9-2015

Exploring Cyber Harassment among Women Who Use Social Media

Sloane Burke Winkelman
California State University Northridge

Jody Oomen-Early
University of Washington Bothell

Ashley D. Walker
Georgia Southern University, awalker@georgiasouthern.edu

Lawrence Chu
Walden University

Alice Yick-Flanagan
Walden University

Universal Journal of Public Health 3(5): 194-201, 2015
DOI: 10.13189/ujph.2015.030504 http://www.hrpub.org

Exploring Cyber Harrassment among Women Who Use Social Media

Sloane Burke Winkelman[1,*], Jody Oomen Early[2], Ashley D. Walker[3], Lawrence Chu[1], Alice Yick-Flanagan[4,5]

[1]Public Health Program, Department of Health Sciences, College of Health and Human Development, California State University Northridge, USA
[2]School of Nursing and Health Studies, University of Washington Bothell, USA
[3]Department of Community Health, School of Public Health, Georgia Southern University, USA
[4]School of Social Work, Walden University, USA
[5]College of Doctoral Studies, Grand Canyon University, USA

Abstract The number of Internet users around the word is at an all-time high. The majority of North Americans are internet users and over two-thirds participate in some kind of social network (i.e. Facebook, Twitter, etc.). Social networks and mobile technology enable individuals to connect instantaneously or asynchronously, across geographic boundaries publicly or anonymously. Few studies exploring cyber harassment have been conducted, primarily because these technologies are relatively recent. The purpose of this descriptive study was to examine U.S. women's experiences with and attitudes toward cyber harassment by way of an anonymous electronic survey. A total of 293 adult women (mean age 24.6) recruited from popular social networking sites participated in the research. The majority of participants (58.5%) reported being a student enrolled at a college or university. Close to 20% repeatedly received an unsolicited sexually obscene message and/or sexual solicitation (excluding Spam messages for all categories) on the Internet. More than 10% (11.5%, n=33) repeatedly received pornographic messages from someone they did not know. More than a third of those who did experience some form of cyber harassment reported feeling anxious. One-fifth indicated they noticed changes in their sleeping and eating patterns as well as feeling helpless because of the harassment. Implications and recommended strategies for health education and personal safety in the online environment are provided.

Keywords Social Networking, Cyber Harassment, Cyber Abuse, Cyber Stalking, Sexual Harassment, Online

1. Introduction

According to the U.S. Department of Justice[1], approximately 12% of women have been stalked at some point in their lifetime and an estimated 20% of Americans have been affected by cyber stalking, persistent emails, or other unwanted contact. More than 1 million women are stalked annually [2]. This figure is most likely much higher when one considers underreporting issues and challenges with established versus self-defined descriptions of stalking. According to the National Institute of Justice(NIJ) [2], close to 2/3 of female stalking victims were stalked by an intimate partner and 81% of women who were stalked by a current or former intimate partner were also physically assaulted by that partner[2]. With the increasing popularity and use of the internet worldwide, stalking and other forms of predatory behavior have emerged in virtual form, referred to as "cyber harassment."

Cyber harassment research is emerging; the term has only recently begun to appear in scholarly journals. The term "cyber harassment" has often been used interchangeably with terms such as "cyber abuse," "cyber stalking" and "cyber bullying.". There is quite a bit of debate among researchers on how to best define these terms therefore consistent consensus of these terms has not yet been reached. Based on previous published research, *Cyber abuse* is a broad term that includes various forms of computer-based online abuse including cyber bullying, stalking, sexual solicitation, and pornography [3].D'Ovidio and Doyle[4], defined cyber stalking as "repeated use of the internet, e-mail or other related digital electronic communication devices to annoy, alarm or threaten a specific individual or group of individuals." *Cyber bullying* often defined as "willful and repeated harm inflicted through the medium of electronic text"[5]. Slonje and Smith [6], referred cyber bullying as " an aggressive act" or behavior that is carried out using electronic means by a group or an individual repeatedly and over time against a victim who cannot easily defend him or herself". However, *cyber harassment* has found to be linked closely with cyber stalking[7]. It is more partner or

relationship focused that encompasses a range of activities such as sending abusive, threatening or obscene emails, text messages, posts on to social networking and blog sites, and phone calls[8,9].

