Examining the Effect of Personalized PII Exposure Alerts on Individuals' Privacy Protection Motivation

Fangyu Lin*, Laura Brandimarte*, Sue Brown*, Hsinchun Chen*
*University of Arizona, Tucson, Arizona, US
fylin@arizona.edu

2024 47th MIPRO ICT and Electronics Convention (MIPRO) | 979-8-3503-8250-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/MIPRO60963.2024.10569404

***Abstract* — Personally Identifiable Information (PII) leakage can lead to identity theft, financial loss, reputation damage, and anxiety. However, individuals remain largely unaware of their PII exposure on the Internet, and whether providing individuals with information about the extent of their PII exposure can trigger privacy protection actions requires further investigation. In this pilot study, grounded by Protection Motivation Theory (PMT), we examine whether receiving privacy alerts in the form of threat and countermeasure information will trigger senior citizens to engage in protective behaviors. We also examine whether providing personalized information moderates the relationship between information and individuals' perceptions. We contribute to the literature by shedding light on the determinants and barriers to adopting privacy protection behaviors.**

Keywords – Personally Identifiable Informtion; Protection Motivation Theory; Personalization; Privacy

I. INTRODUCTION

The EU General Data Protection Regulation (GDPR) defines Personally Identifiable Information (PII) as "any information relating to an identified or identifiable natural person." As the digital transformation increases the accessibility to PII, information privacy has become a significant societal concern. Fifteen million victims were involved in data breaches reported in the third quarter of 2022, and PII, such as emails, names, and physical addresses, is the most compromised data [1]. Hacker communities frequently share or sell millions to billions of stolen credentials (e.g., social security numbers, credit/debit cards, email accounts and passwords) on Dark Net Marketplaces (DNMs), carding shops, and hacker forums [2]. Cybercriminals leverage not only the Dark Web but also the Surface web to develop comprehensive PII profiles of data breach victims [2]. The Surface Web is the part of the Internet that is accessible to the general public without requiring special software or configurations. People Search Engines (PSEs) are a major type of platform on the surface web that exposes a large amount of PII. PSEs are publicly accessible search interfaces that gather PII from proprietary databases, public records, social media platforms, etc. PII leakage (e.g., from dark web platforms, government websites, social media) can lead to identity theft, financial loss, reputation damage, and anxiety [3]. However, individuals remain largely unaware of their PII exposure on the Internet.

Innovative solutions to increase awareness of information privacy risks are essential for encouraging individuals and at-risk populations (e.g., the elderly or teenagers) to take protective actions [4]. However, whether providing individuals with information about the extent of their PII exposure can trigger them to take privacy protection actions requires further investigation. In this pilot study, grounded by Protection Motivation Theory (PMT), we examine whether receiving privacy alerts in the form of threat and countermeasure information will trigger senior citizens to engage in privacy protection behaviors. We also examine whether providing personalized threat and countermeasure information moderates the relationship between information and individuals' perception. We employ a factorial survey method for studying user behavior and perceptions. We manipulate the presence and absence of personalized threat and countermeasure information and measure their effect on senior citizens' privacy protection perceptions and behaviors. We contribute to the literature by shedding light on the determinants and barriers to the adoption of privacy protection behaviors.

The paper is organized as follows. The next section presents an overview of the theoretical foundation grounding this study, including protection motivation theory and personalization. We develop hypotheses and present our research model in the subsequent section. We then describe our methodological approach and research results of a pilot study. Finally, the article continues with a discussion of the results and their implications and finishes with an outlook for future research.

II. THEORETICAL FOUNDATION

A. Protection Motivation Theory

While PII exposure often induces fear among individuals, they do little to take protective actions [5]. To persuade individuals to embrace specific privacy-protective intentions or actions under fear or emotional tension, we adopt fear appeals. Fear Appeals are defined as "persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" [6]. Protection Motivation Theory (PMT) [7] is the leading theoretical foundation examining why individuals are successfully persuaded to follow the recommended actions of fear appeals. At the

center of PMT is the concept of protection motivation, which refers to individuals' intentions to carry out an effective recommended response to protect themselves from any threat [8].

