

BEST PAPER AWARD

From Social Sharing to Security Lessons: Behaviors, Disclosure, and Cyber Threats

Sav Wheeler
Computing & Software Systems
University of Washington
Bothell, WA, USA
savanwh@uw.edu
0009-0002-5282-8355

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

Abstract—As social networking sites (SNSs) have become integral to daily life, concerns about privacy and cybersecurity risks have intensified. Malicious actors exploit SNSs for phishing, malware distribution, and identity-driven attacks, often leveraging personal information voluntarily disclosed by users. This study investigates the relationships between SNS usage, personal information disclosure, cybersecurity behaviors, and experiences with cybersecurity threats. We employed a mixed-methods approach, combining survey data from 275 participants with semi-structured interviews. Correlation analyses revealed that frequency of SNS use and usage motivations—particularly for meeting new people and for self-presentation—were positively associated with higher levels of personal information disclosure. Disclosure of personal information and frequency of SNS usage were also significantly correlated with reported experiences of cybersecurity threats, though less so with protective cybersecurity behaviors. Interview responses highlighted both direct encounters with threats and broader perceptions of privacy vulnerabilities. Together, these findings underscore the complex interplay between social behavior on SNSs and cybersecurity risks, suggesting that greater user education and platform-level safeguards are necessary to mitigate emerging threats. We conclude with implications for cybersecurity awareness efforts and recommendations for future research.

Keywords—social networking sites, cybersecurity behavior, personal information disclosure, social engineering, privacy, mixed methods

I. INTRODUCTION

In a world increasingly dependent on digital infrastructure, threats to digital security abound. The Identity Theft Resource Center reported an all-time high for data compromises in the U.S. in 2023, and the FBI's 2024 Internet Crime Report showed more than \$16 billion in losses from internet scams [1], [2]. CrowdStrike's 2024 report identified malware, denial-of-service, phishing, spoofing, and identity-based attacks as the most common forms of cyberattack [3]. Malware encompasses ransomware, spyware, adware, trojan horses, worms, and rootkits. Phishing uses social engineering over

email, SMS ("SMiShing"), or social media to trick users into sharing sensitive data or downloading malware [4]. Identity-driven attacks often involve masquerading as legitimate users to engage in phishing or distribute malware.

- RQ1: What are the connections between usage patterns of SNSs and cybersecurity behaviors?
- RQ2: Is there a relationship between personal information disclosure on SNSs and cybersecurity threats?

To answer these questions, we analyze user behaviors across three domains:

- Social Networking Site Behavior (SNSB): frequency of use, usage motivations, and personal information disclosure.
- Cybersecurity Behavior (CSB): protective digital behaviors adopted by users.
- Cybersecurity Experience (CSX): prior encounters with cybersecurity threats.

From these, six hypotheses were formulated:

1. H1: Increased SNS frequency correlates positively with good cybersecurity behavior.
2. H2: SNS use for self-presentation (MEPO) or meeting new people (MNPS) negatively relates to good cybersecurity practices.
3. H3: Increased disclosure of personal information negatively relates to good cybersecurity practices.
4. H4: Increased disclosure of personal information positively correlates with experiences of cybersecurity threats.
5. H5: Increased SNS usage frequency positively correlates with personal information disclosure.
6. H6: Good cybersecurity behavior negatively correlates with experiences of cybersecurity threats.

We test these hypotheses using quantitative survey data and qualitative interviews. Figure 1 illustrates the study's domain model.

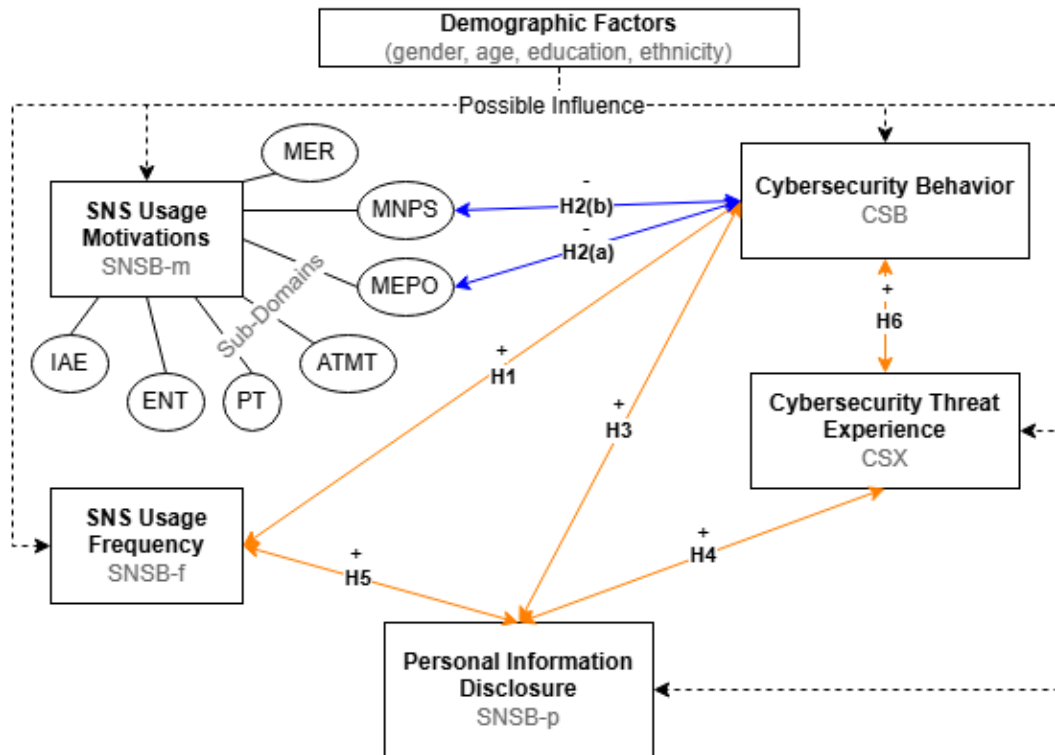


Fig. 1. Study domain model, including domains and hypotheses.