Cyber stalking and cyber harassment research [10-14] has identified the following computer or telecommunication-based harassment mediums including:

- Monitoring e-mail communication
- Sending e-mail that threatens, insults, or harasses.
- Disrupting e-mail communications by flooding a victim's e-mail box with unwanted mail or by sending a virus program.
- Using the victim's e-mail identity to send false messages to others or to purchase goods and services.
- Using the Internet to seek and compile a victim's personal information for use in harassment
- Remailers (Email sent through a third party where the headings are removed, making it virtually impossible to trace its origins)
- Spamming
- Incessant Instant Messaging (IM) or texting
- Posting inappropriate messages or stalking behaviors in chatrooms
- Posting inappropriate messages or stalking behaviors on bulletin boards, blog sites, and/or on social networking site personal pages.
- Website tributes
- Personal data manipulation

All forms of cyber abuse are deliberate and malicious.

Gupta[15]explains the commonality among all forms of cyber abuse, explaining that the acts described above:

> "….rely on all forms of digital media, including instant messaging, blogs, websites, e-mails, chat rooms, and cell phones and both may use anonymity to engage in relentless, and vicious attacks. In all cases, the intent is to threaten, humiliate, and harass the victims by causing emotional distress, demanding submission, spreading lies, and compromising the economic and social wellbeing of the victim."

With the many technological devices (computers, laptops, smart phones, electronic notebooks, etc.) and online communication mediums (Internet, email, blogging sites, social networking sites such as Facebook, Twitter, etc.) one may become more susceptible and accessible to online harassment or stalking [14]. Many internet users are sharing personal information on the internet making this information readily accessible. Search engines and social networking sites are able to identify people's addresses, telephone numbers, ages, and public mention on the internet (such as articles, blogs, Twitter postings, Facebook profiles, student status at a university, employment status at an organization, etc.). For a fee, even further personal information can be obtained [10]. In the past, internet abusers used low-tech monitoring options such as looking at web site browser history and reading deleted e-mail.

However, now stalkers are increasingly using more sophisticated broadly available spyware software as well as various key stroking logging hardware [14]. In addition, people are frequently using online social network and dating sites to search for friendships or romance. There are an estimated 1,200 dating sites available on the internet, and perhaps as many as 7% of adults who go online use these dating services [16]. In a virtual world without boundaries where identities can be changed and anonymity is commonplace, women's risk for experiencing harassment online may be greater than in the "real" world. Therefore, cyber harassment is fast emerging as a major challenge to law enforcement officials [17,18].

It is difficult to quantify acts of cyber harassment for three reasons: 1) The latest national survey on violence against women did not assess cyber harassment or related forms of cyber abuse. Thus, generalizable data on this crime is not available; 2) There is still a minimal amount of information on cyber harassment published in the journals; and 3) as mentioned previously, the term "cyber harassment" has been used interchangeably with other forms of cyber abuse, therefore, statistics specific to cyber harassment may be suspect. However, Spitzberg and Hoobler [13] found that at least 30% of their survey respondents experienced some sort of cyber-based unwanted pursuit. A study among undergraduate students reported that 54% of all respondents knew someone who has been cyber bullied primarily through cell phones, Facebook, and instant messaging [7]. In another study involving college students, that percentage was less. Approximately 10% of the survey respondents reported that they had received repeated e-mails from a significant other (spouse, boyfriend or girlfriend, partner) that threatened, insulted, or harassed [19]. In the same study, 10-15% of 339 students reported receiving repeated e-mail or instant messages that were insulting, harassing or threatening. Over 50% said they had received unwanted pornography. Other studies have found much lower incidences. For example, in one study, approximately 4% of 756 students disclosed having been cyber stalked or harassed [20]. Some of these inconsistencies may stem from lack of a consistent definition of cyber harassment and instrumentation as well as participants' sense of shame.

Cyber harassment and other forms of cyber abuse are largely crimes against women. Growing empirical evidence has shown that more women than men are the victims of cyber stalking or harassment. According to Beran and Li [21], nearly one quarter of female internet users reported of feeling upset or frightened during online chatting regarding things have been said to them. Looking at adolescent populations (aged 10-17), it was reported that approximately 20% (twice as many girls than boys) had been the victim of an online sexual solicitation [22]. A study in the U.K. of people self-identified as being cyber stalked found that almost half (47.5%) reported harassment via the internet, but only 7.2% of the sample was judged to have actually been

cyber stalked[23]. Of the stalking cases that are reported to law enforcement agencies, up to 40% involve electronic stalking from email or cell phone harassment [24].

