Investigating the Relationships Between SNS Usage, Personal Information Disclosure, and Cybersecurity

Sav Wheeler

A thesis

submitted in partial fulfillment of the

requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE & SOFTWARE ENGINEERING

University of Washington

2025

Reading Committee:

Marc J. Dupuis, Chair

David Socha

William Erdly

Program Authorized to Offer Degree:

Computer Science and Software Engineering

University of Washington

Abstract

Investigating the Relationships Between SNS Usage, Personal Information Disclosure, and Cybersecurity

Sav Wheeler

Chair of the Supervisory Committee:
Marc J. Dupuis
Division of Computing and Software Systems

As social networking sites (SNSs) become ubiquitous for daily activities, users and regulators have raised concerns with the state of digital privacy and security. Cyberattacks on SNSs have exposed private data of millions of users, and cybersecurity threats propagate through social engineering over SNSs. To determine whether frequent SNS users who disclose personal information are at greater risk of cyberattacks, I conducted a hybrid survey-interview study measuring the correlations between personal information disclosure, SNS usage, cybersecurity practices, and experiences with cybersecurity threats. The survey findings (n = 275) suggest that SNS usage frequency and usage for MNPS (meeting new people and socializing) or MEPO (make, express, or present more popular oneself) purposes have positive correlations to personal information disclosure. SNS usage frequency and personal information disclosure also had

positive correlations with experienced cybersecurity threats, but little correlation with cybersecurity behavior. Interview responses highlighted how subjects experienced cybersecurity threats within SNSs.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I am incredibly grateful to my reading committee, Dr. Dupuis, Dr. Socha, and Dr. Erdly for this research opportunity, and for your ongoing feedback, flexibility, and crucial insights over the course of this study. To Dr. Dupuis in particular, I would like to extend my deepest thanks for funding this research and helping me through this process over the course of our meetings. This research would not have been possible without your guidance. Finally, I would like to extend my gratitude to my family, without whom I could never have been here to achieve this incredible milestone. Thank you all so much for your continued support in shaping my future.

Chapter 1. INTRODUCTION

In a world increasingly dependent on digital infrastructure, threats to digital security abound. The ITRC reported an all-time high for data compromises in the U.S. in their 2023 Annual Data Breach Report, and the FBI's 2024 Internet Crime Report showed an all-time high of over $16 billion in losses from internet scams (Federal Bureau of Investigation, 2025; Identify Theft Resource Center, 2023). Most recently, a 2024 report from CrowdStrike reported that malware, denial-of-service, phishing, spoofing, and identity-based attacks were the most common forms of cyberattack (Baker, 2024). Malware covers a broad range of malicious software, including ransomware, spyware, adware, trojan horses, worms, and rootkits. Phishing attacks use social engineering techniques over email, SMS (phishing over SMS is often called "SMiShing"), or social media to entice users to download malware or share sensitive information such as account credentials. These threats are closely linked; a phishing attack may be used to distribute malware (He, 2012). Identity-driven attacks, where an attacker masquerades as a legitimate user, may be used to engage in social engineering for phishing or to install malware as a trusted user on critical systems.

For the actors behind these cyberattacks, SNSs present a lucrative target in digital spaces. One of the primary means by which malicious actors launch cyberattacks through SNSs is social engineering, where often, employees are targeted by attackers in order to gain access to information assets within their organizations (Wilcox & Bhattacharya, 2016). Social engineering is a technique where an attacker uses influence, persuasion, or manipulation to pose as another trusted individual or take advantage of people to obtain access to information (Mitnick & Simon, 2003). Social engineers may utilize techniques such as phishing, pretexting (inventing fake scenarios to steal a victim's information), baiting (inviting users to click on a malicious link for

free items), tailgating (using another individual's clearance to gain access to a physical space), ransomware, fake software or websites, pop-up alerts, robocalls, or reverse social engineering (where an attacker causes a problem and claims to be the only person able to fix the problem), gaining the desired information in the process (Salahdine & Kaabouch, 2019).

The prevalence of these threats presents a crucial challenge in the scope of SNS security. Though technologies have been proposed to detect social engineering attacks in advance (Hoeschele & Rogers, 2005; Lansley et al., 2020; Sandouka et al., 2009), as of now, much of the responsibility for avoiding these attacks still falls on the user of SNSs.

1.1 Scope, Domains, and Research Questions

This study aims to investigate the relationship between SNS usage and the behaviors therein, including personal information disclosure, and the potential cybersecurity risk faced by users of social networking sites. It aims to answer the following research questions:

RQ1: What are the connections between usage patterns of social networking sites (SNSs) and cybersecurity behaviors?

RQ2: Is there a relationship between personal information disclosure on SNSs and cybersecurity threats?

For these research questions, simulating the actual threats faced by subjects is beyond the scope of this thesis, and better suited to an experimental study. Instead, this study aims to predict the factors that influence or model threat occurrence by analyzing the behaviors that users take to enhance their digital security, and whether they have encountered cybersecurity threats online in the past. In order to quantify the specific types of behaviors users engage with on SNSs, I also investigate the domain of usage motivations, the typical activities subjects use SNSs with the intention of partaking in. The domains in this study are codified as follows:

- **Social Networking Site Behavior (SNSB)** describes the behaviors users engage in on SNSs.
- **Cybersecurity Behavior (CSB)** describes specific behaviors users might engage in to protect their digital security. The behaviors surveyed in this study are general protective digital behaviors, rather than specific organizational compliance behaviors.
- **Cybersecurity Experience (CSX)** describes a user's amount of past experience with direct cybersecurity threats to them or their digital assets.

This study further divides the domain of SNSB into several subdomains: frequency of use (SNSB-f), usage motivations (SNSB-m), and personal information disclosure (SNSB-p). Frequency of use describes how often a user uses their SNS platform of choice, or social media in general. Usage motivations are based on Horzum's (2016) Facebook Usage Aim Scale (FAU), as adapted by Kircaburun et al. (2020) as the Social Media Usage Aim Scale (SMUAS). This subdomain aims to quantify the different reasons or sub-behaviors users of social media engage in. The specific usage motivations are abbreviated per their abbreviations in the FAU. Finally, personal information disclosure**,** with specific points of information disclosure as described by Koehorst (2013) and Adjei et al. (2020), describes the overall amount of personal information a user of social media discloses.

1.2 HYPOTHESES

Based on these domains, this study aims to test six hypotheses. H1 through H4 were originally formulated during early study design, and H5 and H6 were added when drafting the domain model, prior to data collection. These hypotheses propose various correlations between the domains of SNS usage frequency, SNS usage motivation, personal information disclosure, cybersecurity behavior, and cybersecurity threat experience.

H1: Increased frequency of use of social networking sites correlates positively to good cybersecurity behavior.

The related factors of these domains can potentially balance one another out: while more frequent use of SNSs may lead to more overall risky security behaviors on online platforms (Molok et al., 2014) increased SNS use may also correlate to more frequent exposure to information about digital security and therefore increased threat awareness (Alqurashi et al., 2024). A frequent user of social media may be more "tech savvy" through exposure to information about cybersecurity threats and therefore have increased motive to take protective measures to reduce risk. Security awareness is an important factor in determining behavior (L. Li et al., 2016, 2019; Zwilling et al., 2022), and I hypothesize that increased awareness through social media will predominantly lead to improved cybersecurity behavior.

H2: Usage of social networking sites primarily for the purposes of (a) MEPO (make, express, or present more popular oneself) or (b) MNPS (meeting new people and socializing) negatively relate to good cybersecurity practices.

These two factors of usage motivation are factors in the FAU (Horzum, 2016). For the sake of analysis, this hypothesis is a conjunction of two sub-hypotheses, H2(a) and H2(b). I propose this hypothesis primarily due to the threat vector of social engineering. Online social behaviors, particularly seeking attention and companionship, could be motive for threat actors to target a user of SNSs by exploiting their drive to socialize (Salahdine & Kaabouch, 2019; Wilcox & Bhattacharya, 2016). For example, a threat actor might build a trusting online relationship with a SNS user in order to gain access to their account, personal information, or to later target a phishing attempt.

H3: Increased disclosure of personal information on social networking sites negatively relates to good cybersecurity practices.

Again, the link of cybersecurity awareness may result in a correlation between these domains. I conjecture that a user that is less aware of cybersecurity threats may engage in less secure behavior, and may be more willing to take risks in the amount of personal information they disclose on social media.

H4: Increased disclosure of personal information on SNSs positively correlates to the frequency of users' past experiences of cybersecurity threats.

As per the previous point, a user less aware of cybersecurity threats may be more willing to take risks in the amount of personal information they disclose, and as a result of this, may encounter more digital threats. However, there is a potential counterbalance to this prediction in that increased exposure to cybersecurity threats in the past may, in turn, lead to increased awareness of cybersecurity threats, causing the user to become more secure in future behaviors.

H5: Increased frequency of SNS usage positively correlates to increased personal information disclosure.

Earlier studies have established that extraversion and need for popularity relate to increased personal information disclosure (Christofides et al., 2009; Gosling et al., 2011) as well as frequency of SNS usage (Deng et al., 2013; Gosling et al., 2011). Through this deeper connection of a core motive- a need for socialization- the two domains may have a positive correlation.

H6: Good cybersecurity behavior negatively correlates to experiences with cybersecurity threats.

This hypothesis, while not directly testing relationships questioned by the research questions in this study, aims to complete the representation of hypothesized relationships in the

domain model. It may be such that the relationship between encountering cybersecurity threats and good cybersecurity behavior is implicit, as these good cybersecurity behaviors are defined by their efficacy in reducing users' vulnerability to cybersecurity threats.

For testing correlations in regard to support of these hypotheses, this study utilizes three different alpha levels: $\alpha = .05$, $\alpha = .01$, and $\alpha = .001$. p values that fall under any of these three levels indicate that the data is unusual for the statistical model assuming no correlation, with p values less than .001 indicating the most unusual data. In general, a p value less than .05 is sufficient evidence of correlation assuming no method error, though other factors such as discrepancies between sample size of categories within categorical data and inherent relationships may have some influence on correlations. For example, subjects who use SNSs frequently (SNSB-f) are inherently more likely to use it for a variety of reasons (SNSB-m) than subjects who seldom or never use social media, as the latter would have much less opportunity to use SNSs in a variety of different ways. All p values tested in the scope of this study, regardless of value, will be reported. Figure 1.1 shows the domain model of this study, with correlations labeled by hypothesis number and positive versus negative correlations indicated by both color (orange for positive, blue for negative) and corresponding labels above the hypothesis numbers. The domains of the study are shown as boxes, while the usage motivation factors, per the FAU (Horzum, 2016), are shown as circles linked to the SNSB-m box. Demographic factors, including gender, age, education, and ethnicity, may possibly influence other domains of this study, and as such are included in the modeled correlations via dotted lines.

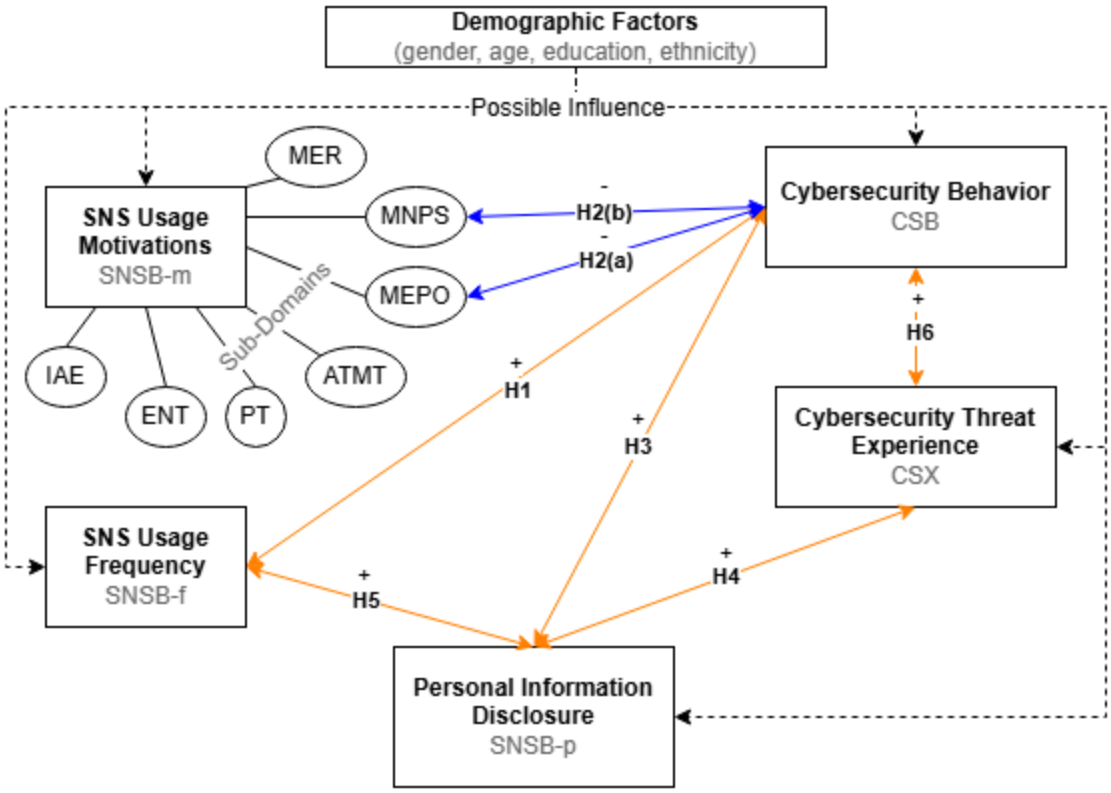

Figure 1.1: Study domain model, including domains and hypotheses

Chapter 2. LITERATURE REVIEW

This chapter provides a review of the state of digital security on SNS spaces and existing research on social media use. The literature review presents the definitions and existing models of research for the domains involved in this study, as well as a brief review of the laws and regulations governing the management and prosecution of digital threats in the U.S. and in international contexts.

2.1 Social Networking Sites and Social Media

A social networking site, or SNS, as defined by Kuss and Griffiths (2011), is a virtual community where users can create individual public profiles, interact with real-life friends, and meet other people based on shared interests. This differs from social media, which refers to the web 2.0 capabilities of producing and sharing user-generated content online, including social networking sites, weblogs, and content communities (Kuss & Griffiths, 2017). SNSs can be considered a subset of social media in this respect, and many of the digital security threats researched in the context of social media may be specific to (or distributed through) social networking sites, such as phishing links or messages, scams, cyber-stalking, or online extortion. This study focuses particularly on popular SNSs in the U.S.; in international contexts, other platforms such as Douyin and Kuaishou have market shares which are competitive with the top U.S. platforms (DataReportal, 2025).

Across other research, "social media" is often used interchangeably with the term SNS to describe SNS platforms with a large userbase or market share (e.g. Alqurashi et al., 2024; Brooks, 2015; Greenwood, 2013; Lau, 2017). Research on the effects of "social media addiction" may refer particularly to the maladaptive usage of SNS platforms (e.g. Balakrishnan & Griffiths, 2017;

Kircaburun et al., 2020; Sun & Zhang, 2021). Additionally, some surveys which focus on the usage of SNSs refer to these platforms as social media (e.g. DataReportal, 2025; Faverio & Sidoti, 2024; Gottfried, 2024; StatCounter, 2025).

Facebook has been the most popular SNS on the market since 2011, with over 3 billion monthly active users (MAUs) as of February 2025 (Ortiz-Ospina, 2019; Statista, 2024). Despite its large market share, Hellemans et al. (2020) found significant sociodemographic differences in the daily active users of Facebook, Twitter, Instagram, and SNSs in general (GSNS), suggesting that insights specific to Facebook cannot necessarily be generalized to other SNSs. Hughes et al. (2012) found that a preference for Facebook or Twitter was associated with differences in users' personality factors, further cementing this variance between SNS user-bases. While Facebook is the most popular SNS overall, among teenagers, YouTube, TikTok, Snapchat, and Instagram are more popular platforms (Faverio & Sidoti, 2024).

2.2 SNS USAGE

SNS usage has continually grown since the advent of SNSs. The first website credited as being social media was Six Degrees, named after the "six degrees of separation" theory, which officially launched in 1997 (Jones, 2025). Early platforms such as MySpace, YouTube, and Reddit gained millions of users in the early period from 2004-2008 (Ortiz-Ospina, 2019). Facebook, launched in 2004, eventually surpassed MySpace as the most-visited social media website, and reached 1 billion users in 2012 (Fowler, 2012; Hall, 2025). From 2017 to 2024, the number of social media users worldwide nearly doubled, from 2.73 billion to 5.17 billion (Statista, 2024). A survey by Perrin and Atske (2021) found that 85% of U.S. adults report that they are online at least daily, with 31% reporting that they are online "almost constantly". For adults aged 18-24, this number increases to 48%.

Many studies have found associations between maladaptive or excessive use of SNSs and factors relating to poor quality of life. Xanidis and Brignell (2016) found that SNS dependence was correlated with decreased sleep quality and cognitive function. Distracting social media usage may have negative impacts on task performance, particularly in an academic or professional setting, though this is highly dependent on the purpose of use of the SNS. Brooks (2015) found that social media usage negatively impacted task performance during professional (versus personal or play) times. Similarly, Lau (2017) found that social media usage for multitasking had a negative impact on cumulative GPA, but social media usage for academic purposes did not affect GPA. Junco et al. (2011) found that students who used Twitter to facilitate academic and co-curricular discussions had higher average engagement and GPAs than students who did not. A later study by Junco (2012) found that time spent on Facebook was positively correlated to time spent in co-curricular activities, but playing games on Facebook was negatively correlated to this.

