 New Security Paradigms Workshop*. 16–28.

Egelman, S., A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. (2013). "Does my password go up to eleven? The impact of password meters on password selection". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2379–2388.

Faklaris, C. (2022). "Toward a Socio-Cognitive Stage Model of Cybersecurity Behavior Adoption". *PhD thesis*. US National Science Foundation.

Faklaris, C., L. Dabbish, and J. I. Hong. (2022). "Do They Accept or Resist Cybersecurity Measures? Development and Validation of the 13-Item Security Attitude Inventory (SA-13)". *arXiv preprint arXiv:2204.03114*.

Faklaris, C., L. A. Dabbish, and J. I. Hong. (2019). "A Self-Report Measure of End-User Security Attitudes (SA-6". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 61–77.

Fanelle, V., S. Karimi, A. Shah, B. Subramanian, and S. Das. (2020). "Blind and Human: Exploring More Usable Audio CAPTCHA Designs". In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 111–125.

Fast, E., B. Chen, J. Mendelsohn, J. Bassen, and M. S. Bernstein. (2018). "Iris: A conversational agent for complex tasks". In: *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–12.

Felt, A. P., A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes. (2015). "Improving SSL warnings: Comprehension and adherence". In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2893–2902.

Felt, A. P., R. W. Reeder, H. Almuhimedi, and S. Consolvo. (2014). "Experimenting at scale with google chrome's SSL warning". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 2667–2670.

Ferguson, A. J. (2005). "Fostering e-mail security awareness: The West Point carronade". *Educause Quarterly*. 28(1): 54–57.

Fishbein, M. (1979). "A theory of reasoned action: some applications and implications."

Fishbein, M. and I. Ajzen. (1977). "Belief, attitude, intention, and behavior: An introduction to theory and research". *Philosophy and Rhetoric*. 10(2).

Fogg, B. (2009). "A behavior model for persuasive design". In: *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive '09*. 1. DOI: 10.1145/1541948.1541999.

Forget, A., S. Komanduri, A. Acquisti, N. Christin, L. F. Cranor, and R. Telang. (2014). "Building the security behavior observatory: An infrastructure for long-term monitoring of client machines". In: *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security*. 1–2.

Frik, A., N. Malkin, M. Harbach, E. Peer, and S. Egelman. (2019a). "A promise is a promise: the effect of commitment devices on computer security intentions". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

Frik, A., L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman. (2019b). "Privacy and security threat models and mitigation strategies of older adults". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 21–40.

Furnell, S., A. Jusoh, and D. Katsabas. (2006). "The challenges of undersatnding and using security: A survey of end-users". *Computers & Security*. 25(1): 27–35.

Gaw, S., E. W. Felten, and P. Fernandez-Kelly. (2006). "Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail". In: *Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI '06)*. New York, New York, USA: ACM Press. 591–600. DOI: 10.1145/1124772.1124862.

George, C., M. Khamis, D. Buschek, and H. Hussmann. (2019). "Investigating the third dimension for authentication in immersive virtual reality and in the real world". In: *2019 ieee conference on virtual reality and 3d user interfaces (vr)*. IEEE. 277–285.

Goecks, J., W. K. Edwards, and E. D. Mynatt. (2009). "Challenges in supporting end-user privacy and security management with social navigation". In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

Goldschlag, D., M. Reed, and P. Syverson. (1999). "Onion routing". *Communications of the ACM*. 42(2): 39–41.

Golla, M., G. Ho, M. Lohmus, M. Pulluri, and E. M. Redmiles. (2021). "Driving 2FA Adoption at Scale: Optimizing Two-Factor Authentication Notification Design Patterns". In: *30th USENIX Security Symposium (USENIX Security 21)*. 109–126.

Green, M. and M. Smith. (2016). "Developers are not the enemy!: The need for usable security apis". *IEEE Security & Privacy*. 14(5): 40–46.

Guan, L., S. Farhang, Y. Pu, P. Guo, J. Grossklags, and P. Liu. (2017). "VaultIME: Regaining User Control for Password Managers through Auto-correction". In: *International Conference on Security and Privacy in Communication Systems*. Springer. 673–686.

Guberek, T., A. McDonald, S. Simioni, A. H. Mhaidli, K. Toyama, and F. Schaub. (2018). "Keeping a low profile? Technology, risk and privacy among undocumented immigrants". In: *Proceedings of the 2018 CHI conference on human factors in computing systems*. 1–15.