Those harassing often do so for long periods with the average time being 4 months to 1 year [18]. Cyber harassment often interferes with women's livelihood, identity, dignity, and well-being [25]. The abuse may prevent women to achieve their professional goals as hiring authorities routinely verify the search engines to collect information regarding the applicant. If there are some negative comments or posts on social networking sites, it may prevent employees to hire the targeted individual [25]. Moreover, the person being harassed is often left with feelings of fear, anxiety, restlessness, insomnia, post-traumatic stress syndrome, depression, distrust, paranoia, frustration, and helplessness. The person may also experience physical injury, economic loss in missed time off work, school, or necessary changes for email accounts, phone numbers, or internet accounts [18,26-29]. The real fear, however, is that offensive and threatening behavior that originates online will escalate into "real life" stalking. If the stalker knows the name of the victim, then it is relatively easy to find out further personal details such as the victim's address and telephone number [30].

The exponential rise of using social networking sites in the last decade is increasing the rate of online victimization [31]. Some national and local government organizations, industries, and business groups are considering protective measures that the consumers could use to alleviate harassment but significant gaps among various networks causing failure of the measures and leaving the consumers at greater risk [31]. Research related to stalking and violence against women "off line" is well established; however, studies investigating cyber harassment are very limited[12-14].The researchers of this study found no existing literature on attitudes toward cyber harassment or other forms of cyber abuse. Thus, the purpose of this descriptive and exploratory study was to examine young women's experiences and attitudes toward cyber harassment and to provide recommendations for educators, criminal justice professionals, and those employed in social service organizations who are working to prevent and protect women against this crime. The research goals for this study were: 1) to explore the phenomenon of cyber harassment and its prevalence among women who participate in social networking sites; 2) to assess these same women's attitudes about cyber harassment; 3) to determine young women's online behaviors that may put them more at risk for cyber harassment; and 4) to recommend strategies for program development that may lead to safety prevention in the online environment.

The research questions for this study are: *1)How is cyber harassment perceived; 2) what do women know about it; and 3) to what extent have women who use the internet experienced cyber harassment*?

2. Method

Recruitment and Sampling/Participants

A convenience sampling design was employed in the study whereby the researchers searched on social networking sites, mainly Facebook for organizations and groups such as national sororities, honorary and social college clubs, national women's groups, and groups that focused on violence and cyber harassment. The researchers chose groups that included a large female network in order to get a higher response rate. These groups also allowed non-members to post announcements and recruitment information to their news feed pages. Once the groups were located, announcements about the study were disseminated to these groups and a link to the study page was provided. Contacts listed for these organizations were also sent an email by the researchers requesting to post a link to the study. The study page included the survey, information about the purpose of the study, and informed consent. It was clearly stated in the research announcement that the survey was examining awareness and attitudes toward cyber harrassment. Participants were informed that this was an anonymous survey and participation was completely voluntary.

The researchers encouraged individuals from the organizations to email the link on to other college women to complete the survey. The link to the survey was made available on some pages for up to one year. A total of 374 individuals completed the survey; however, a total 81 surveys were discarded either because a male or a minor had completed it inadvertently. As a result, the sample consisted of 293 adult women (18 years and older). The demographic profile of participants is summarized in the next section.

Demographic Profile of the Sample

The study included female participants ranging in age from 18 to 70 years of age, with a mean age of 24.61 years (SD = 9.01). Almost a half (49%) fell in the 18-21 years age bracket. The sample tended to be homogeneous in race and ethnicity as the majority (74.9%) self-identified as Caucasian. More than a three-quarters (76.4%) of the participants were also born in the United States. Only 12.8% of the sample were recent immigrants (i.e., resided in the U.S. for less than 1 year). Almost three-quarters (73.7%) of the participants' had at least one parent who were born in the United States.

Over half (58.5%) reported being a student enrolled at a college or university. Of those who were students, a fifth (20.5%) were freshmen. Less than 10% (9.4%) were graduate students. The majority (94%) of the sample indicated they were not affiliated with a sorority. In general, participants were affiliated with a social networking site. In the last year, over a quarter (28.1%) joined at least one social networking site, and 18.5% did not join any social networking sites. Over three quarters (76%) of the sample were not a part of any women's group.

