# CORI N. FAKLARIS – RESEARCH STATEMENT

I am a scholar in **human-computer interaction**. I work in **usable privacy and security**, a subfield that addresses a variety of usability and user interface issues in any system that involves sensitive data and/or is an attack target. In my work, I use a combination of qualitative methods and quantitative methods. My focus is on (1) **understanding human behavior in these systems** and (2) **empowering people** who interact with these systems to act securely in ways that meet their individual and social needs. I study general internet users in the United States in contexts such as romantic relationships, office work, and higher education. I leverage the insights for novel designs and systems. My work is sponsored by the U.S. National Science Foundation under grant no. CNS-1704087. I also am supported by the Center for Informed Democracy and Social Cybersecurity (IDeaS) and the CyLab Security & Privacy Institute.

My research goes to the core of a central problem in computing: **the widespread lack of understanding of cyber-risks that leads to insecure behaviors** [19,41,43–46]. This problem has persisted for decades, in which hundreds of millions of dollars and thousands of hours of staff time have been spent; and yet, **human interaction is still blamed in more than 99 percent of cyberattacks** [44]. My approach rejects the predominant "one size fits all" paradigm for security training and for the design of security tools and practices. Instead, I draw on prior work in social psychology, marketing, public health, and other fields that behavior change unfolds as a process in time and is influenced by relevant social contacts [6,8,17,18,26,28,36]. My overall contribution is **a model of the stages of security behavior change** that will enable designing and directing interventions to those most likely to benefit.

This research so far has led to **15 external publications**, including the refereed papers "A Self-Report Measure of End User Security Attitudes (SA-6)," in Proceedings of the Fifteenth USENIX Symposium on Usable Privacy and Security (SOUPS 2019); "Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships," in Proceedings of the Fourteenth USENIX Symposium on Usable Privacy and Security (SOUPS 2018); and "'It's Problematic but I'm not Concerned': University Perspectives on Account Sharing," in *Proceedings of the ACM: Human-Computer Interaction* (in press). My initial thesis findings will be submitted to the 2022 ACM Conference on Computer-Supported Collaborative Work and Social Computing (CSCW 2022), and the overall findings to the 2023 ACM Conference on Human Factors in Computing Systems (CHI 2023).

In **future work,** I will experimentally test this stage model with different interventions by stage. I also want to explore topics such as how English being used as the language of cybersecurity can be an obstacle to non-native speakers, and how smartphones influence information judgment. I will publish future work in high-quality conference venues and in journals such as the ACM's *Transactions on Human-Computer Interaction* and Elsevier's *Computers & Security* or *Computers in Human Behavior*.

## Developing a stage model of cybersecurity behavior adoption

McAfee estimates that the global costs of cybercrime have now **surpassed $1 trillion** [41]. Further, enterprise security awareness training can **cost around $300,000 and hundreds of staff hours** [29]. While lower-cost solutions exist (such as password managers), people often are not fully aware of what they do or use them regularly [24,33,42,46]. To address the problem, we should look to insights that behavior change unfolds as a process in time, influenced by social contacts [6,8,17,18,26,28,36].

In my PhD thesis, my goal is to **develop a behavior stage model specifically for end-user cybersecurity that accounts for social influences by stage**. The benefits of this are that researchers can analyze a target audience and split it into segments, either by stage in the behavior change process or by individual characteristics. They then can zoom in and identify the processes or factors that differentiate each segment and that can explain the evolution of thinking and emotions about the target behavior.

Towards this goal, I have conducted remote interviews with *N*=17 U.S. residents aged 18 or older. I find that their adoption of security practices can be broken down into four stages: **Threat Awareness** (Step 1), **Security Learning** (Step 2), **Implementation of Practice** (Step 3), and **Maintenance of Practice** (Step 4). Social influences are important to move people to each stage, such as Troubleshooting that helps people to get to Step 4. Usability and other practice characteristics such as Trialability also were important to move them to Step 3. Obstacles to moving to long-term adoption include skipping Threat Awareness (Step 1) and a lack of social supports. For those at Maintenance (Step 4), they reported becoming significant social influences for others, such as giving advice to coworkers or helping older relatives with cybersecurity.


**Figure 1: Diagram of the four steps that were common to people's security narratives (N=17) and the social influences that were commonly most influential at each step.**

Now, I am collecting a dataset from *N*<2000 U.S. residents aged 18 or older **to test the validity** of these findings with regards to one specific security practice, using a password manager. The results will give me the distribution of these steps in the U.S. population and data on the associated behavioral influences. The sample will be of sufficient size to make claims to generalizability [16]. I am collecting data not just about adopters but about non-adopters, who have been neglected in the behavior-stage literature. The resulting quantitative insights will be submitted for publication after graduation.

