Cyber-Victimization of Women in Bahrain:
Psychosocial Impacts

Nov
2022

Author
Fatima Ali

secdev.foundation

Acknowledgment

Author

Fatima Ali (M.Sc. in Social Psychology, Lancaster University 2010) has been a lecturer in the University of Bahrain's College of Health and Sport Sciences since 2007. She is a recognized HEA Fellow (Higher Education Academy, U.K.), a certified specialist in scribble and drawing analysis, and an international certified trainer (Kingston Business Academy). She has extensive experience reviewing, modifying, and teaching courses in prestigious universities in the Kingdom of Bahrain, where she has engaged with students from widely varying backgrounds. Her research interests range from topics in education and learning to studying aggression in children, using both quantitative and qualitative methods. She has served in diverse committee roles at the department and college level. She has also delivered many workshops and training sessions to students, faculty and the wider public.

Partners

Produced by: The SecDev Foundation
This Canada-based NGO works globally to promote digital resilience among vulnerable populations. Working most often with women, youth and at-risk civil society organizations, the Foundation helps people protect themselves from an evolving world of digital harms. Ultimately, that helps people build their own capacity to make life better for themselves and their communities.

Coordinated by: Salam@
This Foundation-supported project promotes digital resilience across the Middle East and North Africa, especially among women and youth. From 2019 to 2022, Salam@ led intensive frontline work—from training to awareness campaigns—in Algeria, Bahrain, Jordan, Kuwait, Libya, Morocco and Tunisia. The team is now leaning into filling the research gap on digital violence against women across the MENA region.

Contents

Introduction

With the increase in the prevalence of using cyberspace, a dramatic rise in incidents of cybercrime followed in recent years (Verizon, 2021). This can be due to the high number of people using smart devices, and the expansion in the age range of users, to include younger and older users. Although cyber-crime occurs in virtual space, being a victim of this crime has great social and emotional consequences in real life. Indeed, the consequences of experiencing crime might range from slight harm to a very tragic experience that leads to trauma. Moreover, the social roles and expectations stemming from society's values and norms might expedite the consequences of cyber-crime especially on female victims.

This research focuses on the psychological and social factors of cyber-crime in the Bahraini context. It highlights the factors involved in reporting crime, the feeling of victimisation and coping with the incident.

Operational Definitions

Cybercrime is defined as any crime that is facilitated or committed using a computer, network, or hardware device" (Gordin & Ford, 2006, p. 14). This definition, like many others, emphasizes any criminal activity targeting end-users that is executed through different networks, or the Internet (Ciardhuáin, 2004; Yue et al., 2019). It includes acts such as phishing, data breaches, data/information theft, identity theft, fraud, cyberstalking, cyberbullying and harassment, child predation, extortion, blackmail, espionage, (Maimon & Louderback, 2019). The social impact of a cyber-attack refers to aspects such as the social disruption caused to people's lives including, but not limited to, family problems, one's own standing in society, losing one's reputation or social standing in society, while psychological impact may include more personal aspects such as an individual's anxiety, worry, anger, outrage, and depression.

Literature Review

Extensive research in the literature has found many factors affecting reporting of cybercrime, the impending sense of victimisation and its consequences. Moreover, gender roles and cultural expectations play a key role in the decisions made by victims.

Social Support

Seeking support has been found to be one of the most effective ways of successfully dealing with victimisation, in an off-line context, as it helps in overcoming possible negative emotional and psychological effects, as well as providing victims with information to prevent future incidents (Cullen, 1994, Littleton, 2010, Stadler et al., 2010). However, it has been found that cybercrime victims rarely share their experience with their family or friends (Cross et al., 2016b, Jansen and Leukfeldt, 2018). A probable reason for this is that victims might fear to be blamed for their victimisation (Conway and Hadlington, 2018, Cross et al., 2016a), thus affecting their willingness to share their experiences with others.

Many studies have found that victimisation deterring behaviours are greatly affected by the person's locus of control (Frieze et al. ,1987; Strobel, Tumasjan, & Sporrle, 2011; Zelenski, Santoro & Whelan, 2012; Roli & Olanrewaju, 2018). People cope with life events using two coping strategies depending on how they view their own control over things: some might take action alone due to the belief that the outcomes of their actions are contingent on what they do (internal locus of control); while others believe that the events occur outside of their personal control, and thus they either blame external factors such as fate, luck and others or they seek external help (external locus of control).

Based on these two intrinsic beliefs, it can be assumed that people move through a series of steps before making an informed decision to report an incident. First, they need to identify themselves as victims, followed by assessing the seriousness of the crime and the perceived consequences, followed finally by reporting or disclosing the crime to either authorities or to a social support system (van de Weijer, Leukfeldt, & Bernasco, 2018). The victim's social support system, which might offer instrumental or expressive/ interactional support, can include family, friends, but also acquaintances such as neighbours or colleagues. Instrumental support can be in the form of offering material aid, behavioural assistance, and information to help in resolving the issue, while examples of expressive support can occur in the form of emotional and social support, maintain self-esteem, and help in coping with stress (Frieze et al., 1987).

While some studies concluded that those who sought professional support found the experience to be healing and helpful (Jansen & Leukfeldt, 2018), as well as reduced depressive feelings (Machmutow, Perren, Sticca, & Alsaker, 2012), other studies emphasised the importance of seeking social support from peers, especially for adolescents as they consider peers to be more effective helpers than adults (Jacobset al. 2015; Livingstone et al., 2011). Also, although most research highlights the benefits of seeking peer support, the negative consequences are rarely mentioned. Indeed, most victims don't seek professional support. In many cases, they seek support from friends or neighbours, leading in some circumstances to escalation of the problem when the perceived social support turns to a new threat. Indeed, qualitative analysis of the cases from Salam@ program conducted in Bahrain, through SecDev has found that in some cases further extortion or threats occurred as a result of divulging the information to a seemingly trusted source. Moreover, some victims might regret "making the issue public" and the possible breach of confidence that might occur, leading to elevation in stress levels.

Perception of Severity/Seriousness of Crime and Decision Making

Two other important components affecting the sense of victimisation and seeking social support that should be considered in more details are: (1) the *perceived severity* of the incident, and (2) the *perceived control* over the incident (Black and Hendy, 2018, Cross et al., 2016a; van de Weijer et al., 2018).

Even though the impact of cybercrime is serious on a macro-level, its consequences on the individual, on a micro-level, might not be perceived on victims as such (Wall, 2008). The underestimation and overestimation of the event might both work as a deterrent to reporting, and/or seeking social support. Certainly, underestimating an event, as a coping strategy, will reduce the likelihood of taking further action, as well as overestimating the incidence, as argued previously, will lead to fear of seeking social support. For example, when a woman who suffered from some sort of cybercrime believes that the incident is serious, her need to be compensated or helped increases, and thus, heavily outweighs the cost of reporting (van de Weijer et al., 2018). She will be more likely to report the incident, seek retribution even though this decision carries with it negative social consequences like shaming or stigmatisation. On the other hand, if she deems the experience as "not serious enough", thinking that it is "not a big deal", then this will work as a deterrent from reporting the incident (Cross et al., 2016a, Wall, 2008).

