Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBER HARASSMENT PREVENTION THROUGH USER BEHAVIOR ANALYSIS ONLINE IN KINGDOM OF SAUDI ARABIA (KSA)

[1]FAHAD ABDULLAH MOAFA, [1]KAMSURIAH AHMAD, [2]WALEED MUGAHED AL-RAHMI, [2]NORAFFANDY YAHAYA, [2]YUSRI BIN KAMIN, [3]MAHDI M ALAMRI

[1]Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia

[2]Faculty of Education, Universiti Teknologi Malaysia, 81310, UTM Skudai, Johor, Malaysia

[3]Faculty of Education, Education Technology Department, King Faisal University, Alahssa, Saudi Arabia

E-mail: [1]fah171393@hotmail.com, [1]kamsuriah@ukm.edu.my [2]waleed.alrahmi@yahoo.com, [2]p-afandy@utm.my, [2]p-yusri@utm.my, [3]mahdi@kfu.edu.sa

ABSTRACT

This research attempted to mitigate the gap in literature concerning a one serious problem in Saudi society and government is cyber harassment. This problem is caused through the increasing use of technology. Accordingly, the main objective was to explore the factors that influence the intention to minimize cyber harassment among Saudi citizen. Nevertheless, the researcher has assured that the Saudis will remain at risk of cyber harassment, until these factors are fully investigated among the Saudi community. In conclusion, this research specifically proposed in future a model and framework for identifying the significant factors that are anticipated to play a major in minimizing cyber harassment among Saudis. The proposed framework will help the administration and decision-makers in the KSA to formulate strategies that can significantly affect anti-cyber harassment among youths.

Keywords: *Cybercrime, Cyber-Harassment, Behavior Analysis, online threats*

1. INTRODUCTION

By the end of the twentieth century and early years of the 21st century, quick developments in telecommunications, computing software and hardware, and data encryption happened. The accessibility of littler, all the more effective and less costly figuring hardware made electronic information preparing inside the range of independent company and the home user. These PCs quickly ended up through the Web. This quick developments has led to the spread of computers everywhere, and the use of the Internet has become accessible to all, and this has many of the advantages and disadvantages of these technologies, where the positives lie in the use of the Internet in many work and study, and in rapid communication with people around the world , And the ease of transferring information to others, but on the other side emerged many disadvantages, when technology is harnessed in the hands of people with bad morals misuse in all forms of this has spread incidents of electronic harassment and harassment, and the threat of others and other forms of the bad use of modern technologies [1]. As mentioned earlier, in the introduction of this study the cyber harassment is the type of cyber-crimes' official reports made by Saudi government authorities, specialized in security aspects of information and electronic crimes indicating that there is a sharp rise in the proportion of electronic crimes, especially in the cyber extortion crimes assured that cybercrime is on the rise across Saudi Arabia. The rate has increased by 57% in 2014 compared to 2013, and protecting against cyber threats is an ongoing management challenge for organizations. (Anti-Harassment Center, KSA Annual Report [2]. Studying minimizing cyber harassment determinants in developing countries like Saudi Arabia does not only serve the development of technology in Saudi but can contribute to the body of knowledge in the area for anti- cyber harassment. This research will be of significance in several areas and provide new knowledge to academics and practical. Cybercrime is about to become increasingly wide spreading, as by 2011, nearly 2.3 billion people, about 1/3rd of the global population would have internet accessibility, where, around

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

60% of the overall internet consumers lives in developing region, with 45% of them are below the age of 25. Indeed, it is estimated that by the end of 2017, around 70% of the global population will subscribe to have a mobile broadband internet access [2].

Several people know about cyber related offences, but few know about the utilization and susceptibility to cybercrime. It is indeed prominent that cyber harassment in the KSA affect peoples' life, more especially that of the younger generation. This lack of awareness in the KSA, more particularly among the youth, paves ways for possible loopholes between safer internets. Against this background, this study attempt to fill in the gaps of cyber harassment data in the KSA. Therefore, the study assesses cyber harassment as a pressing issue among cyber related offences. Available literature on cyber harassment in the KSA are mainly on the victims psyche in relation to the harassment suffered, without looking into the relationship between internet usage, behavioural traits of the users, considering the circumstance that facilitates the harassment. In the Kingdom of Saudi Arabia (KSA), the anti-cybercrime law was approved on the 26, March, 2007, where the kingdom issued a Royal Decree No, M/17 to target cybercrime [74, 75].

Furthermore, reviews, conducted on cyber harassment involved mobile gadgets such as smartphones with ICT and looking into the security risks associated with privacy-sensitive information, such as social communications that need the exposure of confidential personal information. On the other way round, harassment through means of communications includes all the elements of known harassment, but expands the crime into the utilization of electronic gadgets to transmit messages that cause an individual to feel personally aimed for harm. For instance, opening a Facebook account using another person name and profile to harass people could be one form of cyber harassment. Therefore, this study concentrated on three aspects of cyber harassment: cyber-stalking, and cyber bullying.

2. DEFINITION OF CYBER HARASSMENT

One of the primary issues with cyber harassment laws is that more often than not nobody is held in charge of the mischief caused. The casualty cannot sue the genuine culprit on the grounds that digital harassers utilize mysterious names and programming to shield their character. The casualty cannot sue the site since they are invulnerable from obligation through area 230 of the Interchanges Respectability Act. The site isn't even legitimately bound to expel the culpable substance from its pages. All together for cyber harassment casualties to encounter any sort of help, the Web access Suppliers (ISP), and site proprietors must be held at risk for any cyber harassment that happens on their servers or websites.8 notwithstanding, deciding the suitable measure of obligation is troublesome. This is the place web copyright encroachment law can help shape new cyber harassment laws. Web copyright encroachment law holds ISPs at risk for its supporters' infringement if the ISP did not take after specific advances. The third piece of this paper examines the subtle elements of Web copyright encroachment law. At long last, the last segment of this paper talks about the likenesses between cyber copyright law and cyber harassment law, and proposes an authoritative answer for the deficiencies of current cyber harassment law displayed after the Advanced Thousand years Copyright Act [3]. One type of cyber harassment is On-Line mobs. As per Daniel Citron on the web crowds can utilize four sorts of assaults in their online ambushes. "In the first place, assaults include dangers of physical brutality," including demise and assault threats. Next, the attacks attack the casualty's protection. The aggressors hack into the casualty's PC and take individual data, including a standardized savings number, telephone number, and other individual data and afterward post that data on line.12 Third, the attacks can harm the casualty's notoriety and financial openings. The aggressors will post lies about the casualty and send those misleads the casualty's employer. In conclusion, aggressors can utilize innovation to constrain casualties disconnected by planning dissent of benefit assaults. Regularly, these online crowds utilize every one of the four apparatuses to assault [4].