My thesis work is one step toward an envisioned **Socio-Cognitive Stage Model of Cybersecurity Adoption**. Its broader impacts could be akin to that of the Capability Maturity Model [38,47] for software engineering, helping organizations to assess cybersecurity readiness and plan investments. A secondary product would be the development of an algorithm to predict end-user security compliance and classify employees by an envisioned Stage of End-user Cybersecurity Adoption (SECA). Such work could be commercialized to offer it to the public. I also would conduct public scholarship to spread this knowledge among corporate, government and nonprofit groups and organizations.

## Understanding how security attitudes and behaviors connect

A key sub-problem is that many computer users find cybersecurity to be **scary, confusing, or dull** [12]. Such negative attitudes are worrying because prior work has found that attitudes are predictive of people's behavior intentions and actual behaviors [2,11], and attitude change lies at the heart of behavioral persuasion [5,27]. To address this problem, researchers need to examine **what leads to different security attitudes** and **what is their effect on security behavior intentions and on security behaviors** (such as taking a moment to change a compromised password or to set up multi-factor authentication). However, the field of usable security historically has lacked the robust and varied measures of attitude and related constructs that have enabled advances in the social sciences. This has hindered quantitative user research at scale. Researchers have had to create their survey measures of security attitude from scratch, which is time-consuming. Moreover, such custom studies are not easily comparable. The alternative to large-scale surveys – interviews – are also time-consuming to design, to conduct, and to analyze, and they are usually not intended to generalize to an entire population.

**I am an expert** in creating psychological measures for usable security. The most widely known is **SA-6, for six-item security attitude scale** [10]. A person's SA-6 score is the average of their ratings (1=Strongly Disagree to 5=Strongly Agree) of six statements, such as "I often am interested in articles about security threats" and "I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe." To assess SA-6's predictive validity, I adapted the Security Behavior Intention Scale (SeBIS) [9] to measure whether a participant recalled engaging in 10 security practices in the past week. I labeled this new scale the **Recalled Security Actions (RSec) inventory**.

Using a Qualtrics census-representative panel (N=209) [10], I found that security attitude, as measured by SA-6, was significantly positively associated with security behavior intention (SeBIS) and with recalled security behaviors (RSec), and that attitudes significantly varied by social influences. I now am preparing a paper on **a multi-faceted assessment, SA-13**, to address attitudes that are not positive in valence, with publication anticipated after graduation. The SA-13 inventory enables large-scale research into **hesitation and resistance** to adopting security practices (such as using password managers). This will help security designers and marketers to identify and address people's psychological obstacles to adoption.

## Addressing the socio-technical gap in usable security

A second sub-problem in usable security is that of the **socio-technical gap** [1], in which the technical functioning of the system as designed does not support users' social needs. An example is the "1 user-1 account" design for authentication systems. This design creates a dilemma for system users who want to keep their data secure but are using the account in a social context, such as a romantic relationship [23], an office [31], or a research university [in press]. Their logistical and social needs motivate them to **make compromises with security policies** and share the account password to enable multiple people to access a single account. While password managers enable groups to do such sharing securely, many people either have not tried them or do not use them effectively [4,24].

I have mentored several students in research to investigate these issues, with **three achieving first-authorship of published conference papers**. We found, for instance, that romantic couples don't use two-factor authentication despite this being a best practice, mostly because it causes issues when one person tries to log in and the other person can't answer their smartphone notification. We also found that workers reported problems with colleagues who were fired or quit, then changed a shared account password to something unknown, locking them out.

More specifically: Our first paper [23] contributed the novel finding of *relationship maintenance* as a motivator for account sharing among romantic couples, along with household maintenance [20], trust [30], and convenience [30], in a thematic analysis of *N*=174 open-ended survey responses from workers on Amazon Mechanical Turk (Mturk). The second [31] established that such account sharing at work is considered *"normal and easy"* – though still challenging, in a qualitative analysis of *N* = 98 survey responses from Mturk workers and a quantitative analysis of *N*=288 from both Mturk and Prolific. The third [in press], an interview study at a U.S. research university (*N*=23), contributes differences in account sharing practices by job role. It notes the influence of *educational paternalism*, as shown by trust in the campus authorities to keep their data and accounts safe; and *academic freedom*, which implies no limits on tech use and a lack of top-down security mandates.

