Journal of Social Media Research

SPECIAL ISSUE:
SOCIAL MEDIA AND MENTAL HEALTH

Journal of Social Media Research
ISSN: 3062-0945
2025, 2(5), 338-365
https://jsomer.org

RESEARCH ARTICLE OPEN ACCESS

Social media platforms as enablers of college students' experiences of cyber abuse†

Lauren R. Shapiro[1]* and Angela M. Crossman[2]

[1] John Jay College of Criminal Justice, Law & Police Science, USA
[2] John Jay College of Criminal Justice, Psychology, USA
* **Correspondence:** Lauren Shapiro, **Address:** 524 West 59th St, Haaren Hall Rm 43-306, NY, NY 10019, USA. **E-mail:** lshapiro@jjay.cuny.edu
† This research extends a study presented at the American Society of Criminology (ASC, 2023).

Article Info

DOI: 10.29329/jsomer.48

Article History:
Received: 27/06/2025
Revised: 20/09/2025
Accepted: 25/10/2025

Keywords:
social media
cyber abuse
lifestyle routine activities theory
college student victimization
counter abuse strategies

Highlights:

- College students predominantly defined cyber abuse as online harassment, criticizing, flaming, and criminal use.
- Definitions, abusiveness ratings, victimization risk factors, and strategies to thwart abuse varied by age, gender, and race.
- College students can use counter-strategies, but still engage knowingly in risky online behavior.
- More robust education, protections, and remedies are needed to protect college student users from cyber abuse.

Abstract

College students' cyber abuse experiences on social media platforms (SMPs) were investigated to disentangle the impact of various demographic factors on SMP experiences and perceptions in this specific population. This topic is important because of the potential social, emotional, and cognitive harm of cyber abuse to college students, particularly those from previously identified high-risk groups. Informed by Lifestyle Routine Activity Theory, 169 college students (ages 18-21 and 22-27 years) from diverse racial/ethnic backgrounds completed online surveys assessing their definitions of cyber abuse; factors and content affecting those definitions; their judgments of the relative abusiveness of various online behaviors; personal characteristics and behaviors they believe predispose users to becoming targets; and perceived effective responses to cyber abuse. Cyber abuse was predominantly defined as online harassment, but also as criticizing, flaming, and criminal use. Demographic differences emerged for factors and content classified as cyber abuse; abusiveness ratings of different behaviors; characteristics and behaviors predisposing users to victimization; and rankings for strategies to thwart cyber abuse. Findings illustrate both similarities in users' experiences and stark contrasts across demographic characteristics. This study demonstrated that the cyber abuse experiences of 18- to 21-year-olds and 22- to 27-year-olds, men and women, and White and Non-white are not homogeneous. Implications of these findings are discussed.

Citation: Shapiro, L. R. & Crossman, A. M. (2025). Social media platforms as enablers of college students' experiences of cyber abuse. *Journal of Social Media Research, 2*(5), 338-365. https://doi.org/10.29329/jsomer.48

©The Author(s). This is an **open-access** article under the **CC BY-NC-ND license** https://creativecommons.org/licenses/by-nc-nd/4.0/. The authors agree that the text, figures, and documents in the article do not violate the copyrights of third parties and that the publisher is not responsible for any claim or lawsuit by third parties due to copyright infringement. The authors declare that the publisher is not responsible for the article's content and that all responsibility for the article belongs to the authors.

1. Introduction

College students' nearly constant engagement online with little supervision or guidance increases their exposure to technology-facilitated abuse (TFA, herein called "cyber abuse") (Bidgoli et al., 2016; Vorderer et al., 2016). Cyber abuse is operationally defined here as the use of digital technologies (DTs) to send, post, or share negative, harmful, false, or mean content, personal or private information that causes an individual or group reputational harm, embarrassment or humiliation, and/or compromises the victims' privacy, and damages their social, emotional, psychological, financial, and/or physical safety (adapted from eSafety Commissioner, 2022-2025, p. 6; Stopbullying.gov, 2024, para 1; Witwer et al., 2020, p. 3). Cyber abuse can occur partially or wholly online through digital media (e.g., websites, social networking platforms, dating sites, apps, blogs, online games, instant messages, email, forums) or anywhere that "people can view, participate in, or share content" (Stopbullying.gov, 2024, para 1; Witwer et al., 2020). This definition encompasses various forms of contact, online acts, and content that target an individual or group (Powell et al., 2020; Shapiro, 2023). College students have identified social media as the most common medium for cyber abuse (Alqahtani et al., 2018; Bauman & Baldasare, 2015; Carr, 2021). For example, in a Pew Research Center study (Vogels, 2021a), young adults indicated that their recent online cyber abuse was on social media sites (75%), online gaming (30%), and messaging apps/texting (30%). Social media is defined as "a group of internet-based applications that build on the ideological and technical foundations of Web 2.0, and that allow the creation and exchange of user-generated content" (Kaplan & Haenlein, 2010). Research examining the harmful role of social media is crucial because it helps explain the devastating social, cognitive, academic, interpersonal, physical, and emotional effects that cyber abuse can have on individuals, up to and including suicide in some cases (e.g., Brailovskaia et al., 2020; National Academies of Sciences, Engineering, and Medicine, 2016).

Several challenges with the current cyber abuse literature limit our understanding and generalizability of the findings. College student studies vary in their methodologies, including sample demographics (e.g., age, gender, race/ethnicity), online formats (e.g., social media, email, forums), types of cyber abuse (e.g., harassment, stalking, posting obscenities), and data collection procedures (e.g., surveys, interviews, focus groups). In particular, research examining cyber abuse on social media platforms has used participants who are enrolled in college regardless of their age (Bhatnagar & Pry, 2020; Weaver & Swank, 2021) or young adults ages 18 to 29 years old without differentiating whether they are attending or previously attended college (Pew Research Center, 2017). Perrin and Atske (2021) reported that 42% of adults with a college or graduate degree reported being online constantly, compared with 23% with a high school diploma or less. The wide age range in young adult samples presumes an unlikely homogeneity in the younger (18-21) versus older (22-27) groups' choices of social media platforms (SMPs), problematic actions observed and experienced online, and definitions of cyber abuse. For example, Karayigit and Parlade (2023) found that college students ages 18-20 spent significantly more time on social media than those ages 21-24 or 25-29, and that college students ages 18-20 demonstrated higher social media addiction than those ages 25-29. Moreover, cyber abuse rates in this age range differed (Bularca et al., 2024), with younger college students (18-21 years) reporting higher rates than their older counterparts (22-30 years). Moreover, data suggest that SMP choice may differ across age groups. In one unpublished study (Shapiro & Crossman, 2025), college students ages 18-21 and 22-26 year olds, respectively, showed similar rates for their use of YouTube (100%, 99%) and Instagram (92%, 91%), whereas they differed in their use of Snapchat (77%, 64%), TikTok (76%, 69%), and Facebook (59%, 65%).

Also problematic is the lack of sufficient racial, ethnic, and sexual orientation minority representation in college student samples and the narrow operational definition of cyber abuse with diverse samples. For instance, some prior studies used predominantly White and/or female college students (e.g., Bularca et al., 2024; Niu et al., 2024) to investigate one type of cyber abuse on SMPs, typically cyber harassment, often defined by the investigators (e.g., MacDonald & Roberts-Pittman, 2010) or, when undefined, left up to their participants to interpret (e.g., Bularca et al., 2024). However, gender, ethnic/racial, and sexual orientation minorities report higher levels of cyber abuse than their majority counterparts. Yet, the proportion of minority participants in prior studies was quite low, making prevalence rates questionable (e.g., Vogels, 2021a). In addition, the nature of the cyber abuse experiences of college students from different demographic groups is unlikely to be homogenous, making it essential that each of these groups has an opportunity to define and explain how this phenomenon occurred for them and impacted their lives (Charmaraman et al., 2018; Francisco & Felmlee, 2021). Indeed, studies using predominantly minority college students who are Black (Alqahtani et al., 2018), Black and Latinx (Francisco & Felmlee, 2021), or Asian (Charmaraman et al., 2018), and those using equal proportions of Latinx and White students (42.6% vs. 38.7%; Lam et al., 2023, p. 2) to investigate cyber abuse on social media platforms have yielded prevalence rates inconsistent with those reported in other studies in which a low

proportion of minority students participated (e.g., Weaver & Swank, 2021). For example, Lam et al. indicated lower cyberbullying victimization for Latinx than other ethnic/racial groups, albeit their samples were from different regions of the United States (southern Texas and northern Ohio). In contrast, no ethnic/racial differences in cyber abuse were found by Bauman and Baldare (2015) in their predominantly White sample of college students. Additionally, current knowledge about the cyber abuse of college students on social media platforms is disjointed, with some studies examining strategies thwarting abuse and others focusing only on types of abusive behaviors or who becomes a target.

This study focused on college student social media users from diverse backgrounds who described self-defined cyber abuse on SMPs through responses to a mix of qualitative and quantitative survey questions. The literature review is organized as follows: first, an introduction to a Lifestyle Routine Activity Theory framework for understanding cyber abuse on social media platforms; second, a discussion of behaviors and content considered cyber abuse. Next, risk factors for user victimization are discussed. Finally, college students' understanding of risks and counter-strategies are reviewed.

1.1. Lifestyle Routine Activity Theory Framework

Investigations into the harms caused by cyber abuse make clear that the risks and impacts are not equally distributed across all social media users. The Lifestyle Routine Activity Theory framework (LRAT; Cohen et al., 1981) helps researchers to understand college students' vulnerability to cyber abuse by considering the convergence in time and cyberspace of suitable victims whose daily online activities increase their exposure to motivated offenders without the supervision of capable guardians (Felson & Boba, 2010; Leukfeldt & Yar, 2016). By design, digital spaces protect privacy and users' First Amendment rights to free speech, even when the message is deemed offensive, with limited exceptions (Kennedy et al., 2023). That is, there is not a strong presence of oversight on social media (i.e., guardian), particularly for discussion forums, vlogs, or blogs, as these platforms claim that they merely serve as a means for users to express their ideas rather than as creators of content (Kennedy et al., 2023). However, in reality, social media platforms like Facebook, YouTube, and Twitter do edit content to make it consistent with their own moderation rules and terms of service, including removing messages deemed to contain "hate, terrorist or extremist beliefs, nudity, and harassment" (Diaz & Hecht-Felella, 2021, p. 4). Users have raised the lack of transparency on major platforms regarding who makes the determination of which content to delete or keep, with some evidence showing that moderation or censorship of content may depend more on how it affects the business rather than potential harm to users, sometimes resulting in marginalizing protected classes (Diaz & Hecht-Felella, 2021).

Notably, when major social media providers, acting as online guardians, fail to monitor the conduct of their billions of users systematically, they allow motivated offenders and users to interact with little oversight, thereby enabling cyber abuse (Pew Research Center, 2017). Protecting users' rights and privacy makes it difficult for school and criminal justice authorities, as guardians, to determine offenders' identities, investigate and collect evidence of cyber abuse, and prosecute it (Witwer et al., 2020). Failure of guardians to be effective in preventing and mitigating harm to victims and bystanders creates an environment that perpetuates further cyber abuse because users learn there is no way to escape it, nor is there a real remedy when it occurs. College students' nearly ubiquitous internet use (high exposure and proximity), particularly on unsupervised social media platforms that fail to hold offenders accountable for their harmful actions (i.e., the absence of capable guardians), makes them suitable targets for motivated cyber offenders (Reyns et al., 2011). For instance, high rates of cyber abuse have been experienced (10%-33%) and witnessed (5%-88%) by moderate to heavy young adult users of social networks, chat rooms, and games (Reyns et al, 2011, 2012; Vogels, 2021a; Zhou & Peterson, 2025). Young adult users' engagement in risky online activities also makes them suitable targets. For example, by geo-tagging their photos or posting their current location on social media, college students become easy targets for cyber stalkers, whereas by posting opinions and comments on social media, discussion boards, blogs, and vlogs, they become targets for internet trolls and cyber harassers (Felmlee et al., 2018; Lee & Soonah, 2023). Other contributing factors to college students' victimization are the lack of confidence in their abilities, limited cognitive capabilities, few resources for obtaining help, fear of missing out (FOMO), and their high need for approval from others (Shapiro, 2023; Weaver & Swank, 2021).

1.2. Cyber Abuse on Social Media Platforms

The fast rate at which DTs were developed and incorporated into college students' daily lives makes it difficult for them (and society) to understand cyber abuse in terms of its prevalence and seriousness as a crime that results in harm to targets and bystanders (Sobba et al., 2017; Strawhun et al., 2013). Although certain

online actions may be considered harmful, only some of them are criminal (i.e., prohibited by state and/or federal statutes, such as cyber harassment and cyber stalking), some have components that correspond to statutes sufficiently to allow prosecution (e.g., swatting is charged under hoaxes), and the rest are noncriminal (i.e., cannot be prosecuted under specific statutes, such as overuse of DTs hindering the user's engagement in real world activities). Self-report studies provide estimated prevalence rates ranging from 8% to 28% for cyber abuse of college students (see Zalaquett & Chatters, 2014, for review). Variations in prevalence may be due to the type of cyber abuse, the social media platform on which it occurred, the researcher's definition, and the type of data collected. Case in point, college students in Shapiro and Alexandrou's (2019) study who used Facebook and Instagram reported different rates for exposure to violent content (69% vs. 40%), cyber harassment (16% vs. 4%), and cyberstalking (17% vs. 5%).

Interpretations can also affect prevalence estimates. College students could identify cyber abuse by the receiver's interpretation of the message (i.e., negative impact), which admittedly may be misunderstood due to the absence of paralinguistic cues, such as tone (Baldasare et al., 2012; Dredge et al., 2014a). Overall, however, without knowing their relationship, it would be difficult for bystanders to determine whether the interchange between the sender and receiver was abusive (i.e., attempting to cause harm) or merely teasing (Gahagan et al., 2016). Repeating an abusive act, legally required by some states (PenAmerica, 2025), is not considered essential by college students for defining cyber abuse. Instead, they rely on the perceived severity of the act and its public expression on social media platforms, which, for them, serves the same role as repetition (Dredge et al., 2014a).

It is uncertain, then, whether victims and bystanders recognize cyber abuse when exposed to it. Crosslin and Golman (2014) reported that some of the college students in their study first realized they had been victimized in the course of defining cyber abuse. Even if it is identified, Halsop et al. (2021) reported that college students feel obligated to tolerate online abuse due to its pervasiveness rather than take action to stop it from being the "norm." Those who dare to request censorship of offensive acts are likely to become targets and labeled "snowflakes" for being hypersensitive and/or overreacting (Halsop et al., 2021). In qualitative studies, college students often failed to self-identify as victims because they did not share the researchers' definition or set of behaviors comprising cyber abuse (Baldasare et al., 2012; Crosslin & Golman, 2014), instead referring to various online interpersonal harmful acts as "just drama" (Marwick & Boyd, 2014) or "mean, nasty, hateful, rude, inappropriate, and foul" (Gahagan et al., 2016). Thus, the literature emphasizes the need for college students to provide their own views of online risks by self-defining and describing cyber abuse, rather than for researchers to employ a prescribed definition of cyber abuse or none at all (Conway & Hadlington, 2021).