Moreover, in judging online risk, people use four main dimensions: 1) the ability to control or avoid the risk, 2) fear of consequences, 3) unfamiliarity of risks and 4) the immediacy of consequences/impact (Nurse et al. 2011). People react to the risk in several ways based on their dual information processing. While some react logically and analyse the risks, others might react instinctually based on feelings (Dickert et al., 2015). For example, people can decide on acting on risks related to cyber-crime based on their feelings toward specific outcomes (Nurse, 2018).

It was proposed that people might confuse facts with their individual interpretation because perceptions of risk are often based on the interpretation of facts, based on individual judgement, values, beliefs and attitudes (Beck, 1999). Overall, according to Blythe and Camp (2012) the motivation to apply security mechanisms depends on people's belief about their susceptibility to exogenous security threats, their potential severity and the cost and efficacy of preventative or mitigating behaviours.

Self-Efficacy and Locus of Control

Ajzen (2002) introduced the relationship between self-efficacy and perceived behavioural control (locus of control). Self-efficacy is related to the ease or difficulty of performing a behaviour, so a woman who feels capable of taking action and adopting certain behaviours to protect herself will do so. On the other hand, if she has low self-efficacy then she will not take a proactive action to protect herself from cyber-crimes or any protective behaviours to deter those crimes.

Locus of control, as mentioned previously, relates to the extent on which performance of the behaviour depends on the individual or others. Locus of control aims to characterise whether people feel they have strong control over their life (internal locus of control) or whether they must rely on external forces (external locus of control). The locus of control affects our behaviour, learning, and motivation.

High Self-Efficacy and Internal Locus of Control

Women with an internal locus of control feel that success or failure is due to their efforts or abilities. For example, those who have high internal locus of control might actively attempt to resolve the cyber- incident, have less fear, less tendency to avoid threat, as well as more likely to report the incident to authorities. Moreover, individuals with high self-efficacy are more likely to adopt protective measures to avoid falling for cybercrime or to reduce further victimisation in the future. Studies indicate that they can be quick to learn from their mistakes when they become victims of cyber-crime (Reeve, 2017). For example, as an internet user, she will take an active role in gaining the "know-how" about using and implementing virtual protection methods, ensuring the safety of her virtual environment, including setting a strong password, and taking caution in publishing confidential information online, just as she might prevent actual crime or real attack happening to hear by refraining from going to dangerous areas, or having pepper sprays or teasers in her purse.

Low Self-Efficacy and External Locus of Control

Alternately, individuals with an external locus of control are likely to believe that other factors such as luck or the difficulty of the target or the actions of other people are the cause of success or failure. The locus of control can affect how women might react to being victimised by cyber-attack or cyber-crime. For example, women who view themselves incapable of reacting to the virtual threat or attack might try to reduce and control their negative emotions and fear — either consciously or unconsciously — by denying the experience, or through performing risky behaviours (trying to

eliminate the source of the fear and anxiety), or by committing boomerang reactions. Indeed, many researchers have explored the effects of boomerang reactance effects, where the victim adopts an attitude refusing to succumb to the threats of the cyber-attacker, resisting the restriction on their cyber-freedom, thus increasing their susceptibility to further cyber-attacks (Petrič & Roer, 2022; Kuang et al. ,2020). Furthermore, lack of control over a situation that is perceived as threatening or dangerous can give rise to feelings of emotional distress, fear and insecurity leading to irrational behaviours (Sutherland, 2007) or other strong reactions. For example, if people judge themselves as ineffective in exercising control over potential threats, they react with stress and avoidance behaviour. Thus, in the occasion of a phishing scams, the person might judge himself as lacking preventive skills or knowledge for such an incident, leading to desperation and decrease in motivation to act or take any protective actions in the future. If this is to occur on a large scale, it could have a notable social impact.

The Online Disinhibition Effect

It is important to note that alongside the perception of the action and the locus of control, another important aspect needs to be considered. Individuals behave differently in online situations than in off-line face-to-face situations. There is more disinhibition in their actions, decisions, and projection of their identity in the online realm. People are more likely to loosen up, feel less restrained and become more open (Suler, 2004). This could happen due to the misconception of invisibility- a feeling of mistaken incognito, which makes them feel less vulnerable in the way they express themselves or behave therefore they might engage in activities that they otherwise would not. Indeed, an individual who goes through cyber-attack due to this error in cognition – lapse of judgement- might feel ashamed and engage in self- blaming and self- defeating behaviours.

Consequences of Cybercrime

Alongside the financial consequences of cyber-crime, especially in cases of fraud, embezzlement and extortion, cybercrime victimisation can result in several possible psychological, emotional and physiological effects similar to the effects experienced by victims of traditional crimes (Lamet & Wittebrood, 2009; Modic & Anderson, 2015. Studies have indicated a reduced subjective well-being, feelings of depression, fear, shock, distress, sadness, anger and embarrassment due to being a victim of cybercrimes (Cross et al., 2016b, Kaakinen et al., 2018). Moreover, victimisation can influence the victims' perception of themselves and the world around them (DeValve, 2005). For example, victims have claimed feeling stupid or cheated afterwards, and have reported decreased levels of trust in themselves and in others (Jansen & Leukfeldt, 2018), which manifests into physical symptoms, such as sleeplessness or insomnia, nausea or weight loss (Cross et al., 2016a).

Self-blame is one of the feelings most often associated with cybercrime victimisation, leading to feelings of shame and embarrassment (Cross et al., 2016b). Blame occurs as a reaction that helps victims in controlling their emotional response to the event (Green et al., 2010, Jansen and Leukfeldt, 2018). Even though self-blame is traditionally considered a negative reaction, it is also recognized as beneficial to some extent. Indeed, the functional analyst argues that all constructs have their functions and dysfunctions (two sides of a coin). Thus, a woman (with an internal locus of control and high self-efficacy) who perceives that her own actions and behaviours were part of the reason for the cyber-crime, might adopt a "learn from my mistakes" or "what doesn't kill you makes you stronger" attitude, and she would feel more confident about avoiding future incidents and taking up protective behaviours, allowing her to regain control over the situation (Frieze et al., 1987). On the other hand, self-blame also has severe negative consequences, leading to a decrease in reporting the incidents (Bidgoli and Grossklags, 2016, Goucher, 2010, Wall, 2008). Due to cultural upbringing, social and

personality factors, she might feel that she deserves it and must reap the consequences of her actions and online decisions. It might also lead to her reluctance in sharing her experience or venting out due to the widespread victim-blaming discourse — the "she had it coming "philosophy. Indeed, women internalising this philosophy feel that they are partly or wholly to blame, and they might end up feeling too embarrassed to talk about the incident leading to severe psychological and social impact, such as an increased sense of isolation, decreased empathy and social connections, as well as depression and social anxiety. It is important to note that cultural values, gender roles and gender perceptions play a vital role in this. In unforgiving cultures that thoroughly blame women for misfortunes or "not protecting herself", the women are more likely to face the negative consequence side only.