Additionally, studies have highlighted a variety of factors predicting social media usage. Hughes et al. (2012) found that factors of the Big-Five model of personality traits had correlations to online socializing and information seeking as well as preference in social media platform, between Facebook and Twitter. In an expansive literature review, Sun and Zhang (2021) investigated the various models applied to social media addiction (SMA), summarizing many of the positive correlations between other factors and social media usage such as attachment anxiety (Flynn et al., 2018; Hart et al., 2015; Worsley et al., 2018), past negative and present fatalistic time perspectives (Przepiorka & Blachnio, 2016), psychosocial needs (Casale & Fioravanti, 2018), sense of belonging (W. Gao et al., 2017), information acquisition (Balakrishnan & Griffiths, 2017), and other factors.

Just as platform choice of SNSs is eclectic, so too are the types of activities present within social networking. Greenwood (2013), in investigating the connections between attitudes about fame and Facebook use, found differences in reading versus posting and responding, following media figures, and responses to media figure posts between users based on fame attitude. Hughes et al. (2012) also found differences in the usage behaviors on SNSs correlating with personality differences, particularly for socializing and information seeking and exchange, in their study on Facebook and Twitter. Similarly, Amichai-Hamburger and Vinitzky (2010), building on a study by Ross et al. (2009), found connections between personality traits and various behaviors on Facebook, including posting photos, using page features, and sharing personal information.

Horzum's (2016) study on Facebook use established a scale of seven different usage motivations based on the types of activities users of SNSs engage in: maintaining existing relationships (MER); meeting new people and socializing (MNPS); make, express, or present more popular oneself (MEPO); pass time (PT); as a task management tool (ATMT); entertainment (ENT), and informational and educational (IAE). This scale, the Facebook Usage Aim (FAU) scale, was later adapted as the Social Meda Usage Aim Scale (SMUAS) for general usage in measuring social media usage motivations by Kircaburun et al. (2020). This thesis, in turn, utilizes the SMUAS to measure the domain of SNS usage motivations.

2.3 Personal Information Disclosure on Social Media

In the CIA triad of digital security, one of the three concepts of the acronym is confidentiality, control over who has access to information on a need-to-know basis (Samonas & Coss, 2014). A key requirement of cybersecurity is that information that should be protected or confidential is as such. Among information that may require special protection is personally identifiable information

(PII), information that can be used to identify an individual. In the 2015 breach on Anthem Health, for example, cyber-criminals stole more than 37.5 million records of PII, which had not been encrypted in Anthem Health's systems, using targeted phishing attacks against employees to gain access to the company's systems (Office of Public Affairs, 2019; Sienko, 2016; Wright, 2015). Personal information available on SNSs can improve the efficacy of phishing attacks: "social phishing", a form of phishing which utilizes information available on social networks to craft phishing messages from senders mimicking acquaintances of the recipients, which Jagatic et al. (2007) found to increase the effectiveness of phishing attacks fourfold.

Despite the importance of protecting personal information, Norberg et al. (2007) describe a "privacy paradox" in consumer behavior. Despite consumers' concerns about data privacy rights and control over personal information, they found that consumers often freely disclose personal information. Benson et al. (2015) found that control over personal information was negatively associated with information disclosure; however, this finding is contradicted by Christofides et al. (2009). Many users of SNSs provide an abundance of personally identifiable information on SNSs at their own volition: Gross and Acquisti's (2005) survey of Carnegie Mellon University students revealed that the majority of students' Facebook profiles disclosed birthdays, dating preferences, relationship status, political views, various interests, and current residence. Though college-oriented SNSs, which Facebook was at the time of the study, may differ from traditional networking sites, this degree of information disclosure is not uncommon among traditional SNSs. Adjei et al.'s (2020) study found that over 80% of subjects disclosed their names, genders, religions, and school or college on social media. Personality has some bearing on personal information disclosure: per Amichai-Hamburger and Vinitzky (2010), higher neuroticism was associated with increased personal information disclosure. In general, users are willing to disclose

vast amounts of personal information online despite the importance of protecting personal information. This raises an important question: if users will not protect their data, what measures do SNS platforms or providers themselves take to protect their users' data?

2.4 Law, Controversies, and Corporate Structures

SNS providers have an obligation to take measures to ensure the safety of their users, but one key difficulty with ensuring the safety of online spaces is the legal regulation of cybercrime. Because digital spaces generally exist beyond the notions of territoriality, territorial authorities are limited in the means by which they can enforce online regulation (Chawki, 2005; Johnson & Post, 1996). Mugarura and Ssali (2020) found that, in spite of countries enacting anti-cyber and AML legislation, many law enforcement institutions lack the authority to implement regulatory laws for cross-border cases facilitated by digital spaces. Some types of cybersecurity threats may be beyond the domain of regulation altogether: spyware, for example, is often installed onto systems legally through the "clickwrap" software license agreement (Stafford & Urbaczewski, 2004). This is not to say that anti-cybercrime regulation is not without efficacy or merit altogether; Li (2016) reported that the deterrence system supported by Chinese regulatory law played a role in detecting offenses and preventing potential cyber-crimes. Likewise, law enforcement agencies globally have seen successes in regulating person-based cybercrimes, particularly in the cases of cyberstalking, child pornography, and other sex offenses (Ajayi, 2016).

Ian Murphy, aka "Captain Zap", was the first person to be tried and convicted as a felon for a digital crime, following breaking into AT&T's servers in 1981, though the charge at the time was theft, not computer crime (Brenner, 2007; Delio, 2001). Soon after, laws were established in the U.S. to define the scope of computer-specific criminal offenses and their prosecution, such as the Computer Fraud and Abuse Act (CFAA) of 1986, the first felony conviction under which was

in that of Robert Morris in 1991, the creator of the eponymous 1988 Morris worm (Computer Fraud and Abuse Act, 1986; *US v. Morris*, 1990).

While regulating cybercrime is crucial in maintaining the security of users of digital spaces, another key legal consideration in the moderation of online spaces is the human right to privacy. The right to privacy is enshrined in Article 17 of the International Covenant on Civil and Political Rights, signed in 1966 and ratified in 1976 (International Covenant on Civil and Political Rights, 1966). Individual countries and unions have further ratified or enshrined protections of digital privacy rights in their resolutions, treaties, and constitutions, including but not limited to Convention 108, Justice K.S. Puttaswamy vs. Union of India, and the GDPR (Council of Europe, 2018; General Data Protection Regulation, 2016; Supreme Court Observer, 2017).

Convention 108 of the Council of Europe is a 1981 treaty to protect the individual right to privacy. This convention was updated in 2018 to include an obligation to report data breaches, and in 2019 to provide guidelines for the use of artificial intelligence (AI) tools (Council of Europe, 2018, 2019). In India, Article 21 of the Constitution was determined in Justice K.S. Puttaswamy vs. Union of India to extend to the guarantee of digital privacy rights among other Part III rights (Supreme Court Observer, 2017). Finally, for EU member countries, the 2016 General Data Protection Regulation (GDPR) requires certain practices to protect digital privacy of citizens such as appointing a Data Protection Officer, maintaining documentation on the type of data collection, and transparency with the subjects of data collection. It applies to all entities collecting data on EU citizens, including international corporations (GDPR.eu, 2018; General Data Protection Regulation, 2016). The GDPR is limited in that it only protects personal data; other types of data collected by companies such as engagement data, behavior data, and attitudinal data may not be protected (Petersdotter & Höglund, 2024).

Also notable within the domain of SNS data regulation is the fact that many of the most popular social networks in the U.S. are owned by Meta Platforms (formerly Facebook, Inc.), the parent company of Facebook. These include Facebook itself, Instagram, Facebook Messenger, and WhatsApp (Facebook, 2014; Rulsi, 2012). The Meta business model utilizes a two-version system, where users can pay a subscription fee for a premium version of Facebook with no advertising, or use a free version of Facebook where personal data is collected for targeted advertising (Petersdotter & Höglund, 2024). The scale of data collection by Meta raises concerns of privacy with regard to cross-platform data sharing. In 2024, the Turkish competition authority launched in investigation into Meta Platforms over cross-platform data sharing; after commitments by Meta to not share user data across the Threads and Instagram platforms unless users chose to merge their accounts, the investigation was terminated (Reuters, 2024). However, in early 2025, Meta unveiled a "memory" feature for its cross-platform chatbot that would retain and fetch account information across platforms to delivered tailored recommendations, a data-sharing initiative with no opt-out which raises similar antitrust concerns (Joseph, 2025; Roth, 2025).

2.5 Cybersecurity Threats on Social Networking Sites

To understand the risks users of SNSs face, it is important to outline the types of cybersecurity threats present on SNSs. A literature review by Gao et al. (2011) outlines four categories of cybersecurity threats on SNSs: privacy breaches, viral marketing, network structural attacks, and malware attacks.

Firstly, privacy breaches can occur on either the service provider's end, from other users such as friends or followers, or from third-party applications (H. Gao et al., 2011). Attackers can be people known to victims (Shay et al., 2014) or unknown actors impersonating people known to victims through attacks such as profile cloning, where an attacker duplicates a user's profile and

uses the duplicate profile to send friend requests to the original user's friends (Bilge et al., 2009). Many SNSs have also undergone large-scale data breaches as a result of poor internal security or social engineering attacks. Facebook underwent multiple data breaches in 2018 and 2019, exposing hundreds of millions of users' private information altogether (Isaac & Frenkel, 2018; Silverstein, 2019; Wong, 2019). In 2016, a data breach of the MySpace platform exposed 360 million users' passwords (Weise, 2016). A massive data leak in 2020 exposed 235 million profiles of Instagram, YouTube, and TikTok (Winder, 2020). Other platforms including Snapchat, Google+, and Twitter have undergone similar data breaches over the years (Fung, 2014; Goodin, 2018; Zetter, 2013).

Secondly, in the case of viral marketing, spammers exploit social engineering techniques to market products to SNS users (H. Gao et al., 2011). Spamming is categorized as broadcast spam, wherein spammers abuse interaction mechanisms to disseminate information, or the more sophisticated context-aware spam, which takes into account user profile information to procure targeted messages (Brown et al., 2008). Viral marketing is prevalent in combination with account hijacking; a study by Grier et al. (2010) found that, on Twitter, many spam accounts were previously legitimate accounts that had been compromised by spammers. Gao et al. (2011) also classify phishing under the umbrella of viral marketing.

Thirdly, network structure attacks are those which exploit the structure of a social network to launch a cyberattack, such as Sybil attacks, where an individual masquerades as multiple users simultaneously. Sybil attacks work through exploiting the basic framework of entity-to-entity trust on a network; in the absence of a trusted authority, an entity can masquerade as any number of identities, assuming they are not validated simultaneously (Douceur, 2002). In context, this means that a single or small number of users can disproportionately control or attack a larger SNS (Yang

et al., 2014). Social botnets- large scale networks of social bots, automation software that control hijacked accounts on SNSs- may also fall under this category (Boshmaf et al., 2013). These social botnets may be used for spamming, phishing, or DDoS attacks, as well as uses that are not explicitly malicious such as astroturfing (a fake grassroots campaign in the SNS space), social, and informational uses (Abokhodair et al., 2015).

Finally, malware attacks refer to the spreading of malicious software using SNSs as a vector for dispersal. Worms are a common example of this, also commonly examples of social botnets, such as the Koobface malware (Thomas & Nicol, 2010; Xu et al., 2010). Other types of malware include: trojan horses, a type of malware which disguises itself as legitimate software; adware, a type of malware to display unwanted computer ads; spyware, a type of malware that allows remote monitoring of a device; rootkits, well-hidden malware that grants an intruder elevated privileges on a system; backdoors, a type of malware which allows attackers to remotely access devices; and ransomware, a type of malware which encrypts data and locks down file access, requesting a ransom from the victim (Pachhala et al., 2021).

Beyond the domains covered by Gao et al. (2011), misinformation, hate speech, cyberbullying, and incitements of violence are digital threats which can propagate over SNSs which may not directly affect the information security of the victims, but still cause real-world harms (Cao et al., 2023; Cohen-Almagor, 2022; Ebube, 2023; Lidsky, 2011). For example, Facebook played a crucial role in exacerbating the genocide against Rohingya Muslims in Myanmar, as it was the predominant social network in the country and had minimal Burmese-speaking moderators at the time of the genocide, despite warnings from employees, civil society groups, and human rights organizations of rampant hate speech (Maulana & Julyazti, 2025; Pour, 2023; Schissler, 2024).

2.6 Models of Security Behavior

Users' security behaviors are critical deterrents of many of the cybersecurity threats present on SNSs. Two models are typically applied to understand why users behave in secure, or insecure, ways: the Health Belief Model (HBM) and Protection Motivation Theory (PMT) (Janz & Becker, 1984; Maddux & Rogers, 1983; Rosenstock, 1974). Originally developed to measure behaviors with respect to physical health, these models explain why people choose to participate or not participate in health behaviors. They are utilized in the domain of cybersecurity in several studies in an effort to explain security behaviors and security compliance intentions (e.g. Anwar et al., 2017; Lee et al., 2008; L. Li et al., 2019; Tran et al., 2024). The factors of the original Health Belief Model (HBM) include perceived susceptibility, perceived severity, perceived benefits, perceived barriers, health motivation, and cues to action. As defined by the HBM, perceived susceptibility is one's subjective assessment of the risk of contracting a condition, while perceived severity is one's concern regarding the seriousness of contracting an illness, including medical consequences and social consequences. In cybersecurity contexts, these are applied as the subjective assessment of the risk of encountering cybersecurity threats, and one's concern of the seriousness of encountering a cybersecurity threat and its consequences, respectively. Likewise, perceived benefits are defined by the HBM as the beliefs regarding the effectiveness of the actions available in reducing the disease threat, while perceived barriers are the potential negative aspects of a particular health actions that may act as impediments to undertaking a health behavior. In cybersecurity contexts, rather than disease threats, these perceptions are applied in regard to cybersecurity threats and security behaviors. Notably, Aboulnasr et al. (2022) also found that, for consumer activity on SNSs, perceived benefits correlated positively with personal information disclosure.

Protection Motivation Theory (PMT) extends the HBM by taking into account behavioral intention as determinant of actual health behavior. This model considers the factors of perceived susceptibility and perceived severity as with the HBM, and also considers factors of self-efficacy, an individual's expectancies of personal mastery and efficacy, and response efficacy, the expectance that performance of a recommended alternative behavior will avert dangerous consequences (Maddux & Rogers, 1983). Self-efficacy is applied in cybersecurity research as an individual's belief in their capabilities to avert or mitigate a cybersecurity threat.

Social and cultural contexts can influence security behaviors and perceived self-efficacy in cybersecurity. Anwar et al. (2017) found that gender has a significant effect on security self-efficacy, prior experience with computer security, and computer skills, with women self-reporting lower scores in all of these factors. Despite less self-efficacy, however, the study found no significant correlation between gender and self-reported cybersecurity behaviors. Branley-Bell et al. (2022) supported this finding, finding that males self-reported higher self-efficacy but little difference in actual cybersecurity behavior between genders. Herath and Rao (2009) and Ifinedo (2014) also found that women have higher security compliance intentions than men, though a study by Vance et al. (2012) contradicts this finding, with no significant gender difference in security compliance intentions among employees of a Finnish municipal organization. Hoy and Milne (2010) as well as Laric et al. (2009) found that gender also influences the degree of privacy concerns, with greater concern among women than men.

2.7 Experience with Cybersecurity Threats

Studies which quantify aspects of past experience with cyber-threats typically focus on a single type of threat such as account hijacking, loss of important files, or ransomware (Dupuis et al., 2012; Shay et al., 2014; Yilmaz et al., 2023). In interviews conducted by Tian et al. (2020),

participants reported on cybersecurity incidents they had encountered, which were classified as either “bounded” or “fuzzy” depending on the specificity of their limits; malicious software, phishing, and hacking were often experienced and characterized as bounded events, while tracking of online activities, privacy violations, and unpleasant online encounters were experienced and often characterized as fuzzy. Angulo and Ortlieb (2015) also identify scenarios of “privacy panic situations”, which include frequently occurring privacy incidents and common experiences of online privacy-related panic. Many of these situations overlap with cybersecurity threats, such as instances of identity theft, account hijacking, and online stalking or bullying. Often, experiences with cybersecurity threats are a source of shame (Renaud et al., 2022), and result in stress and emotional harm in addition to concrete losses (Budimir et al., 2021; Shay et al., 2014).

Chapter 3. METHOD

This chapter discusses the method of the study, development and contents of the survey and interviews, sampling and distribution methods, and modifications to the initial survey and interview contents.

3.1 OVERVIEW

This study was conducted in a hybrid survey-interview format, with a survey providing quantitative data on potential correlations between the domains of this study while interviews informed both the contents of the survey and provided more depth and detail on respondents' experiences with digital threats on social media. The target number of respondents was 300 for the survey and 30 for the interview. The survey was developed using the Qualtrics survey platform.

There were no exclusion criteria for subjects participating in the survey or interview except for age of consent (18+), and in the case of the survey, that subjects were not employees of the University of Washington, family members of a University of Washington employee, or University of Washington student involved in this particular research, per the University of Washington's Procurement Services policy on Amazon Mechanical Turk usage. Subjects were required to provide their informed consent, with consent forms explaining the topics and procedures of the research, in order to participate in either the survey or interview.

Monetary compensation was provided to incentivize participation in this study, at separate rates for survey and interview participants. Interview participants were compensated at a rate of $20 per interview, while survey participants were compensated at a rate of $3 per response.