3. TYPES OF CYBER HARASSMENT

In order to figure out where does cyber harassment fit in a general classification, we need to first identify what is the meaning of harassment and what does it cover. Since we are interested more in the legal definition regarding this subject, we are going to look at the legal definition of harassment. Looking deep in the Protection from Harassment Act 1997, we will not be able to find a complete definition of harassment however the clear description drawn is that it is an action repeated by a perpetrator which causes alarm or distress. The basis for a claim require a so called course of conduct which means that there must be

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

at least two incidents representing harassment whilst the person being accused knows or ought to know that it would be considered as harassment [1]. There is no general definition of harassment that can be brought into the light, however each entity adopt its own definition. The causes and forms of harassment are wide-ranging and complex. The same behavior may be inoffensive to one person and deeply offensive and intimidating to another. Unintentional or misinterpreted behavior may cause feelings of harassment. Swansea University considers harassment to be the unwanted conduct on the grounds of race, gender, sexual orientation etc. which has the purpose or effect of either violating the claimant's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment for them [2]. On the contrary, [3, 4, 5] students and researchers have a positive attitude and intention to use social media for educational purposes. Cyber harassment is the harassment that takes place in the cyber space using electronic and communication technologies. Those technologies includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites. From the definitions above, many actions fall under the umbrella of cyber harassment. In order to study this subject, we are going to gather the main types of cyber harassments in different classes.

3.1 Sexual cyber harassment

This type covers all form of unwanted verbal or non-verbal conduct of a sexual nature that creates an intimidating, hostile, degrading or offensive environment. This type includes include jokes of a sexual nature, invasion of personal space, inappropriate use of evocative visual display material, and daunting behavior such as asking for sexual favors in return for a favor that the victim needs, unwanted comments on dress and appearance and finally the display of sexual offensive material [2]. A special example of sexual cyber harassment is grooming, where the perpetrator makes friend with the victim and tries to involve him in inappropriate activities. In the UK this behavior is a criminal offence [5]. As per physical sexual harassment cyber sexual harassment also covers harassment based on sexual orientation and sexual reassignment which are prohibited by Sex Discrimination Act 1975.

3.1.1 Based on sexual orientation

This type of cyber harassment considers any behavior deliberate or otherwise, pertaining to sexual orientation. This includes homophobic remarks or jokes, ridicule, threats to disclose sexuality, intimate questions about sexual activity and intrusive questioning about a person's domestic circumstances [2, 3].

3.1.2 Based on sexual reassignment

People who have undergone sexual reassignment procedures are prone to cyber harassment which includes unwanted comments about appearance, dress, and/or questioning about the re-assignment motivations [2, 3].

3.2 Racial cyber harassment

Racial harassment is any behavior, deliberate or otherwise pertaining to race, color, nationality - including citizenship, or ethnic or national origins, which is directed at an individual or group and which is found to be offensive or objectionable to recipients and which creates an intimidating, hostile or offensive environment. This includes inappropriate questioning about racial or ethnic origin, bad name calling, offensive graffiti, insults and racist jokes, and intimidating behavior such as threatening gestures [2, 3].

3.3 Cyber bullying

Bullying is an attempt to lower the value and social status of others in order to leverage the personal social status or self-esteem [6]. In this research we can define bullying as an unwanted, aggressive behavior that involves a real or perceived power imbalance which gets repeated over time [7]. Differences were found in each age group regarding the mode of technology most prevalent for cyber bullying in and out of school. More internet-based bullying through social networking sites was reported than through mobile phones, especially as students get older [8].Being a type of psychological harassment, it can be characterized as offensive, intimidating, malicious or insulting behavior, abuse or misuse of power through means intended to undermine, humiliate, denigrate or injure the recipient including unmerited criticism, isolation or gossip. Cyber bullying takes different forms such as Stolen Identity, Threats, Black Mail, Rumors, Gossip, Abusive Comments, Nasty Pictures [9].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.3.1 Identity Theft

In recent years, the phenomenon of identity theft has gained widespread media coverage and has grown to be a major concern for payment providers and consumers alike[10]. When a personal account is hacked and is being used by a different person, it's online identity have been stolen. In addition, when someone creates an account in the name of a different person, he will be steeling his identity [5, 9].

3.3.2 Spreading rumors and gossip

Rumor or gossip is circulating a story or report of uncertain or doubtful truth. The problem with social networking websites is that anything of that sense posted about someone can be seen by lots of people because it's on a public domain and because the bullies behind it try to spread the message to everyone to make sure they find the abuse [5, 9].

3.3.3 Threats

In recent years, the phenomenon of identity theft has gained widespread media coverage and has grown to be a major concern for payment providers and consumers alike, threats made on the internet could be taken as a criminal offence. It's against the law in the UK to use the phone system, which includes the internet, to cause alarm or distress. Threats are very serious and they can fall under Protection from Harassment Act [5].

3.3.4 Blackmail and extortion

Blackmail and extortion have a wide variety of harmful effects on their victims and the society at large. For the individual victims, blackmail and extortion are psychologically, financially, and often physically traumatizing. They often feel they have nobody to turn to, and are intimidated and disempowered at the same time that they are stripped of their money or possessions. The strain that blackmail and extortion put on individuals as well as their relationships with others exacerbates the financial and material loss that these offences so frequently involve[13]. Blackmail also deprives those involved of the ability to freely and honestly narrate their own relationships[14]. While other researchers consider the use of social media have positive impacts on collaboration and engagement among students [11, 12, 13].

3.3.5 Humiliation and Insults

Erkol et al. have reported that the most common forms of psychological violence were shouting, verbal threat, and abusive language [15]. In previous studies in Iran, abuse, ridicule [16], humiliation and insults [17] were the most common forms of verbal violence, AbuAlRub et al. have indicated that humiliation and bullying have significantly more severe negative effects on victims' mental health than other forms of violence[18].Therefore, psychological violence and its destructive effects on mental health should be considered by healthcare officials and planners[19]. Posting comments and images in order to humiliate a person or insult him falls under the umbrella of cyber bullying. It is often resolved by requesting the hosting website to remove those comments or pictures however repeated actions lead to harassment [5, 9].