Haber, E. and E. Kandogan. (2007). "Security administrators: A breed apart". *SOUPS USM*: 3–6.

Hagger, M. S. (2016). "Non-conscious processes and dual-process theories in health psychology". *Health Psychology Review*. 10(4): 375–380.

Halperin, D., T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. (2008). "Security and privacy for implantable medical devices". *IEEE pervasive computing*. 7(1): 30–39.

Haney, J., Y. Acar, and S. Furman. (2021). ""It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security". In: *30th USENIX Security Symposium (USENIX Security 21)*. 411–428.

Hang, A., A. De Luca, and H. Hussmann. (2015). "I know what you did last week! do you? dynamic security questions for fallback authentication on smartphones". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 1383–1392.

Hans, G. S. (2012). "Privacy policies, terms of service, and FTC enforcement: Broadening unfairness regulation for a new era". *Mich. Telecomm. & Tech. L. Rev.* 19: 163.

Hargittai, E. and K. Dobransky. (2017). "Old dogs, new clicks: Digital inequality in skills and uses among older adults." *Canadian Journal of Communication*. 42(2).

Hartzog, W. and D. J. Solove. (2014). "The scope and potential of FTC data protection". *Geo. Wash. L. Rev.* 83: 2230.

Havron, S., D. Freed, R. Chatterjee, D. McCoy, N. Dell, and T. Ristenpart. (2019). "Clinical computer security for victims of intimate partner violence". In: *28th USENIX Security Symposium (USENIX Security 19)*. 105–122.

Hayashi, E., S. Das, S. Amini, J. Hong, and I. Oakley. (2013). "Casa: context-aware scalable authentication". In: *Proceedings of the Ninth Symposium on Usable Privacy and Security*. 1–10.

Hendrix, M., A. Al-Sherbaz, and B. Victoria. (2016). "Game based cyber security training: are serious games suitable for cyber security training?" *International Journal of Serious Games*. 3(1).

Herley, C. (2009). "So long, and no thanks for the externalities". In: *Proc. NSPW '09*. New York, New York, USA: ACM Press. 133–144. DOI: 10.1145/1719030.1719050.

Herley, C. (2016). "Unfalsifiability of security claims". *Proceedings of the National Academy of Sciences*. 113(23): 6415–6420.

Herley, C. and P. van Oorschot. (2009). "Passwords: If We're So Smart, Why Are We Still Using Them?" *Proceedings of the 13th International Conference on Financial Cryptography and Data Security (FC'09)*. DOI: 10.1007/978-3-642-03549-4_14.

Herley, C., P. C. Van Oorschot, and A. S. Patrick. (2009). "Passwords: If we're so smart, why are we still using them?" In: *International Conference on Financial Cryptography and Data Security*. Springer. 230–237.

Hetcher, S. (2000). "FTC as Internet privacy norm entrepreneur, The". *Vand. L. Rev.* 53: 2041.

Hill Jr, W. A., M. Fanuel, X. Yuan, J. Zhang, and S. Sajad. (2020). "A survey of serious games for cybersecurity education and training".

Ion, I., R. Reeder, and S. Consolvo. (2015). ""...no one can hack my mind": Comparing Expert and Non-Expert Security Practices". In: *Symposium on Usable Privacy and Security (SOUPS)*. 327–346. DOI: 10.1080/0888431022000070458.

Jagatic, T. N., N. A. Johnson, M. Jakobsson, and F. Menczer. (2007). "Social phishing". *Communications of the ACM*. 50(10): 94–100.

Jain, M., R. Tripathi, I. Bhansali, and P. Kumar. (2019). "Automatic generation and evaluation of usable and secure audio ReCAPTCHA". In: *The 21st International ACM SIGACCESS Conference on Computers and Accessibility*. 355–366.

Jansson, K. and R. von Solms. (2013). "Phishing for phishing awareness". *Behaviour & information technology*. 32(6): 584–593.

Jefferson, B. J. (2018). "Predictable policing: Predictive crime mapping and geographies of policing and race". *Annals of the American Association of Geographers*. 108(1): 1–16.

Jin, H., G. Liu, D. Hwang, S. Kumar, Y. Agarwal, and J. Hong. (2022). "Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes". In: *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society. 1571–1571.

Jorgensen, Z. and T. Yu. (2011). "On mouse dynamics as a behavioral biometric for authentication". In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. 476–482.

Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan.

Kajzer, M., J. D'Arcy, C. R. Crowell, A. Striegel, and D. Van Bruggen. (2014). "An exploratory investigation of message-person congruence in information security awareness campaigns". *Computers & security*. 43: 64–76.