II. RELATED WORKS

A. Social Networking Sites and Social Media

A social networking site (SNS) is a virtual community where users create profiles, interact with friends, and meet others with shared interests [5]. SNSs are a subset of social media, which broadly encompasses platforms for generating and sharing content [6]. Many studies use these terms interchangeably [7], [8], [9], [10]. Platforms such as Facebook, Instagram, TikTok, and Snapchat dominate the U.S. market [11], [12]. Differences in platform choice often reflect user demographics and personality traits [13], [14].

B. SNS Usage

SNS use has grown rapidly since early platforms like SixDegrees, MySpace, and YouTube [15], [16]. Today, over 5 billion people use social media worldwide [17], with 85% of U.S. adults online daily [18]. While social media supports communication and learning [19], [20], excessive use is linked to poor sleep, academic decline, and reduced productivity [8], [10], [21]. Motivations for use include maintaining relationships, socializing, entertainment, and information-seeking, as captured in the Facebook Usage Aims (FAU) and Social Media Usage Aims Scale (SMUAS) [22], [23].

C. Personal Information Disclosure

Protecting confidentiality is central to cybersecurity [24]. Yet users often share personally identifiable information (PII) on SNSs despite concerns about privacy, a phenomenon known as the "privacy paradox" [25]. Studies show users disclose birthdays, relationships, and political views on platforms like Facebook [26], [27]. They may also seek support or encouragement from these platforms—disclosing very sensitive information at times in the process [28]. Such disclosures enhance phishing effectiveness [29]. Personality traits, such as neuroticism, also influence disclosure [30].

D. Cybersecurity Threats on SNSs

SNSs expose users to privacy breaches, viral marketing, structural attacks, and malware [31]. Breaches have compromised millions of accounts across platforms such as Facebook, MySpace, and TikTok [32], [33], [34]. Attackers exploit trust relationships through techniques like profile cloning [35]. Malware and botnets also spread via SNSs [36], [37]. Beyond technical risks, SNSs facilitate misinformation, cyberbullying, and hate speech with real-world harms [38], [39].

E. Models of Security Behavior

Two models often guide analysis of cybersecurity behavior. The Health Belief Model (HBM) explains protective behavior through perceived risk, severity, benefits, and

barriers [40], [41]. Protection Motivation Theory (PMT) extends this by including self-efficacy and response efficacy [42]. These frameworks have been applied to cybersecurity compliance and disclosure on SNSs [43], [44], [45], [46]. Gender and cultural contexts can affect self-efficacy, though findings on actual behavior are mixed [47], [48].

F. Experience with Cybersecurity Threats

Research has documented a range of cyber incidents, including phishing, ransomware, and account hijacking [49], [50], [51]. Experiences are often categorized as “bounded” (specific events) or “fuzzy” (ongoing concerns) [52]. Such incidents can produce stress, shame, and emotional harm in addition to financial losses [53], [54].

III. METHODS

A. Overview

We employed a mixed-methods approach combining a survey and semi-structured interviews. The survey provided quantitative data on correlations between SNS usage, disclosure, cybersecurity behaviors, and threat experiences, while interviews offered qualitative depth. Our target was 300 survey responses and 30 interviews. The survey was hosted on Qualtrics, with participants recruited via Amazon’s Mechanical Turk (MTurk). MTurk can be problematic from a quality control standpoint, but if various quality control measures are implemented these issues can mostly be mitigated [55], [56], [57]. Interviews were advertised and conducted in-person with volunteers from a university campus. IRB approval was sought and obtained prior to data collection. This study qualified for exempt status. Informed consent was obtained from all research participants prior to their engagement in the study.

B. Participants and Compensation

Survey participants (18+) were recruited through MTurk, excluding university employees, students, or family members of employees, per institutional policy. Interview participants were recruited through campus advertising. Survey respondents were compensated \$3, while interviewees received \$20. The final dataset included 275 valid survey responses and 12 interview transcripts.

C. Data Protection

Interviewees provided contact information only for scheduling; this was deleted after data collection. Recordings were transcribed using Whisper [58], with personally identifiable information manually redacted. Survey and interview data were anonymized and stored securely. Transcripts will be destroyed following study closure.

D. Survey Development

Survey items were adapted from established sources, covering SNS usage frequency, motivations, personal information disclosure, cybersecurity behavior, and prior experiences with threats. Likert-type scales (0-4 or 0-5) were used. Four attention-check questions ensured data quality;

inconsistent or invalid responses were excluded (76 cases). Table I lists the sources of survey domains.

TABLE I. Survey Question Sources

Survey Domain	Question Sources
SNS Usage Frequency (SNSB-f)	StatCounter 2025; interview responses
SNS Usage Motivations (SNSB-m)	[22], [23]
Personal Information Disclosure (SNSB-p)	[27], [59]
Cybersecurity Threat Experience (CSX)	[49], [50], [51], [60]
Cybersecurity Behavior (CSB)	[43], [61], [62]

E. Interview Development

Interviews (20-30 minutes) followed a semi-structured script of 10-12 open-ended questions about SNS use, disclosure, and experiences with cyber threats. Clarifying follow-ups were used where appropriate. Later sessions added questions on witnessing threats that did not directly affect the participant, reducing reporting bias.