Instruments

The survey consisted of three instruments. The first instrument was the "Personal Experiences with Cyber Harassment Instrument" which included 6 question items where respondents answered either "yes" or "no" to whether they experienced various cyber harassment events in the last 12 months (i.e., receiving unsolicited sexually obscene message, pornographic message, sexual solicitation, online threat or instant message from someone either known and not known to the respondent, and offline harassment due to online harassment). Those who did disclose being cyber harassed were asked one additional question about its effect on them. The respondents were asked to select all that applied: changes in sleeping and eating patterns, nightmares, hyper vigilance, anxiety, helplessness, concerns for personal safety, and/or shock and disbelief. Researchers constructed their own instrument for this instrument and established face and content validity.

Adapted from Feild's 32 item Attitudes Toward Rape Scale and modified by researchers, the second instrument consisted of a Cyber Harassment Attitudes Inventory, and included 32 closed ended questions about the respondents' attitudes toward cyber harassment[32]. After reading a scenario about a woman who has been repeatedly receiving unwanted sexual solicitations, pornographic images and pictures, and sexually obscene messages, respondents were asked the extent to which they agreed to statements using a six point Likert scale, in which "1" is" Strongly Agree" and "6" is "Strongly Disagree". These statements reflected the respondents' beliefs about who is at fault, whether cyber harassment is a crime, myths about the perpetrator, and myths about the victim. The term "repeatedly" in the scenario was left up to the respondents' subjective interpretation. Total scores for each respondent were calculated for the Cyber Harassment Attitudes Inventory. Scores range from 32 to 192 which represent respondents' level of tolerance for cyber harassment. Higher scores indicated more intolerant attitudes cyber harassment. Furthermore, individual mean agreement scores were calculated for each question item in the inventory. The Cronbach alpha measuring internal consistency and intercorrelations among test items for the Cyber Harassment Attitudes Inventory was .76.

In order to complete the third instrument, respondents were first asked whether or not they have ever taken a cyber safety class. They were then asked to complete the "Internet Risky and Safety Behaviors Inventory," which was also developed by the researchers. The Inventory consisted of 17 closed-ended question items that measured the extent to which respondents engaged in online behaviors that were considered risky to their personal safety and 6 closed-ended question items that measured Internet behaviors that promoted online safety in the last 12 months. Items were created based on previously published research findings. Respondents had to select one of three response options: "never," "frequently," and "often." A total Internet risky behavior score was calculated by summing up the point values for the question items. Scores ranged from 17 to 51. Higher scores tended to indicate a greater engagement of risky behaviors on the Internet. Similarly, an overall online safety behavior score was calculated. Scores could range from 6 to 18. Higher scores indicate greater levels of engagement in online safety precautions. The Cronbach alpha for the Internet Risky and Safety Behaviors Scale was .60 indicating acceptable reliability. Procedures for data collection are detailed in the next section.

Data Collection Procedures

The approval from the Institutional Review Board (IRB) at East Carolina University was obtained for this quantitative online study. The link to the survey was made available on some pages for up to one year. Incentives were $20 online gift cards from random drawings to iTunes, Target, or Barnes and Noble based on the participant's choice.

3. Results

Experiences with Cyber Harassment and Psychological Effects

When asked about their experiences with various forms of cyber harassment in the last 12 months (not taking into account spam), 19.9% (n = 57) had repeatedly received an unsolicited sexually obscene message on the Internet from someone they did not know. More than 10% (11.5%, n = 33) had received pornographic messages, and almost one-fifth (19.2%, n = 55) had repeatedly received a sexual solicitation on the Internet from someone they did not know. In the last 12 months, over 10% (12.5%, n = 36) had been threatened online or via text or instant messages by someone they did not know. Not all the perpetrators were unknown to the victims, more than a quarter (27.1%, n = 78) have been threatened online by someone they did know. Finally, 16.1% (n = 46) have been harassed offline in the last 12 months as a result of being harassed online.

As shown in Table 1, those who indicated they experienced some form of cyber harassment in the past 12 months also experienced a range of psychological symptoms. The top three symptoms were shock and disbelief (38.1%), anxiety (34.9%), and fear for personal safety (24.6%). In addition, the respondents frequently reported changes in their patterns of eating and sleeping and also feelings of helplessness.

Table 1. Psychological symptoms experienced in last 12 months due to experiences with cyber harassment

Symptoms	n	%
Changes in sleeping eating patterns	56	20.7
Nightmares	46	17.0
Hypervigilance	50	18.5
Anxiety	95	34.9
Feelings of helplessness	58	21.3
Fear for safety	67	24.6
Feelings of shock and disbelief	103	38.1

There were only two significant findings in experiences with cyber harassment: age and being a student or not. A t-test analysis supported that those who stated they had been threatened via text or instant messaging by someone known to them in the last 12 months were statistically significantly older (m= 26.59) compared to those who were not victimized in this area (m = 23.92) (t = 2.18, df = 276,p=<.05). Second, there was a statistically significant relationship between being a student and having repeatedly received a sexual solicitation on the Internet from an unknown person versus not being a student (r = -.16, p=<.01). Thus, it appeared that those who were not currently students were less likely to have received an online sexual solicitation in the last 12 months.

