

# Exploring the Impact of Previous Experience, and Threats Awareness on Influencing Regular Information Backup Among USA Population

Benard Birundu  
Computing & Software Systems  
University of Washington  
Bothell, WA, USA  
benardb@uw.edu  
0009-0003-7477-6047

Marc J. Dupuis  
Computing & Software Systems  
University of Washington  
Bothell, WA, USA  
marcjd@uw.edu  
0000-0002-5303-2511

**Abstract**—Cybersecurity threats continue to evolve in sophistication, increasingly targeting individuals as the weakest link in the security chain. While technical solutions remain essential, human-centered protective behaviors such as regular information backup are critical to mitigating risks from ransomware, device failure, and accidental deletion. This study investigates how past experiences with cyber incidents and awareness of threats influence backup practices among individuals in the United States. Drawing on Protection Motivation Theory (PMT), we conducted a mixed-methods survey ( $N=308$ ) that measured threat appraisal (perceived severity, vulnerability) and coping appraisal (self-efficacy, response efficacy, response cost), along with threat awareness and prior experience. Multiple regression explained nearly half of the variance in backup behavior ( $R^2=0.498$ ), with self-efficacy and threat awareness emerging as strong positive predictors; response cost was negative and significant. Qualitative responses illustrated experience- and awareness-driven adoption and highlighted common hybrid routines (cloud plus removable media) as well as barriers related to perceived effort or low perceived value. The findings underscore the importance of integrating human factors into cybersecurity programs and suggest concrete levers for awareness, design, and policy that reduce friction and promote routine backups.

**Keywords**—cybersecurity, protection motivation theory, threat awareness, past experiences, information backup, human factors

## 1. INTRODUCTION

The rapid expansion of digital technologies has transformed how individuals interact, work, and store information. However, this growing reliance on information and communication technologies (ICTs) has also increased exposure to cyber threats such as malware, ransomware, phishing, and social engineering [1], [2]. These attacks are not limited to organizations; individuals are often targeted as the weakest link in cybersecurity defenses [3], [4]. The consequences of data loss at the individual level include

financial harm, identity theft, psychological stress, and academic or professional disruption [5], [6]. Beyond the broad catalog of security behaviors, this paper focuses specifically on *regular information backup* as a cornerstone of personal resilience. Backup is a clear, observable action with direct consequences for recovery after ransomware, device loss, or accidental deletion, and it is widely supported by mainstream tools (e.g., automated cloud services, scheduled local images). As such, it offers a well-scoped behavior to examine how threat appraisal and coping appraisal translate into concrete protective routines at the individual level.

While technical defenses such as firewalls and encryption remain critical, research increasingly emphasizes the role of human-centered protective behaviors [7]. One such behavior—regular information backup—provides an essential safeguard against catastrophic data loss. Yet, despite the availability of affordable cloud storage and automated backup tools, many individuals neglect this practice [8]. Understanding what motivates or discourages individuals from engaging in regular backups is thus of significant importance.

This study examines how two factors—previous experiences with cyber incidents and awareness of cyber threats—affect backup behavior. Protection Motivation Theory (PMT) provides the theoretical foundation, framing backup adoption as a function of threat appraisal (perceived severity and vulnerability) and coping appraisal (self-efficacy, response efficacy, and response cost) [9], [10]. Prior research suggests that individuals with negative cyber experiences may adopt more secure habits, and that threat awareness can increase motivation for protective behavior [11], [12]. However, empirical work directly linking these constructs to backup behavior remains limited.

The contributions of this paper are threefold. First, it extends prior cybersecurity behavior research by focusing on backup practices among the general population rather than organizational contexts. Second, it empirically examines how past experiences and threat awareness interact with PMT constructs to influence security behaviors. Third, it provides

actionable insights for the design of awareness programs and public policy aimed at improving individual resilience against data loss.

The remainder of the paper is structured as follows: Section II reviews related work and theoretical foundations. Section III outlines the methodology. Section IV presents results. Section V discusses implications, and Section VI concludes with limitations and directions for future research.