3.3.6 Nasty Pictures

With the availability of cameras on smart phones, uploading a picture of someone became extremely easy. Nevertheless, one needs to obtain permission from the people in the image before posting it on the internet. For instance, taking nude or degrading pictures of someone without his or her permission and posting it is considered bullying and can lead to legal prosecution. Altered digital images may also be offensive to people if not taken care of[5, 9].

3.3.7 Unjustified Criticism

In the cross-cultural study on university students' experiences of bullying in four countries (Pörhölä et al., in submission), the most often experienced form of bullying reported by females across the four countries was found to be unjustified criticism, belittling, or humiliation related to studies[20]. Continuous unjustified criticism is considered bullying especially in schools and in workplaces. Usually a healthy criticism is a constructive one. But when a manager keeps criticizing his subordinate work for no just reason, the employee can raise a case for bullying [5, 9].

4. CYBER STALKING

Cyber-Stalking is defined as the unlawful act of collecting or amassing an individual's private information with regards to the internet, a computer, or alternative electronic network. Cyber stalking involves the use of information and communication technologies as the means and the medium of harassment or intimidation [21]. Cyber stalking involves the use of the Internet, e-mail, or other means of electronic communication to stalk or harass another individual it also involves repeated harassing or threatening behavior [6]. In November

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2012, stalking became a named offence in England and Wales for the first time [22]. Due to the accessibility and availability of communication technologies, the use of social networking sites, chat rooms and other forums through the internet can provide many objects of interests for a stalker. Those include the victim's personal information, a method of direct communication with the victim, a means of surveillance of the victim, the ability to impersonate the victim, damaging the victim's reputation and sabotaging the victim's cyber space [23]. Stalking takes different forms such as:

Monitoring personal life: Continuously monitoring someone's posts, photos, places visited groups of friends [24].

Spyware data gathering: Stalkers use spyware so they can monitor what their victim is doing on his computer or phone at all times [25].

Location tracking: Using the victim's phone GPS to locate and track his position [24].

Impersonate to blame: Create a fake account in the victim's name or hacking into the victim's account in order to use such account for harassing other victim's making the first victim seem as if he is guilty [25].

Taking over online accounts: Hacking into the victim's online accounts to retrieve personal data, images and photograph to satisfy the perpetrator stalking needs [26].

Threats: Threats encountered in cyber stalking are similar to the ones encountered in cyber bullying except that the threats thrown by a stalker are not intending to devalue the victim rather they are intended to cause alarm and distress to force the victim into something they don't want to do. For example stalking an ex-girlfriend and threatening to expose her intimate images if she doesn't come and be intimate with the perpetrator [24].

Provoking: Provoke the victim into a war of words through intentionally flaming a situation online with the aim of damaging the victim's online image [25].

Damaging reputation: To some stalkers, if they are not able to get what they want from their victims, they turn into damaging the victim's reputation. This includes sending, posting, or publishing false rumours and untrue statements [25].

Encouraging others to harass the victim: Many cyber stalkers will involve third parties in the harassment process. For instance, the cyber stalker may advertise the victim's contact details with a message suggesting sexual availability. This is a common form of a harassment and often victims report to receiving hundreds of telephone calls and messages in response to such advertisements [26].

4.1 Type of Stalkers

4.1.1 Intimacy seeker

Intimacy seekers identify the object of their affection as their true love. Some imagine that the person they are stalking reciprocates such feelings. Many "star stalkers" fall into this category. Their sought-after partner's indifference may enrage them. They made up about 34% of the Australian study group. Many intimacy seekers have serious mental illnesses such as delusional disorders, Mullen said, and need psychiatric intervention. They also need help to overcome social isolation. Getting them a pet, he said, might be a good start [27]. People of this type imagine or desire a relationship with someone who is not interested in them but they are convinced that he does [28].

4.1.2 Incompetent Suitor

Incompetent suitors are those whose stalking is sustained by hopefulness. Their stalking of a particular person usually lasts only a short time, but these people who often are intellectually limited then may pursue others. They comprised 15% of the stalkers. With tutoring, they sometimes can acquire acceptable courting and other social skills [27]. Similar to intimacy seeker but is only looking for a sexual encounter and not a long term love relationship [28].

4.1.3 Rejected

Rejected stalkers are motivated by a desire for reconciliation and/or revenge. Their stalking becomes a substitute for the lost relationship, however much of a caricature the stalkers' behavior becomes. Some derive satisfaction from inflicting pain. They often have personality disorders and are among the most persistent and intrusive stalkers. They are predominantly male [27]. When a relationship breaks down, one of the members will feel rejected and might start stalker the other with an intention of reconciliation, revenge, or a fluctuating mixture of both [28].

4.1.4 Resentful

Resentful stalkers often are aggrieved workers who feel humiliated or treated unfairly. They may carry out a vendetta against a specific person or choose someone at random as representative of those they believe harmed them. If convicted, they often resist treatment, and protest that they are the ones being persecuted, striking back at their oppressors. Stalking makes they feel powerful.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

They rarely develop empathy for those they stalk, and are the most difficult group to engage in treatment. They comprised 11% of the total [27]. In this type, a person aim to frighten and distress the victim to have revenge for an actual or supposed injury. The perpetrator seeks a feeling of power and control over his victim how allegedly caused harm to him [28].

4.1.5 Predatory

Predatory stalkers stalk someone as preparation for a physical or sexual assault and take pleasure in causing sadistic pain. Many have paraphilias and prior convictions for sexual offenses. They represented 4% of the stalkers, and were exclusively male; they require treatment appropriate for sexual offenders [27]. The perpetrator is sadistic; he tries to pursuit his victim to obtain sexual gratification. The imagination and the violent sexual fantasies they are looking and planning for excites them while they prepare for the actual sexual assault [28].

4.2 Disability based cyber harassment

Posting comments or images that negatively affect the dignity of people with disabilities is considered harassment. This includes discussion of the effects of a disability on an individual's personal life whether it is physical or mental impairment, learning difficulty or disfigurement, and inappropriate questioning about the impact of someone's disability [2].