On an emotional level, victimisation can lead to the feeling of distress and violation, betrayal and vulnerability, anger and being powerless (Kirwan and Power, 2011). Often, going through a cyber-attack incident might induce feelings of outrage, anxiety, a preference for security over liberty, and little interest in adopting new technology due to loss of confidence in the cyber realm. The victim might also go through the stages of grief, suffering from anger or rage and even bargaining especially if the cyber-attack resulted in the loss of something valuable (the loss can be in any domain such as financial, relationships or even one's reputation). In some cases, victims may even blame themselves and develop a sense of shame; sextortion is a good example of this given how it initially starts (Nurse, 2018). The woman victim might blame herself either for not adopting online protective behaviours, or for her misguided trust in the person she thought she built a close, trusting relationship with. In both cases, the blame, sense of shame and anger with herself are some of the expected consequences. However, in the latter scenario, these feelings and their consequences are intensified by a sense of guilt, gaslighting and the fear of prosecution from her community. Moreover, in most conservative communities and societies, these women who were victims to cyber-crimes, might be seen as incompetent, impure or untrustworthy — tainting the family honour.

The consequence of cyber-crime victimisation, like real life victimisation, might extend to a longer period then the crime itself, leading the individual to fear the re-occurrence of the crime in the future, being on constant guard and distrusting people and their intentions. Indeed, fear of crime can prompt people to change their behaviour. At the level of the individual, people generally respond to the fear of crime by adopting protective or avoidance behaviours (Reid, Roberts & Hilliard, 1998). Phobophobia — the psychological fear of fears (Furedi, 2002) — can lead to stress, intense anxiety, and unrealistic and persistent public fear of crime and danger, regardless of the actual presence of such fear factors. This phenomenon may also relate to the crime complex (Hale, 1996) and therefore cyber-attacks and cybercrime. There are underlying gender differences in the consequences of cybercrime. In conservative cultures, where gender inequality prevails, women are more likely to feel the negative outcome and repercussions, while men are more likely to bypass the incident unscathed. This can be due to the cultural belief held that "a woman is like a white piece of cloth, that can be tainted by mere dust and thus should be protected", and this taint will follow her for the rest of her life, affecting her image in her surroundings and determining her culturally forecasted bleak and desolate future.

The Bahraini Context and Culture

The Kingdom of Bahrain is rich with its heritage, culture, and traditions with Islam being the main practiced religion. The effects of the Islamic and Arabic culture can be strongly sensed and is applied by the people in the patriarchal, family-oriented society. People of Bahrain have a strong cultural, religious, and ethnic identity, behaving conservatively and applying modesty in several aspects of their life including customs, and dress codes. The husband and father head the nuclear family and watches over the morality of his wife and children and unmarried females in the extended family. The basic family structure and patriarchal system persists in varying degree in different households despite the

radical transformation on the family structure brought by modernization, education, and economical demands of the urban life in the last 60- 70 years or so; where women in the family are actively involved in decision making, and in supporting the household needs, with the younger generation gaining more freedom and liberty. It is important to note, that socially, the gender power dynamics are still overtly patriarchal despite the globalisation, openness and accessibility provided by the growing technology.

Female Gender Role and Gender Perceptions

The gender role of females in the Kingdom of Bahrain has faced dramatic changes. In the early part of the 20th century, the role of women was constrained in running the household, childbearing and raising the children. Women were subdued and not allowed any education, where a good woman is one who raised her kids well, helped and obeyed her husband and refrained from disgracing or shaming herself and/or her family. However, with the unfolding of modernization and the opening of all- girl schools in the early 1920s, many families -from the major cities started sending their daughters to school, a practice that was not done until much later in the villages, which led to a great shift in the female roles, value system and gender expectations within the community. Indeed, the women's role has dramatically changed with her leaving the house to work or to receive an education giving her a higher social status and an opportunity to participate in decision-making. Children gain more freedom and become less subordinate to the system of traditional authority as the family becomes more permissive and more liberal values are adopted concerning relations between males and females. All this contributed to the changes in women's status. However, even with the modernization of the family structure and the change in the female role in Bahrain, the traditional and conservative role is still strongly held and valued, following the dictates of the constitution which clearly states that the family is considered the cornerstone of society, lying in religion, ethics, and patriotism. This expanded the role of the female in Bahrain to involve both the traditional and modernised scope.

A typical Bahraini woman must create a balance between her career and the traditional role, prioritising her family over any career advancement. Indeed, being governed by an Islamic, Arabian culture emphasising the purity of women, Bahraini female must preserve her modesty, purity, image, and reputation from any external factor that might tarnish her reputation and damage the family honour. The female's reputation and good standing is a priority, and any threat or incident that might negatively affect or defile this reputation is dealt with utmost discretion or denied and hushed, either by the female herself, or the immediate family or members of society. The first person to blame is usually the female, as it is her expected role to preserve herself and her modesty and to refrain from putting herself in such situations. These reactions and expectations extend beyond the real world to include the cyber realm.

Moreover, while the social interaction of most women was limited to same gender social networking, with the partial liberation of females from the conservative controls, some started communicating with the opposite gender, mostly within socially formed norms and regulations, and under the keen eyes of her family and community. A girl was not allowed to have a mobile phone until she was in university. However, this dramatically changed with the technological growth and acquisition of smart devices and high internet connectivity. The world was freely opened to each girl, where she started exploring the virtual world, and connecting with others from different genders and different social locations.

Research Questions

The aim of this paper is to explore the psychological and social factors involved in feeling of victimisation, reporting crime, as well as, exploring the emotional and mental consequences as well as the applied coping mechanism, as a result of technology-facilitated violence.

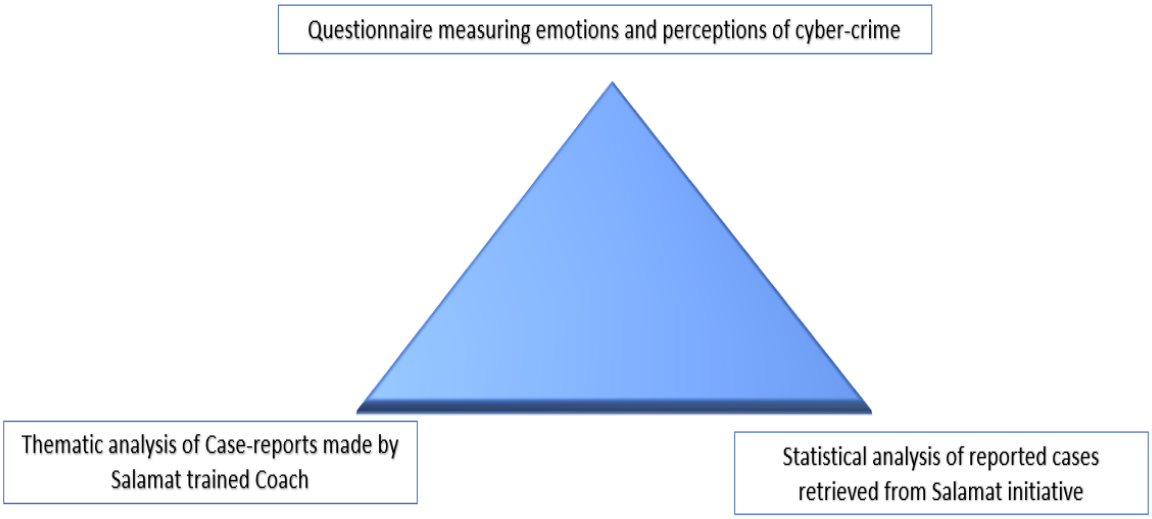
The main research question is: What are the psychological and social factors involved in being a victim of cyber-violence among women of different ages in the Kingdom of Bahrain?