## II. RELATED WORK AND BACKGROUND

### A. *Cybersecurity and Human Factors*

Cybersecurity encompasses technical, organizational, and human dimensions. While organizations have invested heavily in technical controls, individuals remain highly vulnerable due to limited awareness and lack of formal security policies [13], [14]. Studies consistently identify humans as the weakest link in the security chain [3], [15]. As individuals increasingly rely on ICTs for communication, commerce, education, and healthcare, their exposure to risks such as malware, phishing, ransomware, and social engineering grows [16], [17]. These threats can result in identity theft, financial loss, reputational harm, or complete data loss [18], [19].

Regular information backup provides a direct countermeasure to many of these risks by ensuring recovery following accidental deletion, hardware failure, or cyber-attack [5]. Yet adoption is inconsistent, and research has emphasized the need to understand behavioral drivers of this protective practice [8], [20].

### B. *Theoretical Foundations*

Several behavioral theories inform cybersecurity research, including the Theory of Reasoned Action (TRA) [21], the Theory of Planned Behavior (TPB) [22], and the Protection Motivation Theory (PMT) [9], [10]. TRA and TPB emphasize attitudes, subjective norms, and perceived control as determinants of behavioral intention. PMT, however, has gained particular traction in explaining security behaviors due to its focus on perceived threats and coping mechanisms.

### C. *Protection Motivation Theory*

PMT posits that protective behavior results from two cognitive appraisals: threat appraisal and coping appraisal [23]. Threat appraisal includes perceived severity (the seriousness of a threat) and perceived vulnerability (the likelihood of being affected). Coping appraisal incorporates self-efficacy (confidence in one's ability to act), response efficacy (belief in the effectiveness of the action), and response cost (resources required to act). Together, these factors influence whether individuals adopt preventive behaviors such as regular backups [24], [25].

Fear appeals, which highlight the potential consequences of insecure behaviors, are often studied within the PMT framework. When individuals perceive a high likelihood of severe consequences, they are more likely to adopt protective actions, provided coping mechanisms are feasible [26]. Past

studies show that users who perceive themselves as vulnerable to cyber threats are more likely to engage in protective habits such as creating strong passwords or backing up data [27], [28].

While PMT has often been applied to password hygiene, phishing avoidance, and patching, its constructs map naturally to backup: severity and vulnerability capture perceived data loss risk, whereas response efficacy, self-efficacy, and response cost jointly determine whether users configure and sustain routine backups.

### D. *Threat Awareness and Past Experience*

Threat awareness refers to an individual's understanding of cyber risks and ways to mitigate them. Prior work finds that awareness programs and training can improve security compliance and reduce human error [29], [30]. However, awareness alone may not guarantee protective behaviors unless combined with motivation and ease of action [31].

Past experience with cyber incidents also influences future behavior. Individuals who have previously suffered data loss, identity theft, or malware infections are more likely to adopt preventive strategies such as backups [12], [32]. Negative experiences often serve as powerful motivators, reinforcing the adoption of secure habits [33]. However, empirical research directly linking past experience to backup frequency remains scarce.

### E. *Research Gap*

Although backup behavior is a critical protective strategy, existing research has primarily examined organizational settings or general security practices. Few studies have directly assessed how threat awareness and past experiences shape individuals' backup behavior. This study addresses this gap by integrating PMT with these factors to investigate determinants of backup practices among a general U.S. population sample.

## III. METHODOLOGY

### A. *Research Design*

This study employed a quantitative survey with complementary qualitative questions to examine how past experiences and threat awareness influence regular information backup behavior. The research model was grounded in Protection Motivation Theory (PMT), incorporating threat appraisal (severity, vulnerability) and coping appraisal (self-efficacy, response efficacy, response cost).

### B. *Population and Sample*

Institutional Review Board (IRB) approval was sought and obtained prior to participant recruitment. The study qualified for exempt status. Participants were recruited using the crowdsourcing platform Amazon's Mechanical Turk (MTurk), which has shown to be a relatively reliable form of participant recruitment so long as quality control measures are implemented [34], [35]. In the current study, multiple quality

control measures were implemented. This included several attention check questions with obvious answers (e.g., 'select agree for this question in order to get paid'), as well as repeated demographic questions at the beginning and the end of the survey that must match. Those that passed the multiple quality control measures, were 18 years of age or older, and lived in the United States, were included in the study; all others were excluded.

