ID	Titulo	Ano	Área	Link	Resumo	Referência
A01	The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions	2021	Segurança	https://dl.acm.org/doi/abs/10.1145/3429888	Nudging is a promising approach, in terms of influencing people to make advisable choices in a range of domains, including cybersecurity. However, the processes underlying the concept and the nudge's effectiveness in different contexts, and in the long term, are still poorly understood. Our research thus first reviewed the nudge concept and differentiated it from other interventions before applying it to the cybersecurity area. We then carried out an empirical study to assess the effectiveness of three different nudge-related interventions on four types of cybersecurity-specific decisions. Our study demonstrated that the combination of a simple nudge and information provision, termed a "hybrid nudge," was at least as, and in some decision contexts even more effective in encouraging secure choices as the simple nudge on its own. This indicates that the inclusion of information when deploying a nudge, thereby increasing the intervention's transparency, does not necessarily diminish its effectiveness. A follow-up study explored the educational and long-term impact of our tested nudge interventions to encourage secure choices. The results indicate that the impact of the initial nudges, of all kinds, did not endure. We conclude by discussing our findings and their implications for research and practice.	Zimmermann and Renaud. 2021. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. ACM Trans. Comput.-Hum. Interact.
A02	Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations	2021	Segurança	https://www.tandfonline.com/doi/abs/10.1080/0144929X.2021.1876167	Nudging users to keep them secure online has become a growing research field in cybersecurity. While existing approaches are mainly blackbox based, showing aggregated visualisations as one-size-fits-all nudges, personalisation turned out promising to enhance the efficacy of nudges within the high variance of users and contexts. This article presents a disaggregated whitebox-based visualisation of critical information as a novel nudge. By segmenting users according to their decision-making and information processing styles, we investigate if the novel nudge is more effective for specific users than a common black-box nudge. Based on existing literature about critical factors in password security, we designed a dynamic radar chart and parallel coordinates as disaggregated visualisations. We evaluated the short-term effectiveness and users' perception of the nudges in a think-aloud prestudy and a representative online evaluation (N=1.012). Our findings suggest that dynamic radar charts present a moderately effective nudge towards stronger passwords regarding short-term efficacy and are appreciated particularly by players of role-playing games.	Katrin Hartwig & Christian Reuter (2021): Nudging users towards better security decisions in password creation using whitebox-based multidimensional visualisations, Behaviour & Information Technology.
A03	Ethical guidelines for nudging in information security & privacy	2018	Privacidade & Segurança	https://rke.abertay.ac.uk/ws/portalfiles/portal/14922803/Renaud_EthicalGuidelinesForNudgingInInformationSecurityAndPrivacy_Author_2018.pdf	There has recently been an upsurge of interest in the deployment of behavioural economics techniques in the information security and privacy domain. In this paper, we consider the nature of one particular intervention, the nudge, and the way it exercises its influence. We contemplate the ethical ramifications of nudging, in its broadest sense, deriving general principles for ethical nudging from the literature. We extrapolate these principles to the deployment of nudging in information security and privacy. Furthermore, we explain how researchers can use these guidelines to ensure that they satisfy the ethical requirements during nudge trials in information security and privacy. Our guidelines also provide guidance to ethics review boards that are required to evaluate nudge-related research.	Karen Renaud, Verena Zimmermann, Ethical Guidelines for Nudging in Information Security & Privacy, International Journal of Human-Computer Studies (2018).
A04	Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity	2021	Segurança	https://www.emerald.com/insight/content/doi/10.1108/OCJ-03-2021-0009/full/html	Purpose Phishing attacks are the most common cyber threats targeted at users. Digital nudging in the form of framing and priming may reduce user susceptibility to phishing. This research focuses on two types of digital nudging, framing and priming, and examines the impact of framing and priming on users' behavior (i.e. action) in a cybersecurity setting. It draws on prospect theory, instance-based learning theory and dual-process theory to generate the research hypotheses. Design/methodology/approach A 3 × 2 experimental study was carried out to test the hypotheses. The experiment consisted of three levels for framing (i.e. no framing, negative framing and positive framing) and two levels for priming (i.e. with and without priming). Findings The findings suggest that priming users to information security risks reduces their risk-taking behavior, whereas positive and negative framing of information security messages regarding potential consequences of the available choices do not change users' behavior. The results also indicate that risk-averse cybersecurity behavior is associated with greater confidence with the action, greater perceived severity of cybersecurity risks, lower perceived susceptibility to cybersecurity risks resulting from the action and lower trust in the download link. Originality/value This research shows that digital nudging in the form of priming is an effective way to reduce users' exposure to cybersecurity risks.	Kavya Sharma, Xinhui Zhan, Fiona Fui-Hoon Nah, Keng Siau, Maggie X. Cheng (2021). "Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity", Organizational Cybersecurity Journal: Practice, Process and People.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A05	Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online	2017	Privacidade & Segurança	https://dl.acm.org/doi/abs/10.1145/3054926	Advancements in information technology often task users with complex and consequential privacy and security decisions. A growing body of research has investigated individuals' choices in the presence of privacy and information security tradeoffs, the decision-making hurdles affecting those choices, and ways to mitigate such hurdles. This article provides a multi-disciplinary assessment of the literature pertaining to privacy and security decision making. It focuses on research on assisting individuals' privacy and security choices with soft paternalistic interventions that nudge users toward more beneficial choices. The article discusses potential benefits of those interventions, highlights their shortcomings, and identifies key ethical, design, and research challenges.	Alessandro Acquisti, Idris Adjerid, e colaboradores. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. ACM Computing Surveys.
A06	Nudging users towards online safety using gamified environments	2021	Segurança	https://sci-hub.se/10.1016/j.cose.2021.102270	Humans are becoming the root cause of many security vulnerabilities that can compromise a whole network through erroneous or negligent behavior. Human vulnerability is a serious challenge, as users are very limited in their attention to information security warnings and guidelines. This paper describes Security-Robot, a gamified interactive security system that rewards users according to their online security behavior. We evaluate our approach in a randomized controlled experiment against traditional security messages when users need to download software that may be malicious under time pressure. Our results show that a gamified experience reduces the number of downloaded malware without reducing productivity and that presenting preemptive notifications strengthens this effect. Finally, we discuss the implications of our findings to the theory of usable security and the design of interactive security systems.	Petrykina, Y., Schwartz-Chassidim, H., & Toch, E. (2021). Nudging users towards online safety using gamified environments. Computers & Security, 108, 102270.
A07	Stack Overflow Considered Helpful! Deep Learning Security Nudges Towards Stronger Cryptography	2019	Segurança	https://www.usenix.org/conference/usenixsecurity19/presentation/fischer	Stack Overflow is the most popular discussion platform for software developers. Recent research found a large amount of insecure encryption code in production systems that has been inspired by examples given on Stack Overflow. By copying and pasting functional code, developers introduced exploitable software vulnerabilities into security-sensitive high-profile applications installed by millions of users every day. Proposed mitigations of this problem suffer from usability flaws and push developers to continue shopping for code examples on Stack Overflow once again. This points us to fighting the proliferation of insecure code directly at the root before it even reaches the clipboard. By viewing Stack Overflow as a market, implementation of cryptography becomes a decision-making problem: i. e. how to simplify the selection of helpful and secure examples. We focus on supporting software developers in making better decisions by applying nudges, a concept borrowed from behavioral science. This approach is motivated by one of our key findings: for 99.37% of insecure code examples on Stack Overflow, similar alternatives are available that serve the same use case and provide strong cryptography. Our system design is based on several nudges that are controlled by a deep neural network. It learns a representation for cryptographic API usage patterns and classification of their security, achieving average AUC-ROC of 0.992. With a user study we demonstrate that nudge-based security advice significantly helps tackling the most popular and error-prone cryptographic use cases in Android.	Fischer, F., Xiao, H., Kao, C.-Y., Stachelscheid, Y., Johnson, B., Razar, D., Fawkesley, P., Buckley, N., Böttinger, K., Muntean, P., & Grossklags, J. (2019). Stack Overflow Considered Helpful! Deep Learning Security Nudges Towards Stronger Cryptography. Proceedings of the 28th USENIX Security Symposium.
A08	Nudge me right: Personalizing online security nudges to people's decision-making styles	2020	Segurança	Nudge me right: Personalizing online security nudges to people's decision-making styles	Nudges are simple and effective interventions that alter the architecture in which people make choices in order to help them make decisions that could benefit themselves or society. For many years, researchers and practitioners have used online nudges to encourage users to choose stronger and safer passwords. However, the effects of such nudges have been limited to local maxima, because they are designed with the "average" person in mind, instead of being customized to different individuals. We present a novel approach that analyzes individual differences in traits of decision-making style and, based on this analysis, selects which, from an array of online password nudges, would be the most effective nudge each user should receive. In two large-scale online studies, we show that such personalized nudges can lead to considerably better outcomes, increasing nudges' effectiveness up to four times compared to administering "one-size-fits-all" nudges. We regard these novel findings a proof-of-concept that should steer more researchers, practitioners and policy-makers to develop and apply more efforts that could guarantee that each user is nudged in a way most right for them.	Egelman, S., Peer, E. (2020). Nudge me right: Personalizing Online Security Nudges to People's Decision-Making Styles. Computers in Human Behavior, Elsevier.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A09	DIGITAL NUDGES FOR PRIVACY AWARENESS: FROM CONSENT TO INFORMED CONSENT?	2020	Privacidade	(PDF) DIGITAL NUDGES FOR PRIVACY AWARENESS: FROM CONSENT TO INFORMED CONSENT?	Maintaining a private life in our digital world is gradually becoming harder. With Internet services having ever increasing access to personal data, it is crucial to raise user awareness about what privacy guarantees they offer. Regulations have recently been enacted such as the European General Data Privacy Regulation (GDPR). Yet, online service providers still have terms and privacy policies to which users tend to agree without ever viewing or reading them. By using digital nudges, this paper explores how small changes in the choice architecture can be designed to increase the informed consent and privacy awareness of users. The results from a double-blind online experiment (n = 183) show that phrasing the agreement differently and providing a highlights alternative to the existing quick-join choice architecture can significantly increase the number of users who view and read the terms and privacy policy. However, these digital nudges seem to not increase the users' recollection of what they have agreed to. The experimental results are complemented by a field test using one of the proposed designs in the IKEA Place app (n = 81'431)	Bergram, Kristoffer et al. 2020. Digital Nudges for Privacy Awareness: From Consent to Informed Consent?. Twenty-Eighth European Conference on Information Systems (ECIS2020), Marrakesh, Morocco.