To answer this, the following subsidiary questions should be answered:

1. What factors affect reporting or disclosing cyber-attacks among the women in the Kingdom of Bahrain?
2. What are the emotional, social, and mental consequences of being a cyber-victim among women in the Kingdom of Bahrain?

Methodology

Method: A mixed method exploratory research using both primary and secondary data retrieved from Salamat initiative in the Kingdom of Bahrain. To ensure the validity of the data a triangulation method was used.



Sample and Tools

Primary Data: to get greater insight on the female Bahraini population, a snowball sampling technique was used where 402 female participants answered an online questionnaire measuring the participants' behaviours, feelings and perceptions on cyber-crime and cyber-victimizations.
The questionnaire consisted of both closed and open-ended questions, allowing statistical and thematic analysis.

The questionnaire included multiple choice questions with pre-listed choices and a "other" option allowing for an open answer to ensure that all participants had a chance to fully express their feelings and actions taken. Some of the questions were "I had an experience with cybercrime", "after being a victim to cybercrime I felt _____", "what actions did you take after having the issue?" "Who would you feel more comfortable reporting the issue to?", "in your opinion what are the obstacles or fears that might stop people from informing their family that they were exposed to cybercrime?" Participants were automatically directed to the next question depending on their responses.

Moreover, it included 5-likert scale statements ranging from strongly agree to strongly disagree. An example of these questions was: "I felt empowered to report the case to the authorities" and "I felt empowered to report the case to my family".

And to obtain a greater depth of the issue at hand, participants were directed to open-ended questions depending on their responses on previous multiple choice or Likert scale questions. Examples of these questions were: "why did you feel empowered to report your case to authorities?", "why didn't you feel empowered to report your case to authorities?", "why did you regret reporting the case?" and "in your opinion what are the obstacles or fears that might stop people from informing their family that they were exposed to cybercrime?"

Secondary data: 900 anonymous case reports, obtained from Salam@ program in Bahrain, were analysed using both statistical and thematic analysis.

Results and Discussion

Analysis of the case reports from the Salam@ program indicated that women reported more cases of cyber-attacks than men. This could be because women are the primary beneficiaries for Salam@ and therefore the program is designed to attract women.

Thus, this difference in seeking help could be due to socialisation and the gender role expectations in different cultures. Due to social modelling or through subtle encouragement of certain behaviours by socialisation agents such as parents, school systems and the community, females are more likely to show their weakness and accept being powerless in facing the situation, while male are expected to exhibit feelings of strength and independence (Bandura, 1969; Chaplin & Aldao, 2013). Thus, females are more likely to disclose the incidents and seek help. Moreover, due to the fear of consequences that might affect their good standing, reputation and lead to further undesirable social outcomes, women are more likely to seek help to reverse the incident, or at least reduce the social stigma and retribution associated with cybercrime- especially in cases where they are guaranteed utmost confidentiality.

Figure 1: The sex of people reporting cyber crime in the last 15 months (2020-2021)

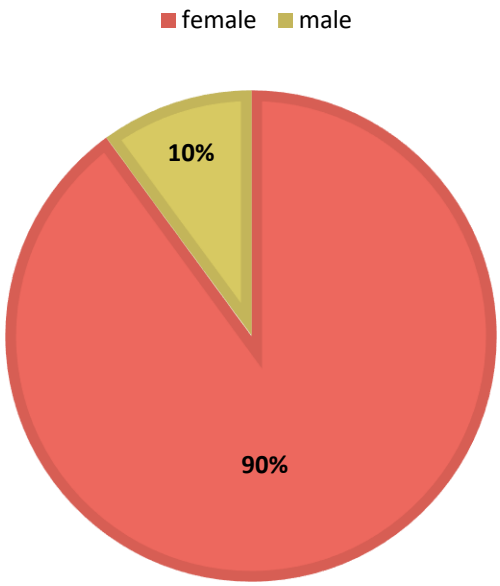
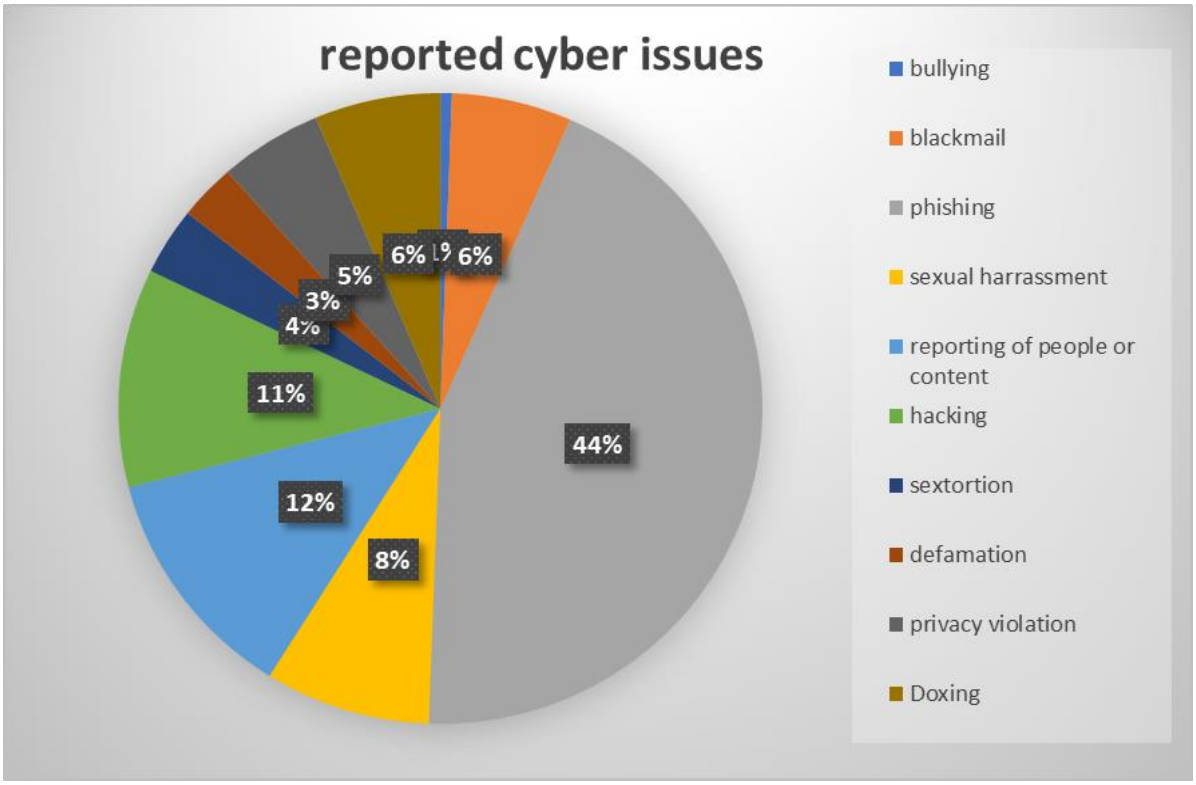