3.2 Data Protection

Contact information was provided by interview participants for initial outreach when scheduling interviews. Following the closure of interviews, this contact information was discarded, and outreach emails to interview participants were deleted. Interview respondents were only linked to their transcripts by the date and time of the interviews themselves, with respect to sign-up forms, which were removed on the closure of interviews.

Recordings were taken and stored locally on an offline device. These were transcribed using a local instance of OpenAI's Whisper model, which provides quality transcription for audio including accents or background noise, both of which were factors affecting the interview recordings (OpenAI, 2022). Personally identifiable information (PII) reported by subjects during interviews such as the names of universities, businesses, or emails were censored during the transcription process via manual review. Following the closure of this study, interview transcripts will also be discarded for data protection purposes.

3.3 Sampling Procedure

Survey sampling was conducted using Amazon's Mechanical Turk (MTurk) platform, an online crowdsourcing market (OCM) that enables the recruiting of "workers" for digital tasks such as survey responses, providing an approximately random sample. MTurk provides several benefits over similar OCMs such as sampling anonymity, controls for participant selection and recruitment, and built-in payment systems (Steelman et al., 2014). A key limitation with this distribution method is that the sample is only random within the population of MTurk users, the implications of which will be discussed in Chapter 5.

Interviews were physically advertised and took place on the University of Washington Bothell campus, so subjects thereof were a convenience sample of voluntary sign-ups. This introduced some self-selection bias into interview responses, which the provision of financial compensation aimed to mitigate. While results from the interviews may not be generalizable to the general public, they provide valuable insights on the digital threats encountered by, and the social media experiences of, a university student population. These insights helped shape the content and structure of the survey to avoid and mitigate other potential reporting biases.

3.4 Interview Development

As interviews were intended to take 20-30 minutes, with an estimate of each interviewee taking 2-3 minutes at most on any given question, the first developed script for the interviews were ten questions. These questions were open-ended and generally asked interviewees for the sum of their experiences regarding each particular topic the survey would later investigate. For example, in looking at the domain of cybersecurity threat experience, interviewees were asked two questions: one on whether they had been the victim of a cyberattack (with some examples given), one on whether they had been tricked into taking actions that would unintentionally put their account at risk (likewise, with examples given). Interviewees were not given a timeframe on the recency of their experiences and were free to share incidents from many years in the past, though if the interviewee did not initially share when a particular incident occurred, I would follow up by asking how recent the incident was.

As these interviews were semi-structured, on occasion, more clarifying questions were introduced to confirm or refine the interviewees' accounts. Over time, additional questions were introduced based on common clarifying questions or follow-ups, for a total of twelve questions in later interviews. Initially, questions about personal information disclosure and cybersecurity

behavior took place before questions about cybersecurity threat experience, but these questions were later moved to the section after cybersecurity threat experience, as with the initial configuration, there was a degree of an implied causal effect that may have led to under-reporting of cybersecurity threat experiences as a defense of one's behavioral responses, as a form of social desirability bias.

One of the questions introduced in the interviews had to do with cybersecurity incidents that did not directly affect participants. As some subjects willingly shared their experiences in witnessing cybersecurity incidents that did not personally affect them, particularly when the subject had not personally experienced an incident, the script was revised to include a question specifically to ask whether subjects had witnessed signs of cybersecurity threats online, regardless of whether they had personally been affected. This was introduced to avoid information bias based on whether subjects shared such information if they had personally experienced their own incidents, and to prevent oversharing or under-sharing by any particular group.

3.5 Survey Development

For the domains of the survey, question inventories were assembled by the consolidation of questions measuring components of the survey domains from other related studies. For example, to quantify usage motivations, the survey utilized Kircaburun et al.'s (2020) adaptation of Horzum's (2016) Facebook Usage Aims Scale (FAU) as the Social Media Usage Aims Scale (SMUAS). The definitions of the factors of this scale are discussed in Chapter 2.2. Survey questions maintained the language of "social media" throughout the survey rather than the formal "social networking sites", as the SNS limitation of the scope of social media was implied in the questions themselves on choice of SNS platforms (and usage thereof). Likert-style questions were

presented in question matrices, with introductions to each section to shorten the length of questions.

Table 3.1 shows the sources of the questions for each of the survey domains.

Table 3.1. Survey question sources

SURVEY DOMAIN	QUESTION SOURCES
SNS Usage Frequency (SNSB-f)	Platform choices from StatCounter (2025), plus additions from interview responses.
SNS Usage Motivations (SNSB-m)	Horzum (2016), Kircaburun et al. (2020).
Personal Information Disclosure (SNSB-p)	Koehorst (2013), Adjei et al. (2020).
Past Experience with Cybersecurity Threats (CSX)	Dupuis et al. (2012), Shay et al. (2014), Angulo and Ortlieb (2015), Yilmaz et al. (2023).
Cybersecurity Behavior (CSB)	Anwar et al. (2017), Ion et al. (2015), Alanazi et al. (2022)

In order to establish whether there is a correlation between threat occurrence and social media behavior, one of the key factors this study measured was whether subjects have experienced cybersecurity threats or incidents in the past. This measurement presents two key limitations. First, subjects may have experienced a cybersecurity threat or incident in the past, but may not be aware of it, leading to an overall underreporting bias. Second, incidence of a cybersecurity threat may not necessarily stem from a threat vector originating from social networking sites. For example, subjects may report phishing incidents that took place over SMS or email rather than an SNS. The implications of these limitations will be discussed further in Chapter 5.2.

The results of initial interviews informed changes necessary to the survey prior to its distribution. First, beyond the top SNSs by market share, Discord and TikTok, two of the three most popular SNSs among interview respondents, were added as SNS options to the survey (the

third, Instagram, was already one of the survey options). Second, as with the interview script, the order of questions with respect to domains was modified such that questions about cybersecurity experiences came before those about personal information disclosure and cybersecurity behavior.

Four response validation questions were included within different subsections of the survey in order to filter out automated responses and respondents which deliberately misreported or did not pay attention to the questions. These questions consisted of an introduction similar to the others within their same subsection, followed by clear instructions for completing the survey and receiving compensation (e.g. “select Strongly Agree to get paid”). Responses that did not correctly answer any one of these validation questions were discarded, and the survey ended early for subjects who failed these validation questions with no compensation provided. Additionally, to further verify that respondents were accurately self-reporting, a repeat of the initial demographic questions were included at the end of the survey. During data analysis, responses which did not match between the initial demographic selections and final demographic selections were discarded as invalid. In total, 76 responses were discarded as invalid based on these criteria.

Chapter 4. DATA ANALYSIS

This chapter discusses the analysis practices and statistical findings of the survey data, as well as highlights and trends from the interviews.

4.1 SURVEY DATA

A total of 352 responses were collected for the survey. After filtering for response validation questions and matching demographic questions, 276 responses remained valid for data analysis. During data analysis, one additional response was dropped, as the subject's reported most frequently used SNSs (Facebook and YouTube) did not align with their reported frequencies of use. Said subject reported never using either of these platforms, but occasionally using other platforms such as Pinterest and TikTok. The final total was 275 responses.

4.1.1 *Respondent Demographics*

Table 4.1 shows the demographic distributions of survey respondents. Age distribution was slightly right-skewed, with the mode age range being 35-39. There were slightly more male respondents than female, with one non-binary or third gender respondent and one respondent that did not disclose gender. A large majority (80%) of respondents were white, and a majority (56.7%) had bachelor's degrees.

Table 4.1. Survey demographics

	Demographic	Number of Respondents	% of Respondents
Age (Years)	20-24	4	1.5%
	25-29	32	11.6%
	30-34	41	14.9%
	35-39	58	21.1%
	40-44	32	11.6%
	45-49	20	7.3%
	50-54	27	9.8%
	55-59	16	5.8%
	60-64	24	8.7%
	65-69	9	3.3%
	70-74	11	4.0%
	75-79	1	0.4%
Gender	Male	145	52.7%
	Female	128	46.5%
	Non-binary/third gender	1	0.4%
	Prefer not to say	1	0.4%
Ethnicity	Asian/Pacific Islander	24	8.7%
	Black	18	6.5%
	White	220	80%
	Hispanic	9	3.3%
	Other/Multiracial	4	1.5%
Education	GED	34	12.4%
	Some University	27	10.1%
	Associate's Degree	22	8.0%
	Bachelor's Degree	156	56.7%
	Master's Degree	29	10.5%
	Law/MBA Degree	3	1.0%
	Doctorate Degree	4	1.5%

4.1.2 *Correlation Analysis*

To analyze the survey data for potential correlations, scores of 0-4 were assigned for the Likert scale options ("Strongly Disagree" = 0, "Disagree" = 1, "Neither Agree nor Disagree" = 2, "Agree" = 3, "Strongly Agree" = 4). For the questions related to frequency of use, scores of 0-5 were

similarly assigned ("Never" = 0, "Rarely" = 1, "Sometimes" = 2, "Often" = 3, "Very Often" = 4, "All the Time" = 5). Based on these numerical scores, this study utilized Pearson correlation testing between the Likert-scaled survey domains and frequency domains using the pearsonr function from the scipy package in Python and validated these tests by comparing results with the equivalent Excel formulas.

The domain of frequency of SNS use (SNSB-f), for the purposes of analysis, is split here into two aggregate statistics: the total average usage across all SNS options available in the survey, and the average usage of the SNSs selected by the respondent. This is because in some cases, subjects might regularly use SNSs other than those that they reported as their most frequently used, contributing to their overall SNS usage. However, there is a natural threshold to how much a larger variety of SNSs can contribute to social media usage, as it would be impossible for a subject to use every SNS listed for several hours a day each within the timeframe of a single day.

Separating the frequency of use into these two categories can inform results and correlations in several ways. For one, subjects that have a higher average use across all SNSs (SNSB-f-ALL) than their most frequently used SNSs (SNSB-f-USED) have a variety of social media accounts that they use frequently. If a statistically significant correlation exists between a survey domain and both the frequency of use across all SNSs (SNSB-f-ALL) and across subjects' frequently used SNSs (SNSB-f-USED), the domain correlation to frequency of use altogether is likely stronger than if there is only a significant correlation to either SNSB-f-ALL or SNSB-f-USED. However, if a statistically significant correlation exists between a survey domain and the frequency of use across all SNSs (SNSB-f-ALL) but *not* the frequency of use across subjects' frequently-used SNSs (SNSB-f-USED), the correlation may be related to aspects of the SNSs that respondents use less often, or to the usage of a variety of SNSs rather than frequency of use of a

small set of platforms. Conversely, if a statistically significant correlation exists between a survey domain and the frequency of use across subjects' frequently-used SNSs (SNSB-f-USED) but *not* the frequency of use across all SNSs (SNSB-f-ALL), the correlation is more likely to be related to the active use or aspects of the subjects' preferred SNSs than their overall use of social media or the variety therein.

For the domain of SNS usage motivations (SNSB-m), the correlations of each of the seven usage motivation factors of the SMUAS (MER, MNPS, MEPO, PT, ATMT, ENT, IAE) were tested against other numeric domains. Correlations between the usage motivation factors themselves are not included here as they are not within the scope of this study.

Table 4.2 shows the correlation matrix, including correlation coefficients (ρ) and p values with indications of significance at the alpha levels of 0.05, 0.01, and 0.001, between the frequency of usage (SNSB-f) subdomains, personal information disclosure (SNSB-p), cybersecurity experience (CSX), and cybersecurity behavior (CSB) to the numeric domains of the survey. Correlations relevant to one or more hypotheses are shown in bold black, while other correlations are shown in lighter gray text.

Table 4.2. Correlation Matrix for SNSB-f, CSX, CSB, and SNSB-p

STAT TESTED	SNSB-F-ALL	SNSB-F-USED	CSX	CSB	SNSB-P
SNSB-F-ALL	N/A	$\rho = .80$ $p < .001$***	$\rho = .48$ $p < .001$***	**$\rho = -.024$** **$p = .70$**	**$\rho = .61$** **$p < .001$*** **
SNSB-F-USED	$\rho = .80$ $p < .001$***	N/A	$\rho = .35$ $p < .001$***	**$\rho = .019$** **$p = .75$**	**$\rho = .48$** **$p < .001$*** **
MER	$\rho = .36$ $p < .001$***	$\rho = .28$ $p < .001$***	$\rho = .17$ $p = .0036$**	$\rho = .10$ $p = .098$	$\rho = .67$ $p < .001$***
MNPS	$\rho = .64$ $p < .001$***	$\rho = .53$ $p < .001$***	$\rho = .51$ $p < .001$***	**$\rho = -.034$** **$p = .58$**	$\rho = .78$ $p < .001$***
MEPO	$\rho = .68$ $p < .001$***	$\rho = .54$ $p < .001$***	$\rho = .56$ $p < .001$***	**$\rho = -.12$** **$p = .046$***	$\rho = .76$ $p < .001$***
PT	$\rho = .20$ $p < .001$***	$\rho = .20$ $p < .001$***	$\rho = .12$ $p = .045$*	$\rho = .023$ $p = .71$	$\rho = .15$ $p = .014$*
ATMT	$\rho = .67$ $p < .001$***	$\rho = .54$ $p < .001$***	$\rho = .54$ $p < .001$***	$\rho = -.026$ $p = .67$	$\rho = .76$ $p < .001$***
ENT	$\rho = .64$ $p < .001$***	$\rho = .52$ $p < .001$***	$\rho = .42$ $p < .001$***	$\rho = .082$ $p = .17$	$\rho = .67$ $p < .001$***
IAE	$\rho = .58$ $p < .001$***	$\rho = .49$ $p < .001$***	$\rho = .46$ $p < .001$***	$\rho = .040$ $p = .51$	$\rho = .56$ $p < .001$***
CSX	$\rho = .48$ $p < .001$***	$\rho = .35$ $p < .001$***	N/A	**$\rho = -.21$** **$p < .001$*** **	**$\rho = .47$** **$p < .001$*** **
CSB	**$\rho = -.024$** **$p = .70$**	**$\rho = .019$** **$p = .75$**	**$\rho = -.21$** **$p < .001$*** **	N/A	**$\rho = -.0036$** **$p = .95$**
SNSB-P	**$\rho = .61$** **$p < .001$*** **	**$\rho = .48$** **$p < .001$*** **	**$\rho = .47$** **$p < .001$*** **	**$\rho = -.0036$** **$p = .95$**	N/A

* $p < .05$

** $p < .01$

*** $p < .001$

All usage motivation factors had a statistically significant positive correlation with SNS usage frequency, including both SNSB-f-ALL and SNSB-f-USED, at the .001 alpha level. Additionally, SNS usage frequency had statistically significant positive correlations with personal

information disclosure at the .001 alpha level. The correlation coefficient between all SNS options and personal information disclosure (ρ = .61) was larger than that between most-frequently-used SNSs and personal information disclosure (ρ = .48), suggesting that using a larger variety of platforms may contribute to personal information disclosure. Personal information disclosure also had a statistically significant positive correlation with every usage motivation factor at the .05 alpha level. The best predictors of personal information disclosure among the motivation factors were MNPS and MEPO.

There were no statistically significant correlations between cybersecurity behavior and frequency of social media usage, personal information disclosure, and almost all usage motivation factors at the alpha level .05. The one usage motivation factor with a significant correlation to cybersecurity behavior was MEPO, with a statistically significant correlation at the alpha level .05 (p = .046) and a negative correlation coefficient, suggesting a slight inverse relationship. Cybersecurity behavior and cybersecurity experiences also had a statistically significant negative correlation at the .001 alpha level (p = .0004).

Conversely, cybersecurity experiences had statistically significant correlations to all domains except for the MER and PT factors of usage motivation at the .001 alpha level, and had statistically significant correlations to these remaining two domains at the .05 alpha level. As all the test statistics in this category except for cybersecurity behavior were positive, this suggests that frequent social media use, increased personal information disclosure, and social media usage for a variety of motivations all correlate with increased experience of cybersecurity threats.

4.1.3 *Analysis of Variance Across Demographic Groups*

For the categorical variables of demographics, one-way ANOVA tests were conducted for each demographic variable with relation to the measured domains using the f_oneway function from

the scipy package in Python, in order to determine whether there were statistically significant correlations between the demographic factors and the survey domains. Demographic variables were not tested for correlation to one another, as that was not within the scope of this study. The test statistics (F) and p values of the ANOVA tests are shown in Table 4.3.

Table 4.3. ANOVA results for demographic groups

STAT TESTED	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	$F = .19$ $p = .90$	$F = 2.15$ $p = .048$*	$F = .19$ $p = .94$	$F = 5.91$ $p < .001$***
MER	$F = .54$ $p = .65$	$F = 2.16$ $p = .047$*	$F = .98$ $p = .42$	$F = 1.75$ $p = .063$
MNPS	$F = .42$ $p = .74$	$F = 3.07$ $p = .0064$**	$F = .62$ $p = .65$	$F = 7.59$ $p < .001$***
MEPO	$F = 1.60$ $p = .19$	$F = 6.05$ $p < .001$***	$F = .80$ $p = .53$	$F = 8.95$ $p < .001$***
PT	$F = .88$ $p = .45$	$F = 4.29$ $p < .001$***	$F = 1.11$ $p = .35$	$F = 2.22$ $p = .014$*
ATMT	$F = 1.10$ $p = .35$	$F = 3.18$ $p = .0050$**	$F = .54$ $p = .70$	$F = 6.57$ $p < .001$***
ENT	$F = 1.07$ $p = .36$	$F = 4.49$ $p < .001$***	$F = .80$ $p = .53$	$F = 5.29$ $p < .001$***
IAE	$F = .15$ $p = .93$	$F = 1.90$ $p = .082$	$F = 1.26$ $p = .28$	$F = 4.07$ $p < .001$***
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	$F = .36$ $p = .78$	$F = 1.88$ $p = .084$	$F = 1.00$ $p = .41$	$F = 1.11$ $p = .36$

* $p < .05$

** $p < .01$

*** $p < .001$

While the demographic variables of gender and ethnicity showed no significant variance between groups across any of the survey domains, age and education had several instances of significant variance between groups with the measured domains. Education had significant variance between groups ($p < .05$) in the domains of frequency of usage (both SNSB-f-USED and SNSB-f-ALL), all usage motivation factors except IAE, personal information disclosure, and cybersecurity experiences. The largest instances of variance between groups, those with p values less than .001, were in the domains of MEPO, PT, ENT, and personal information disclosure. Similarly, age had significant variance between groups ($p < .05$) in all domains except for the MER motivation factor and cybersecurity behavior. For these domains, with the exception of PT, the variance was significant at an alpha level of .001.