A10	SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment	2014	Segurança	https://link.springer.com/chapter/10.1007/978-3-319-07668-3_23	Behavior-change interventions are common in some areas of human-computer interaction, but rare in the domain of cybersecurity. This paper introduces a structured approach to working with organisations in order to develop such behavioral interventions or 'nudges'. This approach uses elements of co-creation together with a set of prompts from the behavior change literature (MINDSPACE) that allows resesarchers and organisational stakeholders to work together to identify a set of nudges that might promote best behavioral practice. We describe the structured approach or framework, which we call SCENE, and follow this description with a worked example of how the approach has been utilised effectively in the development of a nudge to mitigate insecure behaviors around selection of wireless networks.	Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment. DUXU 2014, Part I, LNCS 8517, pp. 229-239. Springer International Publishing Switzerland.
A11	Nudging towards security: developing an application for wireless network selection for android phones	2015	Privacidade & Segurança	Nudging towards security: developing an application for wireless network selection for android phones	People make security choices on a daily basis without fully considering the security implications of those choices. In this paper we present a prototype application which promotes the choice of secure wireless network options, specifically when users are unfamiliar with the wireless networks available. The app was developed based on behavioural theory, choice architecture and good practices informed by HCI design. The app includes several options to 'nudge' users towards selecting more secure public wireless networks. This paper outlines the development and the results of an evaluation of some of the potential app nudges (specifically, presentation order and colour coding). Colour coding was found to be a powerful influence, less so with the order in which we listed the Wi-Fi networks, although the colour x order combination was most effective. The paper contributes to the body of evidence on the effectiveness of cyber-security interventions to empower the user to make more informed security decisions.	James Turland, Lynne Coventry, Debora Jeske, Pam Briggs, Aad van Moorsel, 2015, Nudging Towards security: Developing an Application for Wireless Network Selection for Android Phones, British HCI 2015.
A12	Blockchain-based data privacy management with Nudge theory in open banking	2020	Privacidade & Segurança	Blockchain-based data privacy management with Nudge theory in open banking	Open banking brings both opportunities and challenges to banks all over the world especially in data management. A blockchain as a continuously growing list of records managed by a peer-to-peer network is widely used in various application scenarios; and it is commonly agreed that the blockchain technology can improve the protection of financial data privacy. However, current blockchain technology still poses some challenges in fully meeting the needs of financial data privacy protection. In order to address the existing problems, this paper proposes a new data privacy management framework based on the blockchain technology for the financial sector. The framework consists of three components: (1) a data privacy classification method according to the characteristics of financial data; (2) a new collaborative-filtering-based model; and (3) a data disclosure confirmation scheme for customer strategies based on the	Wang, H., Ma, S., Dai, H.-N., Imran, M., & Wang, T. (2020). Blockchain-based Data Privacy Management with Nudge Theory in Open Banking. Future Generation Computer Systems, Elsevier.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A13	Addressing consumerization of IT risks with nudging	2015	Privacidade & Segurança	https://aisel.aisnet.org/ijispm/vol3/iss3/2/	In this work we address the main issues of Information Technology (IT) consumerization that are related to security risks, and vulnerabilities of devices used within Bring Your Own Device (BYOD) strategy in particular. We propose a 'soft' mitigation strategy for user actions based on nudging, widely applied to health and social behavior influence. In particular, we propose a complementary, less strict, more flexible Information Security policies, based on risk assessment of device vulnerabilities and threats to corporate data and devices, combined with a strategy of influencing security behavior by nudging. We argue that nudging, by taking into account the context of the decision-making environment, and the fact that the employee may be in better position to make a more appropriate decision, may be more suitable than strict policies in situations of uncertainty of security-related decisions. Several examples of nudging are considered for different tested and potential scenarios in security context.	Iryna Yevseyeva, James Turland, Charles Morisset, Lynne Coventry, Thomas Groß, Christopher Laing, Aad van Moorsel. 2015. Addressing Consumerization of IT Risks with Nudging. International Journal of Information Systems and Project Management, Vol. 3, No. 3, pp. 5-22 .
A14	Force vs Nudge: Comparing Users Pattern Choices on SysPal and TinPal	2019	Privacidade & Segurança	https://arxiv.org/abs/1912.04231	Android's 3 × 3 graphical pattern lock scheme is one of the widely used authentication method on smartphone devices. However, users choose 3 × 3 patterns from a small subspace of all possible 389,112 patterns. The two recently proposed interfaces, SysPal by Cho et al. [Cho et al. 2017] and TinPal by the authors [Tupsamudre et al. 2018], demonstrate that it is possible to influence users 3 × 3 pattern choices by making small modifications in the existing interface. While SysPal forces users to include one, two or three system-assigned random dots in their pattern, TinPal employs a highlighting mechanism to inform users about the set of reachable dots from the current selected dot. Both interfaces improved the security of 3 × 3 patterns without affecting usability, but no comparison between SysPal and TinPal was presented. To address this gap, we conduct a new user study with 147 participants and collect patterns on three SysPal interfaces, 1-dot, 2-dot and 3-dot. We also consider original and TinPal patterns collected in our previous user study involving 99 participants [Tupsamudre et al. 2018]. We compare patterns created on five different interfaces, original, TinPal, 1-dot, 2-dot and 3-dot using a range of security and usability metrics including pattern length, stroke length, guessability, recall time and login attempts. Our study results show that participants in the TinPal group created significantly longer and complex patterns than participants in the other four groups. Consequently, the guessing resistance of TinPal patterns was the highest among all groups. Further, we did not find any significant difference in memorability of patterns created in the TinPal group and the other groups.	Harshal Tupsamudre et al. 2019. Force vs Nudge: Comparing Users Pattern Choices on SysPal and TinPal.
A15	Modeling and analysis of influence power for information security decisions	2016	Segurança	Modeling and analysis of influence power for information security decisions - ScienceDirect	Users of computing systems and devices frequently make decisions related to information security, e. g., when choosing a password, deciding whether to log into an unfamiliar wireless network. Employers or other stakeholders may have a preference for certain outcomes, without being able to or having a desire to enforce a particular decision. In such situations, systems may build in design nudges to influence the decision making, e. g., by highlighting the employer's preferred solution. In this paper we model influencing information security to identify which approaches to influencing are most effective and how they can be optimized. To do so, we extend traditional multi-criteria decision analysis models with modifiable criteria, to represent the available approaches an influencer has for influencing the choice of the decision maker. The notion of influence power is introduced to characterize the extent to which an influencer can influence decision makers. We illustrate our approach using data from a controlled experiment on techniques to influence which public wireless network users select. This allows us to calculate influence power and identify which design nudges exercise the most influence over user decisions.	Iryna Yevseyeva, Charles Morisset, Aad van Moorsel, 2016, Modeling and Analysis of Influence Power for Information Security Decisions, Performance Evaluation.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A16	Nudging Users Towards Privacy on Mobile Devices	2011	Privacidade & Segurança	https://kilthub.cmu.edu/articles/conference_contribution/Nudging_Users_Towards_Privacy_on_Mobile_Devices/13028258	By allowing individuals to be permanently connected to the Internet, mobile devices ease the way information can be accessed and shared online, but also raise novel privacy challenges for end users. Recent behavioral research on “soft” or “asymmetric” paternalism has begun exploring ways of helping people make better decisions in different aspects of their lives. We apply that research to privacy decision making, investigating how soft paternalistic solutions (also known as nudges) may be used to counter cognitive biases and ameliorate privacy-sensitive behavior. We present the theoretical background of our research, and highlight current industry solutions and research endeavors that could be classified as nudging interventions. We then describe our ongoing work on embedding soft paternalistic mechanisms in location sharing technologies and Twitter privacy agents.	Rebecca Balebako et al., 2011, Nudging Users Towards Privacy on Mobile Devices, Carnegie Mellon University
A17	NUDGE ME CORRECTLY: SOCIAL PROOF AND RECIPROCITY NUDGES AND THE ONLINE PRIVACY PROTECTION BEHAVIOR OF GENERATION X AND GENERATION Y.	2020	Privacidade	https://essay.utwente.nl/85415/	Generation X and Generation Y both show high online privacy protection behavior due to their online privacy concerns. Therefore, this study focuses on the online privacy context. Currently, nudges are mainly being implemented for the average person in a certain group of people, but there is no further segmentation within this group. Generation segments can be used to target different generations, each with their specific behavior and needs. Therefore, this study investigates the influence of online nudges on the online privacy protection behavior of Generation X and Generation Y. This study showed that the social proof nudge and reciprocity nudge had no different effect on the online privacy protection behavior of Generation X and Generation Y. However, the study showed some interesting outcomes that were not expected; participants with a high level of familiarity and quick decision, plus a low level of uncertainty regarding the fictional corona-app, showed less online privacy protection behavior.	Sanne H. Nijland, 2020, Nudge Me Correctly: Social Proof and Reciprocity Nudges and the Online Privacy Protection Behavior of Generation X and Generation Y, Universidade de Twente.