4.2.1 Age based cyber harassment

This type covers differentiating people based on their age, or commenting on their ability just based on their age. It includes derogatory age-related remarks and unjustifiable dismissal of suggestions based on someone's age [5, 6].

4.2.2 Religious based cyber harassment

Religious Harassment is any behavior deliberate or otherwise, pertaining to religion, religious belief or other similar philosophical belief and it is behavior which can be defined as unwanted conduct violating a person's dignity, or creating an intimidating, hostile, degrading, humiliating or offensive environment. For example: offensive jokes, ridicule and display of offensive material [2].

4.2.3 Political cyber harassment

Political views, physical appearance, gender and race are among the top reasons people say they are harassed online. Some 14% of Americans – representing 35% of those who have encountered any type of harassment online – say they have been the target of online harassment because of their political views [29]. Harassing a person based on his political views or his political affiliation is not allowed under the laws protecting people's freedom of thought. Politicians usually get harassed for their political view and get criticized not on their actions but just for their political position [2].

5. GOVERNMENT ROLE IN FIGHTING CYBER HARASSMENT IN SAUDI ARABIA

Despite the fact that administrations of the created and additionally creating nations are seen decided and currently concentrating on battling and averting digital lawbreakers to keep them from the harm of their digital framework, yet, the very idea of the internet shams various difficulties in actualizing the digital directions in these nations, as it is difficult to characterize and decide the political outskirts and guilty parties in the internet. Additionally, digital offenders and their strategies are endlessly changing, that make it more troublesome somewhat trying for governments and organizations to stay aware of consistently changing systems utilized by digital hoodlums. As indicated by Burglarize Wainwright, Executive of Europol, Criminal Examinations of Digital Violations, recognizing and following the beginning of wrongdoing isn't just mind boggling however at some point unimaginable because of its borderless nature, which is one of the colossal difficulties for the creating scene, who are now innovation lacking (Board of Europe, 2003). In like manner, a few specialists ponder that the digital assaults and digital violations are lucrative wander. In the digital world, the programmers perpetrate sorted out wrongdoing by offering private stolen knowledge [30]. To execute the digital safety effort, adequate number of talented labor is required, while, the second issue in creating nations is the shortage of the gifted digital wrongdoing contenders, as a large portion of the creating nations are looking with the lack of gifted individuals to counter digital assaults. As indicated by Ronald Oble, the Head of Interpol, "a viable digital assault does not require an armed force; it needs only one person. In any case, there is an extreme lack of aptitudes and skill to battle this kind of wrongdoing; at Interpol, as well as in law implementation all over the place". Absence of forensic aptitudes and mastery is another center issue stays unsolved over a long stretch other than across the board utilization of pilfered

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

programming to counteract digital wrongdoing. Because of continuous utilization of pilfered programming, which is more inclined to assaults by infections, malware and Trojans, the control of digital violations turns out to be all the more difficult and troublesome [31].

5.1 Cyber harassment Laws in Saudi Arabia

Most states have recognized that digital crimes have turned into a genuine danger. As needs be, practically every state has laws that specifically address digital stalking or cyber harassment. States address this new wrongdoing by either making a fresh out of the box new law or adjusting current stalking and badgering law to incorporate online conduct. There are two primary sorts of online conduct that states have tended to: digital stalking and cyber harassment In spite of the fact that these three wrongdoings are connected, it is essential to comprehend the distinctions [32]. In spite of the fact that the correct definition varies from state to state, stalking is for the most part characterized as, "a course of lead coordinated at a particular individual that would make a sensible individual feel fear." In examination, "digital stalking is the utilization of the Web, email or other electronic interchanges to stalk. Some state laws incorporate a component of either physical vicinity or a "sound danger" in the stalking statute. “trustworthy risk” is a risk made with the expectation and the obvious capacity to do that risk in order to cause the individual who is the objective of the danger to sensibly fear for his or her safety." Having a prerequisite of physical closeness or solid risk can be tricky in the digital stalking setting since dangers over the web can effortlessly do not have the physical closeness or obvious capacity component[33]. A digital stalker who lives on the opposite side of the nation from his casualty does not have the obvious capacity to complete with his dangers, and, subsequently, the casualty can't record stalking charges against her stalker Cyber harassment is like digital stalking yet does not require a trustworthy threat. Most cyber harassment laws contain three components. To begin with, the publication must have the plan to bug. Second, the message would make a sensible individual feel hassled. Third, the casualty should really feel harassed. Each state's provocation laws are unique, however most laws have these or comparable components [34].

Saudi Arabia's Bureau has affirmed changes to the Kingdom's Against Digital Wrongdoing Law (Imperial Declaration No, M/17 dated 8 Rabi1 1428) that could enable guilty parties to be freely named and disgraced [35]. Article 6 of the Law right now accommodates a punishment of up to five years' detainment and additionally a fine not surpassing three million riyals (USD 800,000) for any individual discovered liable of a scope of offenses, including the "creation, readiness, transmission, or capacity of material impinging on open request, religious esteems, open ethics, and security, through the data system or PCs". The extra powers conceded to the courts under the corrected arrangement will permit the production of a synopsis of the decision in at least one nearby daily papers or some other medium esteemed appropriate by the court with regards to the kind of the wrongdoing, its seriousness and its effect. The production must be made once the decision picks up the status of "definite decision," and the guilty party may likewise be required to pay for the expenses of distribution [36]. It is a fascinating advancement in a district of new security laws. The capacity to distribute a man's name and subtle elements of a criminal offense they have perpetrated – data that would be 'delicate individual information' under European information security laws – makes an exemption to the standard rights that would be accessible to a man to ensure their own protection or notoriety. The impact of the enactment is with the end goal that those rights are lost if the individual is discovered liable of disregarding someone else's protection [37]. Open naming and disgracing has for some time been an apparatus for weight gatherings and activists, especially in nations with high social and reputational esteems. The web and web-based social networking have significantly expanded the simplicity and speed thus, social networking sites also allow for the public sharing of information [38, 39].