The survey itself was completed on the Qualtrics survey platform. The final dataset included responses from 308 individuals, representing varied gender, age, and ethnic backgrounds (see Table I). The sample size exceeded the minimum requirements for correlation and regression analyses, ensuring statistical validity.

TABLE I. Participant Demographics

Demographic	Category	Percentage
Gender Identification	Male	47%
	Female	51%
	Prefer not to say / Other	2%
Age	18-29	34%
	30-39	28%
	40+	38%
Ethnic Identification	White	55%
	Black/African American	15%
	Asian	14%
	Hispanic / Latino	12%
	Other	4%

### C. Survey Instrument

The survey contained both closed- and open-ended items. Quantitative measures assessed constructs such as perceived threat severity, vulnerability, self-efficacy, response efficacy, past experience, and threat awareness. Responses were measured using 5-point Likert scales. Qualitative questions provided participants an opportunity to describe experiences with data loss and backup practices.

### D. Measures

All multi-item constructs were assessed on 5-point Likert scales (1 = strongly disagree, 5 = strongly agree) adapted to the backup context. *Perceived severity* and *perceived vulnerability* captured threat appraisal (e.g., "Losing my files would have serious consequences"; "I am likely to be affected by a cyber incident"). *Self-efficacy* assessed confidence in configuring and maintaining backups (e.g., "I can set up automated backups across my devices"). *Response efficacy* captured beliefs that backups meaningfully limit harm (e.g., "Backups would allow me to recover quickly after an incident"), while *response cost* reflected time/effort or

resource burden. *Threat awareness* assessed recognition of prevalent threats (e.g., phishing, ransomware) and associated consequences. *Past experience* indexed prior incidents (e.g., data loss, compromise) and their perceived impact. Internal consistency was acceptable at the scale level (overall  $\alpha = 0.700$ ); descriptive statistics for individual items are available upon request. Backup behavior was measured as a frequency composite spanning both automated and manual routines across local and cloud media.

### E. Ethical Considerations

Participation was voluntary and anonymous. Informed consent was obtained electronically, and respondents could withdraw at any time. No personally identifiable information was collected.

### F. Data Analysis

Quantitative data were analyzed using descriptive statistics, Pearson correlation, and multiple regression models. Qualitative responses were thematically coded to identify recurring patterns and insights. Both analyses were used to triangulate findings.

## IV. RESULTS

### A. Descriptive Statistics

A total of 308 usable responses remained after data-quality screening (out of 640 submissions). Reliability analysis indicated acceptable internal consistency (Cronbach's  $\alpha = 0.700$ ).

### B. Zero-Order Correlations

Pearson correlations showed that all PMT-related predictors were significantly associated with backup behavior in the expected directions (see Table II). Self-efficacy had the strongest positive association ( $r = 0.473, p < .001$ ), followed by threat awareness ( $r = 0.439, p < .001$ ), perceived severity ( $r = 0.421, p < .001$ ), response efficacy ( $r = 0.401, p < .001$ ), and perceived vulnerability ( $r = 0.385, p < .001$ ). Response cost was negatively related ( $r = -0.243, p = 0.003$ ).

TABLE II. Zero-Order Correlations with Backup Behavior

Predictor	<i>r</i>	<i>p</i>
Self-Efficacy	0.473	< .001
Threat Awareness	0.439	< .001
Perceived Severity	0.421	< .001
Response Efficacy	0.401	< .001
Perceived Vulnerability	0.385	< .001
Past Experience	0.370	< .001
Response Cost (inverse)	-0.243	.003

C. Multiple Regression

A multiple linear regression predicted backup behavior from the PMT variables plus threat awareness and past experience (see Table III). The model fit was strong ( $R^2=0.498$ , Adjusted  $R^2=0.478$ ,  $F(7,300)=27.68$ ,  $p<.001$ ). Standardized coefficients indicated significant positive effects for self-efficacy ( $\beta=0.253$ ,  $t=5.47$ ), threat awareness ( $\beta=0.218$ ,  $t=4.82$ ), perceived severity ( $\beta=0.201$ ,  $t=3.99$ ), response efficacy ( $\beta=0.177$ ,  $t=3.38$ ), and perceived vulnerability ( $\beta=0.186$ ,  $t=3.75$ ); past experience was positive and smaller ( $\beta=0.143$ ,  $t=2.89$ ). Response cost was negative and significant ( $\beta=-0.127$ ,  $t=-2.56$ ).