A18	From Data Disclosure to Privacy Nudges: A Privacy-Aware and User-Centric Personal Data Management Framework	2019	Privacidade & Segurança	https://arxiv.org/pdf/1909.09942	Although there are many privacy-enhancing tools designed to protect users’ online privacy, it is surprising to see a lack of user-centric solutions allowing privacy control based on the joint assessment of privacy risks and benefits, due to data disclosure to multiple platforms. In this paper, we propose a conceptual framework to fill the gap: aiming at user-centric privacy protection, we show that the framework can assess not only privacy risks in using online services but also the added values earned from data disclosure. Through following a human-in-the-loop approach, it is expected that the framework can provide a personalized solution via preference learning, continuous privacy assessment, behavioral monitoring and nudging. Finally, we describe a case study about “leisure travelers” and some areas for further research.	Yang Lu, Shujun Li, Athina Ioannou, Iis Tussyadiah, 2019, From Data Disclosure to Privacy Nudges: A Privacy-aware and User-centric Personal Data Management Framework, DependSys 2019.
A19	Do Password Managers Nudge Secure (Random) Passwords?	2022	Segurança	https://www.usenix.org/conference/soups2022/presentation/zibaei	Passwords are the most popular authentication method due to their simplicity and widespread adoption. However, the prevalence of password reuse undermines its security. A promising strategy to mitigate the risks of password reuse is to use random passwords generated and stored by password managers, yet many users do not use them. Many web browsers have built-in password managers that employ nudges at the time of password creation. These nudges aim to persuade the selection of more secure random passwords; however, little is known about which designs are most effective. We study (n = 558) the efficacy of nudges used by three popular web browsers: Chrome, Firefox, and Safari. Our results suggest Safari’s nudge implementation is significantly more effective than the others at nudging users to adopt a randomly generated password. We examine factors that may contribute to the adoption of randomly generated passwords, reasons that people adopt a randomly generated password (or not), as well as discuss elements of Safari’s nudge design that may contribute to its success. Our findings can be useful in informing both future password manager nudge designs and interventions to encourage password manager use.	Samira Zibaei, Dinah Rinoa Malapaya, Benjamin Mercier, Amirali Salehi-Abari, Julie Thorpe. 2022. Do Password Managers Nudge Secure (Random) Passwords? Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022

ID	Titulo	Ano	Área	Link	Resumo	Referência
A20	Personalized Security Messaging: Nudges for Compliance with Browser Warnings	2017	Segurança	https://blues.cs.berkeley.edu/wp-content/uploads/2018/01/paper-1.pdf	Abstract—Decades of psychology and decision-making research show that everyone makes decisions differently; yet security messaging is still one-size-fits-all. This suggests that we can improve outcomes by delivering information relevant to how each individual makes decisions. We tested this hypothesis by designing messaging customized for stable personality traits—specifically, the five dimensions of the General Decision-Making Style (GDMS) instrument. We applied this messaging to browser warnings, security messaging encountered by millions of web users on a regular basis. To test the efficacy of our nudges, we conducted experiments with 1,276 participants, who encountered a warning about broken HTTPS due to an invalid certificate under realistic circumstances. While the effects of some nudges correlated with certain traits in a statistically significant manner, we could not reject the null hypothesis—that the intervention did not affect the subjects' behavior—for most of our nudges, especially after accounting for participants who did not pay close attention to the message. In this paper, we present the detailed results of our experiments, discuss potential reasons for why the outcome contradicts the decision-making research, and identify lessons for researchers based on our experience	Nathan Malkin, Arunesh Mathur, Marian Harbach, e Serge Egelman. 2017. Personalized Security Messaging: Nudges for Compliance with Browser Warnings. EuroUSEC '17, 29 April 2017, Paris, France.
A21	Privacy nudges as policy interventions: comparing US and German media users' evaluation of information privacy nudges	2017	Privacidade	Privacy nudges as policy interventions: comparing US and German media users' evaluation of information privacy nudges	The protection of individuals' online privacy is one of the main challenges for Internet policy. As the informed consent paradigm has largely failed to ensure privacy protection online, we examine nudging as a tool of soft paternalism as an alternative intervention to sensitize users towards online privacy. Building upon the criticism that nudging is considered being manipulative and reducing people's autonomy in decision-making, we inquire how media users themselves evaluate nudges' effectiveness and intrusiveness. In particular, we distinguish nudges either as targeting heuristic decision-making (system 1) or deliberate decision-making through education and information (system 2). Empirically, we carried out an interview study among German and US media users (N = 52) to address cross-cultural differences in the evaluation of privacy interventions. Our results point to a preference for system 2 nudges. Germans in particular perceive state interventions addressing privacy awareness as more acceptable and helpful than US participants.	Dogruel, L. (2017). Privacy nudges as policy interventions: comparing US and German media users' evaluation of information privacy nudges. Information, Communication & Society, DOI: 10.1080/1369118X.2017.1403642.
A22	Who creates strong passwords when nudging fails	2021	Segurança	https://www.sciencedirect.com/science/article/pii/S2451958821000804	The use of strong passwords is viewed as a recommended cybersecurity practice, as the hacking of weak passwords led to major cybersecurity breaches. The present research investigated whether nudging with messages based on participants' self-schemas could lead them to create stronger passwords. We modeled our study on prior health-related research demonstrating positive results using messages based on self-schema categories (i.e., True Colors categories -compassionate, loyal, intellectual, and adventurous). We carried out an online study, one with 256 (185 women, 66 men, 5 other) undergraduates and one with 424 (240 men, 179 women, 5 other) Amazon Mechanical Turk (MTurk) workers, in which we randomly assigned participants to receive messages that matched or mismatched their self-schema. We also investigated whether differences across the Big Five personality traits, secure password knowledge, attitudes and behavior, need for cognition, and general risk-taking predicted the strength of passwords that participants created during the study. Multiple individual difference variables predicted password strength (i.e., conscientiousness, emotional stability, need for cognition, self-reported secure password knowledge, attitude, and behavior, and general risk-taking). MTurk workers had higher levels of cybersecurity knowledge and created stronger passwords than college students. The nudging messages did not lead to stronger passwords. Implications for strategies to increase the use of secure passwords are discussed.	Kennison, S. M., Jones, I. T., Spooner, V. H., Chan-Tin, D. E. (2021). Who creates strong passwords when nudging fails. Computers in Human Behavior Reports.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A23	The Myth of the Average User: Improving Privacy and Security Systems through Individualization	2015	Privacidade & Segurança	https://dl.acm.org/doi/abs/10.1145/2841113.2841115	While individual differences in decision-making have been examined within the social sciences for several decades, they have only recently begun to be applied by computer scientists to examine privacy and security attitudes (and ultimately behaviors). Specifically, several researchers have shown how different online privacy decisions are correlated with the "Big Five" personality traits. In this paper, we show that the five factor model is actually a weak predictor of privacy attitudes, and that other well-studied individual differences in the psychology literature are much stronger predictors. Based on this result, we introduce the new paradigm of psychographic targeting of privacy and security mitigations: we believe that the next frontier in privacy and security research will be to tailor mitigations to users' individual differences. We explore the extensive work on choice architecture and "nudges," and discuss the possible ways it could be leveraged to improve security outcomes by personalizing privacy and security mitigations to specific user traits.	Serge Egelman e Eyal Peer, 2015, The Myth of the Average User: Improving Privacy and Security Systems through Individualization, NSPW '15, September 08 - 11, 2015, Twente, Netherlands.
A24	Increasing Adoption of Tor Browser Using Informational and Planning Nudges	2022	Privacidade & Segurança	https://petsymposium.org/popets/2022/popets-2022-0040.php	Browsing privacy tools can help people protect their digital privacy. However, tools which provide the strongest protections—such as Tor Browser—have struggled to achieve widespread adoption. This may be due to usability challenges, misconceptions, behavioral biases, or mere lack of awareness. In this study, we test the effectiveness of nudging interventions that encourage the adoption of Tor Browser. First, we test an informational nudge based on protection motivation theory (PMT), designed to raise awareness of Tor Browser and help participants form accurate perceptions of it. Next, we add an action planning implementation intention, designed to help participants identify opportunities for using Tor Browser. Finally, we add a coping planning implementation intention, designed to help participants overcome challenges to using Tor Browser, such as extreme website slowness. We test these nudges in a longitudinal field experiment with 537 participants. We find that our PMT-based intervention increased use of Tor Browser in both the short- and long-term. Our coping planning nudge also increased use of Tor Browser, but only in the week following our intervention. We did not find statistically significant evidence of our action planning nudge increasing use of Tor Browser. Our study contributes to a greater understanding of factors influencing the adoption of Tor Browser, and how nudges might be used to encourage the adoption of Tor Browser and similar privacy enhancing technologies.	Peter Story, Daniel Smullen, Rex Chen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, e Florian Schaub, 2022, "Increasing Adoption of Tor Browser Using Informational and Planning Nudges", Proceedings on Privacy Enhancing Technologies.
A25	Nudging folks towards stronger password choices: providing certainty is the key	2019	Privacidade & Segurança	https://www.cambridge.org/core/journals/behavioural-public-policy/article/nudging-folks-towards-stronger-password-choices-providing-certainty-is-the-key/BAEEAC8EEB22980FA23EEFD809A5C8B7	Persuading people to choose strong passwords is challenging. One way to influence password strength, as and when people are making the choice, is to tweak the choice architecture to encourage stronger choice. A variety of choice architecture manipulations (i.e. 'nudges') have been trialled by researchers with a view to strengthening the overall password profile. None has made much of a difference so far. Here, we report on our design of an influential behavioural intervention tailored to the password choice context: a hybrid nudge that significantly prompted stronger passwords. We carried out three longitudinal studies to analyse the efficacy of a range of 'nudges' by manipulating the password choice architecture of an actual university web application. The first and second studies tested the efficacy of several simple visual framing 'nudges'. Password strength did not budge. The third study tested expiration dates directly linked to password strength. This manipulation delivered a positive result: significantly longer and stronger passwords. Our main conclusion was that the final successful nudge provided participants with absolute certainty as to the benefit of a stronger password and that it was this certainty that made the difference.	Karen Renaud e Verena Zimmermann, 2019, Nudging folks towards stronger password choices: providing certainty is the key. Behavioral Public Policy.