F. Sampling Considerations

MTurk provides approximately random sampling within its user base, though limited to that population [63]. Campus-based interview recruitment introduced some self-selection bias. Together, these methods produced complementary insights: broader coverage via survey data and detailed perspectives via interviews.

IV. RESULTS

A. Survey Data

A total of 352 responses were collected; after filtering invalid or inconsistent entries, 275 remained valid for analysis. Respondents were fairly balanced by gender (53% male, 47% female) and spanned a wide age range (20-79 years). The majority were White (80%), and over half held at least a bachelor’s degree.

1) Correlation Analysis

Pearson correlations were computed across the primary domains: SNS usage frequency (SNSB-f), motivations (SNSB-m), personal information disclosure (SNSB-p), cybersecurity behavior (CSB), and cybersecurity experience (CSX). Results are shown in Table II.

Key findings include:

- SNS usage frequency was strongly correlated with personal information disclosure (H5 supported).
- Disclosure was positively associated with cybersecurity threat experience (H4 supported).
- Cybersecurity behavior was negatively correlated with threat experience (H6 supported).
- No significant correlations were found between SNS usage and cybersecurity behavior (H1 not supported).
- Among usage motivations, self-presentation (MEPO) showed a weak negative correlation with cybersecurity behavior (H2a partially supported).

2) ANOVA Analysis

ANOVA tests examined demographic differences across domains (Table III). Gender and ethnicity showed no significant effects. However, both age and education influenced SNS usage frequency, disclosure, and threat experience, with younger and more educated respondents reporting higher use, disclosure, and experiences.

Figures 2-7 illustrate the scatter plots corresponding to hypotheses H1-H6, showing linear and nonlinear trends. These plots reinforce the statistical findings: strong positive associations for H4 and H5, weaker or nonsignificant results for H1-H3, and a negative association for H6.

TABLE II. Correlation Matrix for SNS Usage, Disclosure, Cybersecurity Behaviors, and Threat Experiences. Significant Values Shown with * $P < .05$, ** $P < .01$, *** $P < .001$.

Statistic Tested	SNSB-f-ALL	SNSB-f-USED	CSX	CSB	SNSB-p
SNSB-f-ALL	---	$\rho = .80^{***}$	$\rho = .48^{***}$	$\rho = -.024$ ($\rho=.70$)	$\rho = .61^{***}$
SNSB-f-USED	$\rho = .80^{***}$	---	$\rho = .35^{***}$	$\rho = .019$ ($\rho=.75$)	$\rho = .48^{***}$
CSX	$\rho = .48^{***}$	$\rho = .35^{***}$	---	$\rho = -.21^{***}$	$\rho = .47^{***}$
CSB	$\rho = -.024$ ($\rho=.70$)	$\rho = .019$ ($\rho=.75$)	$\rho = -.21^{***}$	---	$\rho = -.0036$ ($\rho=.95$)
SNSB-p	$\rho = .61^{***}$	$\rho = .48^{***}$	$\rho = .47^{***}$	$\rho = -.0036$ ($\rho=.95$)	---

TABLE III. ANOVA Results for Demographic Groups Across Survey Domains. * $P < .05$, ** $P < .01$, *** $P < .001$.

Domain	Gender	Education	Ethnicity	Age
SNSB-f-ALL	F=.71, p=.55	F=2.95, p=.0083**	F=.20, p=.94	F=7.87, p<\$.001***
SNSB-f-USED	F=.19, p=.90	F=2.15, p=.048*	F=.19, p=.94	F=5.91, p<\$.001***
SNSB-p	F=1.10, p=.35	F=5.03, p<\$.001***	F=1.29, p=.27	F=5.61, p<\$.001***
CSX	F=.34, p=.79	F=2.26, p=.038*	F=1.94, p=.10	F=7.25, p<\$.001***
CSB	F=.36, p=.78	F=1.88, p=.084	F=1.00, p=.41	F=1.11, p=.36

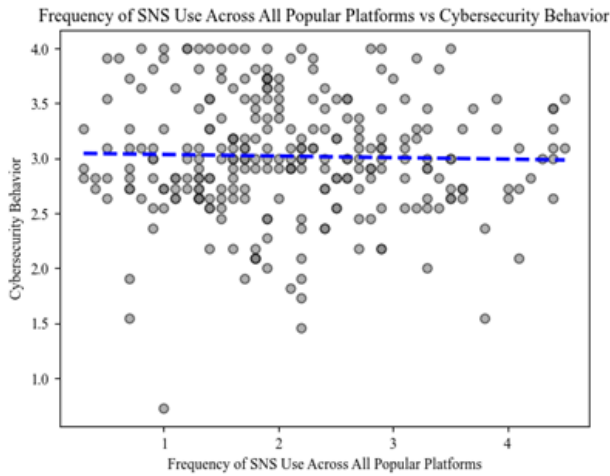


Fig. 2. Frequency of SNS use across all popular platforms (SNSB-f-ALL) vs. cybersecurity behavior (CSB); H1, $p = .70$