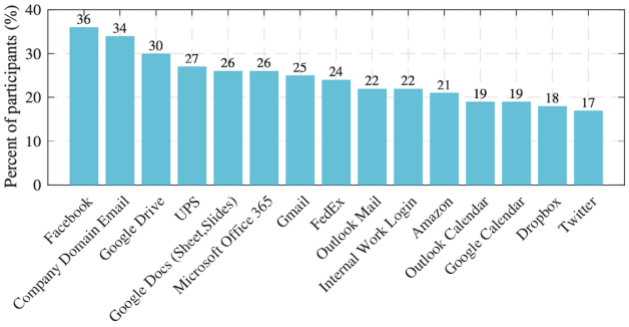


**Figure 2: A chart of the 15 most shared accounts, and percent of people sharing, from an analysis of *N*=288 survey responses on Mturk and Prolific [31].**

Our chief recommendation from this work was to **change the design of authentication systems to allow accounts to be securely shared with multiple people**. These changes have been implemented in several systems, such as Microsoft's Azure Active Directory [7]. I also worked with assistants to design and build out a simple social authentication tool. This tool would let a user log into a research lab account by verifying their answers to questions about what occurred during the last group meeting.

## Investigating mobile-social factors in security incidents

A third sub-problem in usable security is that of users' susceptibility to misinformation. From 2013 to 2018, the number of cybersecurity breaches in which attackers used so-called social methods,

such as spearphishing or other types of misinformation, increased from 17% to 35% [39]. During this time, mobile's share of global internet traffic increased, to about half by 2017 [48]. Given these statistics, it is reasonable to suspect that **the switch to mobile has negatively impacted smartphone users' ability to assess and judge information delivered via the internet** [34]. Technical factors of mobile devices that may constrict users' ability to assess and judge information include smaller screen sizes [49,50], limits on the ability to view sources and navigate among pages and apps (such as to view SSL certificates [51]), and a plethora of call-to-action interface elements [21,40]. Psychological factors that may leave mobile users more open than desktop users to manipulation include increased cognitive overload [34,40] and a greater willingness to self-disclose [22]. How these factors affect users may also vary according to context, such as whether a user is multitasking while using a smartphone [34,40] or able to narrowly focus on a task but constrained by mobile's technical factors in their ability to make sense of information [22]. These factors may also vary by social group context, such as whether the phone is used in a multi-resident household [20], within a romantic relationship [23], or for work purposes [31].

I am eager to collaborate with other researchers to explore these ideas and possible design interventions, such as a haptic "buzz" to keep users focused when they are reading news on a smartphone.

## FUTURE WORK

My chief plans revolve around my envisioned **Socio-Cognitive Stage Model of Cybersecurity Adoption**. I will pursue additional research threads tied to the model. At least two of these will **experimentally validate the resulting model** and **create and test interventions by stage**. A third thread will **experimentally investigate social vs. individually focused interventions by stage**. I anticipate using randomized factorial designs that are deployed first in a pilot lab experiment and second in a larger-scale online experiment. Finally, I will **investigate my stage model in a field study**. I plan to publish the results of these studies in conference venues such as ACM CHI and USENIX Security or SOUPS, and journals such as *Proceedings of the ACM: Human-Computer Interaction* or Elsevier's *Computers & Security* or *Computers in Human Behavior*.

I also will develop and publish additional psychometric measures for use in human factors in cybersecurity and in interdisciplinary research. For instance, it would be useful to explore the degree to which people's security attitudes overlap with their attitudes toward other types of protective actions, such as **getting vaccinations** [3] or **buying insurance** [35], and how these associate with their **evaluation of risk and uncertainty** in general [14,15,32]. I also see **commercial potential** for these psychometric scales, as measures such as the System Usability Scale [25] have been built out into proprietary platforms for quantifying the user experience.

I will mentor undergraduate and graduate students on projects that will further our understanding of how social contexts and behaviors connect, helping us to empower users who have been overlooked in mainstream security design. One such project will explore **how security jargon that originates in the English language, such as "firewall," poses challenges for users whose first language is not English**, and what designs could help them to better communicate about security concerns and problems. Methods such as **diary study**, **storyboards, and "speed dating"** [13] will help define needs and guide the creation of new tools and materials for non-native speakers.

Finally, I will collaborate with research assistants to design an **in-lab experiment** with a small local sample to gather initial data on the degree to which users' performance on information-assessment tasks (such as distinguishing "fake news" from authentic journalism in a simulated social-media interface) differs by the type of device used and the operating system. I anticipate **measuring performance** using objective metrics, such as accuracy rate and time-on-task, along with self-reports assessments. These are an ideal vehicle to introduce students to quantitative measurement of user experience. The insights will be used to make design recommendations and to guide students' creation of prototypes to address any mobile-social factors that are impacting users' information judgments. The insights could also be used by companies such as Apple and Samsung to improve the design of their smartphones.