Attitudes Toward Cyber Harassment

Validity and Factor Structure

Overall, the Cyber Harassment Attitudes Inventory, which was revised based on Feild's original instrument showed relatively good internal consistency; the alpha coefficient (using Cronbach's alpha) was .76. A separate principal components factor analysis of the revised ATR responses, followed by varimax rotations was performed. The factor analysis yielded eight factors with eigenvalues greater than (>) 1. All eight factors were found to be interpretable as well as to possess an adequate number of variables with loadings of sufficient magnitude (>±.30) to warrant interpretation and subsequent scoring. These factors accounted for 61.1% of the variance. Similar to Feild's [33] findings, Factor 1 addresses items that focus on a woman's responsibility for preventing cyber harassment (i.e.: "Nice" women do not experience the type of behaviors that Annie experienced in the scenario). Factor 2 correlated with items that support a woman's responsibility for provoking cyber harassment (i.e.: Women like Annie can provoke the types of behaviors described in the scenario by posting photos of themselves).Factor 3 included many items addressing criminal behavior and how those engaged in this behavior should be penalized. Factor 4 reflected items that support cyber harassment as more of a sexual act or release, rather than a harassing or abusive factor. Factor 5 addresses men using cyber harassment as a form of control or power over recipients. Factor 6 dealt with the legal system and any actions that should be imposed on the perpetrators. Factor 7 addressed women's victimization and finally, Factor 8 correlated with the expected behaviors of women and men in cyber harassment.

Internet Risky and Safety Behaviors

The majority (96.5%, n = 279) had never taken a cyber safety class. However, the overall, respondents did not engage in high levels of risky online behaviors as the mean score was 24.06 (SD = 3.90). Frequencies for each of the online risky behaviors were then calculated to obtain a sense of what specific online risky behaviors respondents tended to engage in and to what extent. Data in Table 2 summarizes behaviors in which adult females engage on the Internet that are considered risky. In the last 12 months, a quarter of the sample reported having posted a sexy or provocative photo of themselves on the Internet, and more than 10% of the sample indicated they have agreed to meet someone face to-face after a few online exchanges.

Table 2. Internet Risky Behaviors Engaged In Last 12 Months[1]

Type of Internet Risky Behavior	n	%
Posted your first and last name on public accessible Internet profiles such as discussion forums, message boards, blogs, and/or chat rooms	163	54.4
Posted your contact information (i.e. cell phone, home phone, email address, city and state) on the Internet	173	57.9
Posted a regular photo of yourself on the Internet	282	94.7
Posted what is considered a provocative or sexy picture of yourself on the Internet	76	25.4
Created what might be considered a provocative name to email address	13	4.3
Make your profile visible to all Internet users	95	98.4
Created a gender specific email address	111	37.1
Invited someone you don't not know to your social networking site	84	28.2
Accepted someone not known to you to Your social networking site	168	56.4
Entered a sex chatroom	23	7.8
Agreed to meet someone face-to-face from the Internet after minimal to a few Internet exchanges	40	13.4
Downloaded pornographic images from pornographic websites	56	18.9
Talked with someone you don't know in a chatroom about sensitive topic matters (i.e., sex, relationships, etc.…)	74	25.7
Returned an email from someone you don't know	96	33.5
Posted your plans on the Internet (i.e., what you'll be doing that day or week etc.)	195	68.1
Used a webcam to talk to someone you don't know on the Internet	24	8.3
Accepted file transfers or opened links from someone you do not know or trust	37	12.8

[1](National Institute of Justice and Centers for Disease Control and Prevention, 1998, added the "sometimes" and "often" categories)

Overall respondents engaged in behaviors that promoted their safety while on the Internet (m = 12.81, SD = 2.18). Frequencies for each of the online safety behaviors were then calculated to obtain a sense of what specific online safety behaviors respondents tended to engage in and to what extent. Data in Table 3 summarizes behaviors that are considered to assist in ensuring some measure of safety when using the Internet. When using social networking sites, the majority of respondents (95%) indicated that they would set up privacy settings so that they could only add someone to their network once they approve it. Over 75% used filtering software programs on their computer; however, only 50% of the respondents created a name that did not divulge their gender or created a neutral name in a chat room.