Saudi Arabia's law changes are a case of the expanding ability of administrators to utilize social disgracing as an impediment for hostile to social offenses. The Chinese government as of late reported expanded punishments for violators of the nation's hostile to smoking laws including open naming and disgracing of smokers, while the laws in the Australian province of Victoria were altered in 2014 to give casualties of aggressive behavior at home the privilege to name and disgrace their assailants [40]. Notwithstanding, it ought to be recalled that, outside these legitimized types of distribution, there are regularly confinements under defamation and security laws that deny immediate and open disgracing of people or organizations. In 2011, the Dubai Name Disgrace site and Twitter page was shut after notices that posting the names

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and implicating photos of awful drivers and organizations giving poor client benefit in the UAE was illicit under nearby criticism laws. Also, in the Unified Kingdom, a police compel was researched by the Data Chief's Office a year ago for potential infringement of the Information Security Act in connection to a battle of naming and disgracing alcoholic drivers [41].

5.2 Challenges for Cyber harassment Laws

In this found that 39 states have perceived the significance of specifically criminalizing cyber harassment is an expansive advance in the privilege direction. In any case, these laws bring requirement challenges. There are three principle cyber harassment law requirement challenges. The principal fundamental challenge is taking in the character of a harasser on the Web. A portion of the harassers are innovatively modern and know how to stay mysterious. They regularly utilize open PCs and anonym punch programming to conceal their personalities when making their illicit, bothering remarks. On the off chance that the casualties can't recognize their harassers, at that point the casualties can't look for any genuine cure [42].

The second test is that regardless of the possibility that a casualty takes in the personality of her harasser, the harasser is probably not going to have enough cash to satisfactorily repay the casualty. In the Auto Concede case the casualties agreed to a sum in the digit extend. That isn't high considering the amount they endured. The third and most imperative test is getting the ISP to evacuate the culpable material once the casualty finds it. What recognizes cyber harassment from customary badgering is that once the fast approaching provocation has ceased, there remains a digital impression of everything that was said. Additionally, everybody with web access can read the annoying remarks [43]. This implies even after the provocation stops, a business that Google looks through a casualty's name will even now discover the greater part of the negative remarks about the casualty[44]. Each of the three difficulties could be tended to by holding ISPs subject for the provocation that happens on their systems. The primary test of finding the guilty party would be tended to by holding the ISP at risk since they have a settled address and area. Casualties would dependably have somebody to consider in charge of the wrongs done to them. The second test of getting satisfactory alleviation would be tended to on the grounds that ISPs by and large have more cash to pay for harms, and they are in a superior position to settle expenses to everybody by charging more for the administrations on account of the expanded obligation. Furthermore, the third test would be illuminated by requiring the ISP to evacuate insulting material. Starting at now, segment 230 of the CDA gives ISPs finish immunity. ISPs have sole watchfulness in the matter of whether they will expel irritating remarks or help with finding the real harassers [45]. By this figure we saw that the hackers and the Harassers has a lot of ways to obtain the personal information for their victims, it includes boots and program viruses, script active x, E- mail attachments,… so they can hack the personal computer, or mobile and obtain all personal information, photos, chats, and threat the victims using it. The researcher sees that Harassment laws should be vigorously enforced and the case must be resolved vigorously to avoid the disasters that result from the fraud of the harassers on the vulnerable victims. See figure 1.

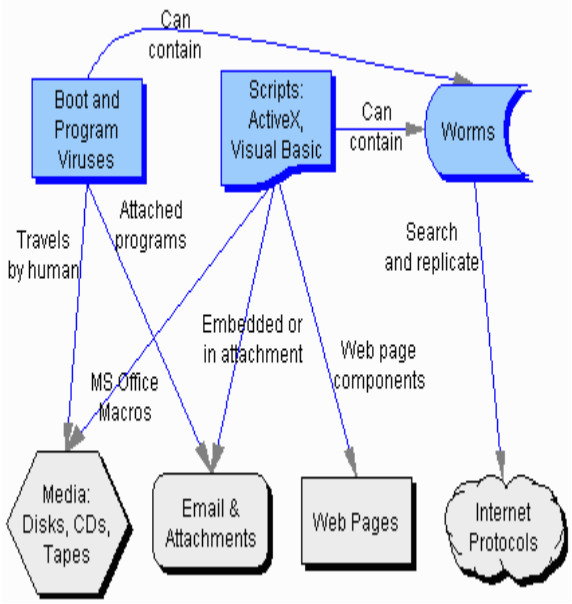

Figure 1: The Styles Of Harassment By Sending Types Of Viruses

6. IMPACTS OF CYBER HARASSMENT

Cyber harassment can have wrecking impacts. The National Kids and Youth Law Center (NCYLC) venture discovers, 'Casualties of digital tormenting are more probable than non-casualties to encounter hindered social and enthusiastic alteration, poor scholarly accomplishment, poor physical wellbeing, low confidence, tension and depression' [46]. Supporting for law change, New Zealand Judge Neil MacLean said in 2012, 'tormenting by cell phone messaging or via web-based networking media, for example, Facebook is "frequently a foundation factor" in suicides

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

preceding the coroners' [47]. The media makes visit interfaces between digital tormenting and suicide. For instance, in 2012, news from Sydney recounted damaging and tenacious Twitter-tweets to surely understood media identity, Charlotte Dawson, who stood up freely against Cyber harassment before her demise by suicide. A 2016 news thing from New Zealand reports the suicide of 12-year old, Kyana Vergara, a casualty of online networking attacks. Such records may fill in as exhibits of the severe idea of internet tormenting [48].

6.1 Cyber harassment Effects

The internet can provide a myriad of services. It is frequently utilized for business transactions, online information exchange, shopping, learning, voting, teleworking, and of course online gaming. Against this backdrop lies the potential for better communication among people, better efficiencies of scale in commerce and enriched personal lives. However, along with these possibilities comes effect in terms of social, financial and ethical behaviors. While most activities carried out over the internet are innocuous, others could beconsidered questionable not satisfying accepted social and ethical norms. These activities are characterized by user-initiated actions frequently detached from the fear of consequence that might be realized in the physical world. Illegal file-sharing, the possibility of sending spam to millions, and the accessibility of explicit adult-oriented materials are examples of potentially destructive behaviors that can adversely affect millions of users, businesses and organizations for instance cyber harassment (cyber stalking cyber bullying). There is no doubt that the repercussion of cybercrime is a serious global concern. The Kingdom of Saudi Arabia (KSA) is one of the many countries that are suffering from cybercrime, according to the report from the Symantec; KSA is one of the most affected countries in the Middle East. In 2014, 62% of Internet users in Saudi Arabia have faced cybercrimes. Cybercrime is rising across the Saudi society, and protecting against cyber threats is an ongoing management challenge for organizations. The Saudi official report estimated that more than 3.6 million people fell as victims of cybercrime [49] which makes them pay US$0.5 billion a year [50]. Saudi Arabia is in the 16th place of the most countries that suffer from cybercrime in the world [51, 52, 53]. As mentioned earlier, in the introduction of this study the cyber harassment is the type of cyber-crimes' official reports made by Saudi government authorities, specialized in security aspects of information and electronic crimes indicating that there is a sharp rise in the proportion of electronic crimes, especially in the cyber extortion crimes assured that cybercrime is on the rise across Saudi Arabia. The rate has increased by 57% in 2014 compared to 2013, and protecting against cyber threats is an ongoing management challenge for organizations. (Anti-Harassment Center, KSA - [54] [49].