TABLE III. Regression Predicting Backup Behavior

Predictor	$\beta$	$t$	$p$
Self-Efficacy	0.253	5.47	< .001
Threat Awareness	0.218	4.82	< .001
Perceived Severity	0.201	3.99	< .001
Response Efficacy	0.177	3.38	< .001
Perceived Vulnerability	0.186	3.75	< .001
Past Experience	0.143	2.89	.004
Response Cost (inverse)	-0.127	-2.56	.011

D. Effect Sizes and 95% Confidence Intervals

For correlations, 95% CIs use Fisher’s  $z$  with  $N=308$  (see Table IV). For regression, 95% CIs use  $SE=\beta/t$  and  $t_{.975,300} \approx 1.97$  (two-sided) (see Table V).

TABLE IV. Correlations with Backup Behavior: 95% CIs ( $N=308$ )

Predictor	$r$	95% CI
Self-Efficacy	0.473	[0.381, 0.555]
Threat Awareness	0.439	[0.344, 0.525]
Perceived Severity	0.421	[0.325, 0.509]
Response Efficacy	0.401	[0.303, 0.491]
Perceived Vulnerability	0.385	[0.286, 0.476]
Past Experience	0.370	[0.269, 0.463]
Response Cost (inverse)	-0.243	[-0.345, -0.135]

TABLE V. Standardized Betas: SE and 95% CIs

Predictor	$\beta$	SE	95% CI
Self-Efficacy	0.253	0.046	[0.162, 0.344]
Threat Awareness	0.218	0.045	[0.129, 0.307]
Perceived Severity	0.201	0.050	[0.102, 0.300]
Response Efficacy	0.177	0.052	[0.074, 0.280]
Perceived Vulnerability	0.186	0.050	[0.088, 0.284]
Past Experience	0.143	0.049	[0.046, 0.240]
Response Cost (inverse)	-0.127	0.050	[-0.225, -0.029]

E. Qualitative Findings

The open-ended responses complement the models by showing how experience and awareness are translated into concrete practices and, for some, into sustained habits. Many participants described prior incidents or close calls as the moment that shifted intentions into sustained habits. One participant reflected, “My previous experiences, including hands-on incidents, showed me how critical strong authentication is.” (P8) Another emphasized the role of accumulated familiarity with technology: “My experience with technology taught me how important it is to keep up with new threats.” (P9) For some, the impact was more about vigilance than skills: “I wouldn’t say they developed my skills, but my awareness definitely improved.” (P10) Indirect exposure also mattered; as one respondent noted, “My husband’s employer was a victim of ransomware and their operations were down for a week.” (P2) Such vicarious experiences reinforced the perceived severity and likelihood of harm, aligning with the study’s PMT-based interpretation.

Threat salience in everyday life further heightened motivation. Several respondents pointed to the realism of phishing attempts as a persistent concern: “I think the worst thing I experience are phishing emails that look very realistic.” (P1) This kind of ambient risk perception dovetailed with the positive associations observed between threat awareness and backup behavior.

Backup routines themselves clustered around a hybrid strategy that balanced convenience and redundancy. Participants frequently paired cloud services with removable media to cover different failure modes. For example: “I use a combination of Google Drive and OneDrive along with a portable hard drive.” (P11) Another described an “all of the above” approach—“OneDrive and Google Drive, flash drives, external hard drives—all of the above.” (P12)—which mirrors best-practice guidance on layered safeguards.

Barriers among non-adopters centered on low perceived value and small but salient response costs, even when awareness was present. A common refrain was the belief that nothing worth protecting was at stake: “I don’t back up info now because I don’t really have anything critical.” (P13) This perception maps onto the response-cost pathway in the quantitative model—if people see little value, even small setup and maintenance costs feel prohibitive. A subset also highlighted technical self-efficacy as enabling proactive action beyond backup; as one participant put it, “My background in log analysis helped detect a suspicious login attempt on our FTP server.” (P5) Together, these accounts illustrate the pathway from perceived threat and experience to practical, repeatable routines, while clarifying why some individuals still delay adoption.