1.3. Behaviors and Content Considered to be Cyber Abuse

Researchers have identified numerous different types of cyber abuse, which we use as an umbrella term to encompass a wide range of online behaviors, including flaming; cyberbullying and harassment; cyberstalking; denigration/spreading information; nonconsensual pornography; doxing; swatting; sextortion; impersonation; exclusion; and exposing, outing and/or trickery (Beran & Li, 2007; Carr, 2021; Nuccitelli, 2012; Witwer et al., 2020). Haslop et al. (2021) found that 85% of their college student sample believed inciting violence against users due to their protected classes (i.e., gender, race/ethnicity, disability, sexuality, religion) through Facebook messages was wrong and should be reported to an academic authority. Posting non-consensual sexually explicit images of a fellow student (89.93%), observing a student sharing a sexually explicit image in a Snapchat group (75%), and a student sending abusive messages to another student (68%) were also deemed to be unacceptable and should be reported to academic authorities (Haslop et al., 2021). College students in Dredge et al.'s (2014a) study indicated that posting or sending cruel, abusive, threatening, and/or offensive messages and images on someone's social media profile (over 50%) and taking information from a social media profile and undermining a person's reputation (at least 40%) constituted cyber abuse.

However, findings regarding college students' ability to classify specific online actions and content as "cyber abuse" based on their own definitions have been inconsistent (Alipan et al., 2020; Tompson & Tomkins, 2025). According to Vogels (2021b), the subjective nature of cyber abuse means that some adults perceive online behaviors (43%), such as offensive name-calling or physical threats, as abusive, some do not (36%), and others (21%) are unsure how to classify them. Women in Zhou and Peterson's (2025) study failed to recognize they were being sexually harassed, often indicating that such interactions were typical in gaming. Social media users' interpretations of whether their recent experiences constituted cyber abuse were tied to the severity (more severe, 63% vs. less severe, 46%) and number of online behaviors they encountered (multiple types, 60% vs. one type, 35%). In one study, cyber abuse, both inside and outside of the university, was identified by college

students as someone: looking at your phone and email without permission; sending you harassing emails, pictures, and pornographic images; posting harassing messages and pictures on social media; and sexing with you against your wishes (Lawler & Moluzzo, 2015). Other online behaviors (e.g., new online friend sends sexual messages, abusive online comments made in response to posted political or feminist/gender equality beliefs, sexually nuanced jokes aimed at making the recipient uncomfortable) were predominantly considered to be sometimes wrong, part of free speech, or not serious enough to be reported to academic authorities (range: 55% to 74%; Haslop et al., 2021). Users' interpretations of online behaviors are strongly related to how they react to these experiences. Adults who perceived recent incidents as abusive were more likely than those who did not classify it as such to indicate they were very to extremely upset (40% vs. 9%; Vogels, 2021b).

1.4. Targeting Online Users for Cyber Abuse

Social media users report being targeted for demographic/identity characteristics (e.g., age, gender, race/ethnicity, sexual orientation), expressed beliefs (e.g., politics, religion), and/or online behaviors (e.g., controversial messages posted publicly). Consistent with LRAT, these may represent instances of the concurrent presence of attractive targets and motivated offenders on social media. For example, college students in Lawler and Moluzzo's (2015, p. 163) study were aware of cyber abuse against individuals in the following groups: women (48%), Lesbian and Gay (31%-53%), minority races/ethnicities (Asian, 17%; Black, 20%; Latin, 20%), physically and developmentally disabled (22%-27%), and Muslims (17%). Victims of online abuse reported that their politics (50%), gender (33%), and ethnic/racial backgrounds (29%) were reasons for being targeted, with social media identified by 75% of them as the most recent online environment (Vogels, 2021a).

The age of online adult users has been identified as a risk factor associated with increased cyber abuse. Bularca et al. (2024, p.9) found that college students aged 18 to 21 (68.5%) were more likely than those 22-25 (54.5%) or 26-30 (15.4%) to be exposed to cyber abuse. Similarly, Vogels (2021a) reported that 64% of young adult online users (18-29) experienced cyber abuse at higher rates than older adults (49%, ages 30-49; 30%, ages 50-64; 21%, ages 65+), most of which (48%) included very severe abusive behaviors. Moreover, most of the cyber abuse reported by these young adults (48%) included high rates of both "less severe" (offensive name calling, 51%; purposeful embarrassment, 40%) and "more severe" forms of online abuse (physical threats, 29%; stalking, 21%; sustained harassment, 20%; and sexual harassment, 25%). Additionally, Vogels (2021a) found that young adults reported the highest levels of each of the six types of online abuse, commonly experiencing offensive name-calling (51%) and purposeful embarrassment (40%).

Gender and sexual orientation are also victim risk characteristics associated with cyber abuse. College students who experienced cyber abuse believed gender was the main reason they were targeted, particularly those who identified as female or transgender (Haslop et al., 2021; Lawler & Moluzzo, 2015). According to Vogels (2021a), women were more likely than men to assign gender as the reason for being targeted (47% vs. 18%). Higher rates of cyber abuse were found for women than men in both a predominantly White sample (15.5% vs. 3.6%, Zalaquett & Chatters, 2014) and an all-Black sample (13.5% vs. 6.5%, Alqahtani et al., 2018). Women were also more likely than men (50% vs. 36%) to interpret recent online experiences as cyber abuse (Vogels, 2021b). Transgender students also experienced higher rates of cyber abuse than men (Haslop et al., 2021). Victimization risk for being targeted online was two to three times higher for women than men (Henson et al., 2011), particularly in regard to unwanted repeated contact (27.9% vs. 16.1%), harassment (24.8% vs. 12.9%), and unwanted sexual advances (17.6% vs. 7.4%, Reyns et al., 2012). However, findings of gender differences are sometimes inconsistent. Vogels (2021a) indicated that more men than women reported cyber abuse overall (43% vs. 38%) and specifically for offensive name-calling (35% vs. 26%), whereas more women than men reported sexual harassment (16% vs. 5%). Sexual orientation has also been found to be indicated as a reason victims were targeted for cyber abuse. Lawler and Moluzzo (2015) reported high rates of cyber abuse directed at Gay (53%) and Lesbian (31%) users. Vogels (2021a) found that more LGB users (50%) than Straight users (12%) reported being victims of cyber abuse. In comparison to heterosexual college students, Reyns et al. (2012) found that non-heterosexual peers were subjected to higher rates of unwanted contact (22.55 vs. 38.6%), sexual advances (12.9% vs. 26.3%), and cyberstalking (39.8% vs. 56.1%), respectively.

Race/ethnicity is another reason mentioned for cyber abuse targeting, particularly by minority college students (Vogels, 2021a). Higher rates of cyber abuse were found for non-White than White college students (56% vs. 41%, Hollis, 2016; 32.8% vs. 22.1%, Reyns et al., 2012). Both Blacks and Hispanics were more likely than Whites (54% vs. 47% vs. 40%) to interpret recent online experiences as abusive (Vogels, 2021b). Vogels (2021a) further indicated that Hispanic users (33%) were more likely than White (23%) and Black users (25%) to experience more severe forms of cyber abuse, for example being stalked (20% vs. 9% vs. 11%, respectively).

The combination of gender and race has also been found to make online users vulnerable to cyber abuse. Felmlee et al. (2018) indicated that "derogatory messages attack women of color on a regular, daily basis on Twitter" and these publicly available messages took less than 30 seconds for them to locate (p. 119). However, the low enrollment of minority students in most survey studies with college students has made a comprehensive analysis difficult to do, thereby leaving it unknown whether the incidence of cyber abuse and its harm differ across racial and ethnic groups (Kowalski et al., 2020).

Victims of cyber abuse may also experience different types and identify distinct reasons for being targeted. For example, Vogels (2021a) found that offensive name-calling (55%), purposeful embarrassment (55%), and physical threats (51%) were mainly attributed to political views, whereas sexual harassment (67%) and stalking (53%) were attributed predominantly to gender. Vogels (2021a) also reported that of the 42% who experienced cyber abuse, male users were more likely than female users (57% vs. 42%) and White users were more likely than both Black and Hispanic users (56% vs. 38% and 38%) to indicate targeting was due to their political views (Vogels, 2021a).

The way people use their social media accounts may also make them targets of cyber abuse. Online victimization was positively related to the number of social media accounts and weekly profile updates, adding strangers as friends, and using a profile tracker (Henson et al., 2011; Reyn et al., 2011). College students are also likely to become victims of cyber abuse when they fail to use privacy settings to control who can contact them, make comments, or see their content; keep their location available to allow others to track them; and provide personally identifiable information indiscriminately on their social media accounts (Lee & Soonah, 2023). Other risky behaviors include having many friends (indiscriminate friending); friending and meeting strangers; pervasive scrolling; posting indiscreet content; and having friends who posted indiscreet content, which predicted mild and severe victimization among college student users (Fansher & Rander, 2019; Peluchette et al., 2015). Peluchette and Karl (2008, cited in Peluchette et al., 2015) indicated that users whose content included comments and photos of alcohol use or sexual activities, sexually explicit images, and obscenities, which was associated with a greater likelihood of them being abused (Dredge et al., 2014b). Although Peluchette et al. (2015) found that harsh cyber abuse was associated with failure to use privacy settings, Henson et al. (2011) cautioned that not sharing sensitive information with strangers is more important for preventing victimization than merely setting privacy settings on profiles. Overall, users who engage in risky behaviors make themselves attractive as potential targets to motivated offenders.

1.5. Strategies to Counter Cyber Abuse

Knowledge about college students' understanding of social risks (e.g., cyber harassment, social information overload, identity theft) and technology risks (e.g., unauthorized access to accounts, service interruptions) from using social media is mixed (Goh et al., 2016). Gen Z students, raised with technology (i.e., digital natives), seem to understand the potential harm of using social media (e.g., reputation harm, financial loss) and know some protective measures they can use to counter these risks (Moallem, 2018). Bhatnagar and Pry (2020) indicated many in their college student sample had a high level of security awareness, such that they knew it was risky to keep accounts public (72.6%) and engaged security features for privacy and control (78.5%), such as maintaining anonymity through fake accounts to protect themselves on social media. McClain et al. (2023) reported that their college student sample was aware of general risks when posting online and made calculations before engaging on contentious sites (e.g., being banned, reputational damage, targeted for hate and verbal attacks). However, despite the majority of college students (84%) knowing that sharing personal information on SMPs is risky (Sharma et al., 2015), their desire to meet new people (gain/benefit), particularly for sexual purposes, outweighed their concerns of being victimized (loss/cost) for evolutionary, psychological, and social reasons (Ellis et al., 2012). Specifically, young adults are primed to be sexually promiscuous, test their own sexual desirability, and engage in various tactics to attract a mate (Ellis et al., 2012). Their underdeveloped prefrontal cortex fails to prevent them from engaging in illogical and impulsive behaviors, while their mature limbic system incentivizes them to seek new, potentially exciting, and rewarding experiences through dopamine release (Reyna & Farley, 2006; Willoughby et al., 2021). Peer pressure, including fear of exclusion and the need for social acceptance, also contributes to young adults' willingness to participate in risky social behaviors (Willoughby et al., 2021). Furthermore, their sense of invulnerability and optimism leads them to believe they can judge whether someone is safe based on his or her public profile (Brandtzaeg & Heim, 2009).

Victims and witnesses of cyber abuse used a combination of mitigation strategies, including confronting the abuser online, blocking the abuser, ignoring the abuser (doing nothing), deleting abusive content, publicly/privately supporting the victim, and reciprocating with abuse (Gahagan et al., 2016). According to

Bularca et al. (2024, p. 10), college students indicated that as victims, 27% would confront the aggressor, 15% would talk to a friend about it, 13% would ignore the situation/do nothing, and 10% would leave the site, whereas as witnesses, 36% would do nothing, 5% would leave the site, 10% would state their opinion to the abuser, 7% would get verbally involved or object, and 8% would seek out the victim. Similarly, bystanders who witnessed cyber abuse typically acted by ignoring the abuse or helping the victim (Sobba et al., 2017).

When college students needed assistance dealing with cyber abuse, the most common method mentioned was to report abusive behavior to an authority (e.g., the website provider, school administration, law enforcement). Lawler and Moluzzo's (2015) sample of college students indicated that they would report being a victim of cyber abuse to various school authorities (13%-37%), security or the police (27%), a Counseling Center (53%), their best friend (68%), or their parents (57%). Bularca et al. reported that 30% of college student victims and 6% of witnesses would report the abuser's account to SMP. Unfortunately, college students may not understand the rules of cyber etiquette or how to report violations. O'Connor et al. (2018) found that only 45% of their college student sample were aware that their university had a cyber abuse policy, 42% knew perpetrators were disciplined, and 21% had been trained to use it to report incidents.

Another problem concerns the impact of official responses to online victims' complaints of digital offenses, with some researchers reporting satisfaction (Graham et al., 2020) and others dissatisfaction by victims (Wolak & Finkelhor, 2016). Colburn et al. (2023) found that certain types of cyber abuse, such as image-based victimization, were positively correlated with high reporting to websites, apps, and police, perhaps as a means of removing the circulating image. In contrast, adult users (ages 18 to 28) in Colburn et al.'s study rarely reported cyber abuse to websites (7.3%) or law enforcement (4.8%), and when users did report it, they were unsatisfied with responses from SMPs (57.8%) and law enforcement (70.2%). For example, of those in Colburn et al.'s study who filed with the police, only 29.8% indicated they were helpful (e.g., conducted an investigation, contacted the responsible person), and 48.5% stated they were not helpful (e.g., victim not taken seriously, police stated they could not do anything). In contrast, adults in Vogels' (2021b) study who considered their recent online experiences to be abusive indicated that very effective solutions for reducing such behaviors on social media included perpetrators being charged with criminal offenses (49%), subjected to permanent (57%) or temporary (33%) suspension on SMPs (57%), SMPs deleting their posts (44%), and requiring all users to disclose their real identities (49%).

1.6. Current Study

Consistent with past research suggesting that cyber abuse prevalence rates are higher in gender and racial minorities than their majority counterparts and in young adults ages 18 to 21 compared to those ages 22 to 27, this study sought a sample that included male and female college students ages 18 to 27 years with racially and ethnically diverse backgrounds. The aims for this project was to understand their: (1) definitions of cyber abuse, factors influencing their identification of online behaviors constituting abuse, and judgments of abusiveness for various types of content; (2) ratings of abusiveness for various online behaviors; (3) beliefs of user features and online behaviors that increased the likelihood of becoming a target; and (4) knowledge of strategies used by victims and bystanders (e.g., ignore, intervene, report) to thwart cyber abuse.

2. Method

2.1. Research Design

The study used a survey design with an available non-random sampling plan. At the first author's request, participating college instructors distributed recruitment letters to their students, inviting them to participate in the survey in exchange for 2 extra credit points. As part of informed consent, participants were informed of the study's goal and assured of confidentiality (i.e., no names or identifying information were included in the data).

2.2. Participants, Procedure, and Ethical Considerations

The sample consisted of 169 undergraduate and graduate students (51% females, 96% were single; 81% identified as heterosexual) from two age groups: 48% were ages 18 to 21 years (M = 20.59, SD = .70) and 52% were ages 22 to 27 years (M = 23.92, SD = 1.74). An additional 20 participants were excluded from the final sample because they did not complete at least 84% of the survey. Congruent with the diverse racial and ethnic identification of the urban college from which they were drawn, 41% of respondents self-identified as Hispanic, 21% as White, 16% as Asian, 11% as Black, 5% as Mixed, 1% as Indigenous, and 5% did not provide their race/ethnicity.