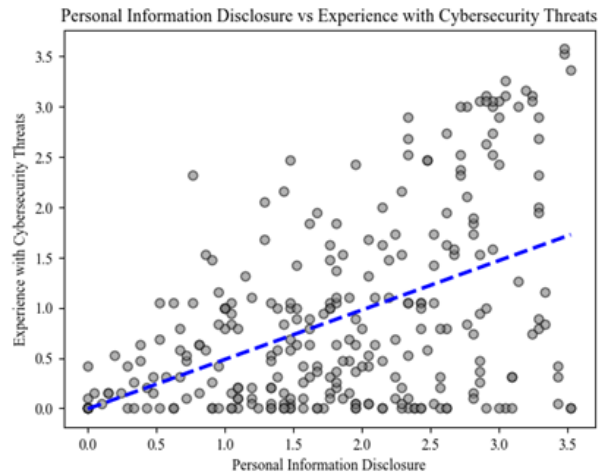


Fig. 5. Personal information disclosure (SNSB-p) vs. experience with cybersecurity threats (CSX); H4, $p < .001$

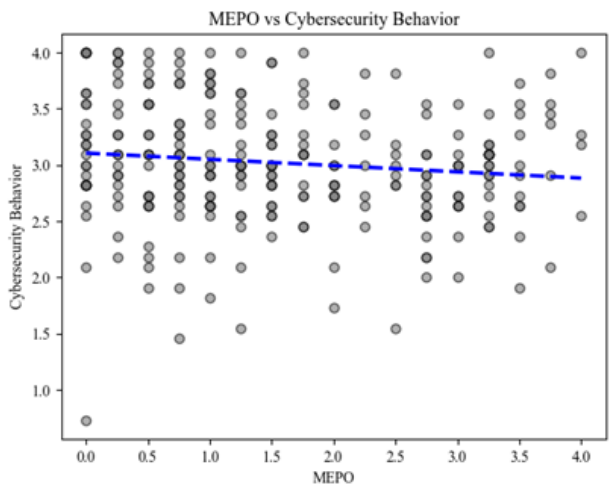


Fig. 3. SNS usage for meeting new people and socializing (MNPS) vs. cybersecurity behavior (CSB); H2, $p = .58$

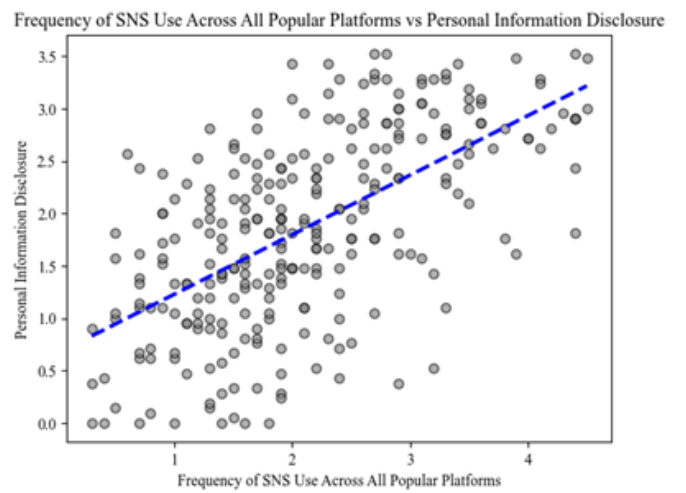


Fig. 6. Frequency of SNS use across all popular platforms (SNSB-f-ALL) vs. personal information disclosure (SNSB-p); H5, $p < .001$

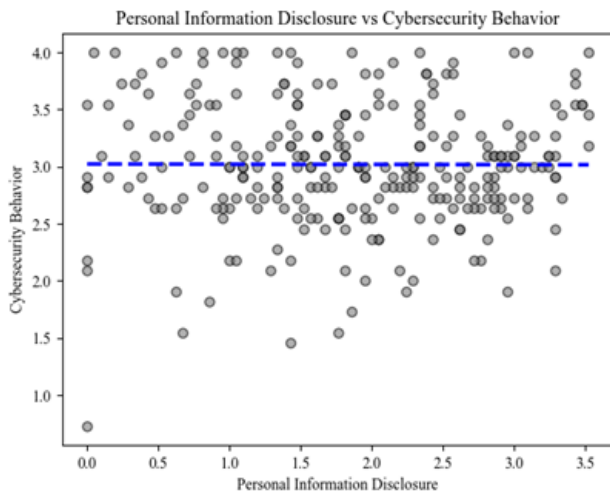


Fig. 4. Personal information disclosure (SNSB-p) vs. cybersecurity behavior (CSB); H3, $p = .95$

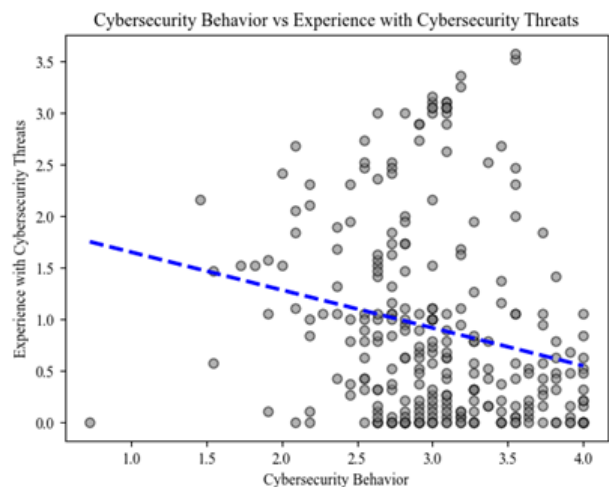


Fig. 7. Cybersecurity behavior (CSB) vs. experience with cybersecurity threats (CSX); H6, $p < .001$

B. Interview Findings

Interviewees reported varied SNS usage patterns, disclosure behaviors, and experiences with threats. Common themes included:

- Frequent encounters with phishing messages and fraudulent friend requests.
- Heightened awareness of threats after prior negative experiences.
- Perceived trade-offs between social connection and privacy.
- Reliance on personal judgment rather than formal cybersecurity strategies.