6.2 The effect of Cyber Harassment in Saudi Arabia

There is no doubt that the repercussion of cybercrime is a serious global concern. The Kingdom of Saudi Arabia (KSA) is one of the many countries that are suffering from cybercrime, according to the report from the Symantec; KSA is one of the most affected countries in the Middle East. In 2014, 62% of Internet users in Saudi Arabia have faced cybercrimes. Cybercrime is rising across the Saudi society, and protecting against cyber threats is an ongoing management challenge for organizations. The Saudi official report estimated that more than 3.6 million people fell as victims of cybercrime [49] which makes them pay US$0.5 billion a year [50]. Saudi Arabia is in the 16th place of the most countries that suffer from cybercrime in the world [51][52][53]. As mentioned earlier, in the introduction of this study the cyber harassment is the type of cyber-crimes' official reports made by Saudi government authorities, specialized in security aspects of information and electronic crimes indicating that there is a sharp rise in the proportion of electronic crimes, especially in the cyber extortion crimes assured that cybercrime is on the rise across Saudi Arabia. The rate has increased by 57% in 2014 compared to 2013, and protecting against cyber threats is an ongoing management challenge for organizations. (Anti-Harassment Center, KSA - Annual Report 2014[49]. A serious problem is worthy of investigation due to the lack of a diagnostic study that focuses on the cyber harassment in KSA. It is reported that there is no study deals with the factors influencing the behavior intention to Minimizing cyber harassment among youth and concern with minimizing such types of crimes [55][49][56]. Consequently, there is an urgent need for caring a thorough study to deeply investigate the cyber harassment factors in the Saudi context. Thus, cyber harassment creates some ethical reflections among society such as illegal relationships, pornography, stealing, lying and other ethics among societies [57].

Journal of Theoretical and Applied Information Technology
31st March 2018. Vol.96. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In the social side, cyber harassment leads to disintegration of the family such as divorce of couples and education leakage from school and university. In the economical and the financial sides there are individual and social problems due to this crime (Ajayi 2016; Anti-Harassment Center KSA - Annual Report 2014; Ojanen et al., 2015)[58]. As has been mentioned earlier, Saudi Arabia is one of the most countries, which have been affected by this dilemma, due to its social conservative culture[58, 52]. According to studies conducted in this area, [55][49][57][60], there are several problems facing the Saudi society and government regarding cyber harassment. The official reports stated that Saudi government spends millions of dollars annually to Minimize cyber harassment and cyber bullying as well as cyber stalking among young people [57].

In this regard, several studies affirm that there is a need for conducting further studies on the effect of cyber harassment on university students. For instance, [61] assured that "further research is needed to expand our understanding of cyber harassment at the university level." The authors reported that when one considers the relatively high percentage of respondents (such as in the case of the current study) who told a parent/guardian or other adult about being cyber-harassment, it would be valuable to know if these respondents are considering a nation-wide survey of undergraduate students would provide valuable data. Additionally, another study was conducted at a university in Turkey and found much higher prevalence rates of cyber harassment victimization at 55.3% of university students [62] . [63][64] recommend that "more research utilizing a university sample is necessary to better understand the prevalence rate among this population." On the other hand, Wright 2016) advises that more attention should be given to addressing cyber victimization on undergraduates in an effort to raise awareness of their behaviors. According to the Center Authority for Statistics (CAS), the single age group of the young adults (i.e., undergraduates) constitutes the highest number among the rest groups such as children and individuals over 30 years old.

The population statistic year 2017 reveals that almost six millions young adults, constituting a quarter (5,749,983) of the total population of KSA (20,427,351), are considered to be university or high institutes learners [66]. All the above mentioned studies provide enough reasons for thoroughly investigating the cyber-harassment phenomenon and its effect on young youths in Saudi universities.

7. ANALYSIS AND DISCUSSION

The variety in the commonness of cyber harassment crosswise over Part States mirrors the utilization of web as a specialized device for the two casualties and culprits in distinctive Part States. Demonstrations of cyber harassment are more typical in nations with high rates of web access6. Considering all types of inappropriate behavior (11 things), ladies were made a request to concentrate on the most genuine occurrence that has transpired since the age of 15. It turned out that by and large the culprit of the most genuine occurrence is an obscure individual (42%), trailed by some person from the work setting or some individual the casualty knows (18%). By far most of culprits are men. Sentiments of defenselessness, nervousness and loss of fearlessness are the most well-known mental outcomes experienced by ladies because of the most genuine occurrence of inappropriate behavior. 35% of ladies having encountered a genuine episode of lewd behavior did not discuss it to anybody before the meeting. As a follow up to the aftereffects of the FRA review, Sami Nevala specified 5 key needs:

- Sanction of the Istanbul Tradition.
- Part States should audit ampleness of existing approaches with respect to inappropriate behavior on the web.
- Web and online networking stages should make moves to proactively help casualties of stalking to report manhandle.
- Bosses' associations and exchange unions should additionally advance consciousness of sexual provocation and empower revealing.
- Elevated amounts of inappropriate behavior experienced by ladies in administration must be tended to. See figure 2.