This study collected survey data on social media use among young adults. The recruitment letter included a link to the Qualtrics platform that allowed participants to complete the survey and provide informed consent to participate. In the last question of the survey, respondents created a code and were instructed to take a photograph, which they shared with their professors to earn extra credit. The research (#2017-1086) was approved by the Integrated Institutional Review Board (November 18, 2022), and the authors complied with publication ethics and copyright policies. No ethical concerns were raised in this study.

2.3. Measures and scoring

The survey consisted of two sections that assessed respondents' demographics and experiences of cyber abuse on social media.

2.3.1. Demographics questions

Six demographic questions were used to obtain respondents' age (18-27), gender identity, sexual orientation, racial/ethnic identity, religion, and marital status. *Age* was categorized as "1/younger" if aged 18 to 21 years and as "2/older" if aged 22 to 27 years. *Gender identity* was scored as "male," "female," or "unspecified." Although multiple options were available for respondents to select, due to small cell counts, the data were collapsed for the following categories: *sexual orientation* was reduced to "1/heterosexual" or "2/non-heterosexual;" *race/ethnicity* was reduced to "1/Non-White" and "2/White;" *religion* was reduced to "1/Catholic and Christian" and "2/Other;" and *marital status* was reduced to "1/Single" and "2/Married."

2.3.2. Social media cyber abuse questions

Seven cyber abuse questions were used. The first four questions focused on negative aspects of social media use and each offered a 'write-in' option, but in most cases, responses were inconsistent, and so no further scoring was performed on those responses unless otherwise specified. Question 1 requested that respondents provide their own definition of "cyber abuse," which allowed for more than one answer. Our initial coding scheme with pre-identified themes based on a reading of the literature was broadened to include additional themes based on terms used by the respondents or adjusted to incorporate conceptually related themes (see Table 1 showing the cyber abuse coding scheme). For each answer, a "0" was scored when the respondent had not provided it, whereas a "1" was scored when it was provided, allowing a total score indicating the number of terms per respondent definition. We also calculated the total number of respondents who provided each definition.

Question 2 probed the extent to which three factors (i.e., number of times, victim's negative emotional and behavioral responses, and content) influenced respondents' decisions to identify specific user behaviors as cyber abuse. Respondents provided yes (scored as "1") or no (scored as "0") answers. Yes responses were followed up by asking for additional information, such as minimum frequency, types of negative emotional responses, and specification of the type of content that made something cyber abuse. These additional responses were further coded for frequency as "once" or "more than once"; for responses as "emotion" or "behavior"; and for content as "violent," "sexual," or "offensive." For Question 3, respondents were shown a list of 12 combined types of content (violent, offensive, sexual, extremist) and media (images, videos, messages) and asked to draw on their observations and experiences to determine their level of abusiveness on a Likert scale from "1/not at all" to "7/extremely". The scores for the 12 combinations of content and media were averaged across categories. Question 4 used a Likert scale ranging from 1 to 7 to determine the respondents' judgments of abusiveness for 27 online behaviors. Ratings for each behavior were averaged across respondents.

For the next two questions, respondents were presented with a variety of user demographics and behaviors and asked to determine which increased the likelihood that a user would become a target of cyber abuse. Question 5 asked respondents to draw on their observations and experiences on social media platforms to determine which ages (11-13, 14-17, 18-25, 26-34); religions (Catholic/Christian, Jewish, Islam, Hindu, Buddhist, Lesser known religions, other); sexual identity (male, female, non-binary); sexual orientation (heterosexual, asexual, transexual, LGBTQQIAA, other); race/ethnicity (White, Black, Latinx, Asian, Pacific Islander/Hawaiian, Indigenous People, People of Color, other), and opinions (political, such as Democrat and Republican; abortion, such as pro-life and pro-choice; and gender role, such as men are superior to women and women and men are equal) best describe the most likely targets of cyber abuse. For each option, a score of "1" was used if selected and a score of "0" was used if it was not selected. It was possible for respondents to select more than one option, in which case, each selection received a score of "1." Due to small cell counts, the data in the following three categories were collapsed to be dichotomous: religion (Catholic/Christian, other);

race/ethnicity (White, Not White); and sexual orientation (heterosexual, non-heterosexual). For Question 6, respondents were asked to select all of the 17 behaviors listed that they believed increased a user's chance of becoming targeted for cyber abuse. For each behavior, a "0" was scored when the respondent had not selected it, whereas a "1" was scored when it was selected, allowing a total score per behavior. The total number of the 17 behaviors each respondent endorsed was also summed.

The last question obtained respondents' judgments of various strategies for dealing with cyber abuse they experienced or witnessed online. Respondents ranked the effectiveness of 13 strategies, and the ranks were averaged for each strategy.

Table 1. Coding scheme of themes, terms, and descriptions for definitions of cyber abuse (Beran & Li, 2007; Carr, 2021; Langos, 2015; Nuccitelli, 2012)

Theme	Description	Terms
Cyber harassment	Offensive messages and threats.	cyberbullying, cyber harassing, abusing, insulting, threatening, verbally abusive, causing emotional harm.
Rumor	Attacking someone's social or professional reputation through harmful or cruel statements.	rumors, lies, false accusations, gossip, defamation
Outing	Tricking a person into revealing personal information that is embarrassing or compromising.	outing, doxing (non-consensual distribution)
Criticizing	Messages involving harsh, hurtful, and humiliating comments and images in reaction to a person, post, video, or photo online.	criticizing, insulting, denigrating, belittling, shaming, disapproving
Flaming	Nasty, vulgar, incendiary, and disruptive messages and actions, or the sharing of offensive and aggressive content to assert power over a person or group.	flaming, trolling, maliciousness, rudeness, mocking, disrupting, irritating, provoking confrontation
Impersonating	Feigning messages from someone to cause ill will; creating fake profiles; and obtaining information to invade their privacy, humiliate them, and taint their reputations.	impersonating, faking, catfishing
Cyberstalking	A form of harassment involving following someone online, causing him or her fear and concerns for safety.	cyberstalking, pursuing online, monitoring someone's online activities, and threatening harm.
Scamming	Endorsing or posting false information or deep fakes (simulated videos or images) created for criminal purposes.	scamming
Blackmailing	Threatening someone's private information or explicit images or videos to get revenge or obtain financial gain.	blackmailing
Sexual abuse	Targeting vulnerable victims for the abuser's own sexual gratification or non-consensual production and distribution of sexually explicit images for revenge or to cause harm to the victim.	sexual abuse, sexting, sextortion, grooming, image-based sexual abuse (revenge porn)
Hacking	Exploiting a weakness in our network security to gain unauthorized access for criminal purposes.	hacking
Criminal use	Taking advantage of others in online activities for the purpose of causing them serious harm or to commit crimes.	wrong use, criminal activities
Overuse	Engaging in social media or the internet to excess, such that the user is harmed psychologically or emotionally.	overusing

2.4. Data Analysis

Respondents' answers were subjected to either 2 (Respondent gender: male, female) X 2 (Respondent age group: Younger, Older) univariate (ANCOVA) or multivariate analysis of covariance (MANCOVA), unless otherwise specified. The covariates were Respondent sexual orientation, dichotomized into heterosexual and non-heterosexual (M = 1.15), and Respondent race, dichotomized into White and non-White (M = 1.22). Post hoc comparisons of means used Bonferroni tests and were significant at $p < .05$, whereas p values were specified for borderline results. Only significant effects are described.

3. Results

3.1. Cyber abuse definitions and factors influencing identification

Respondents' own definitions of cyber abuse were explored in the first analysis. The identified themes for definitions of cyber abuse served as the dependent variables. Table 2 shows the mean proportions (and SEs) for definitions of cyber abuse by respondents' sexual orientation, race, and gender. Non-heterosexual respondents were more likely than heterosexual respondents to define cyber abuse as *cyberstalking*, $F(1, 146) = 4.590$, $p = 0.034$, $\eta^2 = 0.030$ (Power = 0.567), and *scamming*, $F(1,146) = 6.621$, $p = 0.011$, $\eta^2 = 0.043$ (Power = 0.725). A higher proportion of White respondents defined cyber abuse as *criminal use*, $F(1, 146) = 4.810$, $p = 0.030$, $\eta^2 = 0.032$ (Power = 0.587), than non-Whites. Lastly, women defined cyber abuse as *criticizing*, $F(1, 146) = 10.524$, $p = 0.001$, $\eta^2 = 0.067$ (Power = 0.897), more than men. No other main effects or interactions were found for definitions.

Table 2. Definitions of cyber abuse by Respondent sexual orientation, race, and gender[a]

	Sexual Orientation		**Race**		**Gender**	
Definition[b]	Hetero	Non-hetero	White	Non-white	Female	Male
Harassment	.692 (.049)	.708 (.146)	.696 (.058)	.704 (.142)	.637 (.055)	.725 (.053)
Rumor	.068 (.027)	.050 (.081)	.086 (.032)	.032 (.079)	.067 (.031)	.075 (.030)
Outing	.053 (.020)	.000 (.061)	.020 (.024)	.032 (.059)	.045 (.023)	.033 (.023)
Criticize	.304 (.048)	.508 (.144)	.318 (.057)	.495 (.141)	**.436 (.053)**	**.193 (.051)**
Flaming	.141 (.038)	.292 (.116)	.202 (.045)	.231 (.113)	.170 (.044)	.158 (.043)
Impersonation	.020 (.017)	.000 (.050)	.020 (.020)	.000 (.049)	.044 (.019)	.009 (.018)
Cyberstalking	**.026 (.023)**	**.075 (.069)**	.101 (.027)	.000 (.067)	.017 (.026)	.084 (.025)
Scamming	**.000 (.008)**	**.025 (.025)**	.025 (.010)	.000 (.024)	.004 (.009)	.018 (.009)
Blackmail	.005 (.012)	.025 (.035)	.030 (.014)	.000 (.035)	.025 (.014)	.001 (.013)
Sexual abuse	.020 (.020)	.050 (.060)	.070 (.024)	.000 (.059)	.037 (.023)	.043 (.022)
Hacking	.037 (.043)	.000 (.043)	.005 (.017)	.032 (.042)	.002 (.016)	.038 (.016)
Criminal Use	.145 (.039)	.075 (.118)	**.187 (.047)**	**.032 (.115)**	.195 (.045)	.165 (.043)
Overuse	.084 (.027)	.025 (.081)	.061 (.032)	.048 (.079)	.100 (.031)	.045 (.030)

[a] Bold numbers indicate significant differences.
[b] Top 4 definitions based on the proportion of respondents providing each: Generic ($M = .65$), Criticize ($M = .29$), Flaming ($M = .16$), and Criminal use ($M = .14$).

In the second analysis, categories of factors (number of times, respondent emotion, and content) believed to influence the identification of cyber abuse served as the dependent variables. A main effect of Respondent sex was found for content, $F(1, 147) = 5.243$, $p = 0.023$, $\eta^2 = 0.034$ (Power = 0.624), indicating that women believed more than men that content influenced their identification of cyber abuse ($M = .786$, $SE = .054$ vs. $M = .614$, $SE = .051$).

In the third set of analyses, detailed examinations of each factor category (times, emotion, content) that respondents believed influenced their identification of cyber abuse were made using mixed model ANCOVAs with age group and gender as the between-subject variables, race and sexual orientation as the covariates (Respondent sexual orientation, $M = 1.15$; Respondent race, $M = 1.22$), and levels of each factor as the within-subject variables. All significant findings were corrected using the Greenhouse-Geisser method. Analysis of the two levels of how often the behavior occurred ('times'), once vs. more than once, yielded no significant main effects or interactions. For the two levels of victims' negative responses ('emotion'), emotional response vs. behavior, the analysis showed a significant two-way interaction of Respondent race and negative responses, $F(1,147) = 5.042$, $p = 0.026$, $\eta^2 = 0.033$ (Power = 0.607). Figure 1 shows the mean proportions of respondents by race who were influenced by victims' negative emotional and behavioral responses in identifying cyber abuse. Post hoc analyses indicated that White respondents were influenced more than non-White respondents by the victim's negative emotional response, but not behavior, when determining whether cyber abuse occurred. Also, White respondents were influenced more by the victim's negative emotional response than behavior when determining whether cyber abuse occurred, whereas this differentiation was not made by non-White respondents. For 'content', analysis of the three types of content (violent, offensive, sexual) showed no main effects, yet the two-way interaction of Respondent age group and gender was significant, $F(1, 147) = 3.925$, $p = 0.049$, $\eta^2 = 0.026$ (Power = 0.503). Figure 2 shows the mean proportions of respondents by age and gender who

were influenced by the type of content in identifying cyber abuse. For younger respondents, a higher proportion of women than men indicated that content influenced their identification of cyber abuse; no gender differences were found for older respondents. Additionally, a higher proportion of older men than younger men indicated that content influenced their identification of cyber abuse; however, no age differences were found for women.

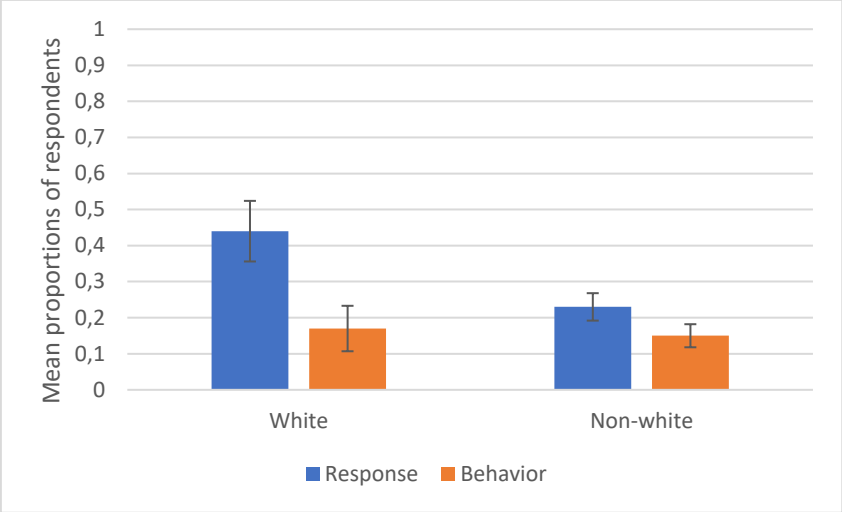

Figure 1. Mean proportions of respondents influenced by the victim's emotional response and behavior in identifying cyber abuse by Respondent race

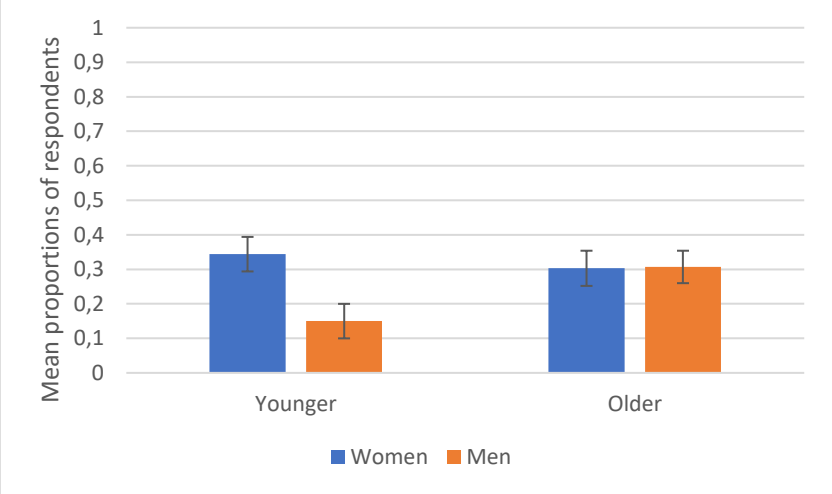

Figure 2. Mean proportions of respondents influenced by the type of content in identifying cyber abuse by Respondent age and gender

In the next analysis, perceived abusiveness levels for the four types of content (violent, sexual, offensive, extremist) and three media types (image, video, message) served as within-subject factors and were analyzed using a mixed-model ANOVA. ANCOVA was not required as no covariates were significant in the previous content analysis. All significant findings were corrected using the Greenhouse-Geisser method. A main effect of Respondent gender, $F(1, 165) = 9.195$, $p = 0.003$, $\eta^2 = 0.053$ (Power = 0.854), indicated that women rated abusiveness higher than men overall ($M = 5.721$, $SE = .136$ vs. $M = 5.131$, $SE = .139$). There was also a main effect of Content, $F(2.848, 469.860) = 4.824$, $p = 0.003$, $\eta^2 = 0.028$ (Power = 0.892), which was interpreted within the significant two-way interaction of Content and Media, $F(3.913, 645.612) = 4.186$, $p = 0.003$, $\eta^2 = 0.025$ (Power = 0.918). Table 3 shows the mean proportions (and SEs) of abusiveness levels across content and media types. Respondents rated images and videos with sexual content as more abusive than violent, offensive, and extremist content. Messages with sexual content were rated as more abusive than those with extremist content. In a comparison of media types, respondents rated messages as more abusive than images when the content was violent and rated videos as more abusive than messages when the content was sexual. No other differences were found.