## REFERENCES


[1] Mark S. Ackerman. 2000. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human–Computer Interact.* 15, 2–3 (September 2000), 179–203. DOI:https://doi.org/10.1207/S15327051HCI1523_5

[2] 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

[3] Dolores Albarracin, Haesung Jung, Wen Song, Andy Tan, and Jessica Fishman. 2021. Rather than inducing psychological reactance, requiring vaccination strengthens intentions to vaccinate in US populations. *Sci. Rep.* 11, 1 (October 2021), 20796. DOI:https://doi.org/10.1038/s41598-021-00256-z

[4] Nora Alkaldi and Karen Renaud. 2016. Why Do People Adopt, or Reject, Smartphone Password Managers? Retrieved December 24, 2020 from https://www.internetsociety.org/doc/why-do-people-adopt-or-reject-smartphone-password-managers

[5] Robert B. Cialdini. 2001. *Influence: science and practice* (4th ed ed.). Allyn and Bacon, Boston, MA.

[6] Anatoli Colicev, Ashish Kumar, and Peter O'Connor. 2019. Modeling the relationship between firm and user generated content and the stages of the marketing funnel. *Int. J. Res. Mark.* 36, 1 (March 2019), 100–116. DOI:https://doi.org/10.1016/j.ijresmar.2018.09.005

[7] curtand. Sharing accounts and credentials - Azure Active Directory. Retrieved November 19, 2021 from https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-sharing-accounts

[8] Carlo C. DiClemente and James O. Prochaska. 1998. Toward a comprehensive, transtheoretical model of change: Stages of change and addictive behaviors. In *Treating addictive behaviors, 2nd ed*. Plenum Press, New York, NY, US, 3–24. DOI:https://doi.org/10.1007/978-1-4899-1934-2_1

[9] 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

[10] 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

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

[12] 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.

[13] Bruce Hanington and Bella Martin. 2012. *Universal Methods of Design: 100 Ways to Research Complex Problems, Develop Innovative Ideas, and Design Effective Solutions*. Rockport Publishers.

[14] Daniel Kahneman and Amos Tversky. 2000. *Choices, Values, and Frames*. Cambridge University Press.

[15] Daniel Kahneman and Amos Tversky. 2012. Prospect Theory: An Analysis of Decision Under Risk. In *Handbook of the Fundamentals of Financial Decision Making*. WORLD SCIENTIFIC, 99–127. DOI:https://doi.org/10.1142/9789814417358_0006

[16] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of Mechanical Turk workers and the US public. In *Symposium on Usable Privacy and Security (SOUPS)*, 37–49.

[17] J A Kelly, J S St Lawrence, L Y Stevenson, A C Hauth, S C Kalichman, Y E Diaz, T L Brasfield, J J Koob, and M G Morgan. 1992. Community AIDS/HIV risk reduction: the effects of endorsements by popular people in three cities. *Am. J. Public Health* 82, 11 (November 1992), 1483–1489. DOI:https://doi.org/10.2105/AJPH.82.11.1483

[18] Matthew W. Kreuter and Ricardo J. Wray. 2003. Tailored and Targeted Health Communication: Strategies for Enhancing Information Relevance. *Am. J. Health Behav.* 27, 1 (November 2003), 227–232. DOI:https://doi.org/10.5993/AJHB.27.1.s3.6

[19] Mary Madden and Lee Rainie. 2015. Americans' Attitudes About Privacy, Security and Surveillance | Pew Research Center. Retrieved February 28, 2019 from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[20] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. 2016. "She'll just grab any device that's closer": A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 5921–5932. Retrieved August 29, 2021 from https://doi.org/10.1145/2858036.2858051

[21] Travis Hines on May 24, 2012 in Design, and Development. Designing (and converting) for multiple mobile densities. *Teehan+Lax*. Retrieved May 12, 2019 from https://www.teehanlax.com/blog/density-converter/

[22] Shiri Melumad and Robert Meyer. 2020. Full Disclosure: How Smartphones Enhance Consumer Self-Disclosure. *J. Mark.* 84, 3 (May 2020), 28–45. DOI:https://doi.org/10.1177/0022242920912732