A26	Guidelines for Ethical Nudging in Password Authentication	2018	Segurança	https://ieeexplore.ieee.org/abstract/document/8531951	Nudging has been adopted by many disciplines in the last decade in order to achieve behavioural change. Information security is no exception. A number of attempts have been made to nudge end-users towards stronger passwords. Here we report on our deployment of an enriched nudge displayed to participants on the system enrolment page, when a password has to be chosen. The enriched nudge was successful in that participants chose significantly longer and stronger passwords. One thing that struck us as we designed and tested this nudge was that we were unable to find any nudge-specific ethical guidelines to inform our experimentation in this context. This led us to reflect on the ethical implications of nudge testing, specifically in the password authentication context. We mined the nudge literature and derived a number of core principles of ethical nudging. We tailored these to the password authentication context, and then show how they can be applied by assessing the ethics of our own nudge. We conclude with a set of preliminary guidelines derived from our study to inform other researchers planning to deploy nudge-related techniques in this context.	Renaud, K. & Zimmermann, V. (2018). Guidelines for Ethical Nudging in Password Authentication. South African Institute of Electrical Engineers, Vol. 109 (2), June 2018.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A27	Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge	2017	Privacidade & Segurança	https://www.sciencedirect.com/science/article/abs/pii/S0144818817300170	Privacy law rests on the assumption that government surveillance may increase the general level of conformity and thus generate a chilling effect. In a study that combines elements of a lab and a field experiment, we show that salient and incentivized consent options are sufficient to trigger this behavioral effect. Salient ex ante consent options may lure people into giving up their privacy and increase their compliance with social norms – even when the only immediate risk of sharing information is mere publicity on a Google website. A right to be forgotten (right to deletion), however, seems to reduce neither privacy valuations nor chilling effects. In spite of low deletion costs people tend to stick with a retention default. The study suggests that consent architectures may play out on social conformity rather than on consent choices and privacy valuations. Salient notice and consent options may not merely empower users to make an informed consent decision. Instead, they can trigger the very effects that privacy law intends to curb.	Hermstrüwer, Yoan; Dickert, Stephan (2017). Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge. International Review of Law and Economics.
A28	Consumerisation of IT: Mitigating Risky User Actions and Improving Productivity with Nudging	2014	Privacidade & Segurança	https://www.sciencedirect.com/science/article/pii/S2212017314003454	In this work we address the main issues of IT consumerisation that are related to security risks, and propose a 'soft' mitigation strategy for user actions based on nudging, widely applied to health and social behaviour influence. In particular, we propose a complementary, less strict, more flexible Information Security policies, based on risk assessment of device vulnerabilities and threats to corporate data and devices, combined with a strategy of influencing security behaviour by nudging. We argue that nudging, by taking into account the context of the decision-making environment, and the fact that the employee may be in better position to make a more appropriate decision, may be more suitable than strict policies in situations of uncertainty of security-related decisions.	Yevseyeva, I., Morisset, C., Turland, J., Coventry, L., Groß, T., Laing, C., & van Moorsel, A. (2014). Consumerisation of IT: Mitigating risky user actions and improving productivity with nudging. Procedia Technology, 16, 508-517.
A29	Dissecting Nudges in Password Managers: Simple Defaults are Powerful	2023	Privacidade & Segurança	https://www.usenix.org/conference/soups2023/presentation/zibaei	Password managers offer a feature to randomly generate a new password for the user. Despite improving account security, randomly generated passwords (RGPs) are underutilized. Many password managers employ nudges to encourage users to select a randomly generated password, but the most effective nudge design is unclear. Recent work has suggested that Safari's built-in password manager nudge might be more effective in encouraging RGP adoption than that of other browsers. However, it remains unclear what makes it more effective, and even whether this result can be attributed to Safari's nudge design or simply its demographics. We report on a detailed large-scale study (n=853) aimed at clarifying these issues. Our results support that Safari's nudge design is indeed more effective than Chrome's. By dissecting the elements of Safari's nudge, we find that its most important element is its default nudge. We additionally examine whether a social influence nudge can further enhance Safari's RGP adoption rate. Finally, we analyze and discuss the importance of a nudge being noticed by users, and its ethical considerations. Our results inform RGP nudge designs in password managers and should also be of interest to practitioners and researchers working on other types of security nudges.	Zibaei, S., Salehi-Abari, A., & Thorpe, J. (2023). Dissecting Nudges in Password Managers: Simple Defaults are Powerful. Proceedings of the Nineteenth Symposium on Usable Privacy and Security (SOUPS).
A30	PDPM: A Patient-Defined Data Privacy Management with Nudge Theory in Decentralized E-Health Environments	2021	Privacidade & Segurança	https://www.jstage.jst.go.jp/article/transinf/E104.D/11/E104.D_2021NGP0015/_pdf	A private decentralized e-health environment, empowered by blockchain technology, grants authorized healthcare entities to legitimately access the patient's medical data without relying on a centralized node. Every activity from authorized entities is recorded immutably in the blockchain transactions. In terms of privacy, the e-health system preserves a default privacy option as an initial state for every patient since the patients may frequently customize their medical data over time for several purposes. Moreover, adjustments in the patient's privacy contexts are often solely from the patient's initiative without any doctor or stakeholders' recommendation. Therefore, we design, implement, and evaluate user-defined data privacy utilizing nudge theory for decentralized e-health systems named PDPM to tackle these issues. Patients can determine the privacy of their medical records to be closed to certain parties. Data privacy management is dynamic, which can be executed on the blockchain via the smart contract feature. Tamper-proof user-defined data privacy can resolve the dispute between the e-health entities related to privacy management and adjustments. In short, the authorized entities cannot deny any changes since every activity is recorded in the ledgers. Meanwhile, the nudge theory technique supports providing the best patient privacy recommendations based on their behaviour activities even though the final decision rests on the patient. Finally, we demonstrate how to use PDPM to realize user-defined data privacy management in decentralized e-health environments.	Jang, S., Rahmadika, S., Shin, S.U., & Rhee, K.-H. (2021). PDPM: A Patient-Defined Data Privacy Management with Nudge Theory in Decentralized E-Health Environments. IEICE Transactions on Information and Systems, E104-D(11).

ID	Titulo	Ano	Área	Link	Resumo	Referência
A31	Helping Smartphone Users Manage their Privacy through Nudges	2017	Privacidade & Segurança	https://kilthub.cmu.edu/ndownloader/files/12254045/preview	The two major smartphone platforms (Android and iOS) have more than two million mobile applications (apps) available from their respective app stores, and each store has seen more than 50 billion apps downloaded. Although apps provide desired functionality by accessing users' personal information, they also access personal information for other purposes (e.g., advertising or profiling) that users may or may not desire. Users can exercise control over how apps access their personal information through permission managers. However, a permission manager alone might not be sufficient to help users manage their app privacy because: (1) privacy is typically a secondary task and thus users might not be motivated enough to take advantage of the permission manager's functionality, and (2) even when using the permission manager, users often make suboptimal privacy decisions due to hurdles in decision making such as incomplete information, bounded rationality, and cognitive and behavioral biases. To address these two challenges, the theoretical framework of this dissertation is the concept of nudges: "soft paternalistic" behavioral interventions that do not restrict choice but account for decision making hurdles. Specifically, I designed app privacy nudges that primarily address the incomplete information hurdle. The nudges aim to help users make better privacy decisions by (1) increasing users' awareness of privacy risks associated with apps, and (2) temporarily making privacy the primary task to motivate users to review and adjust their app settings. I evaluated app privacy nudges in three user studies. All three studies showed that app privacy nudges are indeed a promising approach to help users manage their privacy. App privacy nudges increased users' awareness of privacy risks associated with apps on their phones, switched users' attention to privacy management, and motivated users to review their app privacy settings. Additionally, the second study suggested that not all app privacy nudge contents equally help users manage their privacy. Rather, more effective nudge contents informed users of: (1) contexts in which their personal information has been accessed, (2) purposes for apps' accessing their personal information, and (3) potential implications of secondary usage of users' personal information. The third study showed that user engagement with nudges decreases as users receive repeated nudges. Nonetheless, the results of the third experiment also showed that users are more likely to engage with repeated nudges (1) if users have engaged with previous nudges, (2) if repeated nudges contain new information (e.g., additional apps, not shown in earlier nudges, that accessed sensitive resources), or (3) if the nudge contents of repeated nudges resonate with users. The results of this dissertation suggest that mobile operating system providers should enrich their systems with app privacy nudges to assist users in managing their privacy. Additionally, the lessons learned in this dissertation may inform designing privacy nudges in emerging areas such as the Internet of Things.	Almuhimedi, H. (2017). Helping Smartphone Users Manage their Privacy through Nudges (Doctoral dissertation, Carnegie Mellon University, USA).