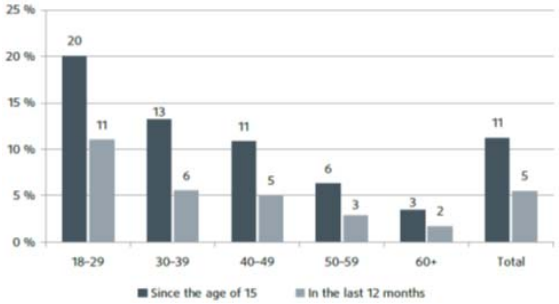

Figure 2: Cyber Harassment By Age Group (%)

The researcher found that Saudi Arabia was positioned first as the most defenseless of the gulf nations to succumb to digital wrongdoings, for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

example, site hacking, as indicated by a measurements report as of late. Cyber laws exist in the Kingdom since the year 2007; be that as it may, its non-mindfulness among youth has made potential lopsidedness between safe web utilization and weakness against wrongdoing. The greater part of the general population thinks about digital wrongdoing however less knows about the related enactment to battle these wrongdoings. The researcher sees that, in KSA it has been clear how PC wrongdoings can influence individuals live. Despite the fact that, the data security is expanded yet additionally the unapproved access for instance were drastically expanded. Knowing the laws of PC violations ought to be viewed as the primary answer for lessen them. Therefore, this should be activated and citizens should be better informed about how to protect themselves from such crimes, and not to be afraid to report them, and to raise awareness about the laws that protect them from such crimes and how to activate them [67]. Web and online networking stages also allowed the public to share information, which can pose an intended or unintended risk for teenagers and young adults. One of the unintended risks is sexing, which creates consequences such as harmed reputations, broken relationships, and shattered friendships. This contrasts with [68, 69] where the social media is used for engagement among students. So, we recommend colleges and universities to encourage student to use social media for educational purpose [70].

7.1 Solutions for fighting Cyber Harassment

The majority of the difficulties that cyber harassment laws right now neglect to address could be tended to by holding ISPs obligated for their endorsers' hassling remarks. Since digital provocation has such huge numbers of similitudes with copyright law, the Computerized Thousand years Copyright Act should function as a model to force risk on ISPs. The fundamental weakness of cyber harassment law is its powerlessness to expel irritating material from the web once it is distinguished. Since this is the greatest concern, this authoritative proposition will have that true objective in mind. In this proposition an ISP will be obligated for the defamatory and badgering remarks made by its supporters unless the, endless supply of guaranteed badgering or maligning, reacts speedily to expel, or impair access to, the material that is guaranteed to be badgering similarly as under the DMCA, an ISP must have an assigned operator to get protestations and must evacuate the culpable material upon dissension. At that point the ISP must send a notice to the endorser that his material has been evacuated and permit the endorser of request it. In the event that the supporter offers it, the ISP must advise the complainant furthermore, the complainant would then be able to document suit against the engaging supporter of decide whether the material meets the components of cyber harassment or slander. In the event that the endorser records a claim with the ISP and the complainant does not document suit against the endorser, at that point the supporter's material will be returned up on the ISP's servers. In the event that the endorser does not offer the objection, at that point the material will stay expelled from the ISP's servers [71]. Furthermore, the ISP must find a way to have the capacity to learn the character of any of its endorsers who take part in criticism or badgering [72]. Despite the fact that the expression "sensible" is an ambiguous term, the courts have involvement in applying a sensible standard and will experience little difficulty applying it to an ISP risk context.140 In this unique situation, sensible will be what is mechanically accessible to ISPs and not excessively troublesome. The sensibility of a few stages to recognize endorsers might be distinctive for a little ISP and an extensive ISP on account of the assets accessible to each. This some portion of the proposition should be analyzed by judges and a gauge of least prerequisites will be set up. Two cases of stages an ISP can take to distinguish their endorsers is spare the Web Convention (IP) address history of their supporters and expect endorsers of sign in before they can post anything on the site [73]. The IP address can be utilized to recognize who is getting to a specific webpage.141 If ISPs were required to spare its endorsers' IP address history, casualties of cyber harassment could subpoena that data to endeavor to recognize the harasser. Likewise, requiring a man to sign in some time recently making remarks on a site page would specifically connect a man's personality to their remarks. Both of these recommendations are sensible in light of the fact that some ISPs as of now keep IP address history142 and a few pages as of now have the alternative to just remark on the off chance that you are signed in Likewise, the ISP must find a way to anticipate endorsers who constantly malign or annoy from proceeded with access to their site. There is no particular methodology that an ISP must take after to fulfill this necessity [45].

8. CONCLUSION AND FUTURE STUDIES

Cyber harassment is a genuine wrongdoing with intense, certifiable impacts on the casualties.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Casualties feel terrified, humiliated, and it can demolish their online notoriety. Many states have straightforwardly tended to Cyber harassment in statutes; be that as it may, genuine alleviation for the casualties is inconceivable since ISPs have finish insusceptibility from obligation for their endorser's cyber harassment. Casualties can't expel the annoying or slandering material from the web, along these lines proceeding with the hurt the casualties endure well after the underlying badgering has finished. We recommend future studies extend studies in this field wherein all factors are included to commensurate with different educational environments around the world.

9. ACKNOWLEDGMENTS

We would like to thank Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia by giving the authors an opportunity to conduct this research. This research is funded by Universiti Kebangsaan Malaysia under Exploratory Research Grant Scheme ERGS/1/2013/ICT07/UKM/02/1.

REFERENCES:

[1] U. K. Legislation, 'Protection from Harassment Act 1997', 1997.

[2] K. Baum, S. Catalano, M. Rand, and K. Rose, "Stalking Victimization in the United States," 2009.

[3] W. M. Al-Rahmi, N. Alias, M. S. Othman, I. A. Ahmed, A. M. Zeki, and A. A. Saged, "Social media use, collaborative learning and students' academic performance: a systematic literature review of theoretical models," Journal of Theoretical & Applied Information Technology, vol. 95, no. 20, pp. 5399-5414, 2017.

[4] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "The effect of social media on researchers' academic performance through collaborative learning in Malaysian higher education," Mediterranean Journal of Social Sciences, vol. 6 no. (4), pp. 193-203, 2015. http://doi:10.5901/mjss.2015.v6n4s1p193

[5] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Social media for collaborative learning and engagement: Adoption framework in higher education institutions in Malaysia," Mediterranean Journal of Social Sciences, vol. 6 no. 3S1, pp. 246-252, 2015. http://doi:10.5901/mjss.2015.v6n3s1p246

[6] J. D. Uptoti, 'COMBATING CYBER-VICTIMIZATION', 2011.