Table IV summarizes key threat types mentioned across interviews.

TABLE IV. Cybersecurity Threats Reported in Interviews

Threat Type	Platforms Reported
Phishing	Facebook, Instagram, Email links
Account Hijacking	Facebook, Twitter
Malware/Scams	WhatsApp, TikTok
Identity Theft Attempts	Instagram, Snapchat

V. DISCUSSION

This study examined the relationships among SNS usage, personal information disclosure, cybersecurity behavior, and experiences with cybersecurity threats. Several hypotheses were supported, while others revealed more complex dynamics.

First, we found that SNS usage frequency strongly correlated with personal information disclosure (H5), aligning with prior research linking extraversion and need for popularity to disclosure behaviors [64], [65], [66]. Disclosure also correlated positively with experiences of cybersecurity threats (H4), consistent with studies suggesting that oversharing increases vulnerability [27], [29]. Finally, good cybersecurity behaviors were negatively associated with threat experiences (H6), reinforcing the protective value of security practices [49], [50].

Other hypotheses were not supported. We found no significant correlation between SNS usage frequency and cybersecurity behavior (H1). This suggests that frequent SNS use does not inherently produce stronger protective behaviors, despite potential for increased exposure to cybersecurity information. Similarly, only weak evidence supported H2: self-presentation (MEPO) showed a slight negative correlation with

cybersecurity practices, while meeting new people (MNPS) was nonsignificant. H3, which predicted a negative relationship between disclosure and cybersecurity practices, was also unsupported.

Demographic analyses revealed that age and education influenced SNS use, disclosure, and threat experience, while gender and ethnicity showed little effect. Younger and more educated respondents were more frequent users, disclosed more personal information, and reported more cybersecurity incidents. Interview findings enriched these results by highlighting users' lived experiences with phishing, account hijacking, and identity theft attempts, as well as the emotional consequences of these threats.

Together, these findings emphasize the importance of addressing disclosure behaviors in cybersecurity education. Simply raising awareness may not be sufficient; targeted interventions that focus on the social motivations driving disclosure may be more effective. Platform-level safeguards, such as stronger default privacy settings and automated phishing detection, are also critical. The use of fear, while commonplace in cybersecurity and multiple other domains, is not recommended given the inconclusive nature of its efficacy in effectuating behavioral change, negative impact on other emotions, and multiple ethical concerns [67], [68], [69].

VI. CONCLUSIONS

This research contributes to understanding the complex interplay between social networking behavior, disclosure practices, and cybersecurity risk. Using a mixed-methods approach, we identified key relationships: SNS frequency and disclosure are strongly linked, disclosure predicts higher exposure to threats, and strong security behaviors reduce those risks. However, frequent SNS use does not guarantee safer behavior, highlighting a gap between awareness and practice.

These findings carry practical implications. Educators and policymakers should prioritize interventions addressing disclosure tendencies and motivations for self-presentation and socializing online. SNS platforms should implement safeguards that mitigate risks stemming from user disclosure. Future research should extend these results through experimental designs that simulate real threats, longitudinal studies tracking disclosure and threat experiences over time, and broader samples beyond MTurk and campus participants.

A. Limitations and Future Work

This study is not without limitations. MTurk sampling restricts generalizability to the broader population, while self-selection bias affects the interview data. Self-reported measures may under- or over-estimate actual behaviors, and some respondents may lack awareness of threats they have experienced. Despite these constraints, the findings provide valuable insight into behavioral patterns on SNSs and their cybersecurity implications.

Future research should refine these findings through experimental approaches that simulate phishing or malware exposure in controlled conditions. Cross-cultural investigations are also warranted, given that disclosure norms and SNS usage patterns vary globally. Incorporating behavioral tracking data could help bridge the gap between reported and actual practices. Ultimately, addressing both individual and structural dimensions of cybersecurity is essential for reducing risk in increasingly interconnected digital environments.

SNSs represent lucrative targets for attackers due to the wealth of personal information available and the potential for social engineering. Attackers frequently manipulate employees through SNSs to access organizational assets [70]. Social engineering exploits influence and manipulation to gain unauthorized access [71], employing phishing, pretexting, baiting, ransomware, fake websites, pop-ups, robocalls, or reverse social engineering [72]. While detection technologies exist [73], [74], [75], much responsibility for defense still falls on end users.