## V. DISCUSSION AND IMPLICATIONS

### A. Theoretical Contributions

This study extends the application of Protection Motivation Theory (PMT) in the cybersecurity domain by demonstrating that threat awareness and past experience significantly shape protective behaviors such as information backup. Consistent with PMT, perceived vulnerability and severity were associated with stronger intentions to protect against data loss. Importantly, the inclusion of past experience as an independent predictor expands PMT’s explanatory power, suggesting that lived incidents of data loss function as strong motivators for behavioral change. These findings support prior work indicating that previous negative experiences can reinforce secure habits [12], [32], while also highlighting the interaction of coping and threat appraisals in a practical context.

### B. Practical Implications

The results also provide clear insights for practitioners, educators, and policymakers. First, awareness campaigns should emphasize not only the prevalence of cyber threats but also the severity of potential consequences. Communicating real-world examples of data loss may strengthen users’ perceptions of vulnerability, thereby motivating protective behavior. Second, training programs should focus on practical skills such as configuring automated backups and managing cloud storage solutions. Third, policy efforts may benefit from integrating backup education into broader digital literacy initiatives, recognizing that individuals often lack organizational structures to guide their behavior.

A practical synthesis is to combine threat salience with low-friction defaults. For instance, awareness messaging can reference realistic incident scenarios (e.g., device loss or a locked cloud account) *alongside* a one-click setup for automated, redundant backups (cloud + periodic local image). First-run wizards can (i) detect unprotected folders, (ii) propose a minimal recurring schedule, (iii) confirm a restore point, and (iv) set a quarterly “restore test” reminder to validate that backups are usable. Because response cost emerged as a significant negative predictor, reducing small setup burdens

(credentials, device selection, storage quotas) is likely to have outsized impact. Clear mental models also matter: interfaces should distinguish antivirus from backup, and show how redundancy addresses distinct failure modes (malware vs. hardware vs. account lockout).

### C. Human-Centered Design

Findings underscore the importance of designing interventions that reduce response cost. Although threat awareness was the strongest predictor, individuals also weighed the time, effort, and resources involved in maintaining regular backups. Simplified tools, user-friendly interfaces, and seamless integration of cloud and local storage can improve adoption. By lowering barriers to action, designers and developers can enhance the likelihood that protective behaviors become routine.

### D. Broader Impact

Finally, this research highlights the need for a holistic approach to cybersecurity that incorporates human factors alongside technical solutions. While firewalls, encryption, and intrusion detection remain vital, they cannot fully mitigate risks if individuals neglect fundamental practices such as data backup. A balanced strategy—combining awareness, training, supportive technologies, and policy reinforcement—offers the greatest potential for improving resilience at the individual and societal levels.

## VI. CONCLUSION AND FUTURE WORK

This study investigated how past experiences with cyber incidents and threat awareness influence individuals’ adoption of regular information backup practices. Drawing on Protection Motivation Theory (PMT), the findings reveal that both past experiences and threat awareness are strong predictors of backup behavior, with self-efficacy also contributing modestly. The results underscore the critical role of human factors in cybersecurity, complementing technical defenses with user-driven protective actions.

The study provides both theoretical and practical contributions. Theoretically, it extends PMT by highlighting the role of past experience as a powerful motivator for secure behavior, reinforcing the idea that lived encounters with data loss significantly shape protective intentions. Practically, the findings suggest that awareness programs and training initiatives should emphasize real-world consequences of data loss and provide hands-on guidance for backup practices. Policy and design interventions that reduce response costs and simplify backup technologies can further encourage adoption.

Several limitations should be acknowledged. The study relied on self-reported survey data, which may be subject to response bias, including satisficing [36]. Additionally, a single research method was employed (i.e., a survey), and thus common method bias may be an issue [37], [38]. While certain factors help mitigate this to some extent (e.g., anonymity of research participants, completing it online), it cannot be

completely ruled out. The sample, while diverse, may not fully represent all demographic groups or professional contexts.

Future studies could employ experimental or longitudinal designs to assess causal relationships and track behavioral change over time. Further research should also examine the role of social influence, cultural factors, and technology usability in shaping backup practices. More broadly, backup is a cornerstone resilience behavior: the same factors that motivate it—clear threat appraisal, high response efficacy, and low response cost—likely generalize to adjacent practices (e.g., updates, recovery planning), offering a path toward human-centered cybersecurity that scales beyond any single tool.