Kang, R., L. Dabbish, N. Fruchter, and S. 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) 2015*. 39–52.

Kapadia, A., G. Sampemane, and R. H. Campbell. (2004). "KNOW why your access was denied: Regulating feedback for usable security". In: *Proceedings of the 11th ACM conference on Computer and Communications Security*. 52–61.

Kaplan, S. A., D. L. Vogel, D. A. Gentile, and N. G. Wade. (2012). "Increasing positive perceptions of counseling: The importance of repeated exposures". *The Counseling Psychologist*. 40(3): 409–442.

Karapanos, N., C. Marforio, C. Soriente, and S. Capkun. (2015). "Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound". In: *24th USENIX security symposium (USENIX security 15)*. 483–498.

Kelley, P. G., J. Bresee, L. F. Cranor, and R. W. Reeder. (2009). "A "nutrition label" for privacy". In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

Kerner, S. M. (2022). "Colonial Pipeline hack explained: Everything you need to know". URL: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Khan, B., K. S. Alghathbar, and M. K. Khan. (2011). "Information security awareness campaign: An alternate approach". In: *International Conference on Information Security and Assurance*. Springer. 1–10.

Klemperer, P., Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer, L. F. Cranor, N. Gupta, and M. Reiter. (2012). "Tag, you can see it! Using tags for access control in photo sharing". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 377–386.

Koscher, K., A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, *et al.* (2010). "Experimental security analysis of a modern automobile". In: *2010 IEEE symposium on security and privacy*. IEEE. 447–462.

Kraemer, S. and P. Carayon. (2007). "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists". *Applied ergonomics*. 38(2): 143–154.

Kroll, T. and S. Stieglitz. (2021). "Digital nudging and privacy: improving decisions about self-disclosure in social networks". *Behaviour & Information Technology*. 40(1): 1–19.

Kropczynski, J., R. Ghaiumy Anaraky, M. Akter, A. J. Godfrey, H. Lipford, and P. J. Wisniewski. (2021). "Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving". *Proceedings of the ACM on Human-Computer Interaction*. 5(CSCW2): 1–23.

Krsek, I., K. Wenzel, S. Das, J. I. Hong, and L. Dabbish. (2022). "To Self-Persuade or be Persuaded: Examining Interventions for Users' Privacy Setting Selection". In: *CHI Conference on Human Factors in Computing Systems*. 1–17.

Kumaraguru, P. and L. F. Cranor. (2005). *Privacy indexes: a survey of Westin's studies*. Carnegie Mellon University, School of Computer Science, Institute for ...

Kumaraguru, P., J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. (2009). "School of phish: a real-world evaluation of anti-phishing training". In: *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

Kumaraguru, P., S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. (2008). "Lessons from a real world evaluation of anti-phishing training". In: *2008 eCrime Researchers Summit*. IEEE. 1–12.

Landau, S. (2013). "Making sense from Snowden: What's significant in the NSA surveillance revelations". *IEEE Security & Privacy*. 11(4): 54–63.

Lebeck, K., K. Ruth, T. Kohno, and F. Roesner. (2018). "Towards security and privacy for multi-user augmented reality: Foundations with end users". In: *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE. 392–408.

Lebek, B., J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler. (2013). "Employees' information security awareness and behavior: A literature review". In: *2013 46th Hawaii International Conference on System Sciences*. IEEE. 2978–2987.

Lerner, A., E. Zeng, and F. Roesner. (2017). "Confidante: Usable encrypted email: A case study with lawyers and journalists". In: *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 385–400.

Li, T., E. B. Neundorfer, Y. Agarwal, and J. I. Hong. (2021). "Honeysuckle: Annotation-guided code generation of in-app privacy notices". *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 5(3): 1–27.

Li, Y., F. Chen, T. J.-J. Li, Y. Guo, G. Huang, M. Fredrikson, Y. Agarwal, and J. I. Hong. (2017). "Privacystreams: Enabling transparency in personal data processing for mobile apps". *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 1(3): 1–26.

Licklider, J. C. (1960). "Man-computer symbiosis". *IRE transactions on human factors in electronics*. (1): 4–11.

Lipford, H. R. and M. E. Zurko. (2012). "Someone to watch over me". In: *Proceedings of the 2012 New Security Paradigms Workshop*. 67–76.