REFERENCES

- [1] F. B. of Investigation, "FBI Releases Annual Internet Crime Report," *FBI*. 2025. [Online]. Available: <https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report>
- [2] I. T. R. Center, "ITRC Annual Data Breach Report," *ITRC*. 2023. [Online]. Available: <https://www.idtheftcenter.org/publication/2023-data-breach-report/>
- [3] K. Baker, "Types of Cyberattacks," *CrowdStrike.com*. 2024. [Online]. Available: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/>
- [4] W. He, "A review of social media security risks and mitigation techniques," *J. Syst. Inf. Technol.*, vol. 14, no. 2, pp. 171–180, Jan. 2012, doi: 10.1108/13287261211232180.
- [5] D. J. Kuss and M. D. Griffiths, "Online Social Networking and Addiction—A Review of the Psychological Literature," *Int. J. Environ. Res. Public Health*, vol. 8, no. 99, pp. 3528–3552, Sep. 2011, doi: 10.3390/ijerph8093528.
- [6] D. J. Kuss and M. D. Griffiths, "Social Networking Sites and Addiction: Ten Lessons Learned," *Int. J. Environ. Res. Public Health*, vol. 14, no. 33, p. 311, Mar. 2017, doi: 10.3390/ijerph14030311.
- [7] D. R. Alqurashi, M. Alghizzawi, and A. Al-Hadrami, "The Role of Social Media in Raising Awareness of Cybersecurity Risks," in *Opportunities and Risks in AI for Business Development: Volume 1*, B. Alareeni and I. Elgedawy, Eds., Cham: Springer Nature Switzerland, 2024, pp. 365–376. doi: 10.1007/978-3-031-65203-5_33.
- [8] S. Brooks, "Does personal social media usage affect efficiency and well-being?," *Comput. Hum. Behav.*, vol. 46, pp. 26–37, May 2015, doi: 10.1016/j.chb.2014.12.053.
- [9] D. N. Greenwood, "Fame, Facebook, and Twitter: How attitudes about fame predict frequency and nature of social media use," *Psychol. Pop. Media Cult.*, vol. 2, no. 4, pp. 222–236, 2013, doi: 10.1037/ppm0000013.
- [10] W. W. F. Lau, "Effects of social media usage and social media multitasking on the academic performance of university students," *Comput. Hum. Behav.*, vol. 68, pp. 286–291, Mar. 2017, doi: 10.1016/j.chb.2016.11.043.
- [11] M. Faverio and O. Sidoti, "Teens, Social Media and Technology 2024," *Pew Research Center*. Dec. 2024. [Online]. Available: <https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/>
- [12] StatCounter, "U.S. top social media sites visit share 2025," *Statista*. Apr. 2025. [Online]. Available: <https://www.statista.com/statistics/265773/market-share-of-the-most-popular-social-media-websites-in-the-us/>
- [13] J. Hellemans, K. Willems, and M. Brengman, "Daily Active Users of Social Network Sites: Facebook, Twitter, and Instagram-Use Compared to General Social Network Site Use," in *Advances in Digital Marketing and eCommerce*, F. J. Martínez-López and S. D'Alessandro, Eds., Cham: Springer International Publishing, 2020, pp. 194–202. doi: 10.1007/978-3-030-47595-6_24.
- [14] D. J. Hughes, M. Rowe, M. Batey, and A. Lee, "A tale of two sites: Twitter vs. Facebook and the personality predictors of social media usage," *Comput. Hum. Behav.*, vol. 28, no. 2, pp. 561–569, 2012, doi: 10.1016/j.chb.2011.11.001.
- [15] M. Jones, "History of Social Media: The Invention of Online Networking," *History Cooperative*. 2025. [Online]. Available: <https://historycooperative.org/the-history-of-social-media/>
- [16] E. Ortiz-Ospina, "The rise of social media," *Our World Data*, Sep. 2019, [Online]. Available: <https://ourworldindata.org/rise-of-social-media>
- [17] Statista, "Number of global social network users 2017-2028," *Statista*. May 2024. [Online]. Available: <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>
- [18] A. Perrin and S. Atske, "About three-in-ten U.S. adults say they are 'almost constantly' online," *Pew Research Center*. Mar. 2021. [Online]. Available: <https://www.pewresearch.org/short-reads/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/>
- [19] R. Junco, "The relationship between frequency of Facebook use, participation in Facebook activities, and student engagement," *Comput. Educ.*, vol. 58, no. 1, pp. 162–171, Jan. 2012, doi: 10.1016/j.compedu.2011.08.004.
- [20] R. Junco, G. Heiberger, and E. Loken, "The effect of Twitter on college student engagement and grades," *J. Comput. Assist. Learn.*, vol. 27, no. 2, pp. 119–132, 2011, doi: 10.1111/j.1365-2729.2010.00387.x.
- [21] N. Xanidis and C. M. Brignell, "The association between the use of social network sites, sleep quality and cognitive function during the day," *Comput. Hum. Behav.*, vol. 55, pp. 121–126, Feb. 2016, doi: 10.1016/j.chb.2015.09.004.
- [22] M. B. Horzum, "Examining the relationship to gender and personality on the purpose of Facebook usage of Turkish university students," *Comput. Hum. Behav.*, vol. 64, pp. 319–328, Nov. 2016, doi: 10.1016/j.chb.2016.06.010.
- [23] K. Kircaburun, S. Alhabash, Ş. B. Tosuntaş, and M. D. Griffiths, "Uses and Gratifications of Problematic Social Media Use Among University Students: a Simultaneous Examination of the Big Five of Personality Traits, Social Media Platforms, and Social Media Use Motives," *Int. J. Ment. Health Addict.*, vol. 18, no. 3, pp. 525–547, Jun. 2020, doi: 10.1007/s11469-018-9940-6.
- [24] S. Samonas and D. Coss, "The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security," *J. Inf. Syst. Secur.*, vol. 10, no. 3, pp. 21–45, 2014.
- [25] P. A. Norberg, D. R. Horne, and D. A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *J. Consum. Aff.*, vol. 41, no. 1, pp. 100–126, 2007, doi: 10.1111/j.1745-6606.2006.00070.x.
- [26] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, in WPES '05. New York, NY, USA: Association for Computing Machinery, Nov. 2005, pp. 71–80. doi: 10.1145/1102199.1102214.
- [27] J. K. Adjei, S. Adams, I. K. Mensah, P. E. Tobbin, and S. Odei-Appiah, "Digital Identity Management on Social Media: Exploring the Factors That Influence Personal Information Disclosure on Social Media," *Sustainability*, vol. 12, no. 2323, p. 9994, Jan. 2020, doi: 10.3390/su12239994.