To better illustrate how the demographic groups of age and education vary with respect to certain domains in which significant variance was found, the average scores for the domains, other than usage motivation factors, is graphed with variance across each demographic group for these two demographics in Figure 4.1, Figure 4.2, Figure 4.3, Figure 4.4, Figure 4.5, Figure 4.6, Figure 4.7, and Figure 4.8. These averages are based on the overall average for the domain by subjects across all Likert-scale mapped questions, with an average of 0 indicating a response of "Strongly Disagree" in all domain questions and an average of 4 indicating a response of "Strongly Agree" in all domain questions by all participants of the demographic. Notably, some groups have much smaller sample sizes (law/MBA and doctorate degrees for education, and the 24-29, 65-69, and 75-79 bins for age), so these bins may not be representative samples for their particular demographics. Figure 4.1, Figure 4.2, Figure 4.3, and Figure 4.4, show the

relationships between education and the numeric domains with *p* values less than .05 from the ANOVA testing.

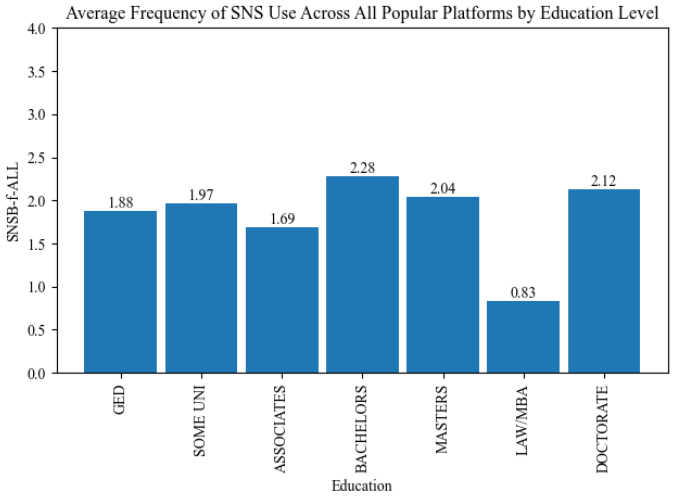

Figure 4.1. Average frequency of SNS use across all popular SNSs (SNSB-f-ALL) by education

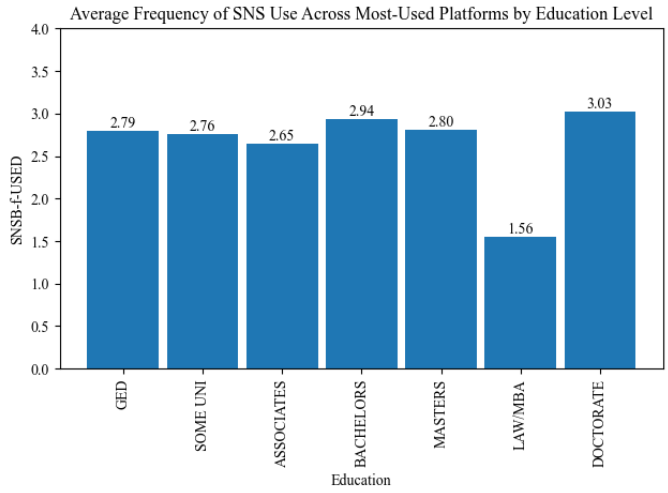

Figure 4.2. Average frequency of SNS use across most-used platforms (SNSB-f-USED) by education

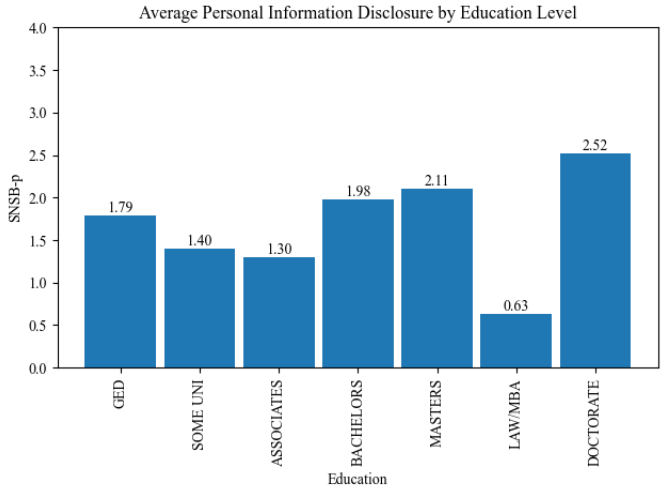

Figure 4.3. Average personal information disclosure (SNSB-p) by education

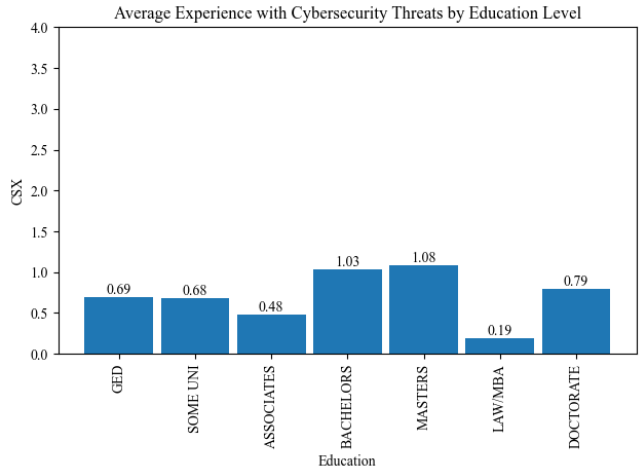

Figure 4.4. Average experience with cybersecurity threats (CSX) by education

Subjects with a law/MBA degree reported much lower SNS use across all surveyed platforms, personal information disclosure, and experience with cybersecurity threats than other groups, likely contributing to some of the variance. Additionally, subjects with doctorate degrees generally reported higher average personal information disclosure. However, it is noteworthy that only three subjects surveyed had law/MBA degrees and only four had doctorate degrees, so these results may also be in part due to a small sample. Therefore, these conclusions may not be applicable to the general population. The contribution of the education demographic to variance in these domains is more likely a result of variance among smaller-sample demographic groups

than indication of a larger trend; discounting the law/MBA and doctorate bins, there is only a slight trend of increasing average experience with cybersecurity threats across education demographics.

Among different age groups, however, there are clear trends in the domains with high variance between groups. Figure 4.5, Figure 4.6, Figure 4.7, and Figure 4.8 show the relationships between age groups and the domains with *p* values less than .05 with respect to age, again with the exception of usage motivations. The final bin, ages 75-79, has no standard error, as there was only one respondent in this bin.

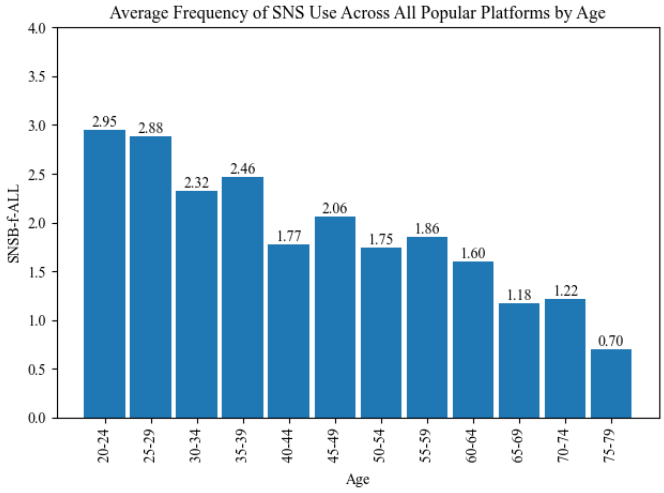

Figure 4.5. Average frequency of SNS use across all popular SNSs (SNS-f-ALL) by age

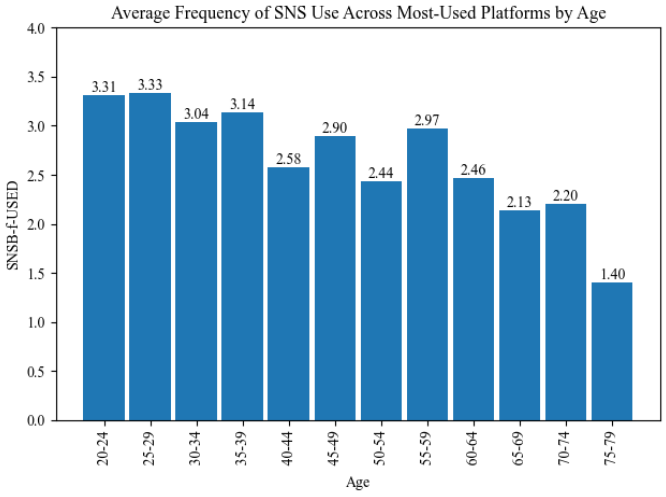

Figure 4.6. Average frequency of SNS use across most -used SNSs (SNS-f-USED) by age

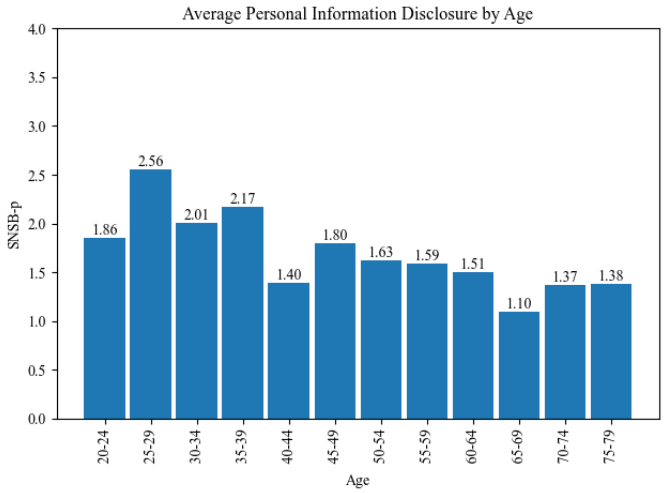

Figure 4.7. Average personal information disclosure (SNSB-p) by age

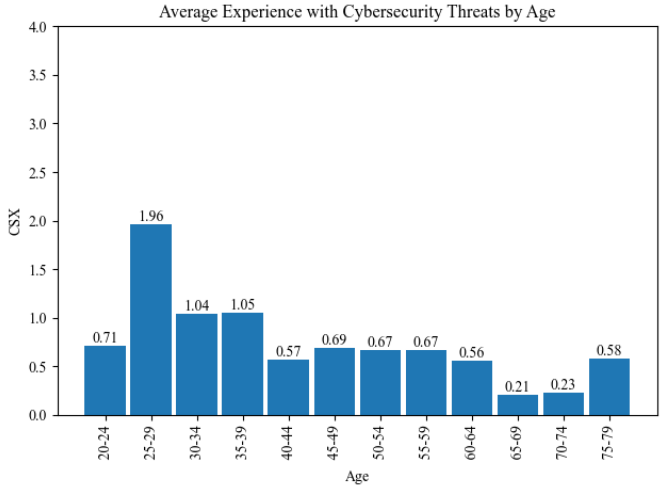

Figure 4.8. Average experience with cybersecurity threats (CSX) by age

Figure 4.5 and Figure 4.6 show clear inverse trends of their domains with respect to age, though there is a higher standard error among the 20-24 age group, a group which had a small sample of only 4 respondents. There is a clear overall relationship between decreasing overall use of social media and increasing age. As well as this, there appears to be a slightly decreasing overall trend in average personal information disclosure as age increases, as seen in Figure 4.7.

The elevated overall occurrence of experience with cybersecurity threats by younger age groups is especially noteworthy with respect to the overall infrequency of cybersecurity incidents. If we assume only a small percentage of the overall population has experienced one or more of the cybersecurity threats surveyed in this study with no influence by age, we would expect to see a direct correlation between the number of respondents in an age group with the frequency of cybersecurity incidents. Instead, the 25-29 demographic, with a smaller sample size than the 35-39 demographic, reported a much higher average threat experience. However, one limitation with respect to this conclusion regarding frequency of cybersecurity threats is the possibility of limited threat awareness. It may be the case that the overall occurrence of cybersecurity threat incidents is the same across age demographics, but older respondents are less aware of the occurrence of these threats when they are present.

I further re-tested the relationships between gender and other domains while excluding the single-respondent categories of “non-binary/third gender” and “prefer not to disclose”, as their 1-person sample sizes for their categories may have skewed the ANOVA results. A two-tailed t-test was utilized between the two remaining categories of male and female on the numeric domains. From these tests, the p values remained greater than .05 for all domains except for the MEPO factor of usage motivations ($p = .03$), where the mean was slightly higher in

female respondents than male ($\bar{x}$ = 1.72 versus $\bar{x}$ = 1.42). This affirms that gender had very little correlation overall with the domains of this survey.

4.1.4 *Scatter Plots of Hypothesized Correlations*

While not all hypothesized domain correlations were supported by evidence from the survey, visual analysis of these domain relationships is prudent to understanding the nature of the relationships themselves, linear or otherwise. Figure 4.9, Figure 4.10, Figure 4.11, Figure 4.12, Figure 4.13, Figure 4.14, Figure 4.15, Figure 4.16, and Figure 4.17 show the scatter plots of the different hypothesized domains, with dotted blue lines representing the lines of best fit. More opaque points on these figures represent places where there are multiple data points with the same values, as the value limitations of Likert-scaled averaging results in many instances identical data points across different responses. The captions of these figures indicate which tested hypothesis each corresponds to, and their *p* values.

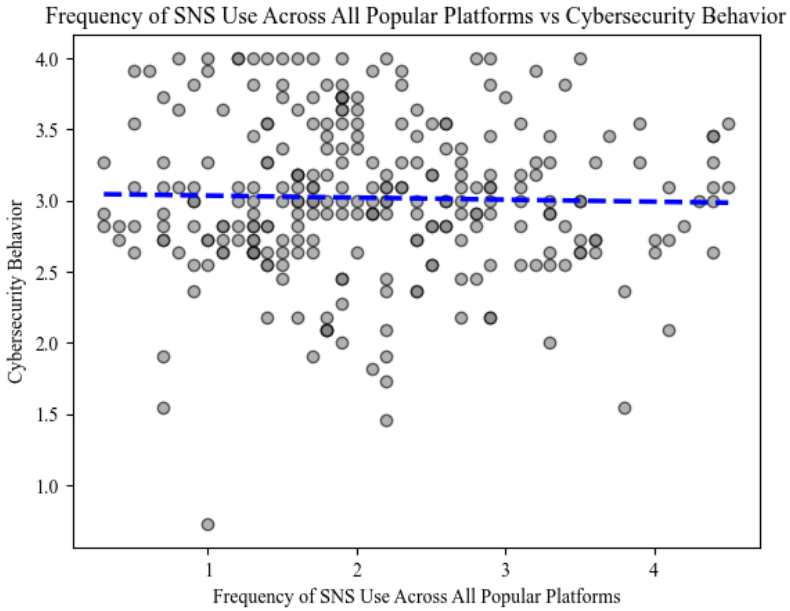

Figure 4.9. Frequency of SNS use across all popular platforms (SNSB-f-ALL) vs. cybersecurity behavior (CSB); H1, p = .70

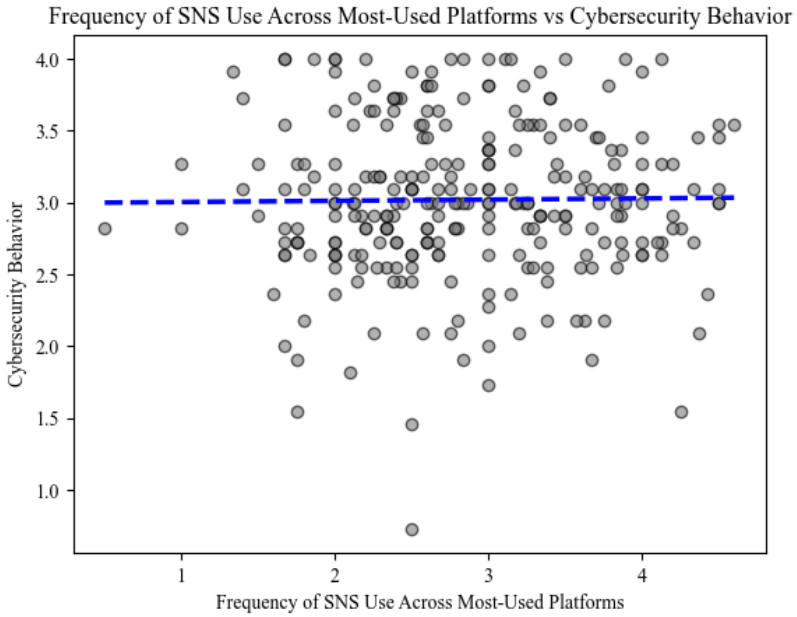

Figure 4.10. Frequency of SNS use across most-used platforms (SNSB-f-USED) vs. cybersecurity behavior (CSB); H1, p = .75