Figure 2 shows the categories of reported cases to Salam@ and indicates that the most reported cases are related to phishing, followed by reporting of people or content, and hacking incidents equating to 44%, 12 % and 11%

respectively. Sexual harassment, sextortion and bullying were among the rarely reported cases. This might be a consequence of the denial of the incident, fear of being exposed and the imaginative fears of the negative sanctions they might face by society. Moreover, it could be due to the reason that people are not aware of what constitutes bullying, defining it under "having fun", "assertiveness" or other less negative definition. (See Figure 2).

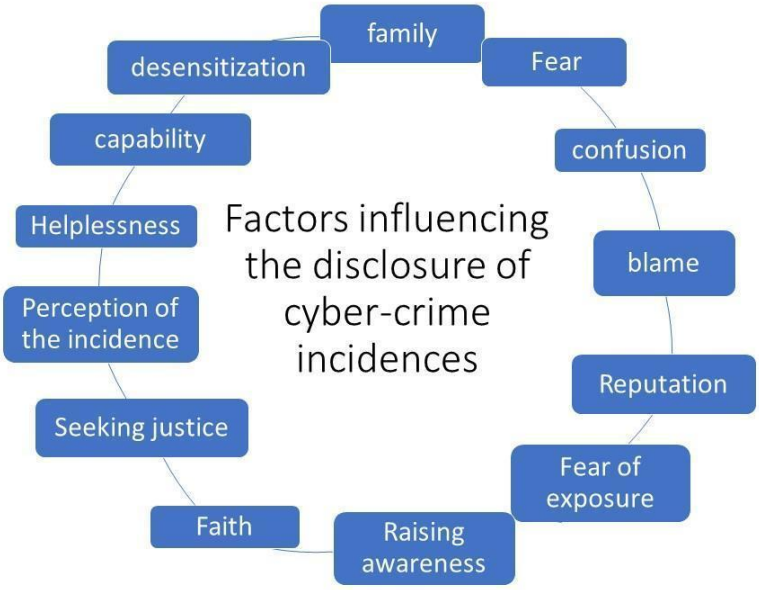
There were some case reports of women seeking psychosocial support after experiencing sextortion. It is important to note that in most cases of sextortion, it usually starts with hacking or phishing, or another form of cyber-crime, which later turns to threats or extortion, including sextortion. For example, a woman might have her device or email hacked, giving the attacker access to personal information, pictures, etc. The attacker might then threaten her with these personal data. Thus, it could be that the victim asked for guidance for the initial cybercrimes from the technical team, while reporting the consequences to the designated coach. In many of these cases, the victims sought help once and never contacted the coach again.

Figure 2: Statistics from technical support on the major categories of cyber-attacks



Q1. What factors affect reporting or disclosing cyber-attacks among the women in the Kingdom of Bahrain?

Thematic analysis of both primary and secondary data indicates that the most prominent factors influencing the decision to report the incidents to the authorities or disclosing it to family members were:



1. Family: respondents reported that the family plays a significant role in determining whether to report the incident—either they did not want their family to know, or they did not want to disgrace their family or tarnish their reputation. Moreover, many respondents reported that "relationship breakup" and "creating family problems" were among many of the fears related to the family category. This negative impact might lead to a sense of isolation, helplessness and depression, and the escalation of the incident, as well as further financial loss due to extortion or 'payment for being quiet'. Indeed, many of the cases emphasised "conservative" family status were a strong deterrent. Moreover, many of the respondents indicated that cyber-crime is considerably a new thing, and they didn't feel that their parents will fully understand what it is, and thus the blame will be mostly shifted on the 'victim'.

   Indeed, analysis of the questionnaire showed that 46.8 % of the respondents didn't feel empowered to inform their family, while 36.5 % felt empowered to do so. The data (Figure 4) indicated that out of the family members, siblings and cousins were preferred in imparting the incident to. This can be attributed to viewing them as cohorts and more likely to understand the situation than parents. In terms of the preference of the parents, the difference margin is almost minimal, with the mother being preferred. This could be due to the perception of the mothers as being generally forgiving and protective towards their kids. On the other hand, friends were the chosen confidants with 63.3% preferring to share the experience of victimisation with their friends, rather than a family member.

Figure 3: Respondents' feeling of empowerment to report the cyber-attack to family members.