Table 3. Abusiveness levels rated by type of content and media[a]

Content	Media			Average
	Images	Videos	Messages	
Violent	**5.282 (.137)**	**5.426 (.132)**	5.573 (.126)	5.427 (.132)
Sexual	**5.685 (.123)**	**5.777 (.121)**	5.599 (.123)	**5.687 (.122)**
Offensive	**5.288 (.126)**	**5.326 (.125)**	5.307 (.127)	5.307 (.126)
Extremist	**5.238 (.131)**	**5.317 (.128)**	5.246 (.131)	**5.282 (.130)**

[a] Bold numbers indicate significant differences.

3.2. Abusiveness ratings

Abusiveness ratings of online behaviors were examined next by a MANCOVA. One main effect of respondents' sexual orientation found for *sharing embarrassing private information*, $F(1, 147) = 4.186$, $p = 0.003$, $\eta^2 = 0.025$ (Power = 0.918) showed that heterosexual respondents rated this behavior as more abusive than non-heterosexual respondents ($M = 5.503$, $SE = .146$ vs. $M = 4.675$, $SE = .439$). Table 4 displays the mean proportions (and SEs) of abusiveness ratings for online behaviors by Respondent race, age, and gender. Main effects of Respondent race for *using sexually offensive name calling/insults*, $F(1, 147) = 4.453$, $p = 0.037$, $\eta^2 = 0.029$ (Power = 0.554), *using religiously offensive name calling/insults*, $F(1, 147) = 4.396$, $p = 0.038$, $\eta^2 = 0.029$ (Power = 0.549), *belittling intelligence through name calling/insults*, $F(1, 147) = 5.463$, $p = 0.021$, $\eta^2 = 0.036$ (Power = 0.596), and *berating through curses/vulgarity*, $F(1, 147) = 4.914$, $p = 0.028$, $\eta^2 = 0.032$ (Power = 0.918) were found. Non-white respondents rated these online behaviors as more abusive than their White counterparts.

Main effects of Respondent age were found for *teasing/laughing at mistakes*, $F(1, 147) = 4.088$, $p = 0.045$, $\eta^2 = 0.027$ (Power = 0.519), and *icing out of group chats*, $F(1, 147) = 5.903$, $p = 0.016$, $\eta^2 = 0.039$ (Power = 0.675), indicating that older respondents rated these behaviors as more abusive than younger respondents (see Table 4). There were also main effects of Respondent gender for *sharing intimate photos without consent*, $F(1, 147) = 3.945$, $p = 0.049$, $\eta^2 = 0.026$ (Power = 0.505), *posting deepfakes*, $F(1, 147) = 5.655$, $p = 0.019$, $\eta^2 = 0.037$ (Power = 0.656), *posting embarrassing private information*, $F(1, 147) = 9.498$, $p = 0.002$, $\eta^2 = 0.061$ (Power = 0.865), *sextorting*, $F(1, 147) = 4.422$, $p = 0.037$, $\eta^2 = 0.029$ (Power = 0.551), *stalking*, $F(1, 147) = 3.858$, $p = 0.051$, $\eta^2 = 0.026$ (Power = 0.497), *teasing/laughing at mistakes*, $F(1, 147) = 12.476$, $p = 0.001$, $\eta^2 = 0.078$ (Power = 0.939), *threatening physical violence*, $F(1, 147) = 9.668$, $p = 0.002$, $\eta^2 = 0.062$ (Power = 0.871), *soliciting group attack*, $F(1, 147) = 8.340$, $p = 0.004$, $\eta^2 = 0.054$ (Power = 0.818), *insulting*, $F(1, 147) = 9.484$, $p = 0.002$, $\eta^2 = 0.061$ (Power = 0.864), *using racially offensive name calling/insults*, $F(1, 147) = 12.621$, $p = 0.001$, $\eta^2 = 0.079$ (Power = 0.942), *using sexually offensive name calling/insults*, $F(1, 147) = 9.162$, $p = 0.003$, $\eta^2 = 0.059$ (Power = 0.852), *using religiously offensive name calling/insults*, $F(1, 147) = 9.900$, $p = 0.002$, $\eta^2 = 0.063$ (Power = 0.878), *belittling intelligence through name calling/insults*, $F(1, 147) = 11.901$, $p = 0.001$, $\eta^2 = 0.075$ (Power = 0.929), *icing out of group chats*, $F(1, 147) = 7.651$, $p = 0.006$, $\eta^2 = 0.049$ (Power = 0.785), *berating through curses/vulgarity*, $F(1, 147) = 7.552$, $p = 0.007$, $\eta^2 = 0.049$ (Power = 0.779), *controlling/intimidating/scaring*, $F(1, 147) = 5.668$, $p = 0.019$, $\eta^2 = 0.037$ (Power = 0.657), and *encouraging self-harm*, $F(1, 147) = 4.186$, $p = 0.043$, $\eta^2 = 0.028$ (Power = 0.529). As shown in Table 4, women rated these specific behaviors as more abusive than men. A significant two-way interaction of Respondent gender and age was found for *sending repeated non-offensive texts and content*, $F(1, 147) = 4.671$, $p = 0.032$, $\eta^2 = 0.031$ (Power = 0.574), and for *controlling/intimidating/scaring*, $F(1, 147) = 7.995$, $p = 0.005$, $\eta^2 = 0.052$ (Power = 0.802). As shown in Figure 3, older men rated both online behaviors as more abusive than younger men, whereas there were no age differences in the ratings by women. Significant gender differences were found for young respondents' ratings of *controlling/intimidating/scaring*, but the other comparisons for both behaviors were not significant.

Table 4. Abusive ratings for online behaviors by Respondent race, age, and gender[a]

Behaviors	Age		Gender		Race	
	Younger	Older	Female	Male	Non-white	White
Sharing intimate photos	6.232 (.158)	6.337 (.152)	**6.506 (.159)**	**6.062 (.153)**	6.285 (.124)	6.236 (.232)
Sharing embarrassing photos	5.610 (.179)	5.918 (.172)	5.973 (.181)	5.555 (.173)	5.776 (.140)	5.694 (.263)

Posting deep fakes	6.037 (.159)	6.090 (.153)	**6.331 (.161)**	**5.796 (.154)**	6.110 (.125)	5.850 (.235)
Spreading malicious rumors	5.951 (.148)	5.892 (.142)	6.122 (.149)	5.721 (.143)	5.922 (.116)	5.862 (.218)
Posting embarrassing information	5.356 (.160)	5.768 (.153)	**5.910 (.161)**	**5.214 (.154)**	5.690 (.130)	5.115 (.244)
Blackmailing	6.402 (.116)	6.581 (.111)	6.621 (.117)	6.361 (.112)	6.541 (.091)	6.312 (.170)
Sextorting	6.573 (.111)	6.614 (.107)	**6.759 (.112)**	**6.428 (.107)**	6.619 (.087)	6.481 (.164)
Stalking	6.243 (.148)	6.366 (.142)	**6.510 (.149)**	**6.100 (.142)**	6.344 (.116)	6.149 (.217)
Teasing user's mistakes	**4.586 (.189)**	**5.118 (.181)**	**5.323 (.191)**	**4.381 (.182)**	4.946 (.155)	4.512 (.291)
Physically threatening violence	6.287 (.131)	6.517 (.126)	**6.690 (.133)**	**6.113 (.127)**	6.502 (.106)	6.038 (.199)
Soliciting group attack	6.257 (.150)	6.243 (.144)	**6.557 (.152)**	**5.943 (.145)**	6.305 (.119)	5.993 (.224)
Catfishing	5.539 (.197)	5.297 (.189)	5.513 (.199)	5.323 (.190)	5.490 (.153)	5.138 (.288)
Impersonating	5.472 (.182)	5.789 (.174)	5.838 (.183)	5.423 (.175)	5.682 (.142)	5.435 (.267)
Insulting	5.282 (.137)	5.426 (.132)	**5.439 (.207)**	**4.545 (.198)**	5.127 (.165)	4.497 (.310)
Racially offensive name-calling	6.040 (.158)	6.066 (.152)	**6.450 (.160)**	**5.656 (.153)**	6.160 (.128)	5.617 (.240)
Sexually offensive name-calling	5.875 (.165)	6.020 (.158)	**6.301 (.167)**	**5.595 (.159)**	**6.089 (.133)**	**5.424 (.249)**
Religiously offensive name-calling	5.795 (.168)	5.945 (.161)	**6.244 (.169)**	**5.497 (.162)**	**6.013 (.135)**	**5.339 (.254)**
Belittling intelligence	5.219 (.180)	5.612 (.172)	**5.854 (.182)**	**4.977 (.174)**	**5.597 (.147)**	**4.764 (.276)**
Icing out of group chat	**4.160 (.216)**	**4.891 (.207)**	**4.948 (.218)**	**4.103 (.208)**	4.645 (.174)	4.097 (.326)
Berating with curses/vulgarity	4.776 (.209)	5.159 (.200)	**5.373 (.211)**	**4.562 (.202)**	**5.154 (.167)**	**4.285 (.312)**
Joking about protected groups	4.847 (.209)	5.329 (.201)	5.283 (.211)	4.893 (.202)	5.189 (.164)	4.751 (.308)
Reposting multiple times	3.180 (.265)	3.817 (.254)	3.546 (.267)	3.451 (.255)	3.586 (.207)	3.273 (.389)
Trolling	3.692 (.234)	4.308 (.225)	4.239 (.236)	3.762 (.226)	4.147 (.184)	3.515 (.346)
Sending repeated texts	3.257 (.252)	3.892 (.242)	3.578 (.254)	3.571 (.243)	3.735 (.200)	3.133 (.375)
Controlling/intimidating/scaring	5.424 (.196)	5.580 (.188)	**5.832 (.198)**	**5.172 (.189)**	5.604 (.159)	5.151 (.297)
Privately sharing personal information	5.654 (.187)	5.703 (.179)	5.659 (.189)	5.698 (.181)	5.801 (.146)	5.284 (.273)
Encouraging self-harm	6.477 (.133)	6.446 (.127)	**6.653 (.134)**	**6.270 (.128)**	6.466 (.105)	6.429 (.197)

[a] Bold numbers indicate significant differences.

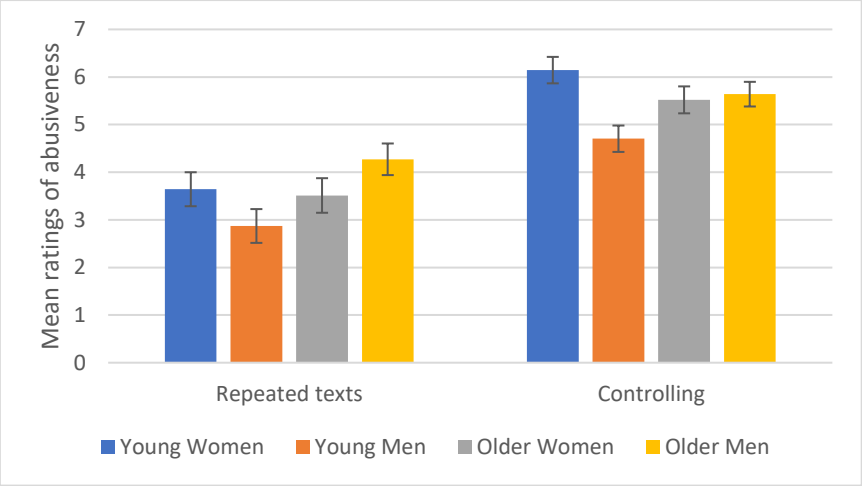

Figure 3. Mean ratings of abusiveness for repeated non-offensive texts and content And for controlling behaviors by Respondent age and gender

3.2. User features and behaviors that increase their likelihood of being targeted

Respondents' beliefs regarding six categories of user features (age, gender, religion, sexual orientation, race, and expressing an opinion) and SMP behaviors likely to increase users' chances of becoming a target were analyzed. The first analysis examined which user features respondents believed affected targeting for cyber abuse using mixed model ANCOVAs with age group and gender as the between-subject factors, race and sexual orientation as the covariates (Respondent sexual orientation, M = 1.15; Respondent race, M = 1.23), and levels of each characteristic as the within-subject factors. A main effect of Respondent race was found for User gender, $F(1, 130) = 6.311$, $p = 0.013$, $\eta^2 = 0.046$ (Power = 0.703), indicating that a higher proportion of non-White than White respondents believed the gender of the user was associated with increased targeting (M = .966, SE = .017 vs. M = .861, SE = .058). A main effect of Respondent gender was found for User opinion, $F(1, 130) = 4.132$, $p = 0.044$, $\eta^2 = 0.031$ (Power = 0.523), showing that a higher proportion of women than men believed expressing opinions on SMPs increased likelihood of being targeted (M = .985, SE = .030 vs. M = .901, SE = .029).

In the next analysis, each user feature was examined separately. Main effects of User age, $F(1, 123) = 4.455$, $p = 0.005$, $\eta^2 = 0.091$ (Power = 0.870), revealed that a higher proportion of respondents believed that users aged 14-17 years (M = .560, SE = .042) are targeted more than those aged 11-13 years (M = .261, SE = .038) and those aged 18-24 years (M = .237, SE = .036), which, in turn, were targeted more than users aged 26-34 years (M = .044, SE = .017). A two-way interaction of Respondent gender and User gender, $F(1, 129) = 3.574$, $p = 0.031$, $\eta^2 = 0.052$ (Power = 0.654), shown in Figure 4, revealed that a higher proportion of men than women believed that male users are targeted for cyber abuse. In contrast, no sex differences were found for female and non-binary users. Women believed that female users are targeted more than non-binary users, who in turn were targeted more than male users. Men believed that female and non-binary users were both targeted more than male users. Main effects of User religion ($F(1, 123) = 4.854$, $p = 0.029$, $\eta^2 = 0.038$ (Power = 0.589), indicated that respondents believed users whose religions are Catholic/Christian are less likely than users of other religions to become targets of cyber abuse (M = .185, SE = .035 vs. M = .870, SE = .030). A main effect of User race, $F(1, 124) = 13.303$, $p = 0.001$, $\eta^2 = 0.097$ (Power = 0.951), showed that respondents believed non-White users are more likely than White users to become targeted for cyber abuse (M = .917, SE = .025 vs. M = .105, SE = .027). There were no significant main effects or interactions for User sexual orientation.