## REFERENCES

- [1] A. Farooq, J. R. A. Ndiege, and J. Isoaho, "Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior," in *2019 IEEE AFRICON*, Accra, Ghana: IEEE, Sep. 2019, pp. 1–8. doi: 10.1109/AFRICON46755.2019.9133764.
- [2] S. E. Smith and M. J. Dupuis, "Phishing Experiments in the Wild: Lessons for Ubiquitous and Context-Aware Security," in *2025 IEEE 16th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, Yorktown Heights, NY, USA: IEEE, Oct. 2025, pp. 0647–0654. doi: 10.1109/UEMCON67449.2025.11267764.
- [3] M. Alshaiikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. Secur.*, vol. 98, p. 102003, Nov. 2020, doi: 10.1016/j.cose.2020.102003.
- [4] J. Tsai and M. Dupuis, "Identification and Operationalization of Key Risks and Mitigations for the Cybersecurity Risk Management of Home Users," in *2024 Cyber Awareness and Research Symposium (CARS)*, Grand Forks, ND, USA: IEEE, Oct. 2024, pp. 1–9. doi: 10.1109/CARS61786.2024.10778868.
- [5] R. Crossler, "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data," in *The 43rd Hawaii International Conference on System Sciences (HICSS)*, Koloa, Kauai, Hawaii, 2010, p. 10.
- [6] M. M. Mariani, M. Ek Styven, and F. Teulon, "Explaining the intention to use digital personal data stores: An empirical study," *Technol. Forecast. Soc. Change*, vol. 166, p. 120657, May 2021, doi: 10.1016/j.techfore.2021.120657.
- [7] J. Twomey, D. Ching, M. P. Aylett, M. Quayle, C. Linehan, and G. Murphy, "Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine," *PLOS ONE*, vol. 18, no. 10, p. e0291668, Oct. 2023, doi: 10.1371/journal.pone.0291668.
- [8] M. Dupuis, R. Crossler, and B. Endicott-Popovsky, "The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information," in *The Dewald Rood Information Security Workshop*, Provo, Utah, 2012.
- [9] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," *J. Psychol.*, vol. 91, no. 1, p. 93, 1975.
- [10] R. Rogers, J. Cacioppo, and R. Petty, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," 1983, pp. 153–177.
- [11] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Jan. 2022, doi: 10.1080/08874417.2020.1712269.
- [12] N. D. Weinstein, "Effects of personal experience on self-protective behavior," *Psychol. Bull.*, vol. 105, no. 1, p. 31, 1989.
- [13] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237–248, 2014.
- [14] B. Alkhazi, M. Alshaiikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132132–132143, 2022, doi: 10.1109/ACCESS.2022.3230286.
- [15] M. C. De Maggio, M. Mastrapasqua, M. Tesei, A. Chittaro, and R. Setola, "How to Improve the Security Awareness in Complex Organizations," *Eur. J. Secur. Res.*, vol. 4, no. 1, pp. 33–49, Apr. 2019, doi: 10.1007/s41125-017-0028-2.
- [16] B. W. Weaver, A. M. Braly, and D. M. Lane, "Training Users to Identify Phishing Emails," *J. Educ. Comput. Res.*, vol. 59, no. 6, pp. 1169–1183, Oct. 2021, doi: 10.1177/0735633121992516.
- [17] S. Alqahtani and P. Nanda, "Effects of Personal Characteristics on Phishing Awareness, Anti-Phishing Tool Usage, and Phishing Avoidance Behavior: A Structural Equation Modeling Approach," in *2024 17th International Conference on Security of Information and Networks (SIN)*, Sydney, Australia: IEEE, Dec. 2024, pp. 1–9. doi: 10.1109/SIN63213.2024.10871302.
- [18] A. Kovacevic, N. Putnik, and O. Toskovic, "Factors Related to Cyber Security Behavior," *IEEE Access*, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.
- [19] C. Cross and T. J. Holt, "Beyond fraud and identity theft: assessing the impact of data breaches on individual victims," *J. Crime Justice*, pp. 1–24, Jul. 2025, doi: 10.1080/0735648X.2025.2535007.
- [20] M. Dupuis and E. Jones, "Cyber Victimization: Tools Used to Combat Cybercrime and Victim Characteristics," in *International Congress on Information and Communication Technology*, Springer Nature Singapore Singapore, 2024, pp. 141–162.
- [21] Martin. Fishbein and I. Ajzen, *Belief, attitude, intention, and behavior : an introduction to theory and research*. Reading, Mass.: Addison-Wesley Pub. Co., 1975.
- [22] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, Dec. 1991, doi: 10.1016/0749-5978(91)90020-T.
- [23] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983, doi: 10.1016/0022-1031(83)90023-9.
- [24] M. Dupuis and R. Crossler, "The Compromise of One's Personal Information: Trait Affect as an Antecedent in Explaining the Behavior of Individuals," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Maui, Hawaii: IEEE, 2019, pp. 4841–4850. doi: 10.24251/HICSS.2019.584.
- [25] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. Inf. Manag.*, vol. 45, pp. 13–24, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.
- [26] 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, 2000, doi: 10.1111/j.1559-1816.2000.tb02308.x.
- [27] A. Vance, M. Siponen, and S. Pahnla, "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manage.*, vol. 49, no. 3–4, pp. 190–198, May 2012, doi: 10.1016/j.im.2012.04.002.
- [28] M. Dupuis, K. Renaud, and A. Jennings, "Fear might motivate secure password choices in the short term, but at what cost?," presented at the Hawaii International Conference on System Sciences, 2022. doi: 10.24251/HICSS.2022.585.
- [29] F. Ugbebor, O. Aina, M. Abass, and D. Kushanu, "Employee cybersecurity awareness training programs customized for SME contexts to reduce human-error related security incidents," *J. Knowl. Learn. Sci. Technol.* ISSN 2959-6386 Online, vol. 3, no. 3, pp. 382–409, Sep. 2024, doi: 10.60087/jklst.vol3.n3.p382-409.
- [30] J. Prümmer, T. Van Steen, and B. Van Den Berg, "A systematic review of current cybersecurity training methods," *Comput. Secur.*, vol. 136, p. 103585, Jan. 2024, doi: 10.1016/j.cose.2023.103585.