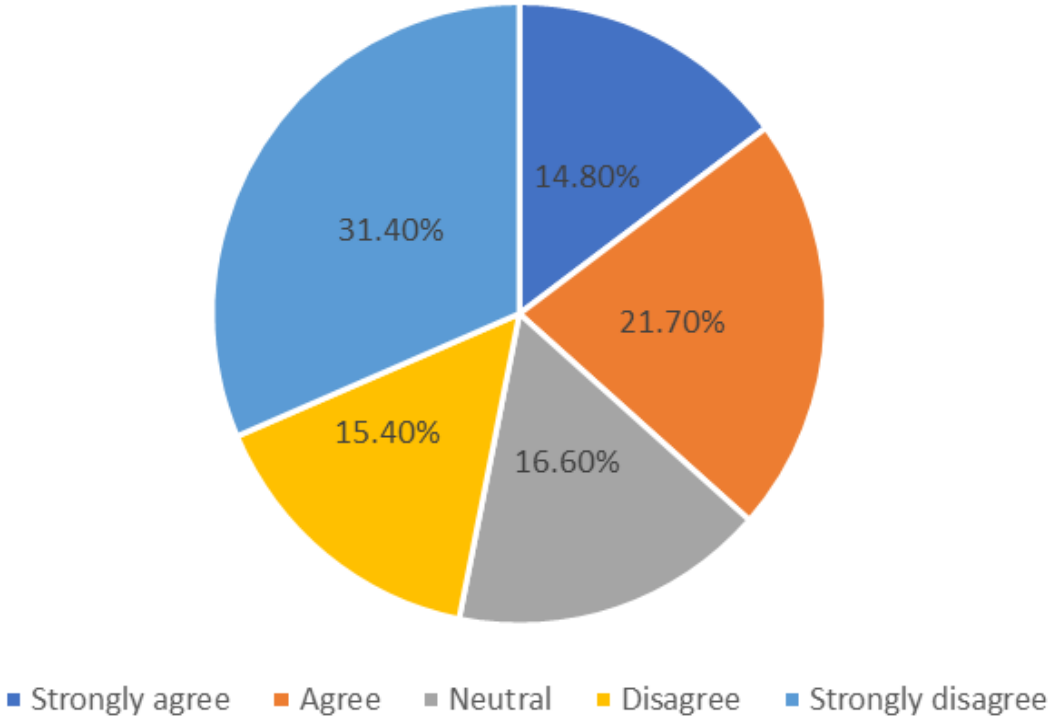
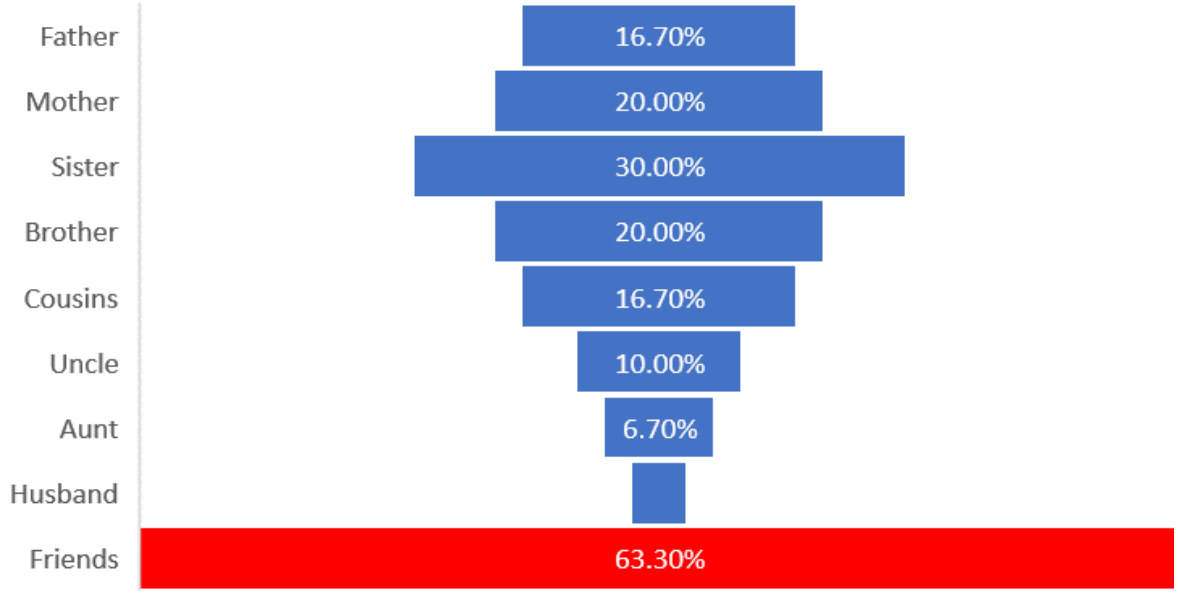


Figure 4: Respondents' preference for reporting the cyber-crime.



2. Awareness and Knowledge: respondents focused on parents' lack of knowledge of social media and cyberspace which might lead to a worse social impact. The general view is that this lack of understanding might lead to a focal blame on the victim, leading to various consequences ranging from mockery "of being I and easy to trick" to withdrawal of rights or getting grounded (such as taking away their smart devices, internet disconnection) and honour killing in extreme cases. Moreover, it was reported that cyber-crime and attacks can be viewed as newly-founded behaviour relating to younger generations, something that parents from older generations cannot comprehend, and reporting it or making it public can be considered a bold behaviour losing the person his credibility and endangering the victim of being looked down at or stigmatised.

   Indeed, within the awareness category, most statements were related to: "..the fact that some parents don't understand how social media works so they will blame it on their child and fear of society" and "..the father or mother don't know about devices and technology, so if something happens, they say that we are the ones who are wrong and they withdraw and deprive us of electronic devices, although we are just a victim, but they don't want to involve themselves in police centres ,legal reports, etc.."

3. Fear is greatly linked to the family and maintaining one's reputation. The inability to open -up to close family members due to decapitating fear – fear of family response, or the fear of shaming and rejection- might lead to the victim internalization of these view, self-censorship, and refusal to report the issue, as well as the exacerbation of the problem by fearing to deny the demands of the perpetrator- demands that ranged from asking for money to sexual favours. In some cases, the victims deferred to someone else for help, who used this situation as a leverage for their own demands and attacks – harming the victim further and making the situation harder to resolve with these added complications. Moreover, respondents emphasised the fear of stigmatisation; where they feared to be reduced to nothing more than "sinners" due to one or few instances of cyber-attacks, as well as the fear of destroying their "image" held by their family. Additionally, some respondents expressed fear of their inability to contain the incident, and fear of their (family's) reaction where the victim is isolated and mistrusted. Victims may also view secrecy as more convenient as they want to forget about the incident.

4. Blame: In most of the cases the respondents emphasised **"blame"** as a factor. Blame can occur as self-blame, self-loathing, and resentment or as fear of being blamed by family members and society. Indeed, many of the victims indicated that they felt they were to blame for placing themselves in such situations using statements such as "it's all my fault" and "I deserved it". In some cases, the victim was accused of infidelity, cheating and general blame for not taking better care or attracting unwanted attention. Some respondents reported that the family might blame them. This blame might stem from lack of understanding social media and the fear of society. Statements such as: "…some families with ignorant thinking that associate everything with shame especially when it is from the girl's side and also some families that are ashamed to raise such topics to their children" were repeated by many respondents.

5. Confusion and feeling of helplessness were associated with not reporting cyber-crime incidents. Many victims reported a feeling of helplessness and confusion, not being able to determine what to do and feeling powerless towards the attack, which made them lose their sense of value.

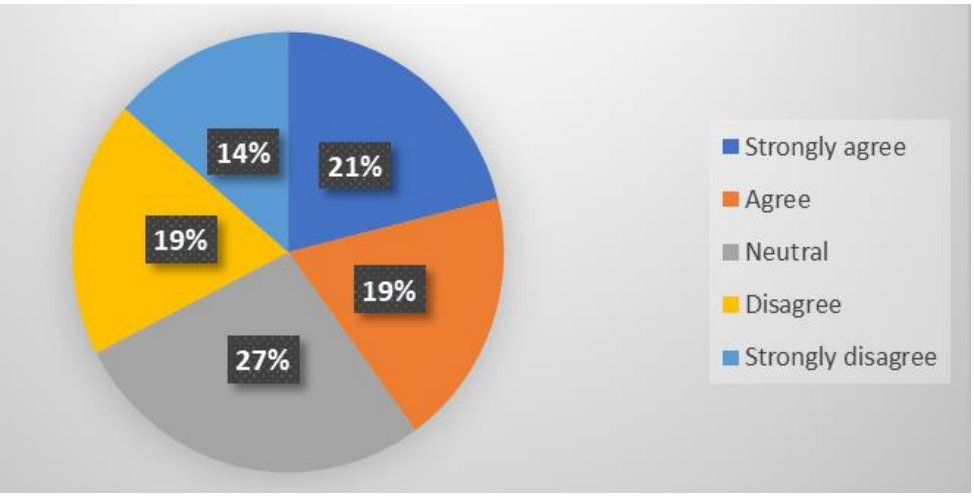
6. One's Capabilities: A few of the respondents believed that they could deal with the issue on their own, and thus did not find the need to escalate or report the incident. This is directly linked to the internal locus of control and high self-efficacy levels. Some individuals are strongly equipped to face these adversities. However, the danger lies with the falsely inflated sense of control. Individuals with unreal sense of capability might make wrong decisions and erroneous actions leading to more damage.