[23] 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

[24] 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
[25] Jeff Sauro PhD. Measuring Usability with the System Usability Scale (SUS) – MeasuringU. Retrieved November 17, 2021 from https://measuringu.com/sus/
[26] 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.
[27] Everett M. Rogers. 2010. *Diffusion of Innovations, 4th Edition*. Simon and Schuster.
[28] Ismail Sahin. 2005. UNDERSTANDING FACULTY ADOPTION OF TECHNOLOGY USING THE LEARNING/ADOPTION TRAJECTORY MODEL: A QUALITATIVE CASE STUDY. *Turk. Online J. Educ. Technol.* 4, 1 (2005), 10.
[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] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password Sharing: Implications for Security Design Based on Social Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '07), ACM, New York, NY, USA, 895–904. DOI:https://doi.org/10.1145/1240624.1240759
[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] Amos Tversky and Daniel Kahneman. 1974. Judgment under Uncertainty: Heuristics and Biases. *Science* 185, 4157 (September 1974), 1124–1131. DOI:https://doi.org/10.1126/science.185.4157.1124
[33] Kami Vaniea and Yasmeen Rashidi. 2016. Tales of Software Updates: The Process of Updating Software. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), ACM, New York, NY, USA, 3215–3226. DOI:https://doi.org/10.1145/2858036.2858303
[34] Arun Vishwanath. 2016. Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. *Comput. Hum. Behav.* 63, (October 2016), 198–207. DOI:https://doi.org/10.1016/j.chb.2016.05.035
[35] PETER WAKKER, RICHARD THALER, and AMOS TVERSKY. 1997. Probabilistic Insurance. *J. Risk Uncertain.* 15, 1 (October 1997), 7–28. DOI:https://doi.org/10.1023/A:1007799303256
[36] 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
[37] Robert S. Weiss. 1995. *Learning From Strangers: The Art and Method of Qualitative Interview Studies*. Simon and Schuster.
[38] 2002. *Capability Maturity Model® Integration for Software Engineering (CMMI-SW), Version 1.1*. Carnegie Mellon Software Engineering Institute, Pittsburgh, Pennsylvania. Retrieved from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2002_005_001_14069.pdf
[39] 2018. *2018 Data Breach Investigations Report*. Verizon Enterprise. Retrieved April 13, 2018 from http://www.verizonenterprise.com/verizon-insights-lab/dbir/
[40] 2019. *2019 Data Breach Investigations Report*. Verizon Enterprise. Retrieved May 8, 2019 from https://enterprise.verizon.com/resources/reports/dbir/
[41] 2021. New Year, New Digital You: Consumer Security Findings from McAfee's Latest Report. *McAfee Blogs*. Retrieved September 19, 2021 from https://www.mcafee.com/blogs/internet-security/new-year-new-digital-you-consumer-security-findings-from-mcafees-latest-report/
[42] 2021. McAfee: Profound Shift in Everyday Technology Highlights New Landscape of Personal Security. Retrieved September 19, 2021 from https://www.businesswire.com/news/home/20210126005247/en/McAfee-Profound-Shift-in-Everyday-Technology-Highlights-New-Landscape-of-Personal-Security
[43] [Tessian Research] The Psychology of Human Error.pdf. Retrieved October 29, 2021 from https://f.hubspotusercontent20.net/hubfs/1670277/%5BTessian%20Research%5D%20The%20Psychology%20of%20Human%20Error.pdf?__hstc=170273983.6aa213222a25e91ce29bfd9645578315.1635528205207.1635528205207.1635528205207.1&__hssc=170273983.5.1635528205208&__hsfp=3390846970
[44] Proofpoint's Annual Human Factor Report Details Top Cybercriminal Trends: More than 99 Percent of Cyberattacks Need Humans to Click | Proofpoint US. Retrieved October 29, 2021 from https://www.proofpoint.com/us/newsroom/press-releases/proofpoints-annual-human-factor-report-details-top-cybercriminal-trends-more
[45] The psychology of cyberthreats. *https://www.apa.org*. Retrieved February 15, 2019 from https://www.apa.org/monitor/2019/02/cyberthreats
[46] 2021 Data Breach Investigations Report. *Verizon Business*. Retrieved September 19, 2021 from https://www.verizon.com/business/resources/reports/dbir/
[47] Capability Maturity Model (CMM). Retrieved February 7, 2018 from http://searchsoftwarequality.techtarget.com/definition/Capability-Maturity-Model?vgnextfmt=print
[48] Mobile percentage of website traffic 2019 | Statistic. *Statista*. Retrieved May 10, 2019 from https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/

[49] Displays. Retrieved May 12, 2019 from https://developer.apple.com/library/archive/documentation/DeviceInformation/Reference/iOSDeviceCompatibility/Displays/Displays.html
[50] Density & resolution. *Material Design*. Retrieved May 12, 2019 from https://material.io/design/layout/density-resolution.html#
[51] How to View SSL Certificate Details in Each Browser and What You Can Learn. Retrieved May 13, 2019 from https://www.globalsign.com/en/blog/how-to-view-ssl-certificate-details