A32	Nudges to Privacy Behaviour: Exploring an Alternative Approach to Privacy Notices	2015	Privacidade & Segurança	https://www.researchgate.net/profile/Nuria-Rodriguez-Priego/publication/281811601_Nudges_to_Privacy_Behaviour_Exploring_an_Alternative_Approach_to_Privacy_Notices/links/55f92bb408aec948c48daef6/Nudges-to-Privacy-Behaviour-Exploring-an-Alternative-Approach-to-Privacy-Notices.pdf	The report seeks to bring behavioural research methods for privacy to the attention of EU policy-makers. It argues that changes in web interface design can be a useful policy alternative to the traditional 'privacy notice' approach. Specifically, it examines whether web interface design has effect on people's online privacy behaviour through an online experiment (n=3229) in four European countries. Results show that the presence of an anthropomorphic character leads to greater disclosure of personal information, both directly and passively and the presence of a privacy notice leads to greater direct information disclosure. Additional psychological constructs (such as subjects' awareness that they were revealing personal information) were also recorded, and a demographic analysis according to gender, age, education and country of residence carried out.	Monteleone, S., van Bavel, R., Rodríguez-Priego, N., & Esposito, G. (2015). Nudges to Privacy Behaviour: Exploring an Alternative Approach to Privacy Notices. European Commission Joint Research Centre, Institute for Prospective Technological Studies.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A33	Enhancing security behaviour by supporting the user	2018	Privacidade & Segurança	https://www.sciencedirect.com/science/article/abs/pii/S0167404818300385	Although the role of users in maintaining security is regularly emphasised, this is often not matched by an accompanying level of support. Indeed, users are frequently given insufficient guidance to enable effective security choices and decisions, which can lead to perceived bad behaviour as a consequence. This paper discusses the forms of support that are possible, and seeks to investigate the effect of doing so in practice. Specifically, it presents findings from two experimental studies that investigate how variations in password meter usage and feedback can positively affect the resulting password choices. The first experiment examines the difference between passwords selected by unguided users and those receiving guidance and alternative forms of feedback (ranging from a traditional password meter through to an emoji-based approach). The findings reveal a 30% drop in weak password choices between unguided and guided usage, with the varying meters then delivering up to 10% further improvement. The second experiment then considers variations in the form of feedback message that users may receive in addition to a meter-based rating. It is shown that by providing richer information (e.g. based upon the time required to crack a password, its relative ranking against other choices, or the probability of it being cracked), users are more motivated towards making strong choices and changing initially weak ones. While the specifics of the experimental findings were focused upon passwords, the discussion also considers the benefits that may be gained by applying the same principles of nudging and guidance to other areas of security in which users are often found to have weak behaviours.	Furnell, S. M., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. Computers and Security. Elsevier. DOI: 10.1016/j.cose.2018.01.016 .
A34	Privacy for IoT: Informed consent management in Smart Buildings	2023	Privacidade & Segurança	https://www.sciencedirect.com/science/article/pii/S0167739X23001322	Smart Buildings (SBs) employ the latest IoT technologies to automate building operations and services with the objective of increasing operational efficiency, maximising occupant comfort, and minimising environmental impact. However, these smart devices – mostly cloud-based – can capture and share a variety of sensitive and private data about the occupants, exposing them to various privacy threats. Given the non-intrusive nature of these devices, individuals typically have little or no awareness of the data being collected about them. Even if they do and claim to care about their privacy, they fail to take the necessary steps to safeguard it due to the convenience offered by the IoT devices. This discrepancy between user attitude and actual behaviour is known as the ‘privacy paradox’. To address this tension between data privacy, consent and convenience, this paper proposes a novel solution for informed consent management in shared smart spaces. Our proposed Informed Consent Management Engine (ICME) (a) increases user awareness about the data being collected by the IoT devices in the SB environment, (b) provides fine-grained visibility into privacy conformance and compliance by these devices, and (c) enables informed and confident privacy decision-making, through digital nudging. This study provides a reference architecture for ICME that can be used to implement diverse end-user consent management solutions for smart buildings. A proof-of-concept prototype is also implemented to demonstrate how ICME works in a shared smart workplace. Our proposed solution is validated by conducting expert interviews with 15 highly experienced industry professionals and academic researchers to understand the strengths, limitations, and potential improvements of the proposed system.	C. Pathmabandu, J. Grundy, M.B. Chhetri, Z. Baig (2023). "Privacy for IoT: Informed consent management in Smart Buildings". Future Generation Computer Systems, 145, 367–383.
A35	Nudging Software Developers Toward Secure Code	2022	Segurança	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9740708	The prevalence of insecure code is one of the main challenges security experts are trying to solve. We study behavioral patterns among developers which largely contribute to insecure software—googling and reusing code from the Web—and apply nudge theory to harness these behaviors and help developers write more secure code.	Felix Fischer, Jens Grossklags (2022). Nudging Software Developers Toward Secure Code. IEEE Security & Privacy.
A36	This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices	2021	Privacidade	https://dl.acm.org/doi/abs/10.1145/3476087	Data protection regulatory policies, such as the European Union's General Data Protection Regulation (GDPR), force website operators to request users' consent before collecting any personal information revealed through their web browsing. Website operators, motivated by the potential value of the collected personal data, employ various methods when designing consent notices (e.g., dark patterns) in order to convince users to allow the collection of as much of their personal data as possible. In this paper, we design and conduct a user study where 1100 MTurk workers interact with eight different designs of cookie consent notices. We show that the nudging designs used in the different cookie consent notices have a large effect on the choices user make. Our results show that color-based nudging bars can significantly impact the participants' decisions to change the default cookie settings, despite using dark patterns. Also, in contrast to previous works, we report that users who do not use ad-blocking software are less likely to modify default cookie settings. Our findings demonstrate the importance of nudged interfaces and the effects orthogonal nudging techniques can have on users' choices.	Fernandez, C. B., Chatzopoulos, D., Papadopoulos, D., & Hui, P. (2021). TThis Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 346. https://doi.org/10.1145/3476087

ID	Titulo	Ano	Área	Link	Resumo	Referência
A37	Nudging Pakistani users towards privacy on social networks	2016	Privacidade & Segurança	https://sci-hub.se/10.1109/sai.2016.7556122	Social Networking Sites (SNS) have been studied extensively over the last 10 years. The area of privacy and security has always been the prominent area of research. With the exponential increase of social networking users the numbers of threats have increased alarmingly; stealing personal information has been the most common threat as the information is later used to carry out subsequent malicious activities. The vulnerabilities are exploited because majority of SNS users are usually unaware of consequences of disclosing personal information over the public forums without proper privacy measures. Unaware users usually choose weak settings and are not mindful regarding posting their personal information online. The users trust their SNS providers for providing necessary security and privacy to their data, this excessive trust and ignorance results in different degrees of privacy violations. Considering the fact that the privacy preferences of users are strongly influenced by cultural and ethnical differences, the following research was conducted to study the privacy concerns of Pakistani users and the privacy problems associated with posting on SNS. It was found that the users are keenly concerned about their privacy however, they are unable to achieve the desired privacy on SNS as a result of the lack of awareness of privacy options, inappropriate settings and the excessive time associated with configuring those settings. Based on the above observations the idea of nudging the user from behavioral science has been proposed to help people make better privacy choices and decisions on online social networks. The proposed model will nudge users while posting by calculating Privacy Score and Accessing Last Modified Privacy Settings for users which will alert users to adjust their privacy settings. The idea of Privacy Nudges will help HCI researchers to build more sophisticated and user friendly Privacy features without getting into lengthy and time consuming details of a...	Baig, R., & Iqbal, M. (2016). Nudging Pakistani users towards privacy on social networks. SAI Computing Conference 2016.
A38	Detection and nudge-intervention on sensitive information in social networks Get access Arrow	2022	Privacidade	https://academic.oup.com/jigpal/article-abstract/30/6/942/6532158	Detecting sensitive information considering privacy is a relevant issue on Online Social Networks (OSNs). It is often difficult for users to manage the privacy associated with their posts on social networks taking into account all the possible consequences. The aim of this work is to provide information about the sensitivity of the content of a publication when a user is going to share it in OSN. For this purpose, we developed a privacy-assistant agent that detects sensitive information. Based on this information, the agent provides a message through a nudge mechanism warning about the possible risks of sharing the message. To avoid being annoying, the agent also considers the user's previous behaviour (e.g. if he previously ignored certain nudges) and adapts the messages it sends to give more relevance to those categories that are more important to the user from the point of view of the privacy risk. This agent was integrated into the social network PESEDIA. We analysed the performance of different models to detect a set of sensitive categories (i.e. location, medical, drug/alcohol, emotion, personal attacks, stereotyping, family and association details, personal details and personally identifiable information) in a dataset of tweets in Spanish. The model that obtained the best results (i.e. F1 and accuracy) and that was finally integrated into the privacy-assistant agent was transformer-based.	Alemany, J., Botti-Cebriá, V., del Val, E., & García-Fornes, A. (2022). Detection and nudge-intervention on sensitive information in social networks Get access Arrow. Journal of Logic and Computation, 30(6), 942-953.
A39	Investigating Responsible Nudge Design for Informed Decision-Making Enabling Transparent and Reflective Decision-Making	2023	Privacidade	https://dl.acm.org/doi/abs/10.1145/3603555.3603567	Consent interfaces are habitually designed to coerce people into sharing the maximum amount of data, rather than making decisions that align with their intentions and privacy attitudes, by leveraging cognitive biases to nudge users toward certain decision outcomes through interface design. Reflection and transparency have been proposed as two design dimensions of a choice architecture constituting a responsible nudge approach capable of counteracting these mechanisms by prompting reflected choice. In a crowdsourced experiment, we evaluate these capabilities of a proposed data-disclosure consent interface design deploying the responsible nudge approach within a realistic setting by exploiting a status quo bias during the sign-up of an online survey platform as a secondary task within a crowdsourcing context. Our results provide insights into a responsible design of consent interfaces, suggesting that prompting reflection significantly decreases the discrepancy between users' privacy attitudes and decision outcomes. Meanwhile, making the presence of a nudge transparent had no significant effect on its influence. Furthermore, identifying individuals' attitudes as a significant predictor of privacy behavior provides a promising direction for future research.	Leimstädtner, D., Sörries, P., & Müller-Birn, C. (2023). Investigating Responsible Nudge Design for Informed Decision-Making Enabling Transparent and Reflective Decision-Making. Mensch und Computer 2023 (MuC '23), Rapperswil, Switzerland. ACM, New York, NY, USA. https://doi.org/10.1145/3603555.3603567

ID	Titulo	Ano	Área	Link	Resumo	Referência
A40	Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance	2016	Privacidade	https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2016.01341/full	Despite their best intentions, people struggle with the realities of privacy protection and will often sacrifice privacy for convenience in their online activities. Individuals show systematic, personality dependent differences in their privacy decision making, which makes it interesting for those who seek to design ‘nudges’ designed to manipulate privacy behaviors. We explore such effects in a cookie decision task. Two hundred and ninety participants were given an incidental website review task that masked the true aim of the study. At the task outset, they were asked whether they wanted to accept a cookie in a message that either contained a social framing ‘nudge’ (they were told that either a majority or a minority of users like themselves had accepted the cookie) or contained no information about social norms (control). At the end of the task, participants were asked to complete a range of personality assessments (impulsivity, risk-taking, willingness to self-disclose and sociability). We found social framing to be an effective behavioral nudge, reducing cookie acceptance in the minority social norm condition. Further, we found personality effects in that those scoring highly on risk-taking and impulsivity were significantly more likely to accept the cookie. Finally, we found that the application of a social nudge could attenuate the personality effects of impulsivity and risk-taking. We explore the implications for those working in the privacy-by-design space.	Coventry, L., Jeske, D., Blythe, J., Turland, J., & Briggs, P. (2016). Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. Frontiers in Psychology.