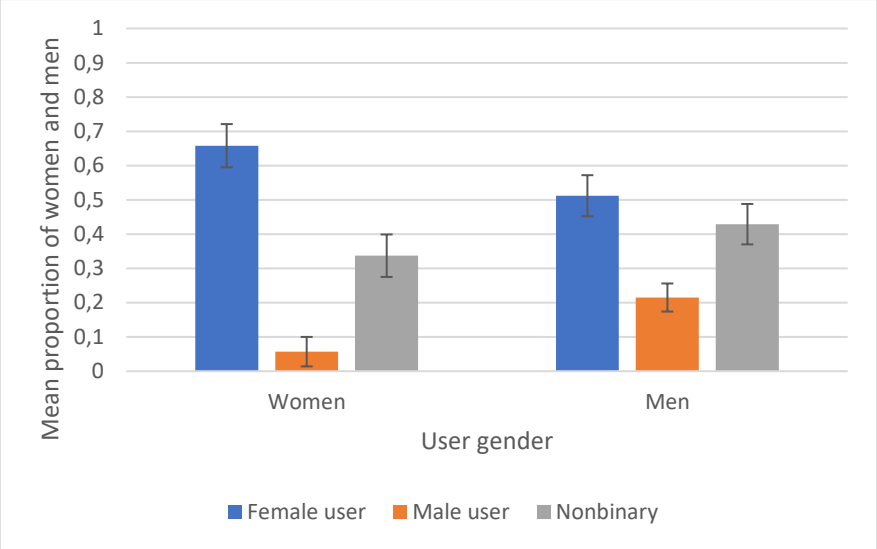

Figure 4. Mean proportion of women and men's beliefs about users being targeted due to their gender

The three types of opinions (politics, abortion, and gender roles) were examined separately in the following ANCOVA analyses. A significant two-way interaction of Respondent age and sex was found for User political opinion expressed, $F(1, 123) = 7.501$, $p = 0.007$, $\eta^2 = 0.057$ (Power = 0.776). A higher proportion of older men than older women (but not younger men versus women) believed that users are targeted for their political opinions (see Figure 5). Also, a higher proportion of younger than older women believed users are politically targeted for cyber abuse, whereas no significant age differences were found for men. Interestingly, the specific political party endorsed by users was not considered to be a relevant factor in determining targeting. For User abortion opinions, a main effect of sex was borderline significant, $F(1, 123) = 3.595$, $p = 0.06$, $\eta^2 = 0.028$ (Power = 0.469), suggesting that women tended to be more likely than men to indicate User abortion opinions increased the likelihood of cyber abuse ($M = .309$, $SE = .038$ vs. $M = .205$, $SE = .038$). A two-way interaction of Respondent age and User abortion opinion, $F(1, 123) = 4.756$, $p = 0.031$, $\eta^2 = 0.037$ (Power = 0.581), indicated that older respondents were more likely than their younger counterparts to believe that users who expressed pro-choice opinions are targeted for cyber abuse, but age differences in targeting were not found for users expressing pro-life opinions (see Figure 6). Also, a higher proportion of younger respondents believe that users who express pro-life opinions are targeted more than those who promote pro-choice opinions for cyber abuse, but this opinion difference was not found with older respondents. For the third type of opinion on User gender roles, a main effect emerged for Respondent sexual orientation, $F(1, 130) = 3.919$, $p = 0.050$, $\eta^2 = 0.030$ (Power = 0.502): heterosexual respondents were more likely than non-heterosexual respondents to believe that users expressing gender-role opinions (regardless of specific view) would be targeted ($M = .420$, $SE = .045$ vs. $M = .125$, $SE = .085$).

In the last analysis, ratings of various online behaviors believed to increase the likelihood of users becoming victims were subjected to a 2 (Respondent gender: male, female) X 2 (Respondent age group: Younger, Older) multivariate analysis of covariance (MANCOVA) with race ($M = 1.22$) and sexual orientation ($M = 1.15$) as covariates. Table 5 shows the means and SEs for ratings of online behaviors by Respondent race, gender, and age. Main effects of Respondent race were found for *friend strangers*, $F(1, 139) = 3.911$, $p = 0.050$, $\eta^2 = 0.027$ (Power = 0.502), and for *post comments on controversial discussion boards*, $F(1, 123) = 3.895$, $p = 0.050$, $\eta^2 = 0.027$ (Power = 0.500). White respondents reported higher ratings than non-White respondents that users would be targeted for these two online behaviors. Main effects of Respondent gender were found for *selfies*, $F(1, 139) = 6.257$, $p = 0.014$, $\eta^2 = 0.043$ (Power = 0.700), *sharing PPI with strangers,* $F(1, 139) = 8.322$, $p = 0.005$, $\eta^2 = 0.056$ (Power = 0.817), and *meet strangers befriended online*, $F(1, 139) = 4.208$, $p = 0.042$, $\eta^2 = 0.029$ (Power = 0.531). A higher proportion of women than men believed that users who *shared personal information with strangers privately* and *agreed to meet strangers befriended online* were at increased risk of being targeted for cyber abuse, whereas a higher proportion of men than women believed that *posting selfies* led to increased risks for targeting. A main effect of Respondent age was found for *comments posted on controversial discussion boards, F(1, 139)* = 3.943, $p = 0.049$, $\eta^2 = 0.028$ (Power = 0.505), such that older

respondents provided higher ratings than younger ones, indicating that this behavior increased users' risk for targeting.

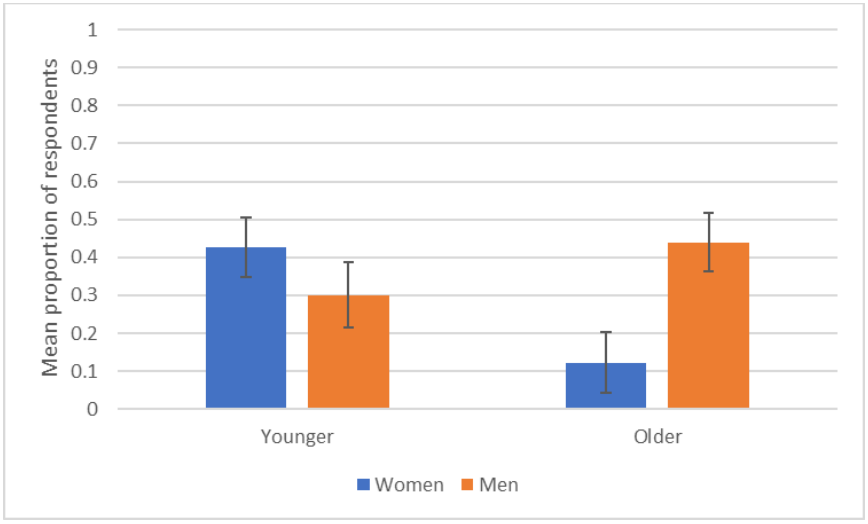

Figure 5. Mean proportion of respondents who believe users are targeted for cyber abuse because of their political opinions by Respondent age and gender

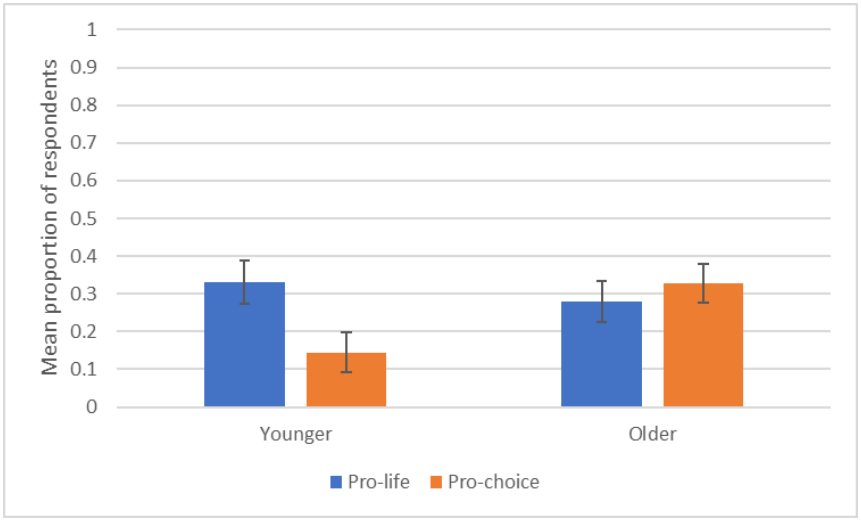

Figure 6. Mean proportion of respondents who believe that users are targeted for cyber abuse because they express pro-life and pro-choice abortion opinions by Respondent age

Table 5. Mean ratings (SEs) of online behaviors that increase the likelihood users will be targeted by Respondent race, gender, and age.

	Race		**Gender**		**Age**		**Overall Means (SEs)**
Strategies	White	Non-white	Female	Male	Younger	Older	
Keep settings public	.694 (.078)	.615 (.044)	.607 (.060)	.672 (.056)	.673 (.058)	.606 (.057)	.639 (.040)
Post PPI*	.806 (.067)	.758 (.039)	.793 (.053)	.741 (.050)	.746 (.051)	.788 (.051)	.767 (.036)
Post selfies	.333 (.080)	.242 (.039)	**.166 (.053)**	**.349 (.050)**	.275 (.052)	.240 (.051)	.257 (.036)

Post pictures of friends	.111 (.053)	.089 (.026)	.054 (.036)	.136 (.034)	.097 (.035)	.094 (.035)	.095 (.025)
Keep GPS location on	.583 (.083)	.489 (.045)	.567 (.062)	.443 (.058)	.477 (.060)	.534 (.059)	.505 (.042)
Geotag images	.278 (.076)	.339 (.043)	.385 (.056)	.242 (.053)	.284 (.055)	.343 (.054)	.313 (.038)
Friend strangers	**.667 (.080)**	**.500 (.045)**	.594 (.061)	.473 (.057)	.540 (.059)	.527 (.058)	.534 (.041)
Share PPI* with strangers privately	.806 (.067)	.691 (.042)	**.820 (.055)**	**.600 (.052)**	.714 (.054)	.706 (.053)	.710 (.037)
Meet strangers befriended online	.556 (.084)	.463 (.045)	**.559 (.061)**	**.386 (.057)**	.432 (.059)	.513 (.058)	.472 (.041)
Like video/image/message	.111 (.053)	.121 (.029)	.111 (.041)	.137 (.038)	.142 (.040)	.107 (.039)	.124 (.028)
Post comments on controversial discussion board	**.778 (.070)**	**.569 (.045)**	.597 (.059)	.634 (.055)	**.695 (.057)**	**.535 (.056)**	.615 (.040)
Post comments on hostile sites	.722 (.076)	.669 (.042)	.678 (.058)	.670 (.054)	.702 (.056)	.645 (.055)	.674 (.039)
Join site where user is in minority group	.394 (.086)	.371 (.044)	.370 (.060)	.380 (.056)	.421 (.058)	.330 (.057)	.375 (.041)
Friend unknown user requests	.750 (.073)	.573 (.045)	.678 (.060)	.530 (.056)	.599 (.058)	.609 (.058)	.604 (.041)
Post provocative profile	.583 (.083)	.492 (.045)	.565 (.062)	.490 (.058)	.488 (.060)	.567 (.059)	.528 (.042)
Use same name across platforms	.194 (.067)	.244 (.039)	.246 (.052)	.210 (.049)	.269 (.051)	.187 (.050)	.228 (.035)
PPI* with selfie on profile	.722 (.076)	.545 (.045)	.610 (.061)	.521 (.057)	.556 (.059)	.575 (.058)	.565 (.041)

[a] Bold numbers indicate significant differences. *PPI refers to personally identifiable information.

3.3. Strategies for responding to online behaviors rated as cyber-abusive

Respondents' effectiveness rankings of strategies to thwart cyber abuse were analyzed using MANCOVA (1-13, with lower numbers indicating the most effective and higher numbers the least effective). As shown in Table 6, a main effect of Respondent sexual orientation was found for *post support for abused user*, $F(1, 142) = 4.695$, $p = 0.033$, $\eta^2 = 0.032$ (Power = 0.576), revealing that this strategy was considered by heterosexual respondents to be a more effective strategy for dealing with cyber abuse than by non-heterosexual respondents. A main effect of Respondent race was found for *ignore abusive user*, $F(1, 142) = 7.756$, $p = 0.006$, $\eta^2 = 0.052$ (Power = 0.790), showing that White respondents considered this strategy to be more effective for dealing with cyber abuse than did non-White respondents. There were also main effects of Respondent gender for *ignore abusive user*, $F(1, 142) = 6.589$, $p = 0.011$, $\eta^2 = 0.044$ (Power = 0.715), *avoid platform temporarily*, $F(1, 142) = 4.350$, $p = 0.021$, $\eta^2 = 0.030$ (Power = 0.544), and *talk to a friend*, $F(1, 142) = 4.706$, $p = 0.032$, $\eta^2 = 0.039$ (Power = 0.577). Men rated *ignore abusive user* and *avoid platform temporarily* as more effective strategies than did women, whereas women rated *talk to friend* as a more effective strategy than did men. A significant two-way interaction of Respondent age and gender was found for *post support for abused user* $F(1, 142) = 4.844$, $p = 0.029$, $\eta^2 = 0.033$ (Power = 0.589). As shown in Figure 7, older women believed this strategy was more effective for dealing with cyber abuse than did younger women, whereas no age differences were found for men. Also, older women tended to believe this strategy was more effective than did older men (p =.052), but no sex differences were found for younger respondents.

Table 6. Rankings for strategies to thwart cyber abuse by Respondent sexual orientation, age, and gender[a]

Strategies	Sexual Orientation		Race		Gender		Overall
	Hetero-sexual	Non-hetero-sexual	Non-White	White	Female	Male	Mean *
Report to social media platform	3.875 (.297)	2.861 (.898)	3.241 (.370)	3.495 (.870)	3.213 (.347)	3.874 (.334)	3.536 (.238)
Request removal of user/content	4.654 (.290)	3.861 (.874)	4.413 (.360)	4.102 (.848)	4.431 (.340)	4.59 (.327)	4.505 (.232)
Report to legal/school authority	5.525 (.342)	6.000 (1.032)	5.568 (.425)	5.957 (1.000)	5.324 (.400)	5.728 (.384)	5.526 (.273)
Block abusive user	3.259 (.286)	4.250 (.863)	4.042 (.356)	3.468 (.837)	3.934 (.332)	3.222 (.319)	3.578 (.227)
Ignore abusive user	5.699 (.372)	5.556 (1.123)	**6.733 (.463)**	**4.522 (1.089)**	**7.031 (.427)**	**5.502 (.411)**	6.266 (.292)
Avoid platform temporarily	7.445 (.337)	7.389 (1.016)	7.425 (.419)	7.409 (.985)	**8.002 (.389)**	**6.875 (.374)**	7.438 (.266)
Remove account	7.095 (.353)	7.083 (1.066)	7.964 (.439)	6.215 (1.034)	7.397 (.417)	7.160 (.401)	7.279 (.285)
Request user stop	9.054 (.330)	8.167 (.996)	8.813 (.410)	8.403 (.966)	9.023 (.385)	9.050 (.370)	9.037 (.263)
Post support for victim	**9.427 (.270)**	**10.722 (.816)**	9.655 (.336)	10.489 (.792)	9.314 (.311)	9.577 (.299)	9.446 (.213)
Talk to friend about it	7.454 (.292)	8.472 (.881)	7.222 (.363)	8.704 (.854)	**6.818 (.336)**	**7.854 (.323)**	7.336 (.230)
Talk to family about it	8.363 (.323)	8.444 (.976)	7.700 (.402)	9.108 (.946)	7.835 (.379)	8.484 (.364)	8.159 (.259)
Solicit others to protest	10.092 (.272)	9.694 (.821)	9.512 (.338)	10.274 (.796)	9.591 (.318)	9.989 (.305)	9.790 (.217)
Remove/limit own content	9.120 (.383)	8.500 (1.157)	8.771 (.477)	8.855 (1.122)	9.090 (.447)	9.285 (.430)	9.187 (.306)

[a] Lower numbers represent strategies ranked as most effective, whereas higher numbers represent strategies ranked as least effective. Numbers in bold indicate significant differences.