According to PMT, a fear appeal triggers the threat appraisal and coping appraisal processes, which will further trigger protection motivation and behaviors [9]. Threat appraisal consists of three constructs: perceived threat severity, perceived threat vulnerability, and maladaptive rewards. Perceived threat severity is the belief about the significance of the threat. Perceived threat vulnerability refers to the beliefs about the probability that the threat will occur. Perceived threat severity and perceived threat vulnerability raise fear in individuals. Maladaptive Rewards are beliefs about behaviors that can decrease fear but will not mitigate the threat. When perceived threat severity, perceived threat vulnerability, and fear outweigh maladaptive rewards, individuals are more likely to have higher protection motivation, thus coping with the threat. Coping appraisal consists of three constructs: response efficacy, self-efficacy, and response costs. Response efficacy is the belief in the effectiveness of a recommended action to mitigate the threat. Self-efficacy refers to confidence in one's ability to undertake the recommended action. Response costs are perceived direct costs (e.g., effort, time, money, or trouble) incurred by the recommended action. When individuals' response efficacy and self-efficacy exceed the response costs for carrying out the protection behavior, individuals will be more likely to engage in it.

Derivations of PMT have been extensively adapted to the information security and privacy context, e.g., installing anti-virus software [9], choosing complicated passwords [10], information disclosure decision-making in social media or general online platforms [11], [12], and adoption of privacy settings [13] or biometrics authentication technologies [14]. Although these studies make significant contributions to the literature, limited studies examined the protection of exposed PII. In addition, little research investigated the antecedents of threat appraisal and coping appraisal, while the importance of the source of information that users adopt to evaluate threats and countermeasures against threats should not be underestimated [15]. A few information security and privacy studies found that one of the main reasons for low willingness to take protective actions is a lack of awareness [16], [17]. This is consistent with data breach studies which found that the majority of individuals are unaware of around 70% of data breach incidents and believe incidents would not affect them [5]. Awareness is defined as an individual's attention, perception, and cognition of physical and non-physical objects [18]. Information from the environment constitutes a stimulus, which triggers the state of being aware of something. Awareness of threats and their respective countermeasures is likely to have bearings on the cognitive processes appraising the threats and coping strategies [15], calling for better communication about exposed PII which could increase individuals' tendency to take protective actions [19]. However, the existing literature shows that even with information related to PII exposure, individuals may still be unaware and ultimately not take any privacy protection measures [20], [21]. We argue that this is due to information not being personalized, which leads to less effectiveness in eliciting behavior changes. We review personalization for further elaboration and explanation.

B. *Personalization*

Drawing from information science literature, personalization is defined as "fine-tuning and prioritizing information based on criteria that include timeliness, importance, and relevance to the audience" [22]. Previous studies found that personalized information about risks is more salient and may be more effective in facilitating behavior changes than unvarying and standardized information [23]. Personalized risk information has been extensively applied to interventions in the health context, such as clinical care and preventive medicine [24], [25]. It significantly increased patients' intentions to undertake recommended treatments or activities to reduce health risks. Similarly, personalized information regarding exposure to environmental stressors (e.g., air pollution, temperature) provided by sensors has been proven to increase participants' self-reported knowledge, awareness, and more precise subjective perceptions of the sources of environmental stressors and the level of exposure in different situations [26]. However, psychological proximity, or the realization that an event can affect you, does not always lead to more concern about or action regarding climate change [27]. In the security and privacy context, therefore, providing information that is more relevant to an individual's immediate living environment may or may not increase their awareness of the urgent need to take protective actions [28]. Since limited studies examine whether personalized information can better trigger an individual's awareness of PII exposure, we fill the gap in the literature by conducting a factorial survey with the presence and absence of personalized threat and countermeasure information and collecting individuals' perception data. We follow the three key components of Information Privacy Awareness (IPA) proposed by Correia and Compeau (2017) to design the fear appeals leveraged in this study. The first element is "literacy of the elements related to information privacy." For the threat information, we include information about the types of PII attributes that can be exposed and the sources of the exposed PII, while for the countermeasure information, we provide instructions to perform the recommended countermeasure. The second element is "the understanding that the elements exist in the current environment." To ensure individuals understand the elements related to information privacy that actually exist in their immediate living environment, we provide threat information, including PII individuals exposed, and countermeasure information, that is the actions they can take to protect the PII they exposed. The third element is the "projection of their impacts in the future." For threat information, we explain the potential privacy risks to individuals, and for countermeasure information, we describe the efficacy of the recommended countermeasure.