Liu, B., M. S. Andersen, F. Schaub, H. Almuhimedi, S. A. Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti. (2016a). "Follow my recommendations: A personalized privacy assistant for mobile app permissions". In: *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 27–41.

Liu, R., J. Cao, K. Zhang, W. Gao, J. Liang, and L. Yang. (2016b). "When privacy meets usability: Unobtrusive privacy permission recommendation system for mobile apps based on crowdsourcing". *IEEE Transactions on Services Computing*. 11(5): 864–878.

Logas, J., A. Schlesinger, Z. Li, and S. Das. (2022). "Image DePO: Towards Gradual Decentralization of Online Social Networks using Decentralized Privacy Overlays". *Proceedings of the ACM on Human-Computer Interaction*. 6(CSCW1): 1–28.

Ma, Y., J. Feng, L. Kumin, and J. Lazar. (2013). "Investigating user behavior for authentication methods: A comparison between individuals with Down syndrome and neurotypical users". *ACM Transactions on Accessible Computing (TACCESS)*. 4(4): 1–27.

Malhotra, N. K., S. S. Kim, and J. Agarwal. (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model". *Information systems research*. 15(4): 336–355.

Mantyjarvi, J., M. Lindholm, E. Vildjiounaite, S.-M. Makela, and H. Ailisto. (2005). "Identifying users of portable devices from gait pattern with accelerometers". In: *Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.* Vol. 2. IEEE. ii–973.

Marne, S. T., M. N. Al-Ameen, and M. K. Wright. (2017). "Learning System-assigned Passwords: A Preliminary Study on the People with Learning Disabilities." In: *SOUPS*.

Maxwell, G. (2013). "CoinJoin: Bitcoin privacy for the real world". In: *Post on Bitcoin forum*. Vol. 3. 110.

Mayer, P., H. Berket, and M. Volkamer. (2016). "Enabling automatic password change in password managers through crowdsourcing". *Proc. PASSWORDS. Springer*.

Mazurek, M. L., P. F. Klemperer, R. Shay, H. Takabi, L. Bauer, and L. F. Cranor. (2011). "Exploring reactive access control". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2085–2094.

Mazurek, M. L., Y. Liang, W. Melicher, M. Sleeper, L. Bauer, G. R. Ganger, N. Gupta, and M. K. Reiter. (2014). "Toward strong, usable access control for shared distributed data". In: *12th USENIX Conference on File and Storage Technologies (FAST 14)*. 89–103.

McCarney, D., D. Barrera, J. Clark, S. Chiasson, and P. C. Van Oorschot. (2012). "Tapas: design, implementation, and usability evaluation of a password manager". In: *Proceedings of the 28th Annual Computer Security Applications Conference*. 89–98.

McDonald, A., C. Barwulor, M. L. Mazurek, F. Schaub, and E. M. Redmiles. (2021). "" It's stressful having all these phones": Investigating Sex Workers' Safety Goals, Risks, and Practices Online". In: *30th USENIX Security Symposium (USENIX Security 21)*.

McSweeny, T. (2018). "Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?" *Geo. L. Tech. Rev.* 2: 514–514.

Mendel, T., D. Gao, D. Lo, and E. Toch. (2021). "An Exploratory Study of Social Support Systems to Help Older Adults in Managing Mobile Safety". In: *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction*. 1–13.

Mendel, T., R. Schuster, E. Tromer, and E. Toch. (2022). "Toward Proactive Support for Older Adults: Predicting the Right Moment for Providing Mobile Safety Help". *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*. 6(1): 1–25.

Micallef, N., M. Just, L. Baillie, and M. Alharby. (2017). "Stop annoying me! an empirical investigation of the usability of app privacy notifications". In: *Proceedings of the 29th Australian Conference on Computer-Human Interaction*. 371–375.

Milka, G. (2018). "The Anatomy of Account Take-Over". In: *USENIX ENIGMA*. URL: https://www.usenix.org/sites/default/files/conference/protected-files/enigma18_milka.pdf.

Moju-Igbene, E., H. Abdi, A. Lu, and S. Das. (2022). ""how do you not lose friends?": Synthesizing a design space of social controls for securing shared digital resources via participatory design jams,"" in: *Proceedings of the 31st USENIX Security Symposium (SEC)*.

Monrose, F. and A. Rubin. (1997). "Authentication via keystroke dynamics". In: *Proceedings of the 4th ACM Conference on Computer and Communications Security*. 48–56.