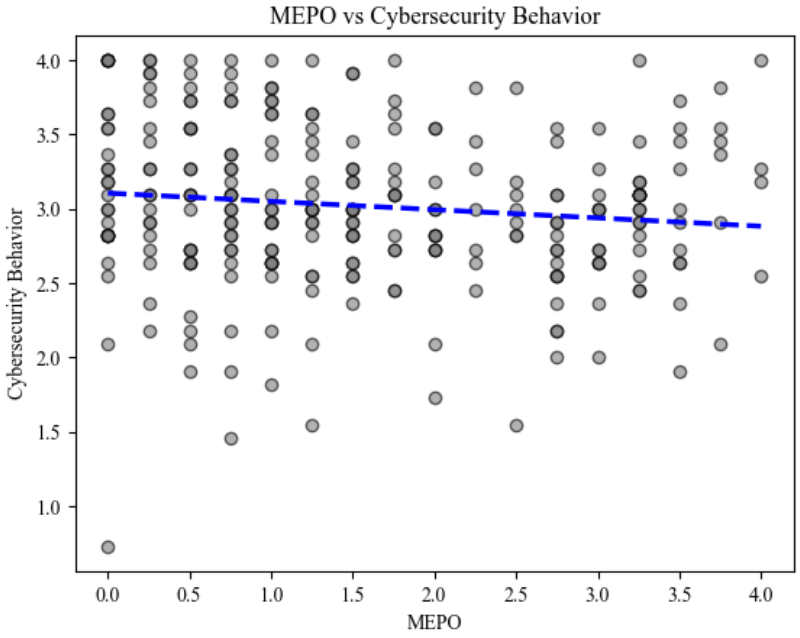

Figure 4.11. SNS usage for making, expressing, or presenting more popular oneself (MEPO) vs. cybersecurity behavior (CSB); H2, p = .045

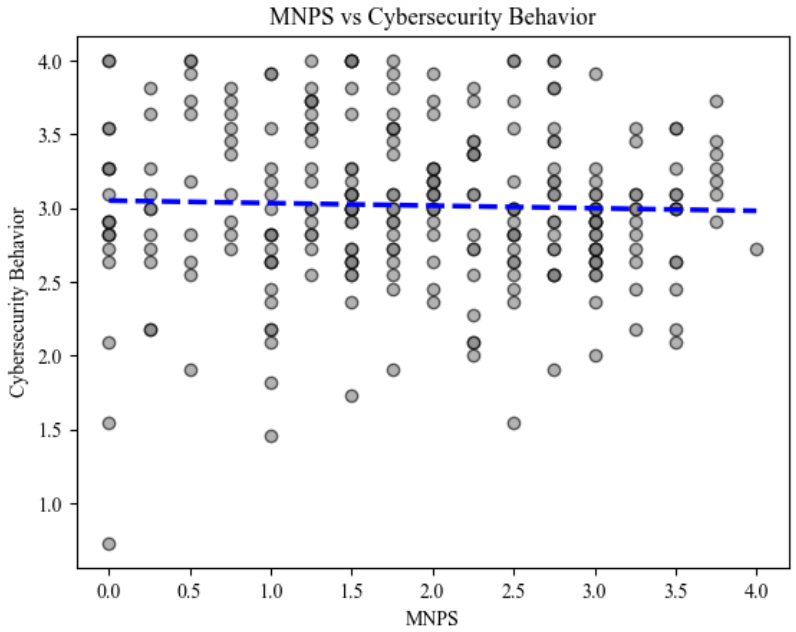

Figure 4.12. SNS usage for meeting new people and socializing (MNPS) vs. cybersecurity behavior (CSB); H2, p = .58

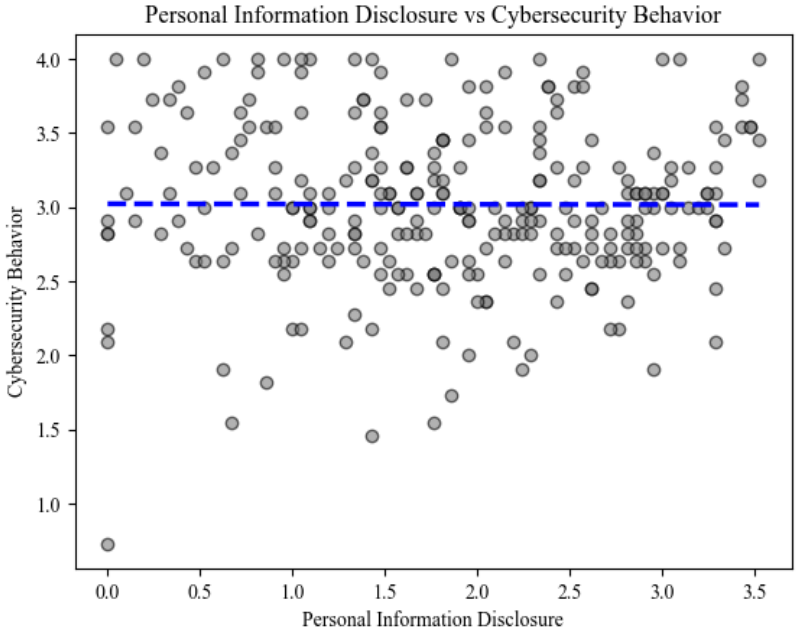

Figure 4.13. Personal information disclosure (SNSB-p) vs. cybersecurity behavior (CSB); H3, p = .95

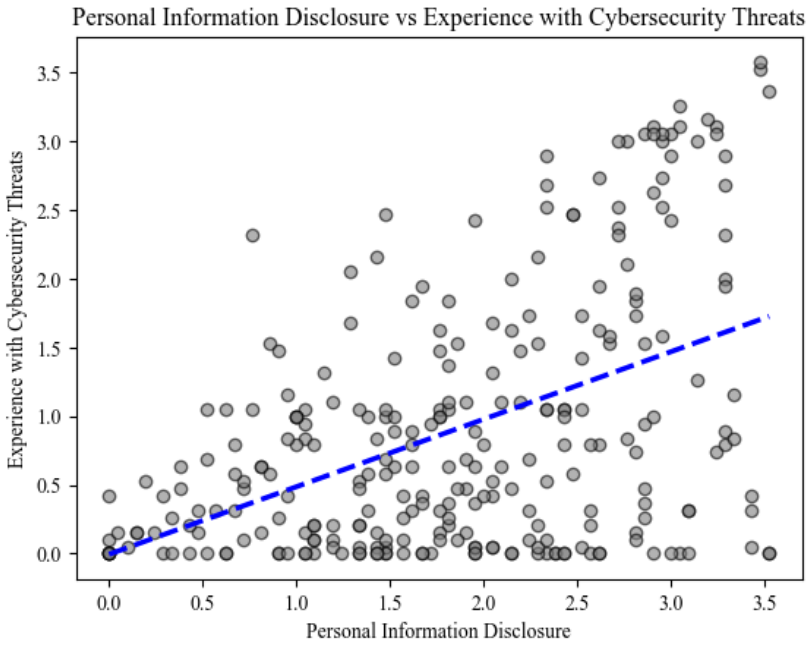

Figure 4.14. Personal information disclosure (SNSB-p) vs. experience with cybersecurity threats (CSX); H4, $p < .001$

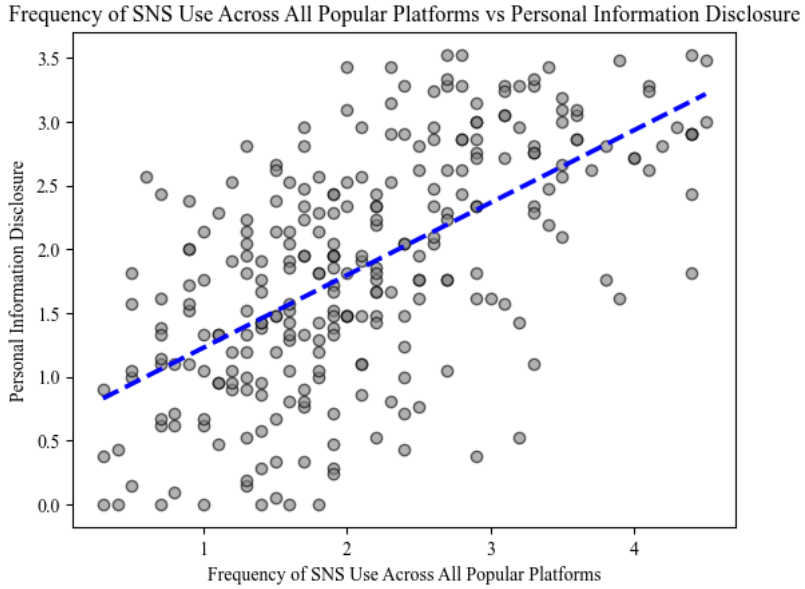

Figure 4.15. Frequency of SNS use across all popular platforms (SNSB-f-ALL) vs personal information disclosure (SNSB-p); H5, $p < .001$

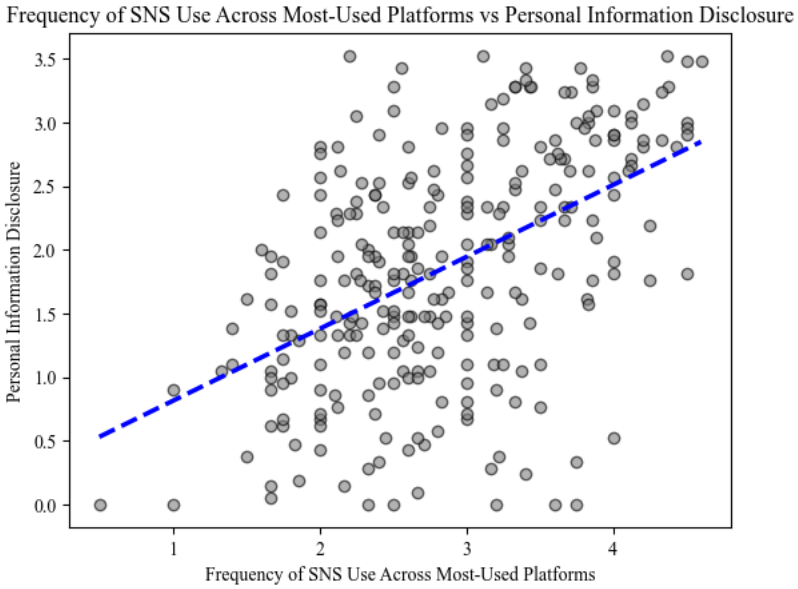

Figure 4.16. Frequency of SNS use across most-used platforms (SNSB-f-USED) vs. personal information disclosure (SNSB-p); H5, $p < .001$

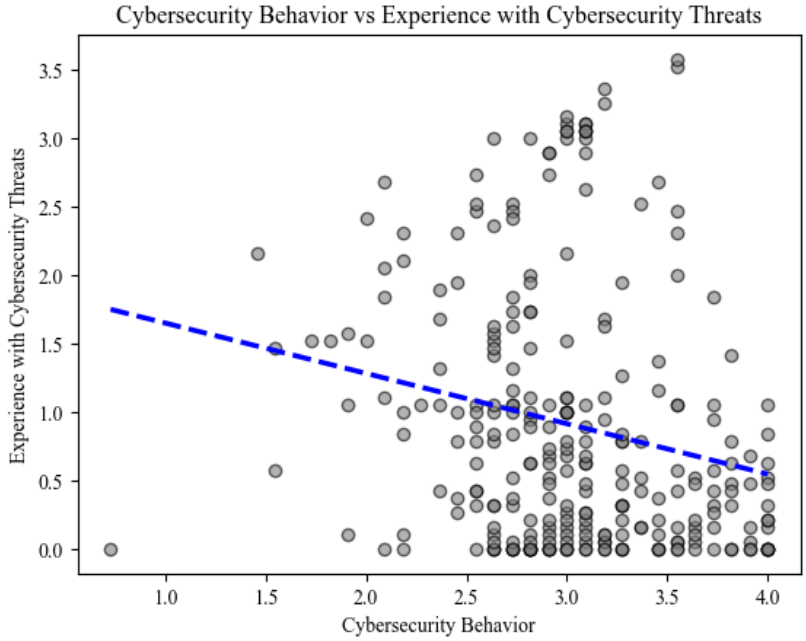

Figure 4.17. Cybersecurity behavior (CSB) vs. experience with cybersecurity threats (CSX); H6, $p < .001$

For the domains with correlations that were not statistically significant, as seen in Figure 4.9, Figure 4.10, Figure 4.12, and Figure 4.13, points were mostly scattered centered around the y-intercept of the line of best fit, with no clear increase or decrease in the domain on the y-axis as

the domain on the x-axis increased. Some subjects were outliers to the general clustering; for example, in Figure 4.10, one respondent occasionally used SNSs, but engaged in almost no cybersecurity practices

Conversely, in the domains with significant correlations, the relationships appeared to be mostly linear, albeit occasionally clustered towards certain modes. For example, in Figure 4.17, there is a slight downward trend between cybersecurity behavior and experience with cybersecurity threats, though most of the x points are on the higher end for cybersecurity behavior and the lower end for experience with cybersecurity threats (the median cybersecurity behavior was 3.0 on the Likert scale; in other words, an average of "Agree" for statements regarding cybersecurity practices). Notably, in Figure 4.14, increasing personal information disclosure did not seem to necessarily predict a higher frequency of experiences with cybersecurity threats, as many subjects with high personal information disclosure averages still had little or no experiences with these threats. Rather, increasing personal information disclosure appears to correlate to a higher range of occurrence of these threats, increasing the maximum while the overall minimum remains the same. With the maximum occurrence far exceeding the line of best fit's predictions on the highest ends of personal information disclosure, the relationship between these domains could possibly be exponential, rather than linear growth.

Figure 4.11 and Figure 4.12, which measure the relationships of usage motivation domains to cybersecurity behavior, appear to have discrete results by comparison to the other scatter plots because of the much more limited number of questions quantifying usage motivations, and thereby the more limited range of averages for these values.

These figures by no means represent the strongest linear relationships among the survey domains. For example, Figure 4.18 shows the correlation between the domains of SNSB-f-ALL

and ENT, where a clear direct linear relationship is evident. However, this correlation was not within the scope of the hypotheses of this study.

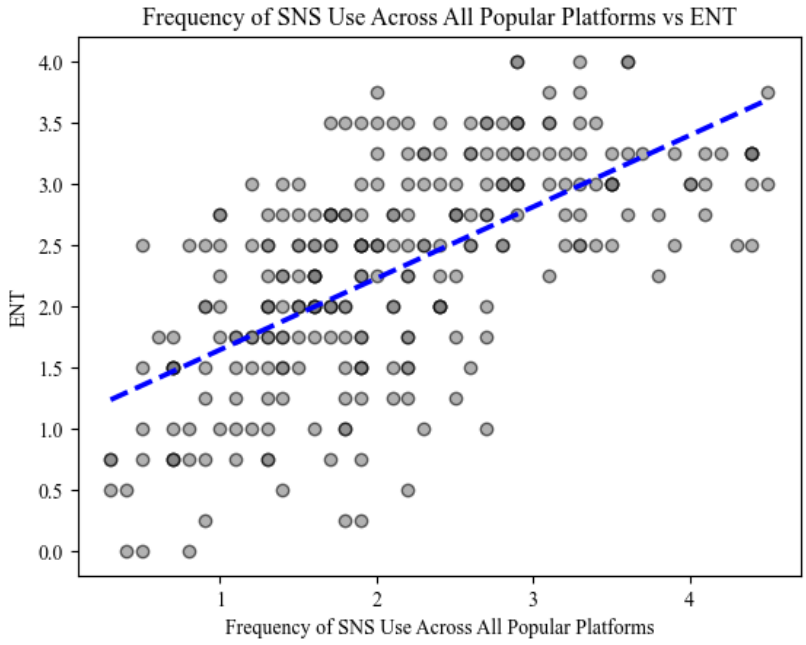

Figure 4.18. Frequency of SNS use across all popular platforms (SNSB-f-ALL) vs. SNS usage for entertainment (ENT); $p < .001$

4.2 Interview Data

The interviews with subjects on their social media behavior elicited more detailed feedback on the current state of social media security, the threats present on popular platforms, and how subjects perceived their own security or vulnerability. While originally, this study aimed for 30 interviews, sign-ups were frequent during the first phase of interviewing but slowed during the second phase. Therefore, only 17 interviews were able to be conducted in total.

4.2.1 *Respondent Demographics*

Interview subjects were mostly in the same age group (20-24), but varied across other demographics, as shown in table. Rather than education in terms of a degree, because the

majority of subjects were undergraduate students, the college level (freshman, sophomore, junior, senior, post-baccalaureate, or not a current student) was used to measure education. Table 4.4 shows the demographic distributions of interview subjects.

Table 4.4. Interview demographics

	Demographic	Number of Respondents	% of Respondents
Age (Years)	18-19	3	17.6%
	20-24	12	70.6%
	25-29	1	5.9%
	40-44	1	5.9%
Gender	Male	7	41.2%
	Female	8	47.1%
	Non-binary/third gender	1	5.9%
	Prefer not to say	1	5.9%
Ethnicity	Asian/Pacific Islander	10	58.8%
	White	2	11.8%
	Hispanic	2	11.8%
	Other/Multiracial	2	11.8%
	Prefer not to say	1	5.9%
College Level	Freshman	2	11.8%
	Sophomore	2	11.8%
	Junior	4	23.5%
	Senior	7	41.2%
	Post-baccalaureate	1	5.9%
	Not a current student	1	5.9%

4.2.2 *SNS Usage Patterns*

Subjects used SNSs for a variety of reasons, including those covered in the SMUAS domains. Some quoted examples of subjects' motivation by each domain are as follows:

- **MER:** "For me it's just to facilitate communications with my friends and family…"; "just to keep connected with like my old friends from high school and also like the

memories."; "I use Instagram for keeping up with people, learning about their lives and stuff."