III. HYPOTHESES

Privacy threat information can be easily and frequently found in the news related to data breaches or data breach

search systems. However, most people rarely read data breach news, hardly use data breach search systems, and typically believe that PII exposure will not affect them [19]. This may be because the privacy threat information (e.g., data breach news) does not provide a direct signal that an individual might be or was actually involved in a data breach incident. We predict that if individuals are provided with personalized information about the types of PII attributes they disclosed in a particular data breach, they will be more likely to perceive the associated risks as relevant to them, thereby decreasing psychological distance and increasing awareness of PII disclosure.

H1. Personalized threat information will positively moderate the relationship between threat information and threat awareness.

On the other hand, information security and privacy are considered complex and abstract for the general public to understand [28]. For example, the general public often incorrectly attributes the cause of privacy attacks, does not know what countermeasures they can take to protect their exposed PII, and overestimates the costs associated with conducting protection measures. Because different types of exposed PII attributes and breaches (e.g., hacking, physically being stolen) require different countermeasures, random or general countermeasure information may not be relevant, understandable, or effective to individuals, thus not raising their awareness. We argue that personalized countermeasure information specifically designed based on individuals' circumstances can increase their understanding of the effective countermeasures and enable them to properly assess whether they can implement the recommended countermeasures. As a result, we propose:

H2. Personalized countermeasure information will positively moderate the relationship between countermeasure information and countermeasure awareness.

Previous studies reported a positive relationship between threat awareness and perceived threat severity and vulnerability and a negative relationship between threat awareness and maladaptive rewards [16], [17]. We argue that the relationships hold in the context of this study. Individuals' understanding of privacy threats is expected to result in more accurate and objective justifications about the risks associated with threats. In particular, a better understanding of the types of PII that are exposed and the sources of exposed PII inform individuals of the potential intensity of negative consequences of threats and the probability of individuals being affected by those threats. For example, one's Social Security Number (SSN) being stolen is considered more severe than other types of PII because SSN is unique and unchangeable. SSN are frequently used for identity theft because of their uniqueness. Suppose individuals' SSN are available for sale on DNMs, and individuals pursue maladaptive rewards, such as simply ignoring that their SSN have been stolen, to avoid fear and refuse to take action. In that case, they can suffer more severe negative consequences due to identity theft or other malicious activities that leverage their exposed SSN. A better understanding of such a condition will lead to higher perceived severity and vulnerability of threats and lower expectations of the benefits that can be gained from maladaptive rewards. Thus, we propose the following hypotheses:

H3a. Threat awareness will positively affect perceived threat severity.
H3b. Threat awareness will positively affect perceived threat vulnerability.
H3c. Threat awareness will negatively affect maladaptive rewards.