Moore, H. and D. Roberts. (2013). "AP Twitter hack causes panic on Wall Street and sends Dow plunging". URL: http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

Mostafa, M. and O. S. Faragallah. (2019). "Development of serious games for teaching information security courses". *IEEE Access*. 7: 169293–169305.

Murthy, S., K. S. Bhat, S. Das, and N. Kumar. (2021). "Individually vulnerable, collectively safe: The security and privacy practices of households with older adults". *Proceedings of the ACM on Human-Computer Interaction*. 5(CSCW1): 1–24.

Napoli, D., S. N. Chaparro, S. Chiasson, and E. Stobert. (2020). "Something Doesn't Feel Right: Using Thermal Warnings to Improve User Security Awareness".

Ng, W. (2012). "Can we teach digital natives digital literacy?" *Computers & education*. 59(3): 1065–1078.

Nicholson, J., L. Coventry, and P. Briggs. (2019). "" If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults". In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–11.

Nicholson, J., V. Vlachokyriakos, L. Coventry, P. Briggs, and P. Olivier. (2018). "Simple nudges for better password creation". In: *Proceedings of the 32nd International BCS Human Computer Interaction Conference 32*. 1–12.

Nielsen, J. and J. Alertbox. (2004). "User education is not the answer to security problems". *Alertbox, October*.

Norberg, P. A., D. R. Horne, and D. A. Horne. (2007). "The privacy paradox: Personal information disclosure intentions versus behaviors". *Journal of consumer affairs*. 41(1): 100–126.

Norman, D. (2013). *The design of everyday things: Revised and expanded edition*. Basic books.

Ohlhausen, M. K. (2014). "Privacy challenges and opportunities: The role of the Federal Trade Commission". *Journal of Public Policy & Marketing*. 33(1): 4–9.

Ohyama, T. and A. Kanaoka. (2015). "Password strength meters using social influence". In: *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'15). Usenix, Berkely, CA*.

Olmstead, K. and A. Smith. (2017). "Americans and Cybersecurity". *Tech. rep.* Pew Research Center. URL: http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/.

Owens, K., O. Anise, A. Krauss, and B. Ur. (2021). "User Perceptions of the Usability and Security of Smartphones as FIDO2 Roaming Authenticators". In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 57–76.

Park, C. Y., C. Faklaris, S. Zhao, A. Sciuto, L. Dabbish, and J. Hong. (2018). "Share and share alike? An exploration of secure behaviors in romantic relationships". In: *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 83–102.

Parsons, K., D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. (2017). "The human aspects of information security questionnaire (HAIS-Q): two further validation studies". *Computers & Security*. 66: 40–51.

Pearman, S., S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor. (2019). "Why people (don't) use password managers effectively". In: *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 319–338.

Petelka, J., Y. Zou, and F. Schaub. (2019). "Put your warning where your link is: Improving and evaluating email phishing warnings". In: *Proceedings of the 2019 CHI conference on human factors in computing systems*. 1–15.

Rader, E., R. Wash, and B. Brooks. (2012). "Stories as informal lessons about security". In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–17.

Redmiles, E. (2018). "Net benefits: Digital inequities in social capital, privacy preservation, and digital parenting practices of US social media users". In: *Proceedings of the International AAAI Conference on Web and Social Media*. Vol. 12. No. 1.

Redmiles, E. M., S. Kross, and M. L. Mazurek. (2016a). "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*. 666–677.

Redmiles, E. M., S. Kross, and M. L. Mazurek. (2017). "Where is the digital divide? a survey of security, privacy, and socioeconomics". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 931–936.

Redmiles, E. M., A. R. Malone, and M. L. Mazurek. (2016b). "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)*. IEEE. 272–288.

Redmiles, E. M., M. L. Mazurek, and J. P. Dickerson. (2018). "Dancing pigs or externalities? Measuring the rationality of security decisions". In: *Proceedings of the 2018 ACM Conference on Economics and Computation*. 215–232.

Reeder, R. W., L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. (2011). "More than skin deep: measuring effects of the underlying model on access-control system usability". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2065–2074.

Reeder, R. W., L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. (2008). "Expandable grids for visualizing and authoring computer security policies". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 1473–1482.

Reisig, M. D., D. P. Mears, S. E. Wolfe, and K. Holtfreter. (2015). "Financial Exploitation of the Elderly in a Consumer Context".

Rezgui, Y. and A. Marks. (2008). "Information security awareness in higher education: An exploratory study". *Computers & security*. 27(7-8): 241–253.