A41	Using Context-Based Password Strength Meter to Nudge Users’ Password Generating Behavior: A Randomized Experiment	2017	Privacidade & Segurança	https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1091&context=hicss-50	Encouraging users to create stronger passwords is one of the key issues in password-based authentication. It is particularly important as prior works have highlighted that most passwords are weak. Yet, passwords are still the most commonly used authentication method. This paper seeks to mitigate the issue of weak passwords by proposing a context-based password strength meter. We conduct a randomized experiment on Amazon MTurk and observe the change in users’ behavior. The results show that our proposed method is significantly effective. Users exposed to our password strength meter are more likely to change their passwords after seeing the warning message, and those new passwords are stronger. Furthermore, users are willing to invest their time to learn about creating a stronger password, even in a traditional password strength meter setting. Our findings suggest that simply incorporating contextual information to password strength meters could be an effective method in promoting more secure behaviors among end users.	Khern-am-nuai, Warut, Yang, Weining, & Li, Ninghui (2017). Using Context-Based Password Strength Meter to Nudge Users’ Password Generating Behavior: A Randomized Experiment. Proceedings of the 50th Hawaii International Conference on System Sciences.
A42	Addressing The Privacy Paradox through Personalized Privacy Notifications	2017	Privacidade & Segurança	https://dl.acm.org/doi/abs/10.1145/3214271	Privacy behaviors of individuals are often inconsistent with their stated attitudes, a phenomenon known as the "privacy paradox." These inconsistencies may lead to troublesome or regrettable experiences. To help people address these privacy inconsistencies, we propose a personalized privacy notification approach that juxtaposes users' general privacy attitudes towards specific technologies and the potential privacy riskiness of particular instances of such technology, right when users make decisions about whether and/or how to use the technology under consideration. Highlighting the privacy inconsistencies to users was designed to nudge them in making decisions in a way that aligns with their privacy attitudes. To illustrate this approach, we chose the domain of mobile apps and designed a privacy discrepancy interface that highlights this discrepancy between users' general privacy attitudes towards mobile apps and the potential privacy riskiness of a particular app, nudging them to make app installation and/or permission granting decisions reflecting their privacy attitudes. To evaluate this interface, we conducted an online experiment simulating the process of installing Android apps. We compared the privacy discrepancy approach with several existing privacy notification approaches. Our results suggest that the behaviors of participants who used the privacy discrepancy interface better reflected their privacy attitudes than the other approaches.	Jackson, C., & Wang, Y. (2018). Addressing The Privacy Paradox through Personalized Privacy Notifications. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(2), Article 68. https://doi.org/10.1145/3214271 .

ID	Titulo	Ano	Área	Link	Resumo	Referência
A43	Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms	2019	Privacidade & Segurança	https://www.sciencedirect.com/science/article/abs/pii/S1071581918302118	Privacy Risk in Online Social Networks (OSNs) is one of the main concerns that has increased in the last few years. Even though social network applications provide mechanisms to control risk, teenagers are not often aware of the privacy risks of disclosing information in online social networks. The privacy decision-making process is complex and users often do not have full knowledge and enough time to evaluate all potential scenarios. They do not consider the audience that will have access to disclosed information or the risk if the information continues to spread and reaches an unexpected audience. To deal with these issues, we propose two soft-paternalism mechanisms that provide information to the user about the privacy risk of publishing information on a social network. That privacy risk is based on a complex privacy metric. To evaluate the mechanisms, we performed an experiment with 42 teenagers. The proposed mechanisms were included in a social network called Pesedia. The results show that there are significant differences in teenagers' behaviors towards better privacy practices when the mechanisms are included in the network.	Alemany-Bordera, J.; Del Val Noguera, E.; Alberola Oltra, J.M.; García-Fornes, A. (2019). Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms. International Journal of Human-Computer Studies, 129, 27-40. https://doi.org/10.1016/j.ijhcs.2019.03.008
A44	Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates	2017	Privacidade & Segurança	https://www.usenix.org/system/files/conference/soups2017/soups2017-mathur.pdf	To keep mobile devices secure, experts recommend turning on auto-updates for applications, but recent research has suggested that users often avoid auto-updating because updates can lead to undesirable consequences such as user interface changes or compatibility issues. Understanding whether there are commonalities amongst users who avoid auto-updates can help us create better mobile application updating interfaces. However, little is known about how users' characteristics associate with their attitudes towards auto-updating their mobile applications, or how we can leverage these characteristics to encourage users to auto-update these applications to improve security. In this paper, by surveying Android users, we establish how users' past experiences with software updating, and users' psychometric traits differentiate those users who avoid application auto-updates from those who do them, as well as users' preferences towards auto-updating their applications. Our findings reveal that users who avoid application auto-updates are more likely to have had past negative experiences with software updating, tend to take fewer risks, and display greater proactive security awareness. Users' perceived level of trust with mobile applications also determined how comfortable they are auto-updating these applications. Based on these findings, we recommend how Android can improve the design of application update systems to encourage users to auto-update and keep their devices secure	Mathur, A., & Chetty, M. (2017). Impact of User Characteristics on Attitudes Towards Automatic Mobile Application Updates. Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).
A45	Prospects for Improving Password Selection	2023	Privacidade & Segurança	https://www.usenix.org/conference/soups2023/presentation/amador	User-chosen passwords remain essential to online security, and yet users continue to choose weak, insecure passwords. In this work, we investigate whether prospect theory, a behavioral model of how people evaluate risk, can provide insights into how users choose passwords and whether it can motivate new designs for password selection mechanisms that will nudge users to select stronger passwords. We run a pair of online user studies, and we find that an intervention guided by prospect theory---which leverages the reference-dependence effect by framing a choice of a weak password as a loss relative to choosing a stronger password---causes approximately 25% of users to improve the strength of their password (significantly more than alternative interventions) and improves the strength of passwords users select. We also evaluate the relation between feedback provided and password decisions and between users' mental models and password decisions. These results provide guidance for designing and implementing password selection interfaces that will significantly improve the strength of user-chosen passwords, thereby leveraging insights from prospect theory to improve the security of systems that use password-based authentication.	Amador, J., Ma, Y., Hasama, S., Lumba, E., Lee, G., Birrell, E. (2023). Prospects for Improving Password Selection. USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A46	Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure	2021	Privacidade	https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0254670	Social norms are powerful determinants of human behaviors in offline and online social worlds. While previous research established a correlational link between norm perceptions and self-reported disclosure on social network sites (SNS), questions remain about downstream effects of prevalent behaviors on perceived norms and actual disclosure on SNS. We conducted two preregistered studies using a realistic social media simulation. We further analyzed buffering effects of critical media literacy and privacy nudging. The results demonstrate a disclosure behavior contagion, whereby a critical mass of posts with visual disclosures shifted norm perceptions, which, in turn, affected perceivers' own visual disclosure behavior. Critical media literacy was negatively related and moderated the effect of norms on visual disclosure behavioral intentions. Neither critical media literacy nor privacy nudge affected actual disclosure behaviors, however. These results provide insights into how behaviors may spread on SNS through triggering changes in perceived social norms and subsequent disclosure behaviors.	Masur, P. K., DiFranzo, D., & Bazarova, N. N. (2021). Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure.
A47	Security Strength Indicator in Fallback Authentication: Nudging Users for Better Answers in Secret Questions	2017	Segurança	https://arxiv.org/ftp/arxiv/papers/1701/1701.03229.pdf	In this paper, we describe ongoing work that focuses on improving the strength of the answers to security questions. The ultimate goal of the proposed research is to evaluate the possibility of nudging users towards strong answers for ubiquitous security questions. In this research we are proposing a user interface design for fallback authentication to encourage users to design stronger answers. The proposed design involves visual feedback to the user based on mnemonics which attempts to give visual feedback to the user on the strength of the answer provided and guide the user to creatively design a stronger answer	Senarath, A., Arachchilage, N. A. G., & Gupta, B. B. (2024). Security Strength Indicator in Fallback Authentication: Nudging Users for Better Answers in Secret Questions.