Previous studies have shown a positive relationship between coping awareness and response efficacy and self-efficacy, and a negative relationship between coping awareness and response cost [16], [17]. In the context of exposed PII protection, we argue that individuals' better understanding of countermeasures to privacy threats will lead to increased confidence and willingness to implement these measures. In particular, recognizing the effectiveness of suggested countermeasures will lead individuals to believe that their efforts will not be in vain. Additionally, understanding step-by-step instructions can give individuals greater confidence in actually implementing countermeasures and make individuals more precisely estimate the response costs. Thus, we hypothesize:

H4a. Countermeasure Awareness will positively affect response efficacy.
H4b. Countermeasure awareness will positively affect self-efficacy.
H4c. Countermeasure awareness will negatively affect response costs.

IV. Empirical Methods

To test the proposed hypotheses, we employed the factorial survey method [30], a hybrid of balanced multivariate experimental designs and sample survey procedures. It has been extensively adopted in sociology [31] and IS [10], [32] research. It overcomes the limitation of surveys in being unable to reduce multi-collinearity and the limitation of experiments in oversimplifying the real world with a limited number of examined conditions.

We propose a three-by-three factorial design. There are three types of threat and three types of countermeasure information. The three types of threat information are Personalized (TPe), Presence (TP), and Absence (TA). In the TPe condition, participants are asked to explore the search functions of two websites, Have I Been Pwned (HIBP) and FastPeopleSearch, and see if they can find their personal records. HIBP allows users to search whether their emails and passwords or phone numbers were breached. It was selected because of the massive coverage of recent breached accounts, approximately 12 billion. In addition, it has been extensively adopted in security and privacy research [33], [34]. FastPeopleSearch is a people search engine specifically designed to collect and publish personal information (e.g., contact information, employment status) from social media, public records, proprietary databases, etc. It was selected because it contains 800 million personal profiles of people across the U.S., has a speedy and relevant search function, and is free to use. Importantly, this treatment does not necessarily guarantee that participants experience a personalized threat, since their PII may not appear on HIBP or FastPeopleSearch. Rather, the

treatment increases the probability that participants are exposed to personalized threat as compared to the other two conditions. In cases like these, where there is imperfect compliance (Angrist 1990; Angrist, Imbens & Rubin 1996), one can use random assignment to the treatment as an instrumental variable (IV). Allowing for heterogeneous effects of the manipulation, the IV estimator represents the average causal effect of personalization on "compliers," or those who find out their PII was indeed exposed. In the TP condition, participants are presented with a list of recent data breach incidents. We developed a static web page using HTML and CSS to display the list. Four data breach incidents were pulled from the most recent incidents published by HIBP in October 2022. In the TA condition, participants receive no information about privacy threats. They are merely pointed to a cybersecurity research lab website with an introduction of the lab.

The three types of countermeasure information are Personalized (CPe), Presence (CP), and Absence (CA). In the CPe condition, participants receive detailed instructions for changing passwords on breached websites and sending a data removal request to FastPeopleSearch. In the CP condition, participants are notified that they can change their passwords or remove their profiles from FastPeopleSearch to reduce privacy risks without detailed instructions. In the CA condition, participants receive no information about countermeasures. They are merely pointed to the same website used in the TA condition.

A. Study Procedure

Participants are directed to an online survey form created with Qualtrics, where they are asked to read and complete the consent form to indicate their agreement to participate in the study. Next, participants are randomly assigned to one of the nine treatment groups. Each group is shown one type of treat information (TPe, TP, or TA) and one type of countermeasure information (CPe, CP, or CA). Participants need to carefully follow the instructions to inspect the website and answer manipulation check questions that specifically ask them to select all the informational items contained on the page. Participants subsequently answer questions about awareness, threat appraisals, and coping appraisals. We also capture demographic information such as age, gender, ethnic group, etc. Following the experiment, all participants read a debriefing form that describes the full purposes of the study. The entire process takes approximately 15 minutes. Upon completion of the study, participants receive compensation.