- **MNPS**: "…specifically social media, like for specifically J-fashion. Because in person in the US, there's not a lot of people who do it... Whereas you can easily meet up with people online."
- **MEPO**: "…LinkedIn, obviously for networking purposes."
- **PT**: "I use YouTube to goof off. Waste time."; "Trying not to doomscroll is very hard. And unfortunately, it's great for procrastinating." "Doomscroll," here, refers to spending excessive time online scrolling through content that makes one feel sad, anxious, or angry (Merriam-Webster), while "goof off" is synonymous with wasting time.
- **ATMT**: "…if I need to finish group projects or something, I can just be like, hey, WhatsApp them or something like that."; "A lot of my schoolwork and club work is done through Discord."
- **ENT**: "There's a couple of web series, like video series that I like on TikTok."; "And then TikTok, I just to send like cute little videos to my friends."; "TikTok and Instagram are mainly just entertainment."
- **IAE**: "Instagram just for like information about like the school, like what events are happening."; "…I get to learn more about pop culture and what's going on, and just like, recent events as well."; "I use to see video game news, discuss about video games…"

Furthermore, one subject noted cultural pressure as a motivating factor for their SNS use: "I think we've constructed kind of like a culture where you don't keep up with what's going on if you're not on social media… I just feel like a lot goes on."

The most popular platforms currently used by interview subjects were Instagram (16 respondents) and TikTok (9 respondents). Other popular platforms (5 respondents each) include Discord, YouTube, Reddit, and Facebook. Four respondents reported having used Snapchat in the past but no longer using it; likewise, two respondents reported having formerly used X/Twitter but no longer using it, and one respondent reported as such for TikTok. Almost all subjects (16 respondents) reported using social media daily, and nearly half (8 respondents) reported using it multiple times or for multiple hours per day. A notable commonality between interview subjects was, in terms of their preference of SNS, seeing other platforms- particularly Facebook- as being for an older demographic. A subject that used Snapchat and Instagram noted those platforms were "…just more trendy among like people my age for those platforms versus Reddit and Facebook. That's a little bit for the older generation, I've noticed." One subject also noted gender demographics as a factor in SNS choice, in the context of group work: "Most of the time the groups, if I'm mostly with men or boys, they do Discord. So it's easier to do group work on that."

By contrast, many of the reasons subjects provided for avoiding particular platforms had to do with the user experience or content available on the platform. One subject noted they prefer not to use Instagram because "…it doesn't feel filtered to me. It doesn't feel clean enough for me to use." Another spoke against the "addicting" nature of the user experience: "…I stopped using TikTok because it got too addicting. So, I was like, okay, let me use Instagram more because it'll be less. But then they integrated Reels in it, so it's kind of like the same thing…" A subject that used both TikTok and Instagram noted an overall preference for TikTok over Instagram "mainly because of algorithm. I think it's a lot more anonymous." One subject simply preferred the humor of the content on TikTok over Instagram Reels. A subject who used both Reddit and X/Twitter

said they generally preferred Reddit, as they were "…not a fan of Twitter because of the toxicity there." For SNSs, "toxicity" refers to the presence of hateful or harmful online content.

4.2.3 *Cybersecurity Threats Encountered*

The most reported cybersecurity threats subjects came across on social media were phishing, false advertisement or scams, spam, and profile cloning. Table 4.5 shows the platforms that respondents reported encountering cybersecurity threats on, as well as the types of threats encountered by respondents. For SNSs where threats were encountered, the table shows the percent of the total interview respondents reporting a threat on that SNS ("% of Total Respondents") and the percent of the respondent selection who reported using that particular SNS which encountered a threat on that same SNS.

Table 4.5. Cybersecurity threats encountered, and SNS threats were encountered on

		Number of Respondents	**% of Total Respondents**	**% of Users**
SNS where threat encountered	Instagram	8	47.1%	50%
	Discord	3	17.6%	60%
	X/Twitter	2	11.8%	0%*
	Reddit	1	5.9%	20%
	Wakie	1	5.9%	100%
Type of threat encountered	Data breach	3	17.6%	N/A
	Spam	4	23.5%	
	Account hijacking	3	17.6%	
	Profile cloning	4	23.5%	
	Phishing	8	47.1%	
	False advertisement or scams	6	35.3%	
	Malware	3	17.6%	
	Cyberbullying	1	5.9%	

* The respondents who reported currently using X/Twitter did not actually report specific cybersecurity threats on X/Twitter; rather, two respondents who had reported formerly using X/Twitter but no longer actively used it both reported experiencing cybersecurity threats on this SNS.

Several subjects highlighted advertisements as a potential threat vector on social media platforms. As one subject describes, "…there will be a lot of ads. Like, if you click on this, you'll get like a brand new iPhone, and if you click the link, it will just, it'll corrupt your computer completely." However, some subjects also said that the threat vectors they had encountered were more often through private messages on the SNS. Regarding phishing or scam links, one subject noted, "anytime that does happen, it's always like, direct messages," and that of the three platforms they used (WhatsApp, TikTok, and Instagram), it always occurred on Instagram. Another subject recounted an instance where an attacker posed as two people over Discord messages, with a more elaborate scheme where one account mimicked the support team for a popular video game company, and the other mimicked a user that had purportedly accidentally reported the target's account with that company for a policy violation, in order to direct the victim to a fake support site and steal their credentials for that video game platform.

Echoing a theme of Shay et al.'s (2014) study on account hijacking, many subjects expressed that attackers took the form of compromised accounts of known acquaintances, to try and utilize the relationship of the account-holder for social engineering purposes. Many subjects refer to these compromised accounts as "bot accounts", suggesting an assumption that these compromises are automated; however, other subjects use this term to refer to accounts created through profile cloning. On account hijacking, one subject recounted:

> *"…a few of my friends, I think they, on their stories, I think they somehow got hacked when they tried to… click on a link or something… I think I tried to ask*

some of their other friends if they got hacked or somewhere. They said they got, they did… even your friends can be, can get hacked and they try to like persuade you to like, click on a link, so your account can get hacked."

Many subjects also recounted instances of profile cloning, as described by Bilge et al. (2009). In an incident of account fraud involving a subject's friend:

"There was this fake account of one of my friends, she reached out for my phone number and then she was asking me for money. I'm like, this seems kind of off, so I checked the account and I checked the, like her actual story, because it was through Instagram, and someone made like a fake account. Like a bot account trying to get people's information."

Another subject echoed the sentiment of the prevalence of bot accounts, noting an interesting change: "…there's always constantly like bots making Instagram accounts. So, people like duplicates changing like a little thing like a last name." It may be the case that duplicated profiles are altered in this way to avoid detection by content or account moderators on SNSs. One subject described the appearance of these bot accounts in more detail:

"So for bots… I've seen a lot of those because I can tell those pictures are taken from Pinterest, and if you press on it you can tell that it's like a new account, and the account just says like, 'oh, old account got hacked' and stuff like that… I've seen a lot of those, like once a week at least."

Different subjects reported encountering these bots more or less frequently, with one reporting that, "You're going to get like 30 bots in a week probably," on Twitter and Discord.

Likewise, some of the subjects whose accounts had been hacked, or who had been the victims of profile cloning, noticed their accounts had been used for social engineering purposes. One subject noted, "someone made a duplicate account of mine and used my same profile picture and messaged people." Another subject described an incident where their Instagram had been hacked, and the hacked account was reaching out to their contacts with advertisements and requesting money. Also taking place on Instagram, one subject described the details of an incident of profile cloning originating from someone they were acquainted with:

> *"…there's been one incident where someone I knew, actually, I couldn't trace it back to them, but they admitted to it, that they put my profile into some sort of website. But it was also, it was like a catfishing porn site, basically… it was basically an Instagram profile with, like, my bio, my face, and screenshots of my posts, except there was a link in the biography with, you know, to the site where it was just immediately graphic. And it was following, basically, my entire following list… people were reaching out to me. And they were like, hey, I think someone's catfishing you. But a lot of people clicked on the link, too."*

One subject, a digital artist, shed light on an additional risk factor: exchange of financial information for the purposes of digitally contracted work. The subject recounted:

> *"…on my public Instagram art page, I'd have 'oh, and commissions are open, DM for more information'. When I was conversing with the person, I was saying like, yeah, I would love to do this project. We were trying to figure out a form of payment. They had a link to a website for me to enter in my information, and I entered in the information that I was comfortable with… but I didn't want to give out my phone number, and especially not my social security number, especially, you know, because identity fraud. So I was like, 'Hey, I'm not comfortable with this.' They kept on pushing, so I'd push back, like, 'Hey I'm not gonna do this,' and I blocked them."*

4.2.4 *Privacy and Security Behaviors*

In terms of digital privacy, some subjects had concerns about the personal data the SNSs they used collected on them, beyond their own information disclosure. One subject noted:

> *"Instagram and TikTok have these… recommended things based on your contact information. And even if you opt out, they'll still be like, 'oh, hey, you might know this person,' and it's like, someone I haven't seen since fifth grade… I don't even have their phone number. I don't follow them anywhere else. It's a little creepy."*

Another subject who used Facebook voiced concerns about Facebook's data collection practices: "Facebook, I try not to share hardly anything, unless it's through iMessage… But even still, I know that Facebook has eyes on the wall, if you will. They're hearing and watching us."

A few subjects had separate accounts, a public-facing account where they disclosed less information and a private account where they disclosed more. However, these private accounts were not without their own risks: one subject recounted a friend who had posted selfies on their

private account had the photos leaked after a hack, and they became the target of persistent cyberbullying.

Finally, in terms of security practices, several subjects used 2-factor authentication (47%) or different passwords (35%) to protect their accounts. However, few utilized any more security measures than this, including subjects who had experienced cybersecurity threats before. Some subjects also listed privacy practices, such as using a VPN, ad/tracker blockers, or fake names online, as security measures. This suggests that subjects overestimate the effectiveness of data obfuscation as a security measure, and that the perceived risks posed by cybersecurity threats over SNSs are insufficient motive for subjects to take robust action for securing their accounts.

Chapter 5. CONCLUSION AND FUTURE WORK

This chapter summarizes the findings of this study, including which hypotheses were supported or not supported, and providing answers to the research questions of the study. The limitations of the study are discussed, as well as opportunities for future research to build on the findings in this study.

5.1 Revisiting Hypotheses and Research Questions

From the survey results, there were many statistically significant correlations across domains, though not all correlations were strong enough to suggest data unusual for the model. Table 5.1 shows the results with relation to the hypotheses involved in this research. The hypotheses in the table are listed by the codified domains; full explanations of the hypotheses can be found in Chapter 1.2.

Evidence from the survey supports hypotheses H2(a), as the usage motivation factor of MEPO had a statistically significant negative correlation with cybersecurity behavior. Additionally, the survey data supports hypotheses H4, as there was a statistically significant positive correlation between personal information disclosure and subjects' experience with cybersecurity threats. H5 was supported as well due to the significant positive correlations between both frequency of usage of all social media platforms surveyed and those selected as the most frequently used platforms by respondents to personal information disclosure (refer to Chapter 4.1.2 for information on the split of the SNSB-f domain into these subdomains). Finally, H6 was supported as evidenced by a significant negative correlation between good cybersecurity behavior and past experience with cybersecurity threats.

Table 5.1. Conclusions of study hypotheses

Hypothesis	**Variable Relation**	**Result**
H1	SNSB-f ↔ CSB (+)	Not Supported (p = .70 for SNSB-f-ALL, p = .75 for SNSB-f-USED).
H2	(a) MEPO ↔ CSB (-) (b) MNPS ↔ CSB (-)	(a) Supported (p = .045) (b) Not supported (p = .58)
H3	SNSB-p ↔ CSB (-)	Not Supported (p = .95)
H4	SNSB-p ↔ CSX (+)	Supported (p < .001)
H5	SNSB-f ↔ SNSB-p (+)	Supported (p < .001 for SNSB-f-ALL and SNSB-f-USED).
H6	CSB ↔ CSX (-)	Supported (p < .001)

Based on the data, this study concludes upon the initial research questions as such:

RQ1: What are the connections between usage patterns of social networking sites (SNSs) and cybersecurity behaviors?

Cybersecurity behaviors are, in general, not strongly correlated with usage patterns of SNSs. This includes variations in frequency of use, types of usage, and personal information disclosure on SNSs. However, usage of SNSs for the purpose of making, expressing, or presenting more popular oneself (MEPO) is associated with slightly poorer cybersecurity behavior.

RQ2: Is there a relationship between personal information disclosure on SNSs and cybersecurity threats?

Increased personal information disclosure correlates with increased experience of cybersecurity threats. This relationship is also supported by other intermediary connections: increased use of SNSs related to increased experience of cybersecurity threats, and increased usage of SNSs also related to increased personal information disclosure.

5.2 Study Limitations

As mentioned in Chapter 3, potential biases arise from the particular means of eliciting responses with regard to past cybersecurity experiences. The first is a potential underreporting bias from populations who may have experienced cybersecurity threats in the past but were not aware of them. This is, in part, mitigated by the fact that experience questions did not include domain-specific language on cybersecurity threats that subjects may not be familiar with, but rather clear colloquial descriptions of the events in question. However, there is still the chance that some subjects may have been unaware of incidents that occurred simply because the nature of the incident did not produce clear red flags in context, such as a stealthy account hijacking or data breach that the subject did not hear about.

Additionally, as incidence of cybersecurity threats may not necessarily stem from a threat vector originating from the SNSs used by subjects, let alone from the subjects' usage behavior, there may be an overall overreporting bias in the domain of cybersecurity experiences by those who encountered threats originating outside of SNSs. This is not to say that the correlation found between SNS usage frequency and cybersecurity experience is thereby invalid; if we assumed that all the cybersecurity threats that subjects encountered originated from beyond social media, the data would be highly unusual for such a correlation. This is particularly true considering many of the threats surveyed are specific to SNSs, such as cyberstalking or a malicious actor posting unsolicited harmful content about the victim. It is not impossible that such a correlation

originates from other factors altogether, though, such as overall computer or phone usage potentially correlating to both SNS usage and cybersecurity threat experience.

Self-reported cybersecurity behavior, experiences, and usage patterns, in general, may suffer from subjects' subjective perspectives on these factors, with limitations in recall or selective reporting. A long-term study could be designed to objectively capture these factors, such as measuring subjects' actual day-to-day usage of SNSs and capturing alerts from antiviruses or notices of data breaches relating to subjects' SNSs of choice. However, such technology is limited in the scope of what factors it could measure; individual incidents of account hijacking or online stalking or harassment would likely still have to be self-reported by subjects.

The subjects of the interviews were not a truly representative sample of the general population. Interview subjects were part of a convenience sample of voluntary self-registration and generally were university students aged 19-24. Furthermore, demographic bias in survey responses may have been induced by the method of distribution. MTurk respondents were limited to users in the U.S., and they would need to have ready access to the internet for responding to surveys. These limitations could reduce the likelihood that lower-income individuals, who may not have ready internet access, could respond to the survey. In practice, while there was a fairly even split among gender demographics, the subjects of the survey were overwhelmingly white and college-educated, factors which may contribute to a cultural bias in the responses to the survey. For example, white respondents might encounter less racially-targeted online harassment than people of color, leading to a slightly lessened overall experience with digital threats. That said, the lack of significant variance between the domains of gender and

race and other survey domains does not suggest that these demographic biases swayed the findings of the survey significantly.

The scale used to quantify the usage motivations for social media is not an objective predictor of social media behavior, but rather a model of behavioral intention. An experimental study would be necessary to qualify whether the motivation factors have a causal relationship to actual usage behavior on SNSs. Furthermore, while Horzum's (2016) FAU scale was validated through confirmatory factor analysis, its original intention was to measure the usage motivations for Facebook in particular. Other validated scales for measuring social media usage exist, covering a variety of platforms from WeChat (Gan & Li, 2018) and SNSs in general (Ifinedo, 2016). In Pertegal et al.'s (2019) review of usage motivation scales, they highlight several additional factors of SNS usage motivations used in scales beyond Horzum's, including curiosity, group influence, and social inclusion- external social pressures which can play an important role in determining how people use an inherently social technology. A future replication of this study could consider utilizing the SMU-SNS scale developed by Pertegal et al. in their 2019 review, as it is a more recently-developed scale based on the common qualities of many others, and has also been tested and validated.

5.3 Future Research

The connections between cybersecurity threat experience and personal information disclosure identified here opens an opportunity for investigation into potential causal effects. For instance, an experimental study could quantify whether subjects playing the role of cyber-attackers are able to craft more effective social engineering attacks using the profiles of users who disclose more personal information versus those who disclose less. While other existing research has

shown that using personal information available on SNSs can make for more effective cyberattacks (Jagatic et al., 2007), these personalized attacks assume that the information with which they are crafted is readily available; in the case of subjects who do not disclose much, if any, personal information, there might be significant differences in an attackers' ability to craft or target such attacks.