Table 3. Internet Safety Behaviors Engaged In Last 12 Months[1]

Type of Internet Safety Behavior	n	%
Change your email address	126	42.0
Used filtering software on your computer	232	77.9
Created a name to use in a chatroom that is neutral or non-descript (i.e., that doesn't indicate your gender, who you are in anyway, etc.)	144	50.2
Set privacy settings in your social networking site so that you can only add someone that you approve	273	95.1
Examined how your social networking sites worked before you joined	214	74.5
Updated your firewall, anti-spyware, and anti-virus software	252	88.1

[1](National Institute of Justice and Centers for Disease Control and Prevention, 1998, added the "sometimes" and "often" categories)

One variable specifically addressed overall engagement with online risky behaviors. Respondents who were not born in the U.S. had higher levels of engagement in online risky behaviors (m = 24.87, SD= 3.92) compared to their native-born counterparts (m = 23.80, SD=3.64) (t = 1.92, df = 273, p=<.01).

4. Discussion

Based on database searches at time of publication, this is one of very few studies using social network sites to recruit participants and the only study on cyber harassment that used this recruitment method. This study was unique and important in terms of recruiting participants from a social networking medium. Other studies have examined cyber harassment among women, but social networking sites were not used to implement the survey instrument.

Twenty percent of the sample (n=57) for this study experienced a form of unwanted cyber harassment. Our findings are lower but close to the findings of Spitzberg and Hoobler [13] who reported at least 30% of their survey respondents experienced some sort of cyber-based unwanted pursuit based on frequency data. Their participants were college students compared to our population who was recruited via social networking sites. More than 25% of the participants in this study were threatened online by someone they knew which indicates a higher prevalence for this behavior than the findings of 10% in Finn's [19] study. In the last 12 months, 25% of the sample reported having posted a sexy or provocative photo of themselves on the Internet, and more than 10% of the sample indicated they agreed to meet someone face to-face after a few online exchanges. This was a significant safety concern. The majority of the respondents reported using safety measures such as software filters, privacy settings, false identities, password confidentiality, etc. to protect their identity and safety; however, there seemed to be a disconnect regarding how posting provocative photos or meeting someone face to face after only a few online interactions may put them at risk for cyber harassment or physical assault. Thus, future education efforts should include scenarios for discussion and highlight the risk in these behaviors.

Furthermore, more than a third of those who did experience some form of cyber harassment reported feeling anxious and one-fifth indicated they noticed changes in their sleeping and eating patterns and feeling helpless as a result of the harassment, signifying the psychosocial ramifications of cyber harassment.

Table 4. Recommended Safety Behaviors

1	Make sure the operating system's automatic updates and firewall are turned on.
2	Use security programs including anti-virus and anti-spyware software, and subscribe to security updates.
3	Run a full system scan at least once a month.
4	Don't open attachments or click on links in e-mails from people you don't know.
5	Don't befriend people you don't know in social networking sites.
6	Don't share too much personal information (full name, address, work, etc.)
7	Use passwords with at least eight characters and numbers and symbols, and change them regularly.
8	Access the Internet through a router - it creates an implicit firewall for you, so bots can't reach your machine directly.
9	Don't use the same password for every account - and use more complex passwords for "important" transactions, such as with your bank.
10	Don't connect to the Internet using a wireless connection without a password.
11	Don't send sensitive information to a Web site that does not begin with "https," which means it's secured.
12	When receiving an e-mail, think about whether it's *really* from the purported sender, rather than an impostor, before taking action.

Although the sample scored low overall in online risky behaviors, there were two areas where women scored most at risk. A quarter of the women in this study (n=73) reported that over the last 12 months, they had posted a sexy or provocative picture of themselves on the internet, and 10% (29) agreed to meet with someone face-to-face after just a few email exchanges, increasing their risk of victimization. Education about cyber harassment and prevention strategies must start early. More education about cyber harassment and safety for both men and women is needed, but especially for young women beginning as early as elementary school since younger children are going online. There may be a lack of understanding about the permanency of what is posted online or sense of invulnerability about victimization. Education to reduce risky behaviors must not only create awareness about the problem of cyber harassment, but aim to change attitudes as well. In 2009, almost 96% of Gen-Y's belonged to some kind of social networking site, and that percentage is predicted to rise again in 2010[34]. While the Internet allows for more interaction and socialization, there are risks that accompany this increased "connectivity." With other forms of violence, women are encouraged to take self-defense classes, assertive training courses and be proactive to promote personal safety. The same can be said about promoting greater awareness of the risks involved in the online world, particularly if young women in college feel a