- [31] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," presented at the International Conference on Cyber Security for Sustainable Society, Sustainable Society Network, 2015, pp. 118–131. doi: 10.48550/ARXIV.1901.02672.
- [32] E. I. M. Collins and J. Hinds, "Exploring Workers' Subjective Experiences of Habit Formation in Cybersecurity: A Qualitative Survey," *Cyberpsychology Behav. Soc. Netw.*, vol. 24, no. 9, pp. 599–604, Sep. 2021, doi: 10.1089/cyber.2020.0631.
- [33] F. Del Popolo Cristaldi, G. Buodo, F. Gambarota, S. Oosterwijk, and G. Mento, "How previous experience shapes future affective subjective ratings: A follow-up study investigating implicit learning and cue ambiguity," *PLOS ONE*, vol. 19, no. 2, p. e0297954, Feb. 2024, doi: 10.1371/journal.pone.0297954.
- [34] M. Dupuis, K. Renaud, and R. Searle, "Crowdsourcing Quality Concerns: An Examination of Amazon's Mechanical Turk," in *The 23rd Annual Conference on Information Technology Education*, Chicago IL USA: ACM, Sep. 2022, pp. 127–129. doi: 10.1145/3537674.3555783.
- [35] P. G. Ipeirotis, F. Provost, and J. Wang, "Quality management on Amazon Mechanical Turk," in *Proceedings of the ACM SIGKDD Workshop on Human Computation*, Washington DC: ACM, 2010, pp. 64–67.
- [36] A. J. Nederhof, "Methods of coping with social desirability bias: A review," *Eur. J. Soc. Psychol.*, vol. 15, no. 3, pp. 263–280, 1985, doi: 10.1002/ejsp.2420150303.
- [37] S. B. MacKenzie and P. M. Podsakoff, "Common method bias in marketing: Causes, mechanisms, and procedural remedies," *J. Retail.*, vol. 88, no. 4, pp. 542–555, 2012, doi: 10.1016/j.jretai.2012.08.001.
- [38] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *J. Appl. Psychol.*, vol. 88, no. 5, pp. 879–903, 2003, doi: 10.1037/0021-9010.88.5.879.