- [28] M. Dupuis, S. Khadeer, and J. Huang, "I Got the Job!": An exploratory study examining the psychological factors related to status updates on facebook," *Comput. Hum. Behav.*, vol. 73, pp. 132–140, 2017, doi: 10.1016/j.chb.2017.03.020.
- [29] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, 2007, doi: 10.1145/1290958.1290968.
- [30] Y. Amichai-Hamburger and G. Vinitzky, "Social network use and personality," *Comput. Hum. Behav.*, vol. 26, no. 6, pp. 1289–1295, Nov. 2010, doi: 10.1016/j.chb.2010.03.018.
- [31] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security Issues in Online Social Networks," *IEEE Internet Comput.*, vol. 15, no. 4, pp. 56–63, Jul. 2011, doi: 10.1109/MIC.2011.50.
- [32] M. Isaac and S. Frenkel, "Facebook Security Breach Exposes Accounts of 50 Million Users," *N. Y. Times*, Sep. 2018, [Online]. Available: <https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html>
- [33] D. Winder, "235 Million Instagram, TikTok And YouTube User Profiles Exposed In Massive Data Leak," *Forbes*. Aug. 2020. [Online]. Available: <https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/>
- [34] E. Weise, "360 million Myspace accounts breached," *USA TODAY*. May 2016. [Online]. Available: <https://www.usatoday.com/story/tech/2016/05/31/360-million-myspace-accounts-breached/85183200/>
- [35] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in *Proceedings of the 18th international conference on World wide web*, in WWW '09. New York, NY, USA: Association for Computing Machinery, Apr. 2009, pp. 551–560. doi: 10.1145/1526709.1526784.
- [36] W. Xu, F. Zhang, and S. Zhu, "Toward worm detection in online social networks," in *Proceedings of the 26th Annual Computer Security Applications Conference*, in ACSAC '10. New York, NY, USA: Association for Computing Machinery, Dec. 2010, pp. 11–20. doi: 10.1145/1920261.1920264.
- [37] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet," *Comput. Netw.*, vol. 57, no. 2, pp. 556–578, Feb. 2013, doi: 10.1016/j.comnet.2012.06.006.
- [38] A. Cao, J. M. Lindo, and J. Zhong, "Can social media rhetoric incite hate incidents? Evidence from Trump's 'Chinese Virus' tweets," *J. Urban Econ.*, vol. 137, p. 103590, Sep. 2023, doi: 10.1016/j.jue.2023.103590.
- [39] R. Cohen-Almagor, "Bullying, Cyberbullying, and Hate Speech," *Int J Technoethics*, vol. 13, no. 1, pp. 1–17, Feb. 2022, doi: 10.4018/IJT.291552.
- [40] N. K. Janz and M. H. Becker, "The Health Belief Model: A Decade Later," *Health Educ. Q.*, vol. 11, no. 1, pp. 1–47, Mar. 1984, doi: 10.1177/109019818401100101.
- [41] I. M. Rosenstock, "The Health Belief Model and Preventive Health Behavior," *Health Educ. Monogr.*, vol. 2, no. 4, pp. 354–386, Dec. 1974, doi: 10.1177/109019817400200405.
- [42] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983.
- [43] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Hum. Behav.*, vol. 69, pp. 437–443, Apr. 2017, doi: 10.1016/j.chb.2016.12.040.
- [44] 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.
- [45] D. V. Tran, P. V. Nguyen, D. Vrontis, S. T. N. Nguyen, and P. U. Dinh, "Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam," *J. Asia Bus. Stud.*, vol. 18, no. 6, pp. 1445–1464, Jan. 2024, doi: 10.1108/JABS-01-2024-0058.
- [46] K. Aboulnasr, G. A. Tran, and T. Park, "Personal information disclosure on social networking sites," *Psychol. Mark.*, vol. 39, no. 2, pp. 294–308, 2022, doi: 10.1002/mar.21595.
- [47] D. Branley-Bell, L. Coventry, M. Dixon, A. Joinson, and P. Briggs, "Exploring Age and Gender Differences in ICT Cybersecurity Behaviour," *Hum. Behav. Emerg. Technol.*, vol. 2022, no. 1, p. 2693080, 2022, doi: 10.1155/2022/2693080.
- [48] A. Vance, M. Siponen, and S. Pahlila, "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.
- [49] 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 Roode Information Security Workshop*, Provo, Utah, 2012.
- [50] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo, "'My religious aunt asked why i was trying to sell her viagra': experiences with account hijacking," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Toronto Ontario Canada: ACM, Apr. 2014, pp. 2657–2666. doi: 10.1145/2556288.2557330.
- [51] Y. Yilmaz, O. Cetin, C. Grigore, B. Arief, and J. Hernandez-Castro, "Personality types and ransomware victimisation," *Digit. Threats Res. Pract.*, vol. 4, no. 4, pp. 1–25, 2023, doi: 10.1145/3568994.
- [52] H. Tian, C. Kanich, J. Polakis, and S. Patil, "Tech Pains: Characterizations of Lived Cybersecurity Experiences," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 250–259. doi: 10.1109/EuroSPW51379.2020.00040.
- [53] K. Renaud, R. Searle, and M. Dupuis, "Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?," in *New Security Paradigms Workshop*, Virtual Event USA: ACM, Oct. 2021, pp. 70–87. doi: 10.1145/3498891.3498896.
- [54] S. Budimir, J. R. J. Fontaine, and E. B. Roesch, "Emotional Experiences of Cybersecurity Breach Victims," *Cyberpsychology Behav. Soc. Netw.*, vol. 24, no. 9, pp. 612–616, Sep. 2021, doi: 10.1089/cyber.2020.0525.
- [55] M. Dupuis, B. Endicott-Popovsky, and R. Crossler, "An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud," in *International Conference on Cloud Security Management*, Seattle, Washington, Oct. 2013.
- [56] 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.
- [57] G. Paolacci, J. Chandler, and P. Ipeirotis, "Running Experiments on Amazon Mechanical Turk," *Judgm. Decis. Mak.*, vol. 5, no. 5, pp. 411–419, 2010, doi: 10.1017/S193029750002205.
- [58] OpenAI, "Introducing Whisper." Apr. 2022. [Online]. Available: <https://openai.com/index/whisper/>
- [59] R. H. G. Koehorst, "Personal information disclosure on online social networks: an empirical study on the predictors of adolescences' disclosure of personal information on Facebook." University of Twente, Aug. 2013. [Online]. Available: <https://essay.utwente.nl/63797/>
- [60] J. Angulo and M. Ortlieb, "'(WTH..!?!)' Experiences, Reactions, and Expectations Related to Online Privacy Panic Situations," in *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 19–38.
- [61] M. Alanazi, M. Freeman, and H. Tootell, "Exploring the factors that influence the cybersecurity behaviors of young adults," *Comput. Hum. Behav.*, vol. 136, p. 107376, Nov. 2022, doi: 10.1016/j.chb.2022.107376.
- [62] I. Ion, R. Reeder, and S. Consolvo, "...No one Can Hack My Mind': Comparing Expert and Non-Expert Security Practices," 2015, pp. 327–346. [Online]. Available: <https://www.usenix.org/conference/soups2015/proceedings/presentation/ion>
- [63] Z. R. Steelman, B. I. Hammer, and M. Limayem, "Data Collection in the Digital Age: Innovative Alternatives to Student Samples," *MIS Q.*, vol. 38, no. 2, pp. 355–378, 2014, doi: 10.25300/MISQ/2014/38.2.02.