B. Measures and Item Development

All constructs are measured using 7-point Likert-type scales from extremely unfamiliar/strongly disagree to extremely familiar/strongly agree. Items measuring threat awareness and countermeasure awareness were adapted from [35], [36] to assess perceived understanding of the topics related to PII exposure. Items measuring perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy were adapted from Crossler (2010) and Witte et al. (1996). Items measuring response costs were adapted from [39]. All items were modified to fit the privacy context. Specifically, wording changes were made so that the items refer to data breaches and privacy-protective countermeasures. We implement IV estimation by using random assignment to the personalized threat information condition as an instrument for participants actually receiving personalized threat information and to estimate the causal effect of personalization.

C. Participants

In the pilot study, we recruited 131 participants from Cloud Research, a participant recruitment platform specifically designed for research. A previous study has shown that participants in Cloud Research responded more accurately, consistently, and reliably compared to alternatives [40]. To participate in this study, participants had to be 18 years of age or older, and able to write and read in English. By evaluating participants' responses to the manipulation check, 25 were removed from our analysis.

V. Data Analysis and Results

We analyzed the proposed research model using an R package called lavaan [41]. Reliability was supported by all composite factor reliability scores (Cronbach's alpha) exceeding 0.70. Convergent validity was supported by large and standardized loadings for all constructs ($p<.05$) and t-values that exceeded statistical significance. The moderating effect of personalized threat information on the relationship between threat information and threat awareness is significant, as well as the moderating effect of personalized countermeasure information on the relationship between countermeasure information and countermeasure awareness, supporting H1 and H2. The direct effects of threat awareness on perceived threat severity and perceived threat vulnerability are significant, supporting H3a and H3b. The direct effect of countermeasure awareness on self-efficacy is significant, supporting H4b. However, effects of threat awareness on maladaptive rewards and countermeasure awareness on response efficacy and response costs are not significant, rejecting H3c, H4a, and H4c.

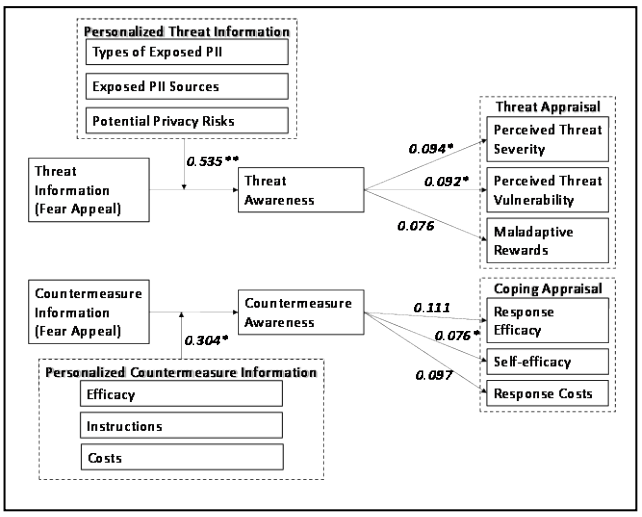

Figure 1. Proposed Research Model

VI. Discussion and Outlook

The proposed research model shows that personalization is essential in persuading individuals to take privacy protective actions. It indirectly influences whether individuals will be aware of the information they receive. The results support the idea that when individuals receive threat information, such as data breach news, they may think it is likely not to affect them. However, when evidence about individuals' specific PII being compromised is presented to individuals, they will pay more attention to absorbing the information. When individuals receive countermeasure information, if it is not directly related to their compromised PII or instructions are not available, individuals tend to ignore the information. On the other hand, when detailed instructions are provided, individuals increase their awareness of the countermeasure information. By increasing the awareness of threats, individuals tend to believe the associated risks are more severe and likely to happen to them. However, their belief in maladaptive rewards remains the same. It could be because they do not consider those items as maladaptive rewards or still believe they are rewards. On the other hand, by increasing the awareness of countermeasures, individuals are more likely to believe that they can implement the protection measures. However, response efficacy and response costs are not affected by countermeasure awareness. This could be due to a strong belief that if PII is compromised, it is impossible to protect it.