A48	DARK AND BRIGHT PATTERNS IN COOKIE CONSENT REQUESTS	2021	Privacidade	https://repository.ubn.ru.nl/bitstream/handle/2066/231659/231659.pdf	Dark patterns are (evil) design nudges that steer people's behaviour through persuasive interface design. Increasingly found in cookie consent requests, they possibly undermine principles of EU privacy law. In two preregistered online experiments we investigated the effects of three common design nudges (default, aesthetic manipulation, obstruction) on users' consent decisions and their perception of control over their personal data in these situations. In the first experiment (N = 228) we explored the effects of design nudges towards the privacy-unfriendly option (dark patterns). The experiment revealed that most participants agreed to all consent requests regardless of dark design nudges. Unexpectedly, despite generally low levels of perceived control, obstructing the privacy-friendly option led to more rather than less perceived control. In the second experiment (N = 255) we reversed the direction of the design nudges towards the privacy-friendly option, which we title "bright patterns". This time the obstruction and default nudges swayed people effectively towards the privacy-friendly option, while the result regarding perceived control stayed the same compared to Experiment 1. Overall, our findings suggest that many current implementations of cookie consent requests do not enable meaningful choices by internet users, and are thus not in line with the intention of the EU policymakers. We also explore how policymakers could address the problem.	Graßl, P., Schraffenberger, H., Zuiderveen Borgesius, F., & Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. Journal of Digital Social Research
A49	Users' Information Disclosure Behaviors during Interactions with Chatbots: The Effect of Information Disclosure Nudges	2022	Privacidade	https://www.mdpi.com/2076-3417/12/24/12660	Drawing from the tension between a company's desire for customer information to tailor experiences and a consumer's need for privacy, this study aims to test the effect of two information disclosure nudges on users' information disclosure behaviors. Whereas previous literature on user-chatbot interaction focused on encouraging and increasing users' disclosures, this study introduces measures that make users conscious of their disclosure behaviors to low and high-sensitivity questions asked by chatbots. A within-subjects laboratory experiment entailed 19 participants interacting with chatbots, responding to pre-tested questions of varying sensitivity while being presented with different information disclosure nudges. The results suggest that question sensitivity negatively impacts users' information disclosures to chatbots. Moreover, this study suggests that adding a sensitivity signal—presenting the level of sensitivity of the question asked by the chatbot—influences users' information disclosure behaviors. Finally, the theoretical contributions and managerial implications of the results are discussed.	Carmichael, L., Poirier, S.-M., Coursaris, C. K., Léger, P.-M., & Sénécal, S. (2022). Users' Information Disclosure Behaviors during Interactions with Chatbots: The Effect of Information Disclosure Nudges. Applied Sciences, 12, 12660.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A50	Privacy protection in tourism: Where we are and where we should be heading for	2019	Privacidade & Segurança	https://kar.kent.ac.uk/71418/1/final.pdf	The link between information privacy concerns and privacy behaviours has been a focus of extensive investigation in various disciplines. However, little attention has been devoted to this issue in the tourism literature. Spurred by technological development and shaped by tourism-related environments, emerging privacy issues call for comprehensive yet context-specific studies to ensure tourists are making beneficial privacy choices. This paper first presents a comprehensive review of state-of-the-art research on privacy concerns and behaviours. Then, it suggests a list of overarching research priorities, merging social and technical aspects of privacy protection approaches as they apply to tourism. The priorities include research to measure tourists' privacy concerns, explore specific biases in tourists' privacy decisions, experiment with privacy nudges, and explore how to integrate privacy nudges in system design. Thus, this paper contributes to guiding the direction of future research on privacy protection in tourism.	Tussyadiah, Iis, Li, Shujun e Miller, Graham (2018). Privacy protection in tourism: Where we are and where we should be heading for. Information and Communication Technologies in Tourism 2019: Proceedings of the International Conference in Nicosia, Cyprus.
A51	Deployment of Source Address Validation by Network Operators: A Randomized Control Trial	2022	Privacidade & Segurança	https://ieeexplore.ieee.org/abstract/document/9833701	IP spoofing, sending IP packets with a false source IP address, continues to be a primary attack vector for large-scale Denial of Service attacks. To combat spoofing, various interventions have been tried to increase the adoption of source address validation (SAV) among network operators. How can SAV deployment be increased? In this work, we conduct the first randomized control trial to measure the effectiveness of various notification mechanisms on SAV deployment. We include new treatments using nudges and channels, previously untested in notification experiments. Our design reveals a painful reality that contrasts with earlier observational studies: none of the notification treatments significantly improved SAV deployment compared to the control group. We explore the reasons for these findings and report on a survey among operators to identify ways forward. A portion of the operators indicate that they do plan to deploy SAV and ask for better notification mechanisms, training, and support materials for SAV implementation.	Lone, Qasim, et al. 2022. "Deployment of Source Address Validation by Network Operators: A Randomized Control Trial." IEEE Symposium on Security and Privacy (SP).
A52	Making privacy personal: Profiling social network users to inform privacy education and nudging	2017	Privacidade	https://stirlab.org/wp-content/uploads/2018/06/2017_Wisniewski_MakingPrivacyPersonal.pdf	Social Network Sites (SNSs) offer a plethora of privacy controls, but users rarely exploit all of these mechanisms, nor do they do so in the same manner. We demonstrate that SNS users instead adhere to one of a small set of distinct privacy management strategies that are partially related to their level of privacy feature awareness. Using advanced Factor Analysis methods on the self-reported privacy behaviors and feature awareness of 308 Facebook users, we extrapolate six distinct privacy management strategies, including: Privacy Maximizers, Selective Sharers, Privacy Balancers, Self-Censors, Time Savers/Consumers, and Privacy Minimalists and six classes of privacy proficiency based on feature awareness, ranging from Novices to Experts. We then cluster users on these dimensions to form six distinct behavioral profiles of privacy management strategies and six awareness profiles for privacy proficiency. We further analyze these privacy profiles to suggest opportunities for training and education, interface redesign, and new approaches for personalized privacy recommendations	Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. International Journal of Human-Computer Studies

ID	Titulo	Ano	Área	Link	Resumo	Referência
A53	Contracting Around Privacy The (Behavioral) Law and Economics of Consent and Big Data	2017	Privacidade	https://www.zora.uzh.ch/id/eprint/257834/1/Contracting_Around_Privacy__The_Behavioral_Law_and_Economics_of_Consent_and_Big_Data.pdf	Abstract: European privacy law rests on the implicit assumption that consent to the process- ing of personal data and the analysis of Big Data is a purely individual choice. Accordingly, privacy lawyers mainly focus on how to empower users to make free and informed choices, for instance through debias- ing and nudging. However, a game theoretical anal- ysis suggests that strategic considerations may be a driving force of consent under certain conditions. In environments relying on the use of Big Data, con- sent is likely to impose negative privacy externalities on other users and constrain their freedom of choice. By contrast, a behavioral economic analysis suggests that users are subject to bounded rational- ity and bounded willpower. While nudges, like default options, can enable users to make protective pri- vacy choices in some cases, correcting cognitive def- icits might facilitate market failures and accelerate the erosion of privacy in other cases. This counterin- tuitive conclusion shows that legal rules on consent and privacy contracts should be grounded on an as- sumption of 'mixed rationalities', i.e. on insights from both standard economics and behavioral econom- ics. Hence, a sharper distinction between 'paternalis- tic nudging' and 'non-paternalistic soft regulation' to counter market failures is warranted	Hermstrüwer, Yoan (2017). Contracting Around Privacy The (Behavioral) Law and Economics of Consent and Big Data. JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law, 8, 9-26.
A54	The disconnection between privacy notices and information disclosure: an online experiment	2016	Privacidade	https://link.springer.com/article/10.1007/s40888-016-0040-4	We studied whether changes to the online environment, i.e. nudges, can lead to changes in privacy behaviour through an on-line experiment (n = 3229) across four European countries. The output measures were obtained through the answers to a questionnaire following a mock online exercise: one revealed the amount of personal information participants were willing to disclose, and the other whether they noticed a privacy policy link. The nudges appeared as changes in the design of a mock search engine (e.g. including an anthropomorphic character, highlighting prior browsing history or changing the look-and-feel to convey greater informality). The nudges did not lead to differences in the amount of personal information disclosed, but did affect whether participants noticed the privacy link or not. Socio-demographic factors were relevant. Compared to younger participants, older participants were less likely to reveal personal information but more likely to notice the privacy policy link. Men were more likely to reveal personal information than women, and more likely to notice the privacy policy link. Finally, significant differences were found between all countries. Participants from Italy chose to reveal least personal information (followed by those in Poland, Germany and the UK), and participants from the UK were significantly less likely to notice the privacy policy link. The implications for policy are that disclosure of personal information is resilient to small changes in the web environment, but this is not the case for awareness of a privacy policy link. Moreover, the fact that age, gender, and country of residence are relevant suggests that differentiated policy approaches depending on the target population may be warranted.	Rodríguez-Priego, N., van Bavel, R., & Monteleone, S. (2016). The disconnection between privacy notices and information disclosure: an online experiment. Econ Polit, 33, 433-461. doi:10.1007/s40888-016-0040-4.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A55	Decision justifications for wireless network selection	2014	Segurança	https://nrl.northumbria.ac.uk/id/eprint/17998/1/Jeske_Coventry_Briggs_2014_STAST.pdf	— A number of security risks are associated with the selection of wireless networks. We examined wireless network choices in a study involving 104 undergraduate social science students. One research goal was to examine the extent to which features (such as padlocks) and colours could be used to ‘nudge’ individuals towards more secure network and away from open (unsecured) network options. Another goal was to better understand the basis for their decision-making. Using qualitative as well as quantitative data, we were able to differentiate groups whose decision were driven by security concerns, those who made convenience-based decisions, and those whose motives were unclear or undefined. These groups made different network choices, in part due to different perceived functionality of the padlock. We further observed significant effects for the use of colour when nudging participants towards more secure choices. We also wanted to examine the role of individual differences in relation to the choices individuals make. Perceived controllability of risk played a role in terms of the extent to which participants would make more secure vs. unsecure choices, although we obtained no significant group differences when we examined these variables in relation to the different decision justification groups. This indicates that perceived risk perceptions and reasons for decisions may relate differently to the actual behavioural choices individuals make, with perceptions of risk not necessarily relating to the reasons that participants consider when making security decisions.	Jeske, Debora, Coventry, Lynne e Briggs, Pamela (2014). Decision justifications for wireless network selection. Socio-Technical Aspects of Security and Trust (STAST) Workshop, July 18, 2014, Vienna, Austria .