- [64] E. Christofides, A. Muise, and S. Desmarais, "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?," *Cyberpsychol. Behav.*, vol. 12, no. 3, pp. 341–345, Jun. 2009, doi: 10.1089/cpb.2008.0226.
- [65] S. D. Gosling, A. A. Augustine, S. Vazire, N. Holtzman, and S. Gaddis, "Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information," *Cyberpsychology Behav. Soc. Netw.*, vol. 14, no. 9, pp. 483–488, Sep. 2011, doi: 10.1089/cyber.2010.0087.
- [66] S. Deng, Y. Liu, H. Li, and F. Hu, "How Does Personality Matter? An Investigation of the Impact of Extraversion on Individuals' SNS Use," *Cyberpsychology Behav. Soc. Netw.*, vol. 16, no. 8, pp. 575–581, Aug. 2013, doi: 10.1089/cyber.2012.0383.
- [67] M. Dupuis, K. Renaud, and A. Jennings, "Fear might motivate secure password choices in the short term, but at what cost?," in *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS) 2022*, Maui, Hawaii, Jan. 2022, pp. 4796–4805. doi: 10.24251/HICSS.2022.585.
- [68] K. Renaud and M. Dupuis, "Cyber Security Fear Appeals: Unexpectedly Complicated," in *New Security Paradigms Workshop (NSPW '19)*, San Carlos, Costa Rica: ACM, Sep. 2019, p. 15. doi: 10.1145/3368860.3368864.
- [69] M. Dupuis and K. Renaud, "Scoping the ethical principles of cybersecurity fear appeals," *Ethics Inf. Technol.*, vol. 23, no. 3, pp. 265–284, Sep. 2021, doi: 10.1007/s10676-020-09560-0.
- [70] H. Wilcox and M. Bhattacharya, "A framework to mitigate social engineering through social media within the enterprise," in *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, Jun. 2016, pp. 1039–1044. doi: 10.1109/ICIEA.2016.7603735.
- [71] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, 2003.
- [72] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet*, vol. 11, no. 44, p. 89, Apr. 2019, doi: 10.3390/fi11040089.
- [73] M. Hoeschele and M. Rogers, "Detecting Social Engineering," in *Advances in Digital Forensics*, M. Pollitt and S. Sheno, Eds., Boston, MA: Springer US, 2005, pp. 67–77. doi: 10.1007/0-387-31163-7_6.
- [74] M. Lansley, S. Kapetanakis, and N. Polatidis, "SEADer++ v2: Detecting Social Engineering Attacks using Natural Language Processing and Machine Learning," in *2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, Aug. 2020, pp. 1–6. doi: 10.1109/INISTA49547.2020.9194623.
- [75] H. Sandouka, A. J. Cullen, and I. Mann, "Social Engineering Detection Using Neural Networks," in *2009 International Conference on CyberWorlds*, Sep. 2009, pp. 273–278. doi: 10.1109/CW.2009.59.