While the preliminary results of this study provide promising insights for the full-scale project, some questions remain unanswered. Whether the privacy threat appraisal and coping appraisal process triggers the intent and actual behavior for privacy protection requires further investigation. Therefore, we aim to conduct a follow-up study to examine the full nomology of protection motivation theory. The estimation of sample size is based on statistical power analysis, extensively used in behavioral research for estimating sample size for SEM (Cohen, 1988; Westland, 2010). The anticipated effect size is 0.1. The desired statistical power level is 0.8. The number of latent variables and observed variables are 17 and 42, respectively. The probability level is 0.05. The minimum sample size to detect the effect is 2,331. Considering the dropout rate and the passing rate of attention check, we expect the full study will require 2,500 participants.

This research aims to extend the current body of knowledge by examining personalized information associated with PII exposure threats and countermeasures as moderators of coping and threat appraisal processes. It offers an insight into the intricate relationship between exposed PII information and awareness and the cognitive processes involved in explaining users' privacy protection intentions. This study highlights the role of fear-appeal manipulations in Privacy studies. This suggestion is in line with the report from Boss and colleagues that fear-appeal manipulation is a core component of the underlying protective behaviors, according to PMT.

The findings of this study will have implications for practice. The findings help practitioners to identify important factors that influence users' privacy protection intention. In particular, practitioners may want to put more emphasis on providing individuals with personalized threat and countermeasure information instead of standardized and general information. Government, financial and insurance institutions, and data breach search services can use the findings of this study to design better monitoring and protection services to educate individuals to increase awareness of privacy risks and data breaches.

Acknowledgment

This material is based upon work supported by the National Science Foundation (NSF) under Secure and Trustworthy Cyberspace (grant No. 1936370), Cybersecurity Innovation for Cyber Infrastructure (grant No. 1917117), and CyberCorps Scholarship-for-Service (grant No. 1921485).

References

[1] SurfShark, "Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022," 2023. https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/.
[2] Y. Liu et al., "Identifying, Collecting, and Monitoring Personally Identifiable Information: From the Dark Web to the Surface Web," in 2020 IEEE International Conference on Intelligence and Security Informatics, ISI 2020, 2020, pp. 1–6.
[3] D. J. Solove and D. K. Citron, "Risk and anxiety: A theory of data-breach harms," Tex. Law Rev., vol. 96, no. 4, pp. 737–786, 2018, doi: 10.2139/ssrn.2885638.
[4] R. E. Crossler and F. Bélanger, "Why would I use location-protective settings on my smartphone? Motivating protective behaviors and the existence of the privacy knowledge–belief gap," Inf. Syst. Res., vol. 30, no. 3, pp. 995–1006, 2019, doi: 10.1287/isre.2019.0846.
[5] Y. Zou, A. H. Mhaidli, A. McCall, and F. Schaub, "'I've got nothing to lose': Consumers' risk perceptions and protective actions after the equifax data breach," in Proceedings of the 14th Symposium on Usable Privacy and Security, SOUPS 2018, 2018, pp. 197–216.
[6] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," Commun. Monogr., vol. 59, no. 4, pp. 329–349, 1992, doi: 10.1080/03637759209376276.
[7] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," J. Psychol., vol. 91, no. 1, pp. 93–114, 1975, doi: 10.1080/00223980.1975.9915803.
[8] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory," J. Appl. Soc. Psychol., vol. 30, no. 2, 2000, doi: 10.1111/j.1559-1816.2000.tb02323.x.
[9] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors," MIS Q., 2015, doi: 10.25300/MISQ/2015/39.4.5.
[10] A. Vance, P. B. Lowry, and D. Eggett, "Using accountability to reduce access policy violations in information systems," J. Manag. Inf. Syst., vol. 29, no. 4, pp. 263–289, 2013, doi: 10.2753/MIS0742-1222290410.
[11] N. Rodríguez-Priego, L. Porcu, and P. J. Kitchen, "Sharing but caring: Location based mobile applications (LBMA) and privacy protection motivation," J. Bus. Res., vol. 140, 2022, doi: 10.1016/j.jbusres.2021.11.022.
[12] A. Chennamaneni and B. Gupta, "The privacy protection behaviours of the mobile app users: exploring the role of neuroticism and protection motivation theory," Behav. Inf. Technol., vol. 42, no. 12, pp. 2011–2029, 2023, doi: 10.1080/0144929X.2022.2106307.
[13] R. Mousavi, R. Chen, D. J. Kim, and K. Chen, "Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory," Decis. Support Syst., 2020, doi: 10.1016/j.dss.2020.113323.
[14] A. Skalkos, I. Stylios, M. Karyda, and S. Kokolakis, "Users' Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach," J. Cybersecurity Priv., vol. 1, no. 4, pp. 743–766, 2021, doi:

10.3390/jcp1040036.
[15] S. Milne, P. Sheeran, and S. Orbell, “Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory,” J. Appl. Soc. Psychol., vol. 30, no. 1, pp. 106–143, 2000, doi: 10.1111/j.1559-1816.2000.tb02308.x.
[16] B. Hanus and Y. “Andy” Wu, “Impact of Users’ Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective,” Inf. Syst. Manag., vol. 33, no. 1, pp. 2–16, 2016, doi: 10.1080/10580530.2015.1117842.
[17] F. Hassandoust and A. A. Techatassanasoontorn, “Understanding users’ information security awareness and intentions: A full nomology of protection motivation theory,” in Cyber Influence and Cognitive Threats, 2019.
[18] P. M. Merikle, “Toward a definition of awareness,” Bull. Psychon. Soc., vol. 22, no. 5, pp. 449–450, 1984, doi: 10.3758/BF03333874.
[19] P. Mayer, Y. Zou, F. Schaub, and A. J. Aviv, “‘Now I’m a bit angry:’ Individuals’ awareness, perception, and responses to data breaches that affected them,” in Proceedings of the 30th USENIX Security Symposium, 2021, pp. 393–410.
[20] A. Frik, L. Nurgalieva, J. Bernd, J. S. Lee, F. Schaub, and S. Egelman, “Privacy and security threat models and mitigation strategies of older adults,” in Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019, 2019, pp. 21–40.
[21] A. Quan-Haase and D. Ho, “Online privacy concerns and privacy protection strategies among older adults in East York, Canada,” J. Assoc. Inf. Sci. Technol., vol. 71, no. 9, pp. 1089–1102, 2020, doi: 10.1002/asi.24364.
[22] W. Bender, “Twenty Years of Personalization: All about the ‘Daily Me,’” Educ. Rev. Mag., vol. 37, no. 5, 2002.
[23] G. J. Hollands and T. M. Marteau, “The impact of using visual images of the body within a personalized health risk assessment: An experimental study,” Br. J. Health Psychol., vol. 18, no. 2, 2013, doi: 10.1111/bjhp.12016.
[24] M. W. Athar, J. D. Record, C. Martire, D. B. Hellmann, and R. C. Ziegelstein, “The effect of a personalized approach to patient education on heart failure self-management,” J. Pers. Med., vol. 8, no. 4, 2018, doi: 10.3390/jpm8040039.
[25] A. I. Perera, M. G. Thomas, J. O. Moore, K. Faasse, and K. J. Petrie, “Effect of a Smartphone Application Incorporating Personalized Health-Related Imagery on Adherence to Antiretroviral Therapy: A Randomized Clinical Trial,” AIDS Patient Care STDS, vol. 28, no. 11, 2014, doi: 10.1089/apc.2014.0156.
[26] A. M. Becker, H. Marquart, T. Masson, C. Helbig, and U. Schlink, “Impacts of Personalized Sensor Feedback Regarding Exposure to Environmental Stressors,” Current Pollution Reports, vol. 7, no. 4. 2021, doi: 10.1007/s40726-021-00209-0.
[27] R. I. McDonald, H. Y. Chai, and B. R. Newell, “Personal experience and the ‘psychological distance’ of climate change: An integrative review,” Journal of Environmental Psychology, vol. 44. 2015, doi: 10.1016/j.jenvp.2015.10.003.