false sense of "safety" or "protection" from their University system or email in sharing their information online. College women may perceive themselves as more protected due to the perceived insularly or controlled environment a university may appear to provide. In the case of Facebook young women may perceive that their information and postings can only be accessed by those in their social network, which is not always the case. Internet safety mechanisms are outlined in Table 4. Findings of the current research confirm the need for targeted safety prevention programs for college students. Innovative technology- based prevention such as safety campaigns on social networking sites (Facebook, Twitter, etc.) and text messaging campaigns that addresses controlling behaviors or cyber harassment could be effective. To promote the recognition of appropriate partner interactions and to encourage healthy relationships, campus-based prevention programs and personal health course content are needed to address these issues among college students. Additionally, advocacy and policy reform to protect electronic information and personal information should be considered.

This study is not without its limitations. The study population is not representative of the population of women in the U.S. since enrollment in the study targeted women's organizations, including anti-violence groups, with an online presence on Facebook. This is evident when examining the sample distribution by age and ethnicity; therefore, the results of the study are not generalizable to the population of women. In addition, participation in the study relied heavily on self-report data, and therefore voluntary response bias on cyber harassment would over represent those who had strong opinions or experiences related to this sensitive topic. Furthermore, referral sampling by individuals in these organizations could overestimate cyber harassment prevalence as women may contact and encourage friends or family members who were victims to participate in the study. However, this study does contribute to the limited research published on this topic and is the first study, which examines women's attitudes towards cyber harassment. It is also the first to use social networking sites as a data source. Moreover, this pilot study can provide a basis for: 1) additional research that further explores the topic of cyber harassment and 2) more comprehensive studies that employ more diverse samples and include both men and women.

5. Conclusions

The exploratory study examines the extent of cyber harassment experienced by women, online behaviors that put them at risk, and provides a basis for future research. According to a recent Neilson's [34] report, social networking has become a fundamental part of the online global experience. In fact, two-thirds of all Internet users engage in some kind of social networking on a daily basis—and many visit social media platforms such as Facebook and Twitter multiple times a day. Online communication mediums can be empowering for women to increase their spheres of influence, access information, promote creativity, and build their confidence in using technology [22]. The Internet and social media are ubiquitous in the Digital Age. Consequently, there is a need to educate individuals about ways in which to enhance personal safety online, to protect one's identity and digital footprint, and what actions a person should take if one is experiencing cyber harassment. It is important for health educators, counselors, social workers, and other practitioners to consider this a public health issue, and to advocate for legislation that deters and criminalizes cyber harassment in all of its various forms.

REFERENCES

[1] U.S. Department of Justice. (2000). Extent, Nature, and Consequences of Intimate Partner Violence. Findings from the National Violence Against Women Survey. Office of Justice Programs (NCJ 181867). Retrieved from https://www.ncjrs.gov/pdffiles1/nij/181867.pdf

[2] National Institute of Justice. Violence Against Women Office. (2001). Stalking and Domestic Violence. The Third Report to Congress under the Violence Against Women Act. Washington, DC: U.S. Department of Justice.

[3] Mishna, F., McLuckie, A., & Saini, M. (2008, January).Cyberabuse: Kids reaching out for help. Oral presentation at the Society for Social Work and Research Thirteenth Annual Conference. New Orleans, LA.

[4] D'Ovidio, R. and Doyle, J. (2003). A Study on Cyber-stalking: Understanding Investigative Hurdles. FBI Law Enforcement Bulletin 72(3): 10–17.

[5] Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. Youth Violence and Juvenile Justice, 4 (2), 148-169.

[6] Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? Personality and Social Sciences, 49, 147-154.

[7] Walker, C. M., Sockman, B. R., & Steven, K. (2011). An exploratory study of cyberbullying with undergraduate university students. TechTrends, 55(2),31-38.

[8] Beran, T., & Qing, L. (2005). Cyber Harassment: A study of a new method for an old behavior. Journal of Educational Computing Research, 32(3), 265-277.

[9] Geach, N., & Haralambous, N. (2009). Regulating Harassment: Is the Law Fit for the Social Networking Age? The Journal of Criminal Law, 241-257.