Roca, J. C., J. J. García, and J. J. De La Vega. (2009). "The importance of perceived trust, security and privacy in online trading systems". *Information Management & Computer Security*.

Roepke, R. and U. Schroeder. (2019). "The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education." *CSEDU (2)*: 58–66.

Rogers, E. M. (1962). *Diffusion of innovations*. Free Press of Glencoe. URL: http://books.google.com/books?id=zw0-AAAAIAAJ.

Rogers, E. M. (2002). "Diffusion of preventive innovations". *Addictive Behaviors*. 27: 989–993.

Ruoti, S., J. Andersen, T. Hendershot, D. Zappala, and K. Seamons. (2016). "Private Webmail 2.0: Simple and easy-to-use secure email". In: *Proceedings of the 29th Annual Symposium on User Interface Software and Technology*. 461–472.

Ruoti, S., J. Andersen, D. Zappala, and K. Seamons. (2015). "Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client". *arXiv preprint arXiv:1510.08555*.

Ruoti, S. and K. Seamons. (2019). "Johnny's journey toward usable secure email". *IEEE Security & Privacy*. 17(6): 72–76.

Sadeh, N., J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. (2009). "Understanding and capturing people's privacy policies in a mobile social networking application". *Personal and ubiquitous computing*. 13(6): 401–412.

Sasse, M. (2003). "Computer security: Anatomy of a Usability Disaster, and a Plan for Recovery". In: *Proc. CHI Workshop on HCI and Security Systems*. Citeseer. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.9019&rep=rep1&type=pdf.

Schaub, F., R. Balebako, A. L. Durity, and L. F. Cranor. (2015). "A design space for effective privacy notices". In: *Eleventh symposium on usable privacy and security (SOUPS 2015)*. 1–17.

Schechter, S., S. Egelman, and R. W. Reeder. (2009). "It's not what you know, but who you know: a social approach to last-resort authentication". In: *Proceedings of the sigchi conference on human factors in computing systems*. 1983–1992.

Schneier, B. (2015). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Scrimgeour, J.-M. and J. Ophoff. (2019). "Lessons learned from an organizational information security awareness campaign". In: *IFIP World Conference on Information Security Education*. Springer. 129–142.

Shan, S., E. Wenger, J. Zhang, H. Li, H. Zheng, and B. Y. Zhao. (2020). "Fawkes: Protecting Privacy against Unauthorized Deep Learning Models". *In Proc. of the 29th USENIX Security Symposium*.

Shay, R., L. Bauer, N. Christin, L. F. Cranor, A. Forget, S. Komanduri, M. L. Mazurek, W. Melicher, S. M. Segreti, and B. Ur. (2015). "A spoonful of sugar? The impact of guidance and feedback on password-creation behavior". In: *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2903–2912.

Sheng, S., L. Broderick, C. A. Koranda, and J. J. Hyland. (2006). "Why johnny still can't encrypt: evaluating the usability of email encryption software". In: *Symposium On Usable Privacy and Security*. ACM. 3–4.

Sheng, S., B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. (2007). "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish". In: *Proceedings of the 3rd symposium on Usable privacy and security*. 88–99.

Shneiderman, B. and P. Maes. (1997). "Direct manipulation vs. interface agents". *interactions*. 4(6): 42–61.

Siponen, M. T. (2000). "A conceptual foundation for organizational information security awareness". *Information management & computer security*.

Smith, H. J., S. J. Milberg, and S. J. Burke. (1996). "Information privacy: Measuring individuals' concerns about organizational practices". *MIS quarterly*: 167–196.

Smith, Z. M. and E. Lostri. (2020). *The hidden costs of cybercrime*. McAfee.

Solove, D. J. (2007). "I've got nothing to hide and other misunderstandings of privacy". *San Diego L. Rev.* 44: 745.

Song, Y., C. Faklaris, Z. Cai, J. I. Hong, and L. Dabbish. (2019). "Normal and easy: Account sharing practices in the workplace". *Proceedings of the ACM on Human-Computer Interaction*. 3(CSCW): 1–25.

Spiekermann, S. (2007). "Perceived control: Scales for privacy in ubiquitous computing". In: *Digital Privacy*. Auerbach Publications. 289–304.

Stanton, J., P. Mastrangelo, K. Stam, and J. Jolton. (2004). "Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices." *AMCIS*. (August): 2–8. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.2938&rep=rep1&type=pdf.

Stobert, E. and R. Biddle. (2014). "A password manager that doesn't remember passwords". In: *Proceedings of the 2014 New Security Paradigms Workshop*. 39–52.