Future studies will also find it prudent to objectively measure factors that were subjectively measured through voluntary self-reporting in this study. For example, measuring the actual social media behaviors of subjects could provide a more accurate measure of behavior, and avoid factors such as recall bias, response and non-response bias, and social desirability bias. Another factor that could be prudent to quantify is social media usage over the long term, as this study only captures a snapshot of the landscape of SNSs in 2025. As noted in the interviews of this study, many subjects who formerly used another platform (in this case, Snapchat) moved away from it in favor of other platforms over time. Even as overall SNS usage continues to climb around the world (Statista, 2024), the SNS preferences of people can shift over time from factors such as UI changes, Terms of Service, or ownership changes, or as alternative platforms become available (de Luna, 2022; Garrahan, 2009; Oshin, 2023).

As a minor finding, the relationship between gender and cybersecurity awareness and behavior has been a point of contention across prior studies, and this study is but one of many now which found no significant correlation between gender and cybersecurity behavior (Anwar et al., 2017; Branley-Bell et al., 2022; Vance et al., 2012). A decreasing divide could be indicative of a broader cultural shift of closing the cybersecurity knowledge gap between genders.

Finally, with the particular profiles of cyberattacks highlighted by interview respondents in this study, this thesis provides insights into the particular experience of users of SNSs with digital threats, and how users recognize (or fail to recognize) malicious actors. Interviews showcase the different forms attacks such as phishing, profile cloning, and false advertisement or scams encountered on social networking sites. Subjects' accounts reveal some of the specific ways in which these threats proliferate and target users of SNSs, making clear that subjects are aware of many of the threats present on SNSs, though this may not necessarily lead to more secure behavior. These insights can help shape how we understand the user experience of social media with relation to digital security, and how users navigate the landscape of digital threats.

BIBLIOGRAPHY

Abokhodair, N., Yoo, D., & McDonald, D. W. (2015). Dissecting a Social Botnet: Growth, Content and Influence in Twitter. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 839–851. https://doi.org/10.1145/2675133.2675208

Aboulnasr, K., Tran, G. A., & Park, T. (2022). Personal information disclosure on social networking sites. *Psychology & Marketing*, *39*(2), 294–308. https://doi.org/10.1002/mar.21595

Adjei, J. K., Adams, S., Mensah, I. K., Tobbin, P. E., & Odei-Appiah, S. (2020). Digital Identity Management on Social Media: Exploring the Factors That Influence Personal Information Disclosure on Social Media. *Sustainability*, *12*(23), Article 23. https://doi.org/10.3390/su12239994

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12. https://doi.org/10.5897/JIIS2015.0089

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Alqurashi, D. R., Alghizzawi, M., & Al-Hadrami, A. (2024). The Role of Social Media in Raising Awareness of Cybersecurity Risks. In B. Alareeni & I. Elgedawy (Eds.), *Opportunities and Risks in AI for Business Development: Volume 1* (pp. 365–376). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65203-5_33

Amichai-Hamburger, Y., & Vinitzky, G. (2010). Social network use and personality. *Computers in Human Behavior*, *26*(6), 1289–1295. https://doi.org/10.1016/j.chb.2010.03.018

Angulo, J., & Ortlieb, M. (2015). *{"WTH..!?!"} Experiences, Reactions, and Expectations Related to Online Privacy Panic Situations*. 19–38. https://www.usenix.org/conference/soups2015/proceedings/presentation/angulo

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Baker, K. (2024). *Types of Cyberattacks*. CrowdStrike.Com. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

Balakrishnan, J., & Griffiths, M. D. (2017). Social media addiction: What is the role of content in YouTube? *Journal of Behavioral Addictions*, *6*(3), 364–377. https://doi.org/10.1556/2006.6.2017.058

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People*, *28*(3), 426–441. https://doi.org/10.1108/ITP-10-2014-0232

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to us: Automated identity theft attacks on social networks. *Proceedings of the 18th International Conference on World Wide Web*, 551–560. https://doi.org/10.1145/1526709.1526784

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2013). Design and analysis of a social botnet. *Computer Networks*, *57*(2), 556–578. https://doi.org/10.1016/j.comnet.2012.06.006

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies*, *2022*(1), 2693080. https://doi.org/10.1155/2022/2693080

Brenner, S. W. (2007). 25—History of computer crime. In K. D. Leeuw & J. Bergstra (Eds.), *The History of Information Security* (pp. 705–721). Elsevier Science B.V. https://doi.org/10.1016/B978-044451608-4/50026-2

Brooks, S. (2015). Does personal social media usage affect efficiency and well-being? *Computers in Human Behavior*, *46*, 26–37. https://doi.org/10.1016/j.chb.2014.12.053

Brown, G., Howe, T., Ihbe, M., Prakash, A., & Borders, K. (2008). Social networks and context-aware spam. *Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*, 403–412. https://doi.org/10.1145/1460563.1460628

Budimir, S., Fontaine, J. R. J., & Roesch, E. B. (2021). Emotional Experiences of Cybersecurity Breach Victims. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 612–616. https://doi.org/10.1089/cyber.2020.0525

Cao, A., Lindo, J. M., & Zhong, J. (2023). Can social media rhetoric incite hate incidents? Evidence from Trump's "Chinese Virus" tweets. *Journal of Urban Economics*, *137*, 103590. https://doi.org/10.1016/j.jue.2023.103590

Casale, S., & Fioravanti, G. (2018). Why narcissists are at risk for developing Facebook addiction: The need to be admired and the need to belong. *Addictive Behaviors*, *76*, 312–318. https://doi.org/10.1016/j.addbeh.2017.08.038

Chawki, M. (2005). A Critical Look at the Regulation of Cybercrime. *IV (4) The ICFAI Journal of Cyberlaw*.

https://scholar.googleusercontent.com/scholar?q=cache:ShwTMVMRb78J:scholar.google.com/+A+critical+look+at+the+regulation+of+cybercrime.&hl=en&as_sdt=0,48

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, *12*(3), 341–345. https://doi.org/10.1089/cpb.2008.0226

Cohen-Almagor, R. (2022). Bullying, Cyberbullying, and Hate Speech. *Int. J. Technoethics*, *13*(1), 1–17. https://doi.org/10.4018/IJT.291552

Council of Europe. (2018, May 18). *128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018) Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016807c65bf%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

Council of Europe. (2019, January 25). *Consultative Committee of The Convention for The Protection of Individuals With Regard to Automatic Processing of Personal Data*. https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

DataReportal. (2025, February). *Biggest social media platforms by users 2025*. Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

de Luna, E. (2022, February 25). *The inside story of how Tumblr lost its way*. Mashable. https://mashable.com/article/how-tumblr-lost-its-way

Delio, M. (2001, February 6). The Greatest Hacks of All Time. *Wired*. https://www.wired.com/2001/02/the-greatest-hacks-of-all-time/

Deng, S., Liu, Y., Li, H., & Hu, F. (2013). How Does Personality Matter? An Investigation of the Impact of Extraversion on Individuals' SNS Use. *Cyberpsychology, Behavior, and Social Networking*, *16*(8), 575–581. https://doi.org/10.1089/cyber.2012.0383

Douceur, J. R. (2002). The Sybil Attack. In P. Druschel, F. Kaashoek, & A. Rowstron (Eds.), *Peer-to-Peer Systems* (pp. 251–260). Springer. https://doi.org/10.1007/3-540-45748-8_24

Dupuis, M., Crossler, R. E., & Endicott-Popovsky, B. (2012, January). *The Information Security Behavior of Home Users: Exploring a User's Risk Tolerance and Past Experiences in the Context of Backing Up Information*. The Dewald Roode Information Security Workshop, Provo, Utah. https://www.researchgate.net/publication/305778441_The_Information_Security_Behavior_of_Home_Users_Exploring_a_User's_Risk_Tolerance_and_Past_Experiences_in_the_Context_of_Backing_Up_Information

Ebube, S. (2023). The Role of Legal Frameworks in Addressing Online Hate Speech and Cyberbullying. *American Journal of Law and Policy*, *1*(1), Article 1.

Facebook. (2014, February 24). *Facebook to Acquire WhatsApp*. Facebook Newsroom. https://web.archive.org/web/20140224184730/http://newsroom.fb.com/News/805/Facebook-to-Acquire-WhatsApp

Faverio, M., & Sidoti, O. (2024, December 12). Teens, Social Media and Technology 2024. *Pew Research Center*. https://www.pewresearch.org/internet/2024/12/12/teens-social-media-and-technology-2024/

Federal Bureau of Investigation. (2025). *FBI Releases Annual Internet Crime Report* [Press Release]. FBI. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report

Flynn, S., Noone, C., & Sarma, K. M. (2018). An exploration of the link between adult attachment and problematic Facebook use. *BMC Psychology*, *6*(1), 34. https://doi.org/10.1186/s40359-018-0245-0

Fowler, G. (2012, October 4). *Facebook Tops Billion-User Mark*. WSJ.Com. https://web.archive.org/web/20121004160522/http://online.wsj.com/article/SB10000872396390443635404578036164027386112.html

Fraud and Related Activity in Connection with Computers, 18 U.S. Code § 1030 (1986). https://www.law.cornell.edu/uscode/text/18/1030

Fung, B. (2014, January 1). A Snapchat security breach affects 4.6 million users. Did Snapchat drag its feet on a fix? *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/

Gan, C., & Li, H. (2018). Understanding the effects of gratifications on the continuance intention to use WeChat in China: A perspective on uses and gratifications. *Computers in Human Behavior*, *78*, 306–315. https://doi.org/10.1016/j.chb.2017.10.003

Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security Issues in Online Social Networks. *IEEE Internet Computing*, *15*(4), 56–63. https://doi.org/10.1109/MIC.2011.50

Gao, W., Liu, Z., & Li, J. (2017). How does social presence influence SNS addiction? A belongingness theory perspective. *Computers in Human Behavior*, *77*, 347–355. https://doi.org/10.1016/j.chb.2017.09.002

Garrahan, M. (2009, December 4). *The rise and fall of MySpace*. Financial Times. https://www.ft.com/content/fd9ffd9c-dee5-11de-adff-00144feab49a

GDPR.eu. (2018, November 7). *What is GDPR, the EU's new data protection law?* GDPR.Eu. https://gdpr.eu/what-is-gdpr/

General Assembly Resolution 2200A (XXI) (1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Goodin, D. (2018, October 8). *Google+ shutting down after data leak affecting 500,000 users*. Ars Technica. https://arstechnica.com/tech-policy/2018/10/google-exposed-non-public-data-for-500k-users-then-kept-it-quiet/

Gosling, S. D., Augustine, A. A., Vazire, S., Holtzman, N., & Gaddis, S. (2011). Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information. *Cyberpsychology, Behavior, and Social Networking*, *14*(9), 483–488. https://doi.org/10.1089/cyber.2010.0087

Gottfried, J. (2024, January 31). Americans' Social Media Use. *Pew Research Center*. https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/

Greenwood, D. N. (2013). Fame, Facebook, and Twitter: How attitudes about fame predict frequency and nature of social media use. *Psychology of Popular Media Culture*, *2*(4), 222–236. https://doi.org/10.1037/ppm0000013

Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010). @spam: The underground on 140 characters or less. *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 27–37. https://doi.org/10.1145/1866307.1866311

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80. https://doi.org/10.1145/1102199.1102214

Hall, M. (2025, April 30). *Facebook*. Britannica Money. https://www.britannica.com/money/Facebook

Hart, J., Nailling, E., Bizer, G. Y., & Collins, C. K. (2015). Attachment theory as a framework for explaining engagement with Facebook. *Personality and Individual Differences*, *77*, 33–40. https://doi.org/10.1016/j.paid.2014.12.016

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171–180. https://doi.org/10.1108/13287261211232180

Hellemans, J., Willems, K., & Brengman, M. (2020). Daily Active Users of Social Network Sites: Facebook, Twitter, and Instagram-Use Compared to General Social Network Site Use. In F. J. Martínez-López & S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce* (pp. 194–202). Springer International Publishing. https://doi.org/10.1007/978-3-030-47595-6_24

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hoeschele, M., & Rogers, M. (2005). Detecting Social Engineering. In M. Pollitt & S. Shenoi (Eds.), *Advances in Digital Forensics* (pp. 67–77). Springer US. https://doi.org/10.1007/0-387-31163-7_6

Horzum, M. B. (2016). Examining the relationship to gender and personality on the purpose of Facebook usage of Turkish university students. *Computers in Human Behavior*, *64*, 319–328. https://doi.org/10.1016/j.chb.2016.06.010

Hoy, M. G., & Milne, G. (2010). Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, *10*(2), 28–45. https://doi.org/10.1080/15252019.2010.10722168

Hughes, D. J., Rowe, M., Batey, M., & Lee, A. (2012). A tale of two sites: Twitter vs. Facebook and the personality predictors of social media usage. *Computers in Human Behavior*, *28*(2), 561–569. https://doi.org/10.1016/j.chb.2011.11.001

Identify Theft Resource Center. (2023). *ITRC Annual Data Breach Report*. ITRC. https://www.idtheftcenter.org/publication/2023-data-breach-report/

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Ifinedo, P. (2016). Applying uses and gratifications theory and social influence processes to understand students' pervasive adoption of social networking sites: Perspectives from the Americas. *International Journal of Information Management*, *36*(2), 192–206. https://doi.org/10.1016/j.ijinfomgt.2015.11.007

Ion, I., Reeder, R., & Consolvo, S. (2015). *{"...No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices*. 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

Isaac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Accounts of 50 Million Users. *The New York Times*. https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Janz, N. K., & Becker, M. H. (1984). The Health Belief Model: A Decade Later. *Health Education Quarterly*, *11*(1), 1–47. https://doi.org/10.1177/109019818401100101

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Jones, M. (2025). History of Social Media: The Invention of Online Networking. *History Cooperative*. https://historycooperative.org/the-history-of-social-media/

Joseph, J. (2025, January 28). *Meta AI Can Now "Remember" What You Tell It Across Apps*. PCMAG. https://www.pcmag.com/news/meta-ai-can-now-remember-what-you-tell-it-across-apps

Junco, R. (2012). The relationship between frequency of Facebook use, participation in Facebook activities, and student engagement. *Computers & Education*, *58*(1), 162–171. https://doi.org/10.1016/j.compedu.2011.08.004

Junco, R., Heiberger, G., & Loken, E. (2011). The effect of Twitter on college student engagement and grades. *Journal of Computer Assisted Learning*, *27*(2), 119–132. https://doi.org/10.1111/j.1365-2729.2010.00387.x

Kircaburun, K., Alhabash, S., Tosuntaş, Ş. B., & Griffiths, M. D. (2020). 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. *International Journal of Mental Health and Addiction*, *18*(3), 525–547. https://doi.org/10.1007/s11469-018-9940-6

Koehorst, R. H. G. (2013, August 28). *Personal information disclosure on online social networks: An empirical study on the predictors of adolescences' disclosure of personal*

information on Facebook. [Info:eu-repo/semantics/masterThesis]. University of Twente. https://essay.utwente.nl/63797/

Kuss, D. J., & Griffiths, M. D. (2011). Online Social Networking and Addiction—A Review of the Psychological Literature. *International Journal of Environmental Research and Public Health*, *8*(9), Article 9. https://doi.org/10.3390/ijerph8093528

Kuss, D. J., & Griffiths, M. D. (2017). Social Networking Sites and Addiction: Ten Lessons Learned. *International Journal of Environmental Research and Public Health*, *14*(3), Article 3. https://doi.org/10.3390/ijerph14030311

Lansley, M., Kapetanakis, S., & Polatidis, N. (2020). SEADer++ v2: Detecting Social Engineering Attacks using Natural Language Processing and Machine Learning. *2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*, 1–6. https://doi.org/10.1109/INISTA49547.2020.9194623

Laric, M. V., Pitta, D. A., & Katsanis, L. P. (2009). Consumer concerns for healthcare information privacy: A comparison of US and Canadian perspectives. *Research in Healthcare Financial Management*, *12*(1), 93–111.

Lau, W. W. F. (2017). Effects of social media usage and social media multitasking on the academic performance of university students. *Computers in Human Behavior*, *68*, 286–291. https://doi.org/10.1016/j.chb.2016.11.043

Lee, D., Larose ,Robert, & and Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454. https://doi.org/10.1080/01449290600879344

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International*

Journal of Information Management, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, L., Xu, L., He, W., Chen, Y., & Chen, H. (2016). Cyber Security Awareness and Its Impact on Employee's Behavior. In A. M. Tjoa, L. D. Xu, M. Raffai, & N. M. Novak (Eds.), *Research and Practical Issues of Enterprise Information Systems* (pp. 103–111). Springer International Publishing. https://doi.org/10.1007/978-3-319-49944-4_8

Li, X. (2016). *Regulation Of Cyber Space: An Analysis Of Chinese Law On Cyber Crime*. https://doi.org/10.5281/ZENODO.56225

Lidsky, L. B. (2011). *Incendiary Speech and Social Media* (SSRN Scholarly Paper No. 1952577). Social Science Research Network. https://papers.ssrn.com/abstract=1952577

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Maulana, M., & Julyazti, N. F. (2025). Regulatory Gaps in Social Media During Humanitarian Conflicts: Facebook and Rohingya Genocide. *Jurnal Economic Resource*, *8*(1), Article 1. https://doi.org/10.57178/jer.v8i1.1183

Mitnick, K. D., & Simon, W. L. (2003). *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons.