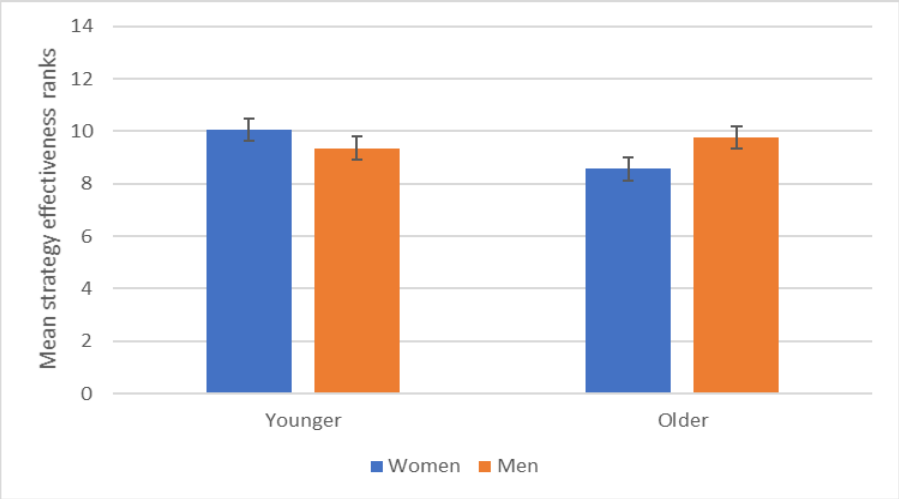

Figure 7. Mean effectiveness rank for supporting the abused victim as a strategy by Respondent age and gender

4. Discussion

The purpose of this study was to gather information from a diverse sample of college students on self-definitions of cyber abuse; factors that affect their identification and perception of cyber abuse on SMPs; and knowledge of user risks and strategies for countering cyber abuse when it occurs. Important benefits of this study's methodology were that participants consisted of racially/ethnically diverse college students between ages 18 and 27, approximately half of whom were men, and both qualitative and quantitative data regarding cyber abuse from younger (18 to 21 years) and older (22 to 27 years) age groups were compared. Below, each of the four study aims is reviewed in light of both the Lifestyle Routine Activity theory framework and previous findings.

4.1. Practical implications for theory and practice

To address our first study aim, a college student sample provided their own definitions of cyber abuse, indicated factors they believe influence their identification of online behaviors that exemplify cyber abuse, and made judgments of abusiveness for various types of content. Respondents provided an average of 1.68 definitions, with the highest proportion of respondents indicating cyber harassment and bullying (65%), followed by criticizing (29%), flaming (16%), and criminal use (14%). While respondents' definitions did incorporate many of the concepts elucidated in prior research (e.g., MacDonald & Roberts-Pittman, 2010), demographic differences emerged, possibly as a reflection of divergent social media or other online experiences and/or resistance to accepting abusive behavior (Bauman & Baldasare, 2015; Halsop et al., 2021; Vogels, 2021b). For instance, women defined cyber abuse as 'criticizing' more often than did men. This result may be explained by findings that women, in comparison to men, conceptualize breaches in politeness, such as criticism, differently (Holmes & Schurr, 2005). They may also experience higher rates of online misogynistic, hateful, and sexual harassment comments targeting their individual characteristics and/or group that negatively affect them, resulting in them avoiding platforms on which such behaviors occurred (Nadim & Fladmoe, 2021). Additional examples included that a higher proportion of White respondents defined cyber abuse as 'criminal use' than did their non-White peers, whereas non-heterosexual respondents were more likely than heterosexual respondents to include 'cyberstalking' and 'scamming' in their definitions. Racial and sexual-orientation differences in defining cyber abuse may be attributed to variations in these groups' rates of cyber victimization. According to Kowalski et al. (2020), non-Whites were more likely than Whites to state that race played a role in their cyber victimization (53.7% vs/ 17./9%). Also, non-heterosexual users were found to experience high rates of cyber stalking (Reyns et al., 2012) and online abuse (Blumenfeld & Cooper, 2010).

However, whether any of these behaviors rises to the level of cyber abuse depends on contextual factors, which students also evaluated. Specifically, respondents provided judgments of abusiveness for various types of content and online behaviors as a function of the number of occurrences, the target's emotion, and the nature of the content. Respondents were not concerned with frequency when determining abusiveness (Dredge et al., 2014a), which was interesting given that there is no consensus among state laws regarding the number of times an act must occur (once vs. more than once) to meet the statute requirement for abuse (PenAmerica, 2025). Group differences were found in the use of victims' responses and content when judging cyber abuse. White respondents relied more on a victim's adverse emotional reaction than did their non-White peers to determine whether cyber abuse occurred, and they also judged negative emotional responses as a more important factor than negative behaviors in determining cyber abuse. Similarly, regarding content, older men and younger women indicated that content influenced their judgments of abusiveness more than it did for younger men.

Respondents also rated the abusiveness of different types of content across media. Overall, raters were nuanced in their perceptions of abusiveness across media types (Lawler & Moluzzo, 2015). Women rated abusiveness higher than men across content (violent, sexual, offensive, extremist) and media type (image, video, message). Sexual images and videos were rated as most abusive, compared to all other types of content, and sexual messages were considered more abusive than those with extremist content. Yet, violent messages were rated as more abusive than violent images, and sexual videos were rated more abusive than sexual messages. No doubt, social and cultural influences impact these perceptions (Vogels, 2021b).

While students were cognizant of both the factors and content that influenced their judgments of cyber abuse, the degree of exposure to (and experience with) cyber abuse seemed to differ as a function of their demographics. Moreover, without capable guardians in the form of SMP administration, students were accepting of cyber abuse as part of the cost of being online, rather than disengaging from toxic environments, thereby further increasing their visibility as suitable victims to motivated offenders. Thus, even for the foundational task

of defining cyber abuse and assessing the abusiveness of the content, demographic differences in this sample of college students emerged that underscore the importance of experience in understanding the impact of cyber abuse on potential victims, bystanders, and other users, including their experience with cyber abuse of various degrees of seriousness, as noted below.

For the second study aim, college students rated the abusiveness of various online behaviors and, here again, demographic differences emerged, likely reflecting individuals' varied experiences. For instance, heterosexual respondents rated sharing embarrassing private information as more abusive than did non-heterosexual respondents. Concerning race/ethnicity, non-White respondents rated sexually and religiously offensive insults, belittling intelligence, and berating with vulgarity as more abusive than did White respondents. It is plausible that sub-group differences in being subjected to such abusive behaviors, such as through microaggressions or explicit insults, could inform such ratings (Bauman & Baldasare, 2015). Age effects also appeared, as did numerous gender effects, with women rating behaviors as more abusive than men. Older respondents tended to find behaviors more abusive than did younger ones, particularly men. Yet most salient were consistent gender differences with women rating more behaviors, particularly those classified as image-based sexual abuse (e.g., sharing non-consensual intimate photos), as more abusive than did men (also see Haslop et al., 2021). Two exceptions were sending repeated, non-offensive texts and controlling behaviors, which older men rated as more abusive than did women. Due to the absence of diversity in past studies, demographic differences were not reported, yet previous college students identified as cyber abuse many of the same behaviors as did ours (Lawler & Moluzzo, 2015; Vogels, 2021b).

Together, these findings highlight the extent to which variation exists in perceptions of cyber abuse. The abuse is, to some extent, in the eye of the beholder. Yet, in line with LRAT, these ratings likely also aligned with differential experiences of cyber abuse by specific user groups. For instance, women are especially and uniquely likely to experience abuse in online gaming contexts, perhaps informing their reflections on what constitutes abuse and to what degree different behaviors are abusive (Ahmead et al., 2024; Tompson & Tomkins, 2025; Zhou & Peterson, 2025). Additionally, Haslop et al. (2021) indicated that the prevalence of repeated unsolicited sexual images sent to women was so common that they were considered to be the norm. Often, the responsibility for protecting users from abuse is unfairly placed on the users themselves rather than on the platforms, which, as guardians, should proactively shield them as per the terms of service user agreement contracts (Shapiro, 2023; Zhou & Peterson, 2025). Such pressure likely contributed to college students' beliefs that they are capable of handling various online social and technology risks, consequently resulting in them failing to use protective measures (McClain et al., 2023; Sharma et al., 2015).

To address our third aim, college students indicated which demographic features and online behaviors they believed increased the likelihood of a user being targeted. Respondents' own demographics were associated with different opinions about user features that contributed to targeting. Specifically, user opinion was mentioned more by women than men as potential targeting risks, whereas user gender was mentioned by non-Whites more than Whites, highlighting intersectional differences. User age predicted risk for cyber abuse such that adolescents (ages 14-17) were considered to be more vulnerable to victimization than preadolescents (11-13) or adults ages 18 to 24, whereas adults ages 26 to 34 were considered least likely to be targeted.

Targeting risk was reported to be greater for users who were non-White and those who practiced non-Catholic/Christian religions. Interestingly, respondents' own gender and race influenced their beliefs about the risks associated with user gender. Specifically, men believed that female and non-binary users were both targeted more than male users, whereas women thought female users were targeted more than non-binary users, who were targeted more than male users. Men indicated higher rates than women for male users to be targeted for cyber abuse. Non-White respondents believed more than White respondents that gender increased targeting risk for cyber abuse. Past research found that college students reported being targeted for their appearance, particularly those who identify as women, nonbinary, or non-heterosexual; are minority ethnicities/races; and/or practice minority religions (Haslop et al., 2021; Hollis, 2016; Lawler & Moluzzo, 2015; Pew Research Center, 2017). The current findings replicated past research (Reyns et al., 2012; Vogels, 2021a) showing gender differences in the identification of gender as a reason for targeting. The perception by our college student sample that older adolescents were more vulnerable to cyber abuse than younger adolescents supported work by Trinidad et al. (2025), who found that older adolescents (aged 15 to 18) reported a higher prevalence of negative experiences on social networks than did younger adolescents (aged 12 to 14). It was also consistent with Bularca et al. (2024), who found that young adults ages 18 to 21 reported being targeted for cyber abuse more than those ages 22 to 25 or 26 to 30.

Respondents also indicated that users' opinions contributed to them becoming victims of cyber abuse. Specifically, older men and younger women were more concerned than older women that users who expressed their political beliefs would be targeted. These findings contrast with those from Vogels (2021a), who indicated that male or White users were attacked the most for expressing political opinions. Fear of reprisals for expressing one's political opinion is consistent with McClain (2021), who found that adults did not want to post or share their political views because they feared being attacked (32%) or having it used against them (33%). While no party differences were found in McClain's study, our study found greater criticism of Republican than Democratic views. Women also indicated that users' expression of abortion opinions increased their targeting for cyber abuse. The type of abortion opinion expressed was considered to be a factor in being targeted differently according to respondent age. Older respondents believed that pro-choice opinions would make users vulnerable to cyber abuse, whereas younger respondents believed that pro-life opinions would make users likely to be targeted. Lastly, heterosexual respondents were concerned that users' gender role opinions would increase their vulnerability to cyber abuse.

Respondents also indicated that users' online behaviors make them targets for cyber abuse. Of the 17 online behaviors presented to respondents, five were judged to be low risk (0%-33%), nine of moderate risk (34%-67%), and three of high risk (68%-100%). Gender differences were found for one low-risk, one moderate-risk, and one high-risk behavior. Men believed that users are targeted for posting selfies, while women indicated that users are targeted for meeting strangers and sharing personal private information with strangers. Race differences were observed for two moderate-risk behaviors. White respondents believed that users are targeted for two behaviors: friending strangers and commenting on controversial discussion boards. Age differences were noted for one moderate-risk behavior. Older college students (ages 22-27) thought that posting comments on controversial discussion boards increased users' likelihood of being targeted. Past research supports these findings, showing that certain online behaviors—especially indiscriminate friending and posting indiscreet content such as alcohol use, sexual activities, sexually explicit images, personally identifiable information, and geotagging—increased users' risks of cyber abuse (Dredge et al., 2014b; Lee & Soonah, 2023; Peluchette et al., 2015). According to a study by Ngo et al. (2020, p. 440), socializing online (83%) and communicating with strangers (21%) were linked to increased risk for specific types of cyber abuse, such as harassment by nonstrangers (increased by 230%) and unwanted porn (increased by 110%). Ngo et al. reported that cybercrime victimization—like receiving unwanted pornographic messages and photographs, harassment—was also predicted by posting selfies (18%) and sharing personally identifiable information (7% home address, 14% phone number, 8% sexual orientation). Students were aware that their online lifestyle choices and social media behaviors, such as frequent posting, sharing photos, and revealing personal information (Fansher & Randa, 2019; Marcum & Higgins, 2021), increased their vulnerability and visibility to motivated offenders (Leukfeldt & Yar, 2016). However, they continued to engage in these risky behaviors due to impulsivity, reward seeking, optimism, invulnerability, and the anticipation of social and sexual gains (Ellis et al., 2012; Willoughby et al., 2021).

Consistent with LRAT, college students in this study were cognizant that users who exhibited certain demographics (non-White, preteens, female), expressed their political and abortion opinions, and/or engaged in moderate and high-risk online behaviors, particularly interacting with strangers, increased their visibility to motivated offenders and, ultimately, their risk of being victimized. It was unclear, however, whether this knowledge translated into users' self-guardianship by changing their own behaviors to reduce their accessibility and visibility to motivated offenders as targets (Tompson & Tomkins, 2025). Also unknown was whether traditional guardians, such as family and school programs, by informing specific groups that they are at risk for being targeted or by educating them about the risks associated with specific online behaviors, were effective in reducing users' vulnerability to cyber abuse (Haslop et al., 2021; Vogels, 2021a).