A56	A Value-centered Exploration of Data Privacy and Personalized Privacy Assistants	2022	Privacidade	https://link.springer.com/article/10.1007/s44206-022-00028-w	In the current post-GDPR landscape, privacy notices have become ever more prevalent on our phones and online. However, these notices are not well suited to their purpose of helping users make informed decisions. I suggest that instead of utilizing notice to elicit informed consent, we could repurpose privacy notices to create the space for more meaningful, value-centered user decisions. Value-centered privacy decisions, or those that accurately reflect who we are and what we value, encapsulate the intuitive role of personal values in data privacy decisions. To explore how we could design for such decisions, I utilize Suzy Killmister’s Four-Dimensional Theory of Autonomy (4DT) to operationalize value-centered privacy decisions. I then utilize 4DT to help design a system—called a value-centered privacy assistant (VcPA)—that could help create the space for value-centered data privacy decisions using privacy notices. Using this 4DT lens, I further assess the degree that an existing technology, personalized privacy assistants (PPAs), use notices in a manner that allows for value-centered decision-making. I lastly utilize insights from the PPA assessment to inform the design of a VcPA, concluding that a VcPA could utilize notices to assist users in value-centered app selection and in other data privacy decisions.	Carter, S. E. (2022). A Value-centered Exploration of Data Privacy and Personalized Privacy Assistants. Digital Society.
A57	On the impact of warning interfaces for enabling the detection of Potentially Unwanted Applications	2016	Segurança	https://pure.hw.ac.uk/ws/portalfiles/portal/10755205/EUsec16_final.pdf	We conducted a large-scale online study with 26,000 software installations during which we asked user (participants) whether they wanted to enable or disable the detection of Potentially Unwanted Applications (PUAs – potentially malicious software, such as adware or spyware). PUAs are notoriously difficult to manage, e.g., legal challenges can preclude default options that could otherwise be set for PUAs detection or removal. Our study was performed with an IT security software provider (ESET) who gave us access to the participants (antivirus product beta users). We used a between-subjects design with 15 conditions (a starting-point control interface, and 14 new "warning" interfaces). Despite the fact that many software companies (e.g., Microsoft, AVAST, AVG, McAfee, Kaspersky Lab) are struggling with PUAs detection, there are few studies focused on this topic. Our results indicate a strong desire for PUAs detection by users. In particular, enabling PUAs detection was chosen by 74.5% of our participants for our initial control interface. Further, a modified interface in which the option to enable PUAs detection was presented first resulted in 89.8% of participants choosing to enable PUAs detection (a statistically significant increase from the control).	Stavova, V., Matyas, V., & Just, M. (2016). On the impact of warning interfaces for enabling the detection of Potentially Unwanted Applications. Proceedings of The 1st European Workshop on Usable Security.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A58	Shining a Light on Dark Patterns	2021	Privacidade & Segurança	https://academic.oup.com/jla/article/13/1/43/6180579	Dark patterns are user interfaces whose designers knowingly confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions. They typically exploit cognitive biases and prompt online consumers to purchase goods and services that they do not want or to reveal personal information they would prefer not to disclose. This article provides the first public evidence of the power of dark patterns. It discusses the results of the authors' two large-scale experiments in which representative samples of American consumers were exposed to dark patterns. In the first study, users exposed to mild dark patterns were more than twice as likely to sign up for a dubious service as those assigned to the control group, and users in the aggressive dark pattern condition were almost four times as likely to subscribe. Moreover, whereas aggressive dark patterns generated a powerful backlash among consumers, mild dark patterns did not. Less educated subjects were significantly more susceptible to mild dark patterns than their well-educated counterparts. The second study identified the dark patterns that seem most likely to nudge consumers into making decisions that they are likely to regret or misunderstand. Hidden information, trick question, and obstruction strategies were particularly likely to manipulate consumers successfully. Other strategies employing loaded language or generating bandwagon effects worked moderately well, while still others such as "must act now" messages did not make consumers more likely to purchase a costly service. Our second study also replicated a striking result in the first experiment, which is that where dark patterns were employed the cost of the service offered to consumers became immaterial. Decision architecture, not price, drove consumer purchasing decisions. The article concludes by examining legal frameworks for addressing dark patterns. Many dark patterns appear to violate federal and state laws restricting the use of unfair and deceptive practices in trade. Moreover, in those instances where consumers enter into contracts after being exposed to dark patterns, their consent could be deemed voidable under contract law principles. The article also proposes that dark pattern audits become part of the Federal Trade Commission (FTC)'s consent decree process. Dark patterns are presumably proliferating because firms' proprietary A-B testing has revealed them to be profit maximizing. We show how similar A-B testing can be used to identify those dark patterns that are so manipulative that they ought to be deemed unlawful.	Luguri, J., & Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. Journal of Legal Analysis, 13(1), 43-109.
A59	From Design Requirements to Effective Privacy Notifications: Empowering Users of Online Services to Make Informed Decisions	2021	Privacidade	https://www.tandfonline.com/doi/full/10.1080/10447318.2021.1913859	Privacy notifications issued by Transparency-Enhancing Tools (TETs) constitute a conceptual means of informing users of online data services about how their personal data are processed. We elicit a set of design requirements that reflect the particularities of privacy notifications received on mobile phones. Pursuing the principles of human-centered design, we evaluate the efficacy of a prototypical implementation for the context of personal health tracking in an iterative lab study. Our findings show that privacy notifications have the potential to facilitate usable transparency and informed decision-making in terms of improving privacy in the designated usage context. The feedback obtained during the evaluation of the prototype lends itself to a refined set of design requirements. We discuss these requirements as building blocks that can help designers create usable artifacts that accommodate the needs of users of mobile health services.	Murmann, P., & Karegar, F. (2021). From Design Requirements to Effective Privacy Notifications: Empowering Users of Online Services to Make Informed Decisions. International Journal of Human-Computer Interaction.
A60	Scaring People is Not Enough: An Examination of Fear Appeals within the Context of Promoting Good Password Hygiene	2021	Privacidade & Segurança	https://pure.strath.ac.uk/ws/portalfiles/portal/129840026/Dupuis_etal_SIGITE_2021_Scaring_people_is_not_enough_an_examination_of_fear_appeals.pdf	Fear appeals have been used for thousands of years to scare people into engaging in a specific behavior or omitting an existing one. From religion, public health campaigns, political ads, and most recently, cybersecurity, fear appeals are believed to be effective tools. However, this assumption is often grounded in intuition rather than evidence. We know little about the specific contexts within which fear appeals may or may not work. In this study, we begin to examine various components of a fear appeal within the context of password hygiene. A large-scale randomized controlled experiment was conducted with one control and three treatment groups: (1) fear only; (2) measures needed and the efficacy of such measures, and (3) fear combined with measures needed and the efficacy of such measures. The results suggest that the most effective way to employ a fear appeal within the cybersecurity domain is by ensuring that fear is not used on its own. Instead, it is important that information on the measures needed to address the threat and the efficacy of such measures is used in combination with information about the nature of the threat. Since many individuals that enter the information technology profession become the de facto security person, it is important for information technology education programs to distill in students the inadequacy of fear, on its own, in motivating secure actions.	Dupuis, M., Jennings, A., & Renaud, K. (2021). "Scaring People is Not Enough: An Examination of Fear Appeals within the Context of Promoting Good Password Hygiene". In Proceedings of the 22nd Annual Conference on Information Technology Education USB Stick (SIGITE '21).
A61	Audience Segregation in Social Network Sites	2010	Privacidade	https://ieeexplore.ieee.org/abstract/document/5590533	In recent years research has shown that most social network sites pose serious privacy and security risks for individual users. From the existing analyses of privacy and security risks in social network sites we deduce that one of the biggest categories of privacy risks revolves around the notion of `audience segregation', i.e. the partitioning of different audiences and the compartmentalization of social spheres. Since audience segregation is an important mechanism in everyday interactions between people in the real world, we argue that social network sites ought to include this mechanism as well. Current social network sites lack this mechanism. We present Clique, a privacy-preserving social network site that provides `audience segregation' to its users as an alternative.	van den Berg, B., & Leenes, R. E. (2010). Audience segregation in social network sites. Proceedings for SocialCom2010/PASSAT2010.

ID	Titulo	Ano	Área	Link	Resumo	Referência
A62	“It’s up to the Consumer to be Smart”: Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit	2023	Privacidade & Segurança	https://par.nsf.gov/servlets/purl/10401024	Smart home technologies offer many benefits to users. Yet, they also carry complex security and privacy implications that users often struggle to assess and account for during adoption. To better understand users’ considerations and attitudes regarding smart home security and privacy, in particular how users develop them progressively, we conducted a qualitative content analysis of 4,957 Reddit comments in 180 security- and privacy-related discussion threads from /r/homeautomation, a major Reddit smart home forum. Our analysis reveals that users’ security and privacy attitudes, manifested in the levels of concern and degree to which they incorporate protective strategies, are shaped by multidimensional considerations. Users’ attitudes evolve according to changing contextual factors, such as adoption phases, and how they become aware of these factors. Further, we describe how online discourse about security and privacy risks and protections contributes to individual and collective attitude development. Based on our findings, we provide recommendations to improve smart home designs, support users’ attitude development, facilitate information exchange, and guide future research regarding smart home security and privacy	Li, J., Sun, K., Huff, B. S., Bierley, A. M., Kim, Y., Schaub, F., & Fawaz, K. (2023). “It’s up to the Consumer to be Smart”: Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23).