Stobert, E., T. Safaie, H. Molyneaux, M. Mannan, and A. Youssef. (2020). "ByPass: Reconsidering the usability of password managers". In: *International Conference on Security and Privacy in Communication Systems*. Springer. 446–466.

Story, P., D. Smullen, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. (2020). "From intent to action: Nudging users towards secure mobile payments". In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 379–415.

Strand, K. L. (2018). "Influencing factors and effectiveness of a security awareness campaign". *MA thesis*. NTNU.

Stylios, I. C., O. Thanou, I. Androulidakis, and E. Zaitseva. (2016). "A review of continuous authentication using behavioral biometrics". In: *Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference*. 72–79.

Sultana, M., P. P. Paul, and M. Gavrilova. (2014). "A concept of social behavioral biometrics: motivation, current developments, and future trends". In: *2014 International Conference on Cyberworlds*. IEEE. 271–278.

Sunshine, J., S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. (2009). "Crying wolf: An empirical study of ssl warning effectiveness." In: *USENIX security symposium*. Montreal, Canada. 399–416.

Thaler, R. H. and C. R. Sunstein. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.

Thorpe, J., B. MacRae, and A. Salehi-Abari. (2013). "Usability and security evaluation of GeoPass: a geographic location-password scheme". In: *Proceedings of the Ninth symposium on usable privacy and security*. 1–14.

Tiefenau, C., M. Häring, K. Krombholz, and E. Von Zezschwitz. (2020). "Security, availability, and multiple information sources: Exploring update behavior of system administrators". In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 239–258.

Tiefenau, C., E. von Zezschwitz, M. Häring, K. Krombholz, and M. Smith. (2019). "A usability evaluation of Let's Encrypt and Certbot: usable security done right". In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1971–1988.

Ur, B., F. Alfieri, M. Aung, L. Bauer, N. Christin, J. Colnago, L. F. Cranor, H. Dixon, P. Emami Naeini, H. Habib, *et al.* (2017). "Design and evaluation of a data-driven password meter". In: *Proceedings of the 2017 chi conference on human factors in computing systems*. 3775–3786.

Vance, A., J. L. Jenkins, B. B. Anderson, D. K. Bjornn, and C. B. Kirwan. (2018). "Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments". *MIS Quarterly*. 42(2): 355–380.

Vance, A., B. Kirwan, D. Bjornn, J. Jenkins, and B. B. Anderson. (2017). "What do we really know about how habituation to warnings occurs over time? A longitudinal fMRI study of habituation and polymorphic warnings". In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2215–2227.

Vaniea, K., L. Bauer, L. F. Cranor, and M. K. Reiter. (2012). "Out of sight, out of mind: Effects of displaying access-control information near the item it controls". In: *2012 Tenth Annual International Conference on Privacy, Security and Trust*. IEEE. 128–136.

Vaniea, K. and Y. Rashidi. (2016). "Tales of software updates: The process of updating software". In: *Proceedings of the 2016 chi conference on human factors in computing systems*. 3215–3226.

Vaniea, K. E., E. Rader, and R. Wash. (2014). "Betrayed by updates: how negative experiences affect future security". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2671–2674.

Vannini, S., R. Gomez, and B. C. Newell. (2020). ""Mind the five": Guidelines for data privacy and security in humanitarian work with undocumented migrants and other vulnerable populations". *Journal of the Association for Information Science and Technology*. 71(8): 927–938.

Venkatesh, V. and H. Bala. (2008). "Technology acceptance model 3 and a research agenda on interventions". *Decision sciences*. 39(2): 273–315.

Venkatesh, V. and F. D. Davis. (2000). "A theoretical extension of the technology acceptance model: Four longitudinal field studies". *Management science*. 46(2): 186–204.

Venkatesh, V., M. G. Morris, G. B. Davis, and F. D. Davis. (2003). "User acceptance of information technology: Toward a unified view". *MIS quarterly*: 425–478.

Verizon. (2020). "Data Breach Investigations Report". *Tech. rep.*

Verizon. (2022). "Data Breach Investigations Report". *Tech. rep.*

Wang, Y.-C., R. Kraut, and J. M. Levine. (2012). "To stay or leave? The relationship of emotional and informational support to commitment in online health support groups". In: *Proceedings of the ACM 2012 conference on computer supported cooperative work*. 833–842.