Finally, college students ranked the effectiveness of 13 online behavioral strategies used by victims and bystanders to prevent cyber abuse. Four strategies were considered to be the most effective, based on the proportion of respondents who ranked them first through fourth, with overall mean ranks ranging from 3.54 to 5.52 out of 13. These included blocking the abusive user (75%), reporting abuse to SMP (70%), requesting SMP remove the abusive user or content (62%), and reporting to a school or legal authority (48%). Notably, none of the mean ranks for these platform strategies differed significantly by age, gender, sexual orientation, or race, indicating that these strategies were generally the first methods most respondents used to address cyber abuse. Previous studies show that college students often choose these strategies as victims and/or bystanders. Gahagan et al. (2016) found that 27% of cyber-victimized college students used blocking the abuser. Interestingly, Bularca et al. (2024) observed that more students reported incidents to the platform when they

were victims (30%) compared to witnesses (6%). According to a national sample of young adults (ages 18 to 28, Colburn et al., 2023), only 7.3% of 1,952 cyber abuse victims reported incidents to SMPs, with 42.2% of these finding the SMP helpful, though only 29.2% believed reporting improved the situation (p. 11651). There were no differences in reporting incidents to SMP based on victim gender (6.4% men vs. 7.3% women, p. 11652). When asked to whom they would report cyberbullying, college students in Lawler and Molluzzo's (2015) study selected school authorities (37% to Dean of Students, 23% to Dean of College), college security (27%), and local law enforcement (27%). Yet, victims in Colburn et al.'s (2023) study demonstrated low reporting rates to law enforcement (4.8%), and only 29.8% of these reports led to helpful responses, such as investigation, contacting the abusive user, showing sympathy, or providing resources (p. 11652). Dissatisfaction with law enforcement's handling of cases reduces the likelihood of future reports and increases the risk of ongoing abuse (Ahmead et al., 2024). However, students may also be unaware of how to report cyber abuse officially (Bidgoli et al., 2016). The use of the strategy requesting SMP to remove the abuser or content has not been specifically studied before, though it might be included under the category of reporting abuse to SMP.

Respondents ranked four of the listed strategies as moderately effective based on the proportion of respondents who ranked them 5th through 8th, with overall mean ranks ranging from 6.26 to 7.43 out of 13—avoiding platform temporarily (43%), ignoring abusive user (41%), removing the account (41%), and talking to a friend about it (40%). There were gender differences in perceived strategy effectiveness for avoiding the platform temporarily, which was preferred by men, and talking to a friend, which was preferred by women. The strategy to ignore the abusive user showed both gender and racial differences, with men and Whites endorsing it as more effective than did women and non-Whites. Past research supports that college students use at least three of these strategies when dealing with cyber abuse. According to Bularca et al. (2024), college students reported using strategies such as leaving the site (10% as victims, 5% as witnesses), ignoring the situation (13% as victims, 36% as witnesses), and talking to a friend about it (15% as victims). In Gahagan et al. (2016), college students used strategies like ignoring the abuser or incident (33% as victims and 55% as witnesses) and talking to friends (33% as victims); the latter was also used by college victims in Lawler and Moluzzo's (2015) study (13% fraternity/sorority members, 68% best friends). "Doing nothing" (similar to "ignoring the situation") was indicated by 17% of college students, whereas "getting away" (similar to "avoiding the platform") was used by 13% of college students in Alqahtani et al.'s (2018) study. The strategy of "removing an account" has not been previously examined.

Respondents ranked five of the listed strategies as the least effective based on the proportion of respondents rating them as 9th through 13th, with overall mean ranks ranging from 8.15 to 9.78 out of 13. These strategies include "soliciting others to help protest abusive behavior" (71%), "posting support for the victim" (70%), "removing or limiting one's own content" (64%), "requesting the user to stop" (62%), and "talking to family about it" (50%). The strategy of posting support for the victim was most endorsed by heterosexual and older female college students. No differences were found in ranked effectiveness for the remaining three strategies based on age, gender, sexual orientation, or race. Past research shows that college students have used similar advocate-like strategies to deal with cyber abuse (Moallem, 2018), such as witnesses supporting victims (15%, Gahagan et al., 2016; 8%, Bularca et al., 2024) and victims talking to their family (40%, Ahmead et al., 2024; 57%, Lawler & Moluzzo, 2015). The "request to stop from the user" has been previously reported as "telling the cyberbully to stop" (13% as victims, Alqahtani et al., 2018); "confronting the aggressor" (27% as victims, Bularca et al., 2024; 20% as victims and 24% as witnesses, Gahagan et al., 2024); and "making one's opinion clear to the aggressor" or "objecting to harassment" (10% and 7%, respectively, Bularca et al., 2024). However, the strategies of "soliciting help to protest abusive behavior" and "removing or limiting one's own content" have not been examined in previous research.

Three of the four strategies that were seen as the most effective by respondents involved "asking for help from SMP and legal guardians" to address cyber abuse, which aligns with LRAT (Ahmead et al., 2024). Past experiences where reporting cyber abuse led to satisfactory outcomes may have influenced the choice to appeal to authority. However, nine additional strategies for preventing cyber abuse included various self-protection methods (e.g., block user, avoid platform), possibly developed in response to dissatisfaction with formal guardians' actions when respondents and bystanders previously requested intervention (O'Connor et al., 2018; Wolak & Finkelhor, 2016). Alternatively, this could indicate a complete lack of capable guardians, leading users to seek their own solutions. The study did not directly address whether users perceive an absence of capable guardians, but the results suggest that such an absence could lower user protections, creating an environment vulnerable to cyber exploitation and increasing the chances that motivated offenders will target and abuse

attractive users. One clear result of ineffective or absent guardianship was that students had to endure cyber abuse incidents, choosing to stay online even when they were subjected to further victimization.

4.2. Limitations and future directions

Our sample of racially and ethnically diverse urban college students included equal representation of men and women; however, there were some limitations to this research. The study included a low proportion of non-heterosexual respondents. Additionally, despite having a racially diverse sample, this study could not distinguish experiences among different racial and ethnic groups, as members were unequally represented, leading to the grouping of non-white groups into a single category. As noted in the literature, social media experiences vary by race and ethnicity, making this an important variable for future research to explore. Therefore, the first recommendation for future studies is to replicate our research with diverse college students in other large urban areas and to carefully examine the intersectionality of age, gender, sexual orientation, and race/ethnicity by ensuring equal representation of these groups. Another limitation is that the study relied on self-reported data on cyber abuse on social media, which may be subject to bias in retrospective reports (Verbeij et al., 2021). However, concerns about recalling past experiences should be minimal since respondents were not asked for detailed accounts, which can be distorted. A final limitation is that this study employed a mixed-method approach. Future research should incorporate focus groups or open-ended surveys to explore how college students' social media platform use relates to past exposure to cyber abuse. Of particular interest would be whether guardians offer valuable advice on navigating social media safely, including how to avoid becoming targets and the importance of reporting incidents, and whether victims change their behaviors afterward, such as avoiding certain social media platforms known for abuse.

Our findings suggest there is a disconnect between the necessary and available remedies to protect college student users from cyber abuse. As predicted by LRAT theory, the failure of capable guardians to fulfill their duty to users creates opportunities for exploitation, with individual users trying different solutions with varying success. We therefore offer several practical suggestions for social media platforms, educators, policymakers, and law enforcement agencies to address this issue better. To protect and support students, colleges could provide more resources, training, and warnings about cyber abuse. As new technologies emerge, this need becomes more urgent. Students also require honest feedback on risky online behaviors they engage in and the consequences, both online and offline. While colleges may not control social media platforms or related behaviors, teaching students the importance of safe and responsible technology use is within their scope—and is reflected in emerging educational efforts around responsible use of generative AI. Expanding the focus to include responsible technology use would benefit all users. Colleges could also establish reporting mechanisms for abuse to designated campus authorities, such as their chief information officer or other technology staff. Although they don't control the platforms, students may be more willing to report abuse to familiar local authorities who can provide information, support, and resources to help protect them. Social media platforms must adhere to their own policies and offer meaningful protections for users requesting them. Policymakers should also take part in efforts to hold social media platforms accountable, if not for the actions of bad actors, then at least for enforcing their own policies and safeguarding users.

Law enforcement agencies will no doubt need to enhance training as cyber abuse and exploitation become increasingly sophisticated. However, because satisfaction with law enforcement responses tends to be low, an enhanced role in educating users may be more beneficial, perhaps in partnership with colleges. Educating students about their rights, appropriate uses of social media, and the legal parameters and limitations may empower users.

5. Conclusion

This topic is important because of the potential social, emotional, and cognitive harm caused by cyber abuse to college students, especially those in previously identified high-risk groups. Past studies failed to use age- and gender-representative, racially diverse college student samples, making both their cyber abuse prevalence rates and the generalizability of their findings questionable. This study showed that the cyber abuse experiences of 18- to 21-year-olds and 22- to 27-year-olds, men and women, and White and non-White individuals are not homogeneous.

Statement of Researchers

Researchers' contribution rate statement:	**First Author:** Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, software, supervision, validation, visualization, writing- original draft preparation, writing - review & editing.. **Second Author:** Data curation, formal analysis, validation, visualization, writing- reviewing & editing.
Conflict statement:	"The authors declare that they have no conflict of interest."
Data Availability Statement:	The data supporting this study's findings are available on request from the corresponding author. However, the data are not publicly available due to privacy or ethical restrictions.
Acknowledgements:	We verify and confirm that everyone who contributed to this manuscript is either listed as an author or acknowledged as a contributor in the acknowledgement section. Graduate student assistants acknowledged on this paper include Dayanna Uyaguari, Jia-Yi Mai, and Dangyeong Jo, They assisted by doing initial literature searches and review, coding data, and inputting data into the dataset.
Funding:	This project was supported by the Office of Advancement of Research (OAR) award on July 26, 2022.
Presentation(s) or Awards at a meeting:	This research extends a study presented at the American Society of Criminology (ASC, 2023).
Ethical Considerations:	This research, 2017-1086, was approved by the City University of New York University Integrated Institutional Review Board, dated November 18, 2022. All procedures followed were by the ethical standards of the committee responsible for human experimentation (institutional and national) and with the Helsinki Declaration of 1975, as revised in 2000. Informed consent was obtained from all participants for being included in the study.
Author Biographies	
Lauren R. Shapiro	Dr. Lauren R. Shapiro earned a PhD in Cognitive-Developmental Psychology from Rutgers University in 1990 (M.S., Ohio University, 1985; B.A., University of Buffalo, 1983) and a M.S. in Criminal Justice (Law specialization) in 2009 from Indiana State University. She is a Professor in the Department of Law, Police Science, & Criminal Justice Administration at John Jay College. Her research interests include interpersonal cybercrime, social media use and abuse, juvenile criminal stereotypes, eyewitness testimony and suggestibility, radicalization and terrorism, and children's storytelling. Her work has been presented at conferences and published in journals (Applied Cognitive Psychology, Child Development, Criminal Law Bulletin, Developmental Psychology, Journal of Applied Developmental Psychology, Security Journal). Dr. Shapiro authored the 2023 book, Cyberpredators and Their Prey, and coauthored the 2016 book, Multidisciplinary Investigation of Child Maltreatment. Dr. Shapiro is a member of the Journal of Applied Security Research editorial board and a Panel Reviewer for the Office of Justice Programs Grants Committee.
Angela M. Crossman	Dr. Angela M. Crossman earned a PhD in Developmental Psychology from Cornell University in 2001 (M.A., Cornell University, 1998; B.A., Dartmouth College, 1994). She is a Professor in the Department of Psychology at John Jay College-CUNY and a faculty member in the Psychology Doctoral Program at the CUNY Graduate Center. She currently serves as Interim Dean of Faculty at John Jay College. Her research interests include the reliability and credibility of children's testimony, the socialization and development of lying and truth-telling, and adolescent sexting behavior. Her research has been funded by the National Science Foundation and the Canadian Social Sciences and Humanities Research Council (with Dr. Victoria Talwar). Her research has been published in Developmental Review, the Journal of Experimental Child Psychology, and Trauma, Violence & Abuse. She is a member of the Child Maltreatment editorial board and a Fellow of the Association for Psychological Science.

6. References

Ahmead, M., ElSharifl, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. *Crime Science, 13*, 29-47. https://doi.org/10.1186/s40163-024-00230-w

Alipan, A., Skues, J.L., Theiler, S., & Wise, L. (2020). Defining cyberbullying: A multifaceted definition based on the perspectives of emerging adults. *International Journal of Bullying Prevention, 2*, 79–92. https://doi.org/10.1007/s42380-019-00018-6

Alqahtani, S., Elbedour, S., Freeman, K., Ricks, E., Reed, G., K. W., & Merrick, J. (2018). Cyberbullying in colleges and universities: A survey of student experiences and attitudes about cyberbullying. *International Journal of Child and Adolescent Health, 11(1)*, 73-97. https://novapublishers.com/shop/volume-11-issue-1-international-journal-of-child-and-adolescent-health/

https://www.questia.com/library/journal/1P4-2102830582/cyberbullying-in-colleges-and-universities-a-survey

Baldasare, A., Bauman, S., Goldman, L., & Robie, A. (2012). Chapter 8 cyberbullying? Voices of college students. In L. A. Wankel & C. Wankel (Eds.), *Misbehavior online in higher education* (pp. 127–155). Bingley, U.K.: Emerald Group Publishing Limited. https://doi.org/10.1108/s2044-9968(2012)0000005010

Bauman, S., & Baldasare, A. (2015). Cyber aggression among college students: Demographic differences, predictors of distress, and the role of the university. *Journal of College Student Development, 56(4)*, 317–330. https://doi.org/10.1353/csd.2015.0039

Beran, T., & Li, Q. (2007). The relationship between cyberbullying and school bullying. *The Journal of Student Wellbeing, 1(2)*, 15-33. https://doi.org/10.21913/jsw.v1i2.172

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal, 18(1)*, 48-58.

https://files.eric.ed.gov/fulltext/EJ1246231.pdf

Bidgoli, M., Knijnenburg, B.P., & Grossklags, J. (2016). *When cybercrimes strike undergraduates*. 2016 APWG Symposium on Electronic Crime Research. DOI: 10.1109/ECRIME.2016.7487948

Blumenfeld, W. J., & Cooper, R. M. (2010). LGBT and allied youth responses to cyber-bullying: Policy implications. International *Journal of Critical Pedagogy, 3(1)*, 114-133. https://janeway.uncpress.org/ijcp/article/id/626/

Brailovskaia, J., Schillack, H., & Margraf, J. (2020). Tell me why are you using social media (SM)! Relationship between reasons for use of SM, SM flow, daily stress, depression, anxiety, and addictive SM use– An exploratory investigation of young adults in Germany. *Computers in Human Behavior, 1o113*, 106511.

https://www.sciencedirect.com/science/article/abs/pii/S0747563220302636

Brandtzaeg, P.B., & Heim, J. (2009). Why people use social networking sites. In A.A. Ozok and P. Zaphiris (Eds.), *Online communities* (pp. 143-152). Berlin: Springer-Verlag.