7. Desensitisation: Cyber-attackers are attracted by certain attributes in the victims that leads to further attacks. In many cases, the victim might suffer from repetitive attacks from one person - directed solely on her, such as phishing scams, identity theft or even extortion or attacks from different people. Moreover, the probability of having people they know suffering from the same can lead to a sense of desensitisation – where cybercrimes become a norm (they become equipped with the belief that it's a rite of passage- "everyone gets attacked at least once in their lifetime"). Some respondents noted that they have been receiving the same message over a period of time so they got 'used to it'.
8. Perception of the Situation: The seriousness/significance attributed to the situation can affect whether the case is reported or not. The less significant the attack is perceived, the less likely for it to be reported. Some participant commented that "the incident was not important and did not warrant reporting it to the authorities", while others saw the situation in a frightening and threatening light, and thus statements such as the following were reported: "they wouldn't report the incident because they were afraid that the family would know". Also, underreporting may be because the violence is not perceived as significant by the victim.
9. Prolonged Process. Respondents reported that the prolonged process of reporting and delays in getting results reduce the motivation of reporting the cases to authorities. Victims felt that even though the cases were reported, and the perpetrator was informed, it didn't act as a deterrent, especially with the realisation that resolving the cases would take a very long time. Some respondents commented: "…informing the family is not more important than reporting to the police, and when we tell the aggressor that we are going to the police, he is not afraid, as he knows that the police will not do anything and there will be no communication in following up the case, so the aggressor continues."

While most of the discussed factors so far were strong deterrents of reporting the case to family members or authorities, content analysis of the responses and the cases have found other factors that increased the likelihood of reporting the incidents:

1. Faith and Trust: Respondents have reported that having strong faith in Allah and in the authorities helped them take the necessary steps to bring the criminals (cyber-attackers) to justice. They reported that their faith and trust that Allah will save them from the incident was a strong motivation, as well as their trust in the authority's action. Indeed, 40 % of the respondents indicated that they felt empowered to reach out and report the incident to the authorities (Figure 6).

Figure 6: Empowerment to report the incident to authorities

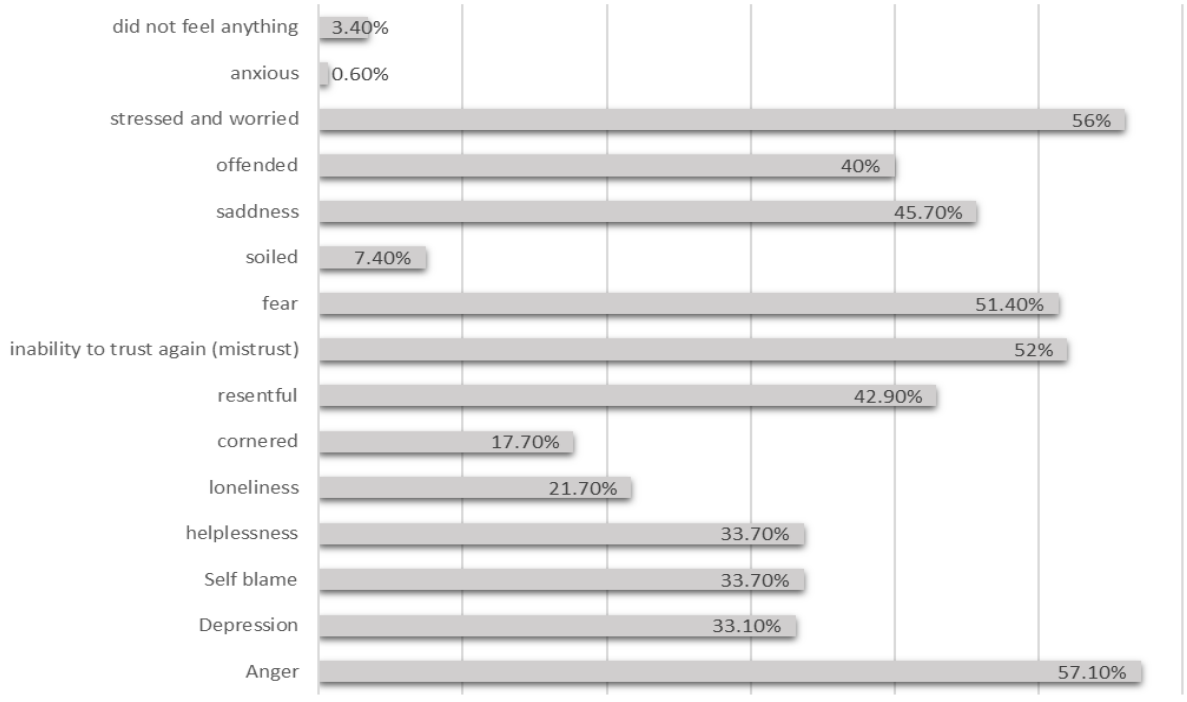


2. Seeking Justice: The feeling of being unjustifiably wronged strongly motivated the victim to seek justice and retribution. Many of the respondents reported that they believed that the culprit needs to be stopped by the authorities to prevent further extortion and threats. Respondents commented with statements such as "to reach the culprit and get my full vengeance" and "so the authorities would do the needful, and I can retrieve my accounts".
3. Raising Awareness: Those who reported and vocalised their experience as cyber victims wanted to spread awareness among their peers and to the public. Applying this positive thinking technique aids the healing process, as well as encourages others to stop being victims, and to take a stand. It raises the awareness among the families as well, shifting the blame from the victim to the perpetrator. Participants shared statements such as: "to protect others", "so everyone becomes aware" and "so others don't fall in the same trap".

Q2. What are the emotional, social, and mental consequences of being a female cyber-victim in the Kingdom of Bahrain?

Analysis of primary data showed that most emotional, social and mental consequences concur with the studies reviewed in the literature. Most participants reported feelings of loneliness, isolation, resentfulness among others (see Figure 7).

Figure 7: Emotional, social and mental consequences of being victimized by cyber crime



Most of these feelings, especially stress and social isolation, can intensify depending on the perceived severity of the situation, the presence of social support and the locus of control. They can readily affect the mental status and physical health of victims, leading to overly (unhealthy) protective measures such as distrust and self-isolation that might be generalised from the cyber-world to the real world, affecting social interactions, communication and overall quality of life. Moreover, feelings of depression, anger and stress can exert severe pressure on the person, affecting them both mentally and physically (O'Connor, Thayer, & Vedhara, 2021). It has been established that severe

stress may cause sleep disturbance and eating disorders and affect overall immunity, while clinical depression may lead to suicidal thoughts or behaviours (Woods, 2022).