Wang, Q., H. Jin, and N. Li. (2009). "Usable access control in collaborative environments: Authorization based on people-tagging". In: *European Symposium on Research in Computer Security*. Springer. 268–284.

Wang, S., C. Faklaris, J. Lin, L. Dabbish, and J. I. Hong. (2022). "'It's Problematic but I'm not Concerned': University Perspectives on Account Sharing". *Proceedings of the ACM on Human-Computer Interaction*. 6(CSCW1): 1–27.

Wang, Y. (2018). "Inclusive security and privacy". *IEEE Security & Privacy*. 16(4): 82–87.

Wang, Y., P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh. (2014). "A field trial of privacy nudges for facebook". In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 2367–2376.

Wash, R. (2010). "Folk models of home computer security". In: *Proc. SOUPS '10*. New York, New York, USA: ACM Press. 1. DOI: 10.1145/1837110.1837125.

Wash, R., E. Rader, K. Vaniea, and M. Rizor. (2014). "Out of the loop: How automated software updates cause unintended security consequences". In: *10th Symposium On Usable Privacy and Security (SOUPS) 2014)*. 89–104.

WebAIM. (2017). "Screen Reader User Survey #7 Results".

Whitten, A. and J. Tygar. (1999). "Why Johnny can't encrypt: A usability evaluation of PGP 5.0". In: *Proc. SSYM'99*. 14–28. URL: http://www.usenix.org/events/sec99/full_papers/whitten/whitten.ps.

Wickins, J. (2007). "The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification". *Science and Engineering Ethics*. 13(1): 45–54.

Wikipedia. (2021). "2017 Equifax data breach". URL: https://en.wikipedia.org/wiki/2017_Equifax_data_breach.

Wilson, G., H. Maxwell, and M. Just. (2017). "Everything's Cool: Extending Security Warnings with Thermal Feedback". In: *Proceedings of the 2017 CHI conference extended abstracts on human factors in computing systems*. 2232–2239.

Wobbrock, J. O. (2009). "Tapsongs: tapping rhythm-based passwords on a single binary sensor". In: *Proceedings of the 22nd annual ACM symposium on User interface software and technology*. 93–96.

Wogalter, M. S. (2006a). "Behavioral compliance: Theory, methodology, and results". In: *Handbook of warnings*. CRC Press. 335–354.

Wogalter, M. S. (2006b). "Communication-human information processing (C-HIP) model". *Handbook of warnings*: 51–61.

Woo, S., E. Kaiser, R. Artstein, and J. Mirkovic. (2016). "Life-experience passwords (leps)". In: *Proceedings of the 32nd Annual Conference on Computer Security Applications*. 113–126.

Wu, Y., W. K. Edwards, and S. Das. (2022a). ""A Reasonable Thing to Ask For": Towards a Unified Voice in Privacy Collective Action". In: *CHI Conference on Human Factors in Computing Systems*. 1–17.

Wu, Y., W. K. Edwards, and S. Das. (2022b). "SoK: Social Cybersecurity". In: *IEEE Symposium on Security and Privacy (Oakland)(2022). https://sauvikdas. com/uploads/paper/pdf/36/file. pdf*.

Xiao, S., J. Witschey, and E. Murphy-Hill. (2014). "Social influences on secure development tool adoption: why security tools spread". In: *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*. 1095–1106.

Xu, H., S. Gupta, M. B. Rosson, and J. M. Carroll. (2012). "Measuring mobile users' concerns for information privacy".

Yao, Y., D. Lo Re, and Y. Wang. (2017). "Folk models of online behavioral advertising". In: *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 1957–1969.

Yıldırım, M. and I. Mackie. (2019). "Encouraging users to improve password security and memorability". *International Journal of Information Security*. 18(6): 741–759.

Zhang, Z., Z. Zhang, H. Yuan, N. M. Barbosa, S. Das, and Y. Wang. (2021). "WebAlly: Making Visual Task-based CAPTCHAs Transferable for People with Visual Impairments". In: *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 281–298.

Zhao, Y., J. Ye, and T. Henderson. (2014). "Privacy-aware location privacy preference recommendations". In: *Proceedings of the 11th international conference on mobile and ubiquitous systems: Computing, networking and services*. 120–129.

Zuboff, S. (2015). "Big other: surveillance capitalism and the prospects of an information civilization". *Journal of information technology*. 30(1): 75–89.

Zurko, M. E. and R. T. Simon. (1996). "User-centered security". In: *Proceedings of the 1996 workshop on New security paradigms*. 27–33.