Bularca, M.C., Cristescu, S., Netedu, A., & Coman, C. (2024). Analyzing the cyberbullying phenomenon on social media from the perspective of students. *Frontiers in Psychology, 15*, 1458079. https://doi.org/10.3389/fpsyg.2024.1458079

Carr, L.W. (2021*). Cyberbullying experiences among college students*. Middle Tennessee University.

https://jewlscholar.mtsu.edu/server/api/core/bitstreams/c09b1d99-1e26-4a2f-9039-4a518952c08e/content

Charmaraman, L., Chan, H.B., Chen, S., Richer, A., & Ramanudom, B. (2018). Asian American social media use: From cyber dependence and cyber harassment to saving face. *Asian American Journal of Psychology, 9(1)*, 72-86.

https://www.researchgate.net/publication/323951191_Asian_American_social_media_use_From_cyber_dependence_and_cyber_harassment_to_saving_face

Cohen, L.E., Kluegel, J.R., & Land, K.C. (1981). Social inequality and predatory criminal victimization. An exposition and test of a formal theory. *American Sociological Review, 46,* 505-524. https://doi.org/10.2307/2094935

Colburn, D.A., Finkelhor, D., & Turner, H.A. (2023). Help-seeking from websites and police in the aftermath of technology-facilitated victimization. *Journal of Interpersonal Violence, 38* (21022), 11642-11665. https://doi.org/10.11777/08862605231186156

Conway, G., & Hadlington, L. (2021). Their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. *Policing: A Journal of Policy, 15*(1), 119-129. https://doi.org/10.1093/police/pay098

Crosslin, K., & Golman, M. (2014). ''Maybe you don't want to face it'' – College students' perspectives on cyberbullying. *Computers in Human Behavior, 41*, 14-20. https://doi.org/10.1016/j.chb.2014.09.007

Diaz, A., & Hecht-Felella, L. (2021). *Double standards in social media content moderation*. Brennan Center for Justice. New York School of Law. https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014a). Cyberbullying in social networking sites: An adolescent victim's perspective. *Computers in Human Behavior, 36*, 13-20. https://doi.org/10.1016/j.chb.2014.03.026

Dredge, R., Gleeson, J., & de la Piedad Garcia, X. (2014b). Presentation on Facebook and risk of cyberbullying victimisation. Computers in Human Behavior, 40, 16-22. https://doi.org/10.1016/j.chb.2014.07.035

eSafety Commissioner. (2022-2025). *eSafety strategy*.
https://www.esafety.gov.au/sites/default/files/202208/eSafety%20Strategy%202022-25.pdf

Ellis, B.J., Del Guidice, M., Dishion, T.J., Figueredo, A.J., Gray, P., Griskevisius, V., Hawley, P.H., Jacobs, W.J., James, J., Volk, A.A., & Wilson, D.S. (2012). The evolutionary basis of risky adolescent behavior: Implications for science, policy, and practice. *Developmental Psychology, 48(3)*, 598-623. DOI: 10.1037/a0026220.

Fansher, A.K., & Randa, R. (2019). Risky social media behaviors and the potential for victimization: A descriptive look at college students victimized by someone met online. *Violence and Gender, 6(2*), 115-123. https://doi.org/10.1089/vio.2017.0073

Felmlee, D., Rodis, P.I., & Francisco, S.C. (2018). What a B!TCH!: Cyber aggression toward women of color. In M.T. Segal and V. Demos (eds.), *Gender and the media: Women's places* (pp. 105-123, Vol. 26: Advances in gender research). UK: Emerald Publishing Ltd. https://doi.org/10.1108/S1529-212620180000026008

Felson, M., & Boba, R. (2010). *Crime and everyday life.* Thousand Oaks, CA: Sage Publications. https://doi.org/10.4135/9781483349299

Francisco, S.C., & Felmlee, D. (2021). What did you call me? An analysis of online harassment towards Black and Latinx Women. *Race and Social Problems, 14*(4), 1-13. https://doi.org/10.10007/s12552-021-09330-7

Gahagan, K., Vaterlaus, J.M., & Frost, L.R. (2016). College student cyberbullying on social networking sites: Conceptualization, prevalence, and perceived bystander responsibility. *Computers in Human Behavior, 55*, 1097-1105. https://doi.org/10.1016/j.hb.2015.11.019

Goh, S. H., Di Gangi, P. M., Rivera, J. C., & Worrell, J. L. (2016). Graduate student perceptions of personal social media risk: A comparison study. *Issues in Information Systems, 17(4)*, 109-119. https://doi.org/10.48009/4_iis_2016_109-119

Graham, A., Kulig, T. C., & Cullen, F. T. (2020). Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice special issue: Policing cybercrime. *Policing: An International Journal of Police Strategies and Management, 43(1)*, 1–16. https://doi.org/10.1108/PIJPSM-07-2019-0115

Haslop, C., O'Rourke, F., & Southern, R. (2021). #NoSnowflakes: The toleration of harassment and an emergent gender-related digital divide, in a UK student online culture. *Convergence: The International Journal of Research into New Media Technologies, 27(5)*, 1418-1438. https://doi.org/10.1177/1354856521989270

Henson, B., Reyns, B.W., & Fisher, B.S. (2011). Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review, 36*(3), 253-268. https://doi.org/10.1177/0734016811399421

Hollis, L.P. (2016). Cybershaming—technology, cyberbullying, and the application to people of color. In *The coercive community college: Bullying and its costly impact on the mission to serve underrepresented populations (pp.* 125-135). Diversity in Higher Education (Vol. 18). UK: Emerald Publishing Limited.

Holmes, J., & Schnurr, S. (2005). Politeness, humor, and gender in the workplace: Negotiating norms and identifying contestation. *Journal of Politeness Research, 1(1)*, 121-149. Doi. 10.1515/jplr.2005.1.1.121

Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53, 59-68. http://dx.doi.org/10.1016/j.bushor.2009.09.003

Karayigit, C., & Parlade, J. (2023). Social media use among U.S. college students attending a midwestern university. *Journal of Educational Technology & Online Learning, 6(2)*, 329-341. http://doi.org/10.31681/jetol.1196222

Kennedy, R., Lawrence, W.Y., Rountree, J., & UHD CPD Election Public Deliberation Team. (2023). Social media regulation: How should we decide what speech is acceptable/unacceptable on social media? https://www.uhd.edu/documents/academics/humanities/news-community/center-public-deliberation/social-media-regulation-issue-guide-2023.pdf

Kowalski, R. M., Dillon, E., Macbeth, J., Franchi, M., & Bush, M. (2020). Racial differences in cyberbullying from the perspective of victims and perpetrators. *American Journal of Orthopsychiatry, 90*(5), 644-652. https://doi.org/10.1037/ort0000492

Lam, T.N., Jensen, D.B., Hovey, J.D., & Roley-Robers, M.E. (2023). College students and cyberbullying: How social media use affects social anxiety and social comparison. *Heliyon, 8*, e12556. https://doi.org/10.1016/j.heliyon.2022.e12556

Langos, C. (2015). Cyberbullying: The shades of harm. *Psychiatry, Psychology and Law, 22*(1), 106–123. https://doi.org/10.1080/13218719.2014.919643

Lawler, J.P., & Molluzo, J.C. (2015). A comprehensive survey on student perceptions of cyberbullying at a major metropolitan university. *Contemporary Issues in Education Research, 8(3),* 159-170. doi:https://doi.org/10.19030/cier.v8i3.9347

Lee, G., & Soonah, A. (2023). Anonymity and gender effects on online trolling and cybervictimization. *Journal of Cybersecurity Education, Research and Practice, 1, Article 5, 1-7.* https://doi.org/10.32727/8.2023.14

Leukfeldt, E.R., & Yar, M. (2016). Applying Routine Activity Theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

McClain, C. (2021). *70% of U.S. social media users never or rarely post or share about political, social issues*. https://www.pewresearch.org/short-reads/2021/05/04/70-of-u-s-social-media-users-never-or-rarely-post-or-share-about-political-social-issues/

McClain, C., Rainie, L., & Bell, P. (2023). *Life on social media platforms, in users' own words*. https://www.pewresearch.org/internet/2023/06/07/life-on-social-media-platforms-in-users-own-words/#different-purposes

MacDonald, C.D., & Roberts-Pittman, B. (2010). Cyberbullying among college students: Prevalence and demographic differences. *Procedia Social and Behavioral Sciences, 9,* 2003-2009. https://doi.org/10.1016/j.sbspro.201.12.436

Marcum, C. D., & Higgins, G. E. (2021). A systematic review of cyberstalking victimization and offending behaviors. *American Journal of Criminal Justice, 46*(6), 882–910. https://doi.org/10.1007/s12103-021-09653-6

Marwick, A., & Boyd, D. (2014). 'It's just drama': Teen perspectives on conflict and aggression in a networked era. *Journal of Youth Studies, 17*(9), 1187–1204. https://doi.org/10.1080/13676261.2014.901493.

Moallem, A. (2018). Cyber security awareness among college students. In Tareq Z. Ahram and Denise Nicholson (eds), *Advances in Human Factors in Cybersecurity: Proceedings for the AHFE 2018 International Conferences on Human Factors in Cybersecurity* (pp. 79-87). Orlando, FL. https://doi.org/10.1007/978-3-319-94782-2_8

Nadim, M., & Fladmoe, A. (2019). Silencing Women? Gender and Online Harassment. *Social Science Computer Review*, *39*(2), 245-258. https://doi.org/10.1177/0894439319865518

National Academies of Sciences, Engineering, and Medicine. (2016). *Preventing bullying through science, policy, and practice*. Washington, DC: The National Academies Press. https://doi.org/10.17226/23482.

Ngo, F.T., Piquero, A.R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review, 45(4*), 430-451. https://doi.org/10.1177/073401682093417

Niu, Y., Brown, B.B., Fan, T., & Lee, Y. (2024). Shelter in the online world? Benefits and risks associated with social media use for college students' mental health in the early stage of COVID-19 pandemic. *Translational Issues in Psychological Science, 10(2)*, 216-231. https://doi.org/10.1037/tps0000414.

Nuccitelli, M. (2012). 2012 Cyber bullying tactics. *Forensic Examiner, 21(3)*, 24-27. https://www.academia.edu/1440077/2012_Cyber_Bullying_Tactics

O'Connor, K., Drouin, M., Davis, J., & Thompson, H. (2018). Cyberbullying, revenge porn and the mid-sized university: Victim characteristics, prevalence and students' knowledge of university policy and reporting procedures. *Higher Education Quarterly, 72(4)*, 344-359. https://doi.org/10.1111/hequ.12171

Peluchette, J.V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem? *Computers in Human Behavior, 52*, 424-435. https://doi.org/10.1016/j.chb.2015.06.028

Perrin, A., & Atske, S. (2021). *About three-in-ten U.S. adults say they are 'almost constantly' online. 31% of American adults are online almost constantly*. Pew Research Center. https://www.pewresearch.org/fact-tank/2021/03/26/about-three-in-ten-u-s-adults-say-they-are-almost-constantly-online/?utm_source=Pew+Research+Center&utm_campaign=3dda4f6f5f-Weekly_2021_03_27&utm_medium=email&utm_term=0_3e953b9b70-3dda4f6f5f-401029614

PenAmerica. (2025). *State laws & online harassment*. https://onlineharassmentfieldmanual.pen.org/state-laws-online-harassment/

Pew Research Center. (2017). *Online harassment 2017*. http://www.pewinternet.org

Powell, A., Scott, A.J., & Henry, N. (2020). Digital harassment and abuse: Experiences of sexuality and gender minority adults. *European Journal of Criminology, 17*(2), 199-223. https://doi.org/10.1177/1477370818788006

Reyna, V.F., & Farley, F. (2006). Risk and rationality in adolescent decision making: Implications for theory, practice, and public policy. *Psychological Science in the Public Interest, 7*(1), 1-44. https://doi.org/10.1111/j.1529-1006.2006.00026.x

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., Henson B., Fisher B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behaviour, 33*(1), 1–25. https://doi.org/10.1080/01639625.2010.538364

Shapiro, L.R. (2023*). Cyberpredators and their prey*. Boca Raton, FL: CRC Press. ISBN: 978-0-3675-5171-1 https://doi.org/10.4324/9781003092292

Shapiro, L.R., & Alexandrou, A. (2019, March). Online security: Protecting adolescents and young adults from exposure to extremism and criminal victimization. In L. R. Shapiro (Chair), *Preventing violent crime*. Academy of Criminal Justice Science, Baltimore, Maryland.

Shapiro, L.R., & Crossman, A. (2025). *Social media use by racially diverse urban college students*. Manuscript in preparation. John Jay College.

Sharma, B. K., Jain, M., & Tiwari, D. (2015). Students' perception towards social media with special reference to management students of Bhopal Madhya Pradesh. *International Journal of Engineering and Applied Sciences, 2(1)*, 30-34. https://www.ijeas.org/download_data/IJEAS0201014.pdf

Sobba, K. N., Paez, R. A., & ten Bensel, T. (2017). Perceptions of cyberbullying: An assessment of perceived severity among college students. *TechTrends, 61(6)*, 570–579. https://doi.org/10.1007/s11528-017-0186-0

Strawhun, J., Adams, N., & Huss, M.T. (2013). The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence and Victims, 28*(4), 715-730. https://doi.org/10.1891/0886-6708.11-00145

Stopbullying.gov. (2014). *What is cyberbullying*. https://www.stopbullying.gov/cyberbullying/what-is-it

Tompson, L., & Tomkins, J. (2025). Assessing risky online behavior for cyberharassment and cyberstalking among university students in New Zealand. *Violence and Victims, 40(3)*, 359-375. https://doi.org/ 10.1891/VV-2023-0144.

Trinidad, A., Marcos, V., Montes, A., and Seijo, D. (2025). Negative online experiences, worry, and risk perception among adolescents: gender differences and implications for cybercrime awareness. *Cyberpsychology, Behavior, and Social Networking, 28*, 348-353. https://doi.org/10.1089/cyber.2024.0476

Verbeij, T., Pouwels, J.L., Beyens, I., & Valkenburg, P.M. (2021). The accuracy and validity of self-reported social media use measures among adolescents. *Computers in Human Behavior Reports, 3,* 100090.

https://doi.org/10.1016/j.chbr.2021.100090

Vogels, E.A., (2021a). *The state of online harassment*. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

Vogels, E.A. (2021b). *Some Americans who have been targeted by troubling behaviors online wouldn't call it 'harassment*'. https://www.pewresearch.org/short-reads/2021/01/22/some-americans-who-have-been-targeted-by-troubling-behaviors-online-wouldnt-call-it-harassment/

Vorderer, P., Kromer, N., & Schneider, F.M. 2016). Permanently online—permanently connected: Explorations into university students' use of social media and mobile smart phones. *Computers in Human Behavior, 63*, 694-70.

https://doi.org/10.1016/j.chb.2016.05.085

Weaver, J.L., & Swank, J.M. (2021). An examination of college students' social media use, fear of missing out, and mindful attention. *Journal of College Counseling, 24*(2), 1332-145. https://doi-org.ez.lib.jjay.cuny.edu/10.1002/jocc.12181

Willoughby, T., Heffer, T., Good, M., & Magnacca, C. (2021). Is adolescence a time of heightened risk taking? An overview of types of risk-taking behaviors across age groups. *Developmental Review, 61*, 100980. https://doi.org/10.1016/j.dr.2021.100980.

Witwer, A.R., Langton, L., Vermeer, M.J.D., Banks, D. (2020). *Countering technology- facilitated abuse: Criminal justice strategies for combatting nonconsensual pornography, sextortion, doxing, and swatting*. The Rand Corporation< RR-A108-3, 1-25,

Countering Technology-Facilitated Abuse: Criminal Justice Strategies for Combating Nonconsensual Pornography, Sextortion, Doxing, and Swatting | RAND

Wolak, J., & Finkelhor, D. (2016). *Sextortion: Findings from a survey of 1,631 victims*. Crimes Against Children Research Center. https://calio.dspacedirect.org/ handle/11212/3037

Zalaquett, C. P., & Chatters, S.S.J. (2014). Cyberbullying in college: Frequency, characteristics, and practical implications. *Sage Open*, pp. 1-8. DOI: 10.1177/2158244014526721

Zhou, Y., & Peterson, Z. D. (2025). Women's experiences of sexual harassment in online gaming. *Violence Against Women, 31*(8), 2037-2052. https://doi.org/10.1177/10778012241252021