When respondents were asked of their initial response to the cybercrime, 6.7% reported that they deactivated all social media accounts and emails, and 6.7% stopped contacting anyone beside the immediate family members. 30% of the participants reported that they continued using the social media, emails and online accounts while exerting more caution in their security measures and their on-line behaviours. 20% reported that they did not change the way they used the technology or their social media.

Some participants were inspired by the experience and opted to use it as a foundation to increase awareness among the public, overriding the fears of shaming and blame. Indeed, 23.3% reported that they used social media to publicise the issue (the public status of their account was not shared), while 36.7% informed their friends so they can be more cautious.

Conclusion

This paper put the victim at the centre of the analysis of cybercrime, claiming that the victim's perception of the crime and the risk associated with it, shape their actions and decisions around the crime. This includes decisions over reporting the crime, and decisions over-seeking help and support from friends and family.

Overall, the culture of fear and shaming still exists strongly, which exacerbates the emotional and mental consequences of cyber-victimisation and deters from reporting the incidents to either family members or the authorities. This can be changed by increasing the awareness of cyber-security and causes of cybercrime by reaching out to different communities in the society. Educating the younger generation should only be part of the movement, with a strong focus on generation X; those born before the 1980s. This can create a society that supports young women when they are exposed to cyber-crime, with a shift from blaming the victim to supporting and defending the victim, whilst uniting against the perpetrators.

References

Roli, A. and Olanrewaju, A. (2018). Emotional intelligence and self-management training programs in reducing peer victimization among Nigerian adolescents: interaction effects of locus of control and gender. B*ritish Journal of Psychology Research,* 6,2, pp 1-12.

Strobel, M., Tumasjan, A., & Sporrle, M. (2011). Be yourself, believe in yourself, and be happy: Self-efficacy as a mediator between personality factors and subjective wellbeing. Scandinavian Journal of Psychology, 52, 43-48.

Zelenski, J.M., Santoro, M.S., & Whelan, D.C. (2012). Would introverts be better off if they acted more like extraverts: Exploring the emotional and cognitive consequences of counter-dispositional behaviour? Emotion, 12, 290-303

Jacobs, N. C. L., Goossens, L., Dehue, F., Völlink, T., & Lechner, L. (2015). Dutch cyberbullying victims' experiences, perceptions, attitudes and motivations related to (coping with) cyberbullying: Focus group interviews. *Societies, 5*(1), 43–64. https://doi.org/10.3390/soc5010043.

Livingstone, S., Haddon, L., Görzig, A., & Olafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full findings and policy implications from the EU Kids Online survey of 9–16 year olds and their parents in 25 countries. (EU Kids Online, Deliverable D4). London, UK: EU Kids Online Network. Accessed June 2022: http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf.

Petrič, G., & Roer, K. (2022). The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. *Telematics and Informatics*, *67*, 101766.

Kuang, J., Delea, M.G., Thulin, E. et al. (2020). Do descriptive norms messaging interventions backfire? Protocol for a systematic review of the boomerang effect. Syst Rev 9, 267. https://doi.org/10.1186/s13643-020-01533-0

Lamet, W., & Wittebrood, K. A. (2009). Nooit meer dezelfde: Gevolgen van misdrijven

voor slachtoffers. Sociaal en Cultureel Planbureau, 1–94.

Modic, David & Anderson, Ross. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. IEEE Security & Privacy. 13. 99-103. 10.1109/MSP.2015.107.

Cross, C., Richards, K., & Smith, R. G. (2016a). Improving responses to online fraud victims:An examination of reporting and support. Criminology Research Grant Scheme. Australian Institute of Criminology. ttp://crg.aic.gov.au/reports/1617/29-131 4-FinalReport.pdf.

Cross, C., Richards, K., & Smith, R. G. (2016b). The reporting experiences and support needs of victims of online fraud. Trends and Issues in Crime and Criminal Justice, 518, 1–14.

Kaakinen, Markus & Keipi, Teo & Räsänen, Pekka & Oksanen, Atte. (2017). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. Cyberpsychology, Behavior, and Social Networking. 21. 10.1089/cyber.2016.0728.

DeValve, E. (2005). A qualitative exploration of the effects of crime victimization for victims of personal crime. Applied Psychology in Criminal Justice, 1 (2), pp. 71 – 89.

Jansen, J. and Leukfeldt, E. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. Journal of Qualitative Criminal Justice and Criminology, 6 (2), pp. 205 - 228

Green, D. L., Choi, J. J., & Kane, M. N. (2010). Coping strategies for victims of crime: Effects of the use of emotion-focused, problem-focused, and avoidance-oriented coping. *Journal of Human Behavior in the Social Environment, 20*(6), 732–743. https://doi.org/10.1080/10911351003749128

Frieze, I., Hymer, S. and Greenberg, M. (1987) Describing the Crime Victim: Psychological Reactions to Victimisation. *Professional Psychology: Research and Practice*, 18 (4), pp. 299-315

Bandura, A. (1969). *Principles of behavior modification.* Holt, Rinehart & Winston; New York, NY.

Chaplin,T., and Aldao A. (2013).Gender differences in emotion expression in children: A meta-analytic review. *Psychological Bulletin,*139:735–765. doi:10.1037/a0030737.

O'Connor, D. B., Thayer, J. F., & Vedhara, K. (2021). Stress and health: A review of psychobiological processes. *Annual review of psychology*, *72*, 663-688.

Woods, N. (2022). Users' Psychopathologies: Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior. In *Cyber Security* (pp. 93-134). Springer, Cham.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigations. *International Journal of Digital Evidence*, 3(1), 1–22. https://dblp.org/rec/journals/ijde/Ciardhuain04

Yue, W. T., Wang, Q.-H., & Hui, K.-L. (2019). See no evil, hear no evil? Dissecting the impact of online hacker forums. *MIS Quarterly*, 43(1), 73–95. https://doi.org/10.25300/MISQ/2019/13042

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology*, 2(1), 191–216. https://doi.org/10.1146/annurev-criminol-032317-092057

Verizon. (2021). 2021 Data Breach Investigations Report. Retrieved January 2022, from 2021-data-breach-investigations-report.pdfx (verizon.com)

Baldry, A. (2004). 'What about bullying?': An experimental field study to understand students' attitudes towards bullying and victimization in Italian middle schools. British Journal of Educational Psychology, Dec 2004, 74.

Cullen, F.T. (1994). Social support as an organizing concept for criminology: Presidential address to the academy of criminal justice sciences. Justice Quarterly, 11(4), 527 559.

Littleton HL (2010). The impact of social support and negative disclosure reactions on sexual assault victims: A cross-sectional and longitudinal investigation. *Journal of Trauma and Dissociation*, 11, 210–227

Stadler, Christina & Feifel, Julia & Rohrmann, Sonja & Vermeiren, Robert & Poustka, Fritz. (2010). Peer-Victimization and Mental Health Problems in Adolescents: Are Parental and School Support Protective? Child psychiatry and human development. 41. 371-86. 10.1007/s10578-010-0174-5.