[10] Finn, J., &Banach, M. (2000). Victimization online: The downside of seeking human services for women on the internet. CyberPsychology& Behavior,3(2), 243-254.

[11] Lucks, B. D. (2001). Electronic crime, stalkers, and stalking: Relentless pursuit, harassment, and terror online in cyberspace 2001. In J. A. Davis (Ed.). Stalking crimes and victim protection: Prevention, intervention, threat assessment, and case management. Boca Raton, FL: CRC Press.

[12] Spence-Diehl, E. (2003). Stalking and technology: The double-edged sword. Journal of Technology in Human Services, 22(1), 5-18.

[13] Spitzberg, B., &Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. New Media & Society, 4, 71-92.

[14] Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. Violence Against Women, 13, 842-856.

[15] Gupta, U. (2010). Cyberharrassment in Academica 2008. University Business. Retrieved from http://www.universitybusiness.com/viewarticle.aspx?articleid=1081&p=1#0

[16] Avins, M. (2000, February 13). Dates that Click.Los Angeles Times, pp. E1-4.

[17] Cupach, W. R., &Spitzberg, B. H. (1998). Obsessive relational intrusion and stalking. In B. H. Spitzberg and W. R. Cupach (Eds.). The dark side of close relationships. Hillsdale, New Jersey: Erlbaum.

[18] Spitzberg, B. H., &Cupach W. R. (2001). Paradoxes of pursuit: Toward a relational model of stalking-related phenomena. In Davis, J. (Ed.).Stalking, stalkers and their victims: Prevention, intervention, and threat assessment. Boca Raton, FL: CRC.

[19] Finn, J. (2004). A survey of online harassment at a university campus. Journal of Interpersonal Violence, 19, 468-483.

[20] Alexy, E., Burgess, A. W., Baker, T., &Smoyak, S. (2005). Perceptions of cyberstalking among college students. Brief Treatment and Crisis Intervention, 5, 79-289.

[21] Beran, T. and Li, Q. (2007). The relationship between cyberbullying and school bullying. The Journal of Student Wellbeing, 1(2), 15-33.

[22] Sharples, M., Graber, R., Harrison, C., & Logan, K. (2009). E-safety and Web 2.0 for children aged 11–16.Journal of Computer Assisted Learning, 25(1), 70-84.

[23] Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? Psychology, Crime & Law, 13(6), 627-640.

[24] U.S. Department of Justice. (2010). Stalking and domestic violence: Report to congress 2001. Retrieved fromhttp://www.ncjrs.gov/pdffiles1/ojp/186157.pdf

[25] Citron, D. K. (2009). Law's expressive value in combating cyber gender harassment. Michigan Law Review , 3 (108), 373-415.

[26] National Institutes of Justice. (2014) Stalking. Retrieved from http://www.nij.gov/topics/crime/stalking/Pages/welcome.aspx

[27] Kamphuis, J. H., Emmelkamp, P. M, & Bartak, A. (2003). Individual differences in post-traumatic stress following post-intimate stalking: Stalking severity and psychosocial variables. British Journal of Clinical Psychology, 42, 145–156.

[28] Pathé, M., & Mullen, P. E. (1997). The impact of stalkers on their victims. British Journal of Psychiatry, 170, 12–17.

[29] U. S. Department of Justice. (1998). Stalking in America: Findings from the National Violence Against Women Survey (NCJ 169592). Retrieved from https://www.ncjrs.gov/pdffiles/169592.pdf

[30] Ellison, L., &Akdeniz, Y. (1998). Cyberstalking: The Regulation of Harrassment on the Internet. Criminal Law Review. December Special Edition: Crime, Criminal Justice and the Internet, 29-48.

[31] PR Newswire. (2013). Cyberstalking is a real crime: One in five Americans affected by unwanted contact. Retrieved at http://www.prnewswire.com/news-releases/cyberstalking-is-a-real-crime-one-in-five-americans-affected-by-unwanted-contact-186985781.html

[32] Barnett, N. J. ,&Feild, H. S. (1977). Sex differences in university students' attitudes toward rape. Journal of College Student Personnel, 18, 93-96.

[33] Feild, H. (1978). Attitudes toward rape: A comparative analysis of police, rapists, crisis counselors, and citizens. Journal of Personality and Social Psychology 36(2), 156-179.

[34] Neilson. Neilson Net Ratings. 2009. Retrieved August 15, 2009 at: http://enus.nielsen.com/tab/product_families/nielsen_netratings