[28] H. de Bruijn and M. Janssen, “Building Cybersecurity Awareness: The need for evidence-based framing strategies,” Gov. Inf. Q., vol. 34, no. 1, 2017, doi: 10.1016/j.giq.2017.02.007.
[29] J. Correia and D. Compeau, “Information Privacy Awareness (IPA): A Review of the Use, Definition and Measurement of IPA,” in Proceedings of the 50th Hawaii International Conference on System Sciences (2017), 2017, pp. 4021–4030, doi: 10.24251/hicss.2017.486.
[30] P. H. Rossi and A. B. Anderson, “The Factorial Survey Approach. An Introduction,” in Measuring Social Judgments: The Factorial Survey Approach, 1982, pp. 15–67.
[31] L. Wallander, “25 years of factorial surveys in sociology: A review,” Soc. Sci. Res., vol. 38, no. 3, pp. 505–520, 2009, doi: 10.1016/j.ssresearch.2009.03.004.
[32] S. Al-Natour, H. Cavusoglu, I. Benbasat, and U. Aleem, “An empirical investigation of the antecedents and consequences of privacy uncertainty in the context of mobile apps,” Inf. Syst. Res., vol. 31, no. 4, pp. 1037–1063, 2020, doi: 10.1287/isre.2020.0931.
[33] G. Sood and K. Cor, “Pwned: The risk of exposure from data breaches,” in WebSci 2019 - Proceedings of the 11th ACM Conference on Web Science, 2019, doi: 10.1145/3292522.3326046.
[34] G. Biczók, M. Horváth, S. Szebeni, I. Lám, and L. Buttyán, “The Cost of Having Been Pwned: A Security Service Provider’s Perspective,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2020, vol. 12515 LNCS, doi: 10.1007/978-3-030-64455-0_10.
[35] S. Talib, N. L. Clarke, and S. M. Furnell, “An analysis of information security awareness within home and work environments,” in ARES 2010 - 5th International Conference on Availability, Reliability, and Security, 2010, pp. 196–203, doi: 10.1109/ARES.2010.27.
[36] J. L. Spears and H. Barki, “User participation in information systems security risk management,” MIS Q., vol. 34, no. 3, pp. 503–522, 2010, doi: 10.2307/25750689.
[37] R. E. Crossler, “Protection motivation theory: Understanding determinants to backing up personal data,” in Proceedings of the Annual Hawaii International Conference on System Sciences, 2010, pp. 1–10, doi: 10.1109/HICSS.2010.311.
[38] K. Witte, K. A. Cameron, J. K. McKeon, and J. M. Berkowitz, “Predicting risk behaviors: Development and validation of a diagnostic scale,” J. Health Commun., vol. 1, no. 4, pp. 317–342, 1996, doi: 10.1080/108107396127988.
[39] S. Milne, S. Orbell, and P. Sheeran, “Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions,” Br. J. Health Psychol., vol. 7, no. 2, pp. 163–184, 2002, doi: 10.1348/135910702169420.
[40] D. J. Hauser, A. J. Moss, C. Rosenzweig, S. N. Jaffe, J. Robinson, and L. Litman, “Evaluating CloudResearch’s Approved Group as a solution for problematic data quality on MTurk,” Behav. Res. Methods, pp. 1–12, 2022, doi: 10.3758/s13428-022-01999-x.
[41] Y. Rosseel, “Lavaan: An R package for structural equation modeling,” J. Stat. Softw., vol. 48, 2012, doi: 10.18637/jss.v048.i02.