Molok, N. N. A., Ali, A. Md., Talib, S., & Mahmud, M. (2014). Information security awareness through the use of social media. *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, 1–6. https://doi.org/10.1109/ICT4M.2014.7020668

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, *24*(1), 10–28. https://doi.org/10.1108/JMLC-11-2019-0092

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Office of Public Affairs. (2019, May 9). *Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People*. U.S. Department of Justice Archives. https://www.justice.gov/archives/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including

OpenAI. (2022, April 13). *Introducing Whisper*. https://openai.com/index/whisper/

Ortiz-Ospina, E. (2019). The rise of social media. *Our World in Data*. https://ourworldindata.org/rise-of-social-media

Oshin, O. (2023, July 10). Twitter traffic plunges after Musk takeover, Threads debut [Text]. *The Hill*. https://thehill.com/policy/technology/4089784-twitter-traffic-plunges-after-musk-takeover-threads-debut/

Pachhala, N., Jothilakshmi, S., & Battula, B. P. (2021). A Comprehensive Survey on Identification of Malware Types and Malware Classification Using Machine Learning Techniques. *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, 1207–1214. https://doi.org/10.1109/ICOSEC51865.2021.9591763

Perrin, A., & Atske, S. (2021, March 26). About three-in-ten U.S. adults say they are ‘almost constantly’ online. *Pew Research Center*. https://www.pewresearch.org/short-reads/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/

Pertegal, M.-Á., Oliva, A., & Rodríguez-Meirinhos, A. (2019). Development and validation of the Scale of Motives for Using Social Networking Sites (SMU-SNS) for adolescents and youths. *PLOS ONE*, *14*(12), e0225781. https://doi.org/10.1371/journal.pone.0225781

Petersdotter, L., & Höglund, J. E. (2024). *“Pay or OK”,: A law and business study on Meta’s business model* [Master’s thesis, Uppsala University]. https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-533584

Pour, H. N. (2023). Transitional justice and online social platforms: Facebook and the Rohingya genocide. *International Journal of Law and Information Technology*, *31*(2), 95–113. https://doi.org/10.1093/ijlit/eaad016

Przepiorka, A., & Blachnio, A. (2016). Time perspective in Internet and Facebook addiction. *Computers in Human Behavior*, *60*, 13–18. https://doi.org/10.1016/j.chb.2016.02.045

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Renaud, K., Searle, R., & Dupuis, M. (2022). Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil? *Proceedings of the 2021 New Security Paradigms Workshop*, 70–87. https://doi.org/10.1145/3498891.3498896

Reuters. (2024, December 5). Turkish antitrust authority ends Meta probe over Threads data-sharing. *Reuters*. https://www.reuters.com/technology/turkish-antitrust-authority-ends-meta-probe-over-data-sharing-2024-12-05/

Rosenstock, I. M. (1974). The Health Belief Model and Preventive Health Behavior. *Health Education Monographs*, *2*(4), 354–386. https://doi.org/10.1177/109019817400200405

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human Behavior*, *25*(2), 578–586. https://doi.org/10.1016/j.chb.2008.12.024

Roth, E. (2025, January 27). *Meta AI will use its 'memory' to provide better recommendations*. The Verge. https://www.theverge.com/2025/1/27/24352992/meta-ai-memory-personalization

Rulsi, E. (2012, April 11). *Facebook Buys Instagram for $1 Billion—NYTimes.com*. The New York Times. https://web.archive.org/web/20120411095346/https://dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), Article 4. https://doi.org/10.3390/fi11040089

Samonas, S., & Coss, D. (2014). THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. *Journal of Information System Security*, *10*(3), 21–45.

Sandouka, H., Cullen, A. J., & Mann, I. (2009). Social Engineering Detection Using Neural Networks. *2009 International Conference on CyberWorlds*, 273–278. https://doi.org/10.1109/CW.2009.59

Schissler, M. (2024). Beyond Hate Speech and Misinformation: Facebook and the Rohingya Genocide in Myanmar. *Journal of Genocide Research*, 1–26. https://doi.org/10.1080/14623528.2024.2375122

Shay, R., Ion, I., Reeder, R. W., & Consolvo, S. (2014). "My religious aunt asked why i was trying to sell her viagra": Experiences with account hijacking. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2657–2666. https://doi.org/10.1145/2556288.2557330

Sienko, C. (2016, June 11). *The Breach of Anthem Health—The Largest Healthcare Breach in History | Infosec*. Infosec. https://www.infosecinstitute.com/resources/healthcare-information-security/the-breach-of-anthem-health-the-largest-healthcare-breach-in-history/

Silverstein, J. (2019, April 4). *Hundreds of millions of Facebook user records were exposed on Amazon cloud server*. https://www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The Ghost in the Machine. *The Communications of the Association for Information Systems*, *14*(1), 49.

StatCounter. (2025, April 14). *U.S. top social media sites visit share 2025*. Statista. https://www.statista.com/statistics/265773/market-share-of-the-most-popular-social-media-websites-in-the-us/

Statista. (2024, May). *Number of global social network users 2017-2028*. Statista. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data Collection in the Digital Age: Innovative Alternatives to Student Samples. *MIS Quarterly*, *38*(2), 355–378.

Sun, Y., & Zhang, Y. (2021). A review of theories and models applied in studies of social media addiction and implications for future research. *Addictive Behaviors*, *114*, 106699. https://doi.org/10.1016/j.addbeh.2020.106699

Supreme Court Observer. (2017, August 24). *Judgment of the Court in Plain English (I)*. Supreme Court Observer. https://www.scobserver.in/reports/k-s-puttaswamy-right-to-privacy-judgment-of-the-court-in-plain-english-i/

Thomas, K., & Nicol, D. M. (2010). The Koobface botnet and the rise of social malware. *2010 5th International Conference on Malicious and Unwanted Software*, 63–70. https://doi.org/10.1109/MALWARE.2010.5665793

Tian, H., Kanich, C., Polakis, J., & Patil, S. (2020). Tech Pains: Characterizations of Lived Cybersecurity Experiences. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 250–259. https://doi.org/10.1109/EuroSPW51379.2020.00040

Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: An empirical investigation of public servants in Vietnam. *Journal of Asia Business Studies*, *18*(6), 1445–1464. https://doi.org/10.1108/JABS-01-2024-0058

US v. Morris (Court of Appeals, 2nd Circuit December 4, 1990).

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Weise, E. (2016, May 31). *360 million Myspace accounts breached*. USA TODAY. https://www.usatoday.com/story/tech/2016/05/31/360-million-myspace-accounts-breached/85183200/

Wilcox, H., & Bhattacharya, M. (2016). A framework to mitigate social engineering through social media within the enterprise. *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, 1039–1044. https://doi.org/10.1109/ICIEA.2016.7603735

Winder, D. (2020, August 19). *235 Million Instagram, TikTok And YouTube User Profiles Exposed In Massive Data Leak*. Forbes. https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/

Wong, Q. (2019, December 19). *Millions of Facebook user phone numbers exposed online, security researchers say*. CNET. https://www.cnet.com/news/privacy/millions-of-facebook-user-phone-numbers-exposed-online-security-researchers-say/

Worsley, J. D., McIntyre, J. C., Bentall, R. P., & Corcoran, R. (2018). Childhood maltreatment and problematic social media use: The role of attachment and depression. *Psychiatry Research*, *267*, 88–93. https://doi.org/10.1016/j.psychres.2018.05.023

Wright, A. D. (2015, February 10). *Lessons Learned from Anthem Data Breach*. SHRM. https://www.shrm.org/topics-tools/news/technology/lessons-learned-anthem-data-breach

Xanidis, N., & Brignell, C. M. (2016). The association between the use of social network sites, sleep quality and cognitive function during the day. *Computers in Human Behavior*, *55*, 121–126. https://doi.org/10.1016/j.chb.2015.09.004

Xu, W., Zhang, F., & Zhu, S. (2010). Toward worm detection in online social networks. *Proceedings of the 26th Annual Computer Security Applications Conference*, 11–20. https://doi.org/10.1145/1920261.1920264

Yang, Z., Wilson, C., Wang, X., Gao, T., Zhao, B. Y., & Dai, Y. (2014). Uncovering social network Sybils in the wild. *ACM Trans. Knowl. Discov. Data*, *8*(1), 2:1-2:29. https://doi.org/10.1145/2556609

Yilmaz, Y., Cetin, O., Grigore, C., Arief, B., & Hernandez-Castro, J. (2023). Personality Types and Ransomware Victimisation. *Digital Threats: Research and Practice*, *4*(4), Article 4.

Zetter, K. (2013, February 4). *Twitter hacked: 250,000 accounts believed compromised*. Wired UK. https://web.archive.org/web/20130204085709/https://www.wired.co.uk/news/archive/2013-02/02/twitter-hacked

Zwilling, M., Klien ,Galit, Lesjak ,Dušan, Wiechetek ,Łukasz, Cetin ,Fatih, & and Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

APPENDIX A: INTERVIEW SCRIPT

What social media websites or applications do you use the most often?

How often would you say you use them?

What are your primary motivations for using social media?

Why do you use the specific social media platforms that you do?

Have you ever been the victim of a cyber-attack, such as being stalked or extorted online, having one of your accounts hijacked, or hearing your account was involved in a data breach?

Have you ever been tricked into unintentionally doing something that would put your accounts at risk, such as entering credentials on a fake log-in page, sending a stranger your private information online, or downloading unwanted software that pretended to be a legitimate app?

Regardless of whether you have personally been affected by cybersecurity threats, have you seen things like scam messages, strange links or downloads pop up on your social media feeds or pages?*

Thinking about the profile of your most frequently used social media app or website, what kinds of information do you share there?

Does the amount of information you share differ from platform to platform? (Why?)*

Could someone reasonably find your profile if they only knew you in “real life”? (Why?)

Are there any specific practices that you use to protect your digital accounts, such as using different passwords, reviewing security settings, or using antivirus software?

Do you have any questions for me about this study?

* Questions added over time following initial interviews.

APPENDIX B: SURVEY QUESTIONS

Note: Consent forms, while included at the beginning of the survey, are not included within this Appendix, for concision. Multi-part questions such as (7) were presented as question matrices, with each sub-section a row and each response option a column. Study domains are presented in brackets before each question here, though these domains were not listed on the survey as presented to subjects.

(1) Are you an employee of the University of Washington, family member of a University of Washington employee, or University of Washington student involved in this particular research?

- Yes
- No

(2) [GENDER] What gender do you most closely identify with?

- Male
- Female
- Non-Binary / Third Gender
- Prefer not to say

(3) [EDUCATION] What is the highest level of education you have obtained?

- Did NOT graduate high school (12th grade or less)
- Graduated high school or equivalent (GED)
- Some college, no degree

- Associate degree
- Bachelor's degree
- Master's degree
- Law degree, M.B.A., or other professional degree
- Doctorate degree

(4) [ETHNICITY] What ethnicity do you primarily identify with?

- Asian/Pacific Islander
- Black/African-American
- White/Caucasian
- Hispanic
- Native American/Alaskan Native
- Other/Multi-Racial

(5) [AGE] What is your current age?

- Under 18
- 18-19
- 20-24
- 25-29
- 30-34
- 35-39
- 40-44
- 45-49
- 50-54

- 55-59
- 60-64
- 65-69
- 70-74
- 75-79
- 80-84
- 85-89
- 90 & above

(6) [SNSB-f] Which of the following social media websites or applications do you use, if any?

- Facebook
- Pinterest
- Instagram
- X / Twitter
- Reddit
- YouTube
- LinkedIn
- Snapchat
- TikTok
- Discord
- Other (Please Specify)

(7) [SNSB-f] How often do you use the following social networking platforms?

(a) Facebook

(b) Pinterest

(c) Instagram

(d) X / Twitter

(e) Reddit

(f) YouTube

(g) LinkedIn

(h) Snapchat

(i) TikTok

(j) Discord

(k) Other

- Never
- Rarely (once every month or so)
- Sometimes (once every week or so)
- Often (once every day or two)
- Very Often (a few times a day)
- All the Time (several times a day or more)

(8) [SNSB-m] Here are a number of characteristics that may or may not apply to you. For example, do you agree that you use social media to meet new friends? Please indicate the extent to which you agree or disagree with each statement.

I use social media...

(a) [MER] To stay in touch with friends or people I know.

(b) [MER] To find out what acquaintances or friends are doing now.

(c) [MER] To maintain relationships with people I may not get to see very often.

(d) [MER] To keep in touch with relatives.

(e) [MNPS] To meet new friends.

(f) To select agree for this question to get paid.*

(g) [MNPS] To develop a romantic relationship.

(h) Because my friends do.

(i) Primarily for socializing.

(j) As a popularity contest to have more social media friends.

(k) To be cool.

(l) To find information about celebrities and keep track of them.

(m) To update my own status/profile.

(n) To occupy my time.

(o) To pass the time when I am bored

(p) To distract myself.

(q) To use the applications within social media.

(r) To store and organize photographs.

(s) To create an activity group.

(t) To store and organize contact information (such as e-mail addresses).

(u) To store and organize birthdates and appointments.

(v) To play games.

(w) To listen to music.

(x) To read funny text (jokes, riddles, stories, etc.).

(y) To share videos and images.

(z) To find or spread information.

(aa) To select disagree for this question to get paid.*

(bb) To keep abreast of current events.

(cc) To express my views on a subject.

(dd) To access activities for educational purposes.

(ee) To reach materials about a course subject.

(ff) To join an educational or instructional group.

- Strongly Disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

(9) [SNSB-p] Here are a number of characteristics that may or may not apply to you. Please indicate the extent to which you agree or disagree with each statement.

(a) I share my first name on social media.

(b) I share my last name on social media.

(c) I share my age on social media.

(d) I share my birthday on social media.

(e) I share my gender on social media.

(f) I share what town I live in on social media.

(g) I share my address on social media.

(h) I share where I work on social media.

(i) I share my profession on social media.

(j) I share select strongly disagree for this question.*

(k) I share who my family members are on social media.

(l) I share if I have a relationship on social media.

(m) I share my interests on social media.

(n) I share my political views on social media.

(o) I share my religious views on social media.

(p) I share my academic qualifications on social media.

(q) I share what school or college I attended on social media.

(r) I share my phone number on social media.

(s) I often use social media to keep my friends up-to-date on what I'm doing at that moment

(t) I often share on social media where I am at that moment.

(u) I often share pictures I'm in on social media.

(v) I often select strongly agree for this question to get paid.*

(w) I often react to pictures or messages of other social media users.

- Strongly Disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

(10) [CSX] Here are a number of experiences that may or may not apply to you. For example, in the past, have you lost important information or files? Please indicate the extent to which you agree or disagree with each statement.

In the past...

(a) I have lost important information or files.

(b) Someone has broken into one of my personal email or online social networking accounts.

(c) I have found out that my personal data was being leaked or obtained by someone who I do not approve of.

(d) I have found out that someone hacked my account or accessed it without my permission or knowledge.

(e) I have found out that someone else was using my identity and personal information to pretend to be me on the internet.

(f) I have seen someone else posting things or spreading rumors about me on the internet which may damage my reputation privately or professionally.

(g) I have felt uncomfortable because someone seemed to be stalking me on the internet.

(h) I have felt uncomfortable because someone seemed to be threatening, bullying, or bothering me on the internet.

(i) I have found out that another person or a company has shared my personal information with others or posted information about me on the internet without consulting me first.

(j) I have had one of my online accounts accessed by someone without my consent.

(k) I have noticed unauthorized online transactions on any of my bank accounts.

(l) I have been tricked into buying goods, software or services online that turned out to be fake or counterfeit.

(m) I have been tricked into sending money to someone I met online.

(n) Someone has said something to me privately online in order to make me feel bad or scared.

(o) Someone has posted something about me publicly online in order to make me feel bad or scared.

(p) Someone revealed sexual images, videos or details of me online without my consent.

(q) Someone intentionally locked me out of any of my devices or disabled access to my data remotely.

(r) I have been asked to provide a payment in order to prevent sexual images, videos or details being posted online (or used against me in some other way).

(s) I have been asked to provide a payment in order to prevent stolen data or files being posted online (or used against me in some other way).

- Strongly Disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

(11) [CSB] Here are a number of characteristics that may or may not apply to you. Please indicate the extent to which you agree or disagree with each statement.

(a) I use different passwords for my different social media accounts.

(b) I usually review privacy/security settings on my social media sites.

(c) I keep the anti-virus software on my computer up-to-date.

(d) I watch for unusual computer behaviors/responses (e.g., computer slowing down or freezing up, pop-up windows, etc).

(e) I do not open email attachments from people whom I do not know.

(f) I have never sent sensitive information (such as account numbers, passwords, and social security number) via email or using social media.

(g) I back up important files on my computer.

(h) I always act on any malware alerts that I receive.

(i) I don't click on short URLs posted on social media sites unless I know where the links will really take me

(j) I install a new version of my device's operating system (OS) software shortly after it is discovered that it is available.

(k) I check if the website I'm visiting uses HTTPS.

- Strongly Disagree
- Disagree
- Neither agree nor disagree
- Agree
- Strongly agree

(12) [GENDER] What gender do you most closely identify with?*

- Male
- Female
- Non-Binary / Third Gender
- Prefer not to say

(13) [EDUCATION] What is the highest level of education you have obtained?*

- Did NOT graduate high school (12th grade or less)
- Graduated high school or equivalent (GED)
- Some college, no degree
- Associate degree
- Bachelor's degree

- Master's degree
- Law degree, M.B.A., or other professional degree
- Doctorate degree

(14) [ETHNICITY] What ethnicity do you primarily identify with?*

- Asian/Pacific Islander
- Black/African-American
- White/Caucasian
- Hispanic
- Native American/Alaskan Native
- Other/Multi-Racial

(15) [AGE] What is your current age?*

- Under 18
- 18-19
- 20-24
- 25-29
- 30-34
- 35-39
- 40-44
- 45-49
- 50-54
- 55-59
- 60-64

- 65-69
- 70-74
- 75-79
- 80-84
- 85-89
- 90 & above

* Response validation questions intended to filter out automated or unreliable responses. Repeated demographic questions, for example, were checked against the original set for consistency.