[7] G. Mccallion and J. Feder, 'Student Bullying : Overview of Research, Federal Initiatives, and Legal Issues', 2013.

[8] D. Cross, 'Australian covert bullying prevalence study', no. May, 2009.

[9] F. Lives, 'What is cyber bullying?', 2013. .

[10] C. M. Kahn and J. M. Liñares-Zegarra, 'Identity theft and consumer payment choice: Does security really matter?', J. Financ. Serv. Res., vol. 50, no. 1, pp. 121–159, 2016.

[11] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Exploring the factors that affect student satisfaction through using e-learning in Malaysian higher education institutions," Mediterranean Journal of Social Sciences, vol. 6, no. 4, 299, 2015.

[12] W. M. Al-Rahmi and A. M. Zeki, "A model of using social media for collaborative learning to enhance learners' performance on learning," Journal of King Saud University - Computer and Information Sciences, vol. 29, no. 4, pp. 526–535, Oct. 2017. http://dx.doi.org/10.1016/j.jksuci.2016.09.002

[13] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "The Role of Social Media for Collaborative Learning to Improve Academic Performance of Students and Researchers in Malaysian Higher Education," The International Review of Research in Open and Distributed Learning, vol. 16, no. 4, Nov. 2015.

[14] O. Phillips, 'Blackmail in zimbabwe: Troubling narratives of sexuality and human rights', Int. J. Colorectal Dis., vol. 29, no. 11, pp. 345–364, 2014.

[15] H. Erkol, M. R. Gökdoğan, Z. Erkol, and B. Boz, 'Aggression and violence towards health care providers - A problem in Turkey?', J. Forensic Leg. Med., vol. 14, no. 7, pp. 423–428, 2007.

[16] M. Rafati Rahimzadeh, A. Zabihi, and S. J. Hosseini, 'Verbal and physical violence on nurses in hospitals of Babol University of Medical Sciences', J. hayat, vol. 17, no. 2, pp. 5–11, 2011.

[17] H. R. Koohestani, N. Baghcheghi, K. Rezaei, A. Abedi, A. Seraji, and S. Zand, 'Occupational violence in nursing students in arak, iran', Iran. J. Epidemiol., vol. 7, no. 2, pp. 44–50, 2011.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[18] R. F. AbuAlRub and A. H. Al-Asmar, 'Psychological violence in the workplace among Jordanian hospital nurses', J. Transcult. Nurs., vol. 25, no. 1, pp. 6–14, 2014.

[19] A. H. Fallahi Khoshknab M, Oskouie F, Najafi F, Ghazanfari N, Tamizi Z, 'Psychological Violence in the Health Care Settings in Iran: A Cross-Sectional Study', Nurs Midwifery Stud, vol. 4, no. 1, pp. 1–6, 2015.

[20] G. S. Smith, M. A. Minor, and H. M. Brashen, 'Cyberbullying in Higher Education: Implications and Solutions', J. Educ. Res. Pract., vol. 4, no. 1, pp. 50–60, 2014.

[21] I. Vasiu and L. Vasiu, 'Cyberstalking Nature and Response Recommendations', Acad. J. Interdiscip. Stud., vol. 2, no. 9, pp. 229–234, Oct. 2013.

[22] G. S. Online, 'Cyberstalking', 2013. .

[23] M. Pittaro, 'Cyber Stalking'. pp. 277–297, 22-Feb-2011.

[24] Jenifer, 'DIGITAL-STALKING', 2014. .

[25] M. Uma and G. Padmavathi, 'A Survey on Various Cyber Attacks and their Classification', vol. 15, no. 6, pp. 391–397, 2013.

[26] K. Sissing, 'A criminological exploration of cyber stalking in South Africa', no. June, 2014.

[27] L. Lamberg, P. Mullen, and M. Pathe, 'Stalking disrupts lives , perpetrators are often mentally ill', Am. Med. Assoc., vol. 286, no. 5, pp. 1–6, 2001.

[28] P. E. Mullen, M. Pathé, and R. Purcell, Stalkers and Their Victims, Second Edi. Cambridge University Press, 2008.

[29] MONICA ANDERSON, 'Key takeaways on how Americans view – and experience – online harassment'. [Online]. Available: http://www.pewresearch.org/fact-tank/2017/07/11/key-takeaways-online-harassment/. [Accessed: 15-Mar-2018].

[30] M. Chester, Kayleigh L, Callaghan, Mary, Cosma, Alina, Donnelly, Peter, Craig, Wendy, Walsh, Sophie, Molcho, 'Cross-national time trends in bullying victimization in 33 countries among children aged 11, 13 and 15 from 2002 to 2010', Eur. J. Public Health, vol. 25, no. Oxford University Press, pp. 61–64, 2015.

[31] G. Corcoran, Lucie, Guckin, Conor Mc , Prentice, 'Cyberbullying or cyber aggression?: A review of existing definitions of cyber-based peer-to-peer aggression', Societies, vol. 5, no. Multidisciplinary Digital Publishing Institute, pp. 245–255, 2015.

[32] I.-P. Union, 'Sexism, Harassment, and Violence against Women Parliamentarians', Issues Brief, Oct., 2016.

[33] N. A. Komsan, 'Sexual Harassment in the Arab Region : Cultural Challenges and Legal Gaps', Egypt. Cent. Women's Rights Address, no. December, pp. 13–14, 2009.

[34] B. H. Spitzberg and G. Hoobler, 'Cyberstalking and the technologies of interpersonal terrorism', New Media Soc., vol. 4, no. 1, pp. 71–92, 2002.

[35] R. Moore, Cybercrime: Investigating high-technology computer crime. 2010.

[36] K. Dashora and P. P. Patel, 'Cyber Crime in the Society: Problems and Preventions', J. Altern. Perspect. Soc. Sci., vol. 3, no. 1, pp. 240–259, 2011.

[37] Poulomi Banarjee, 'Nasik Police play big boss for internet voyeurs', Hindustan Times, 2007.

[38] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "The effectiveness of using e-learning in Malaysian higher education: A case study Universiti Teknologi Malaysia," Mediterranean Journal of Social Sciences, vol. 6, no. 5, pp. 625- 637, 2015. https://doi.org/10.5901/mjss.2015.v6n5s2p625

[39] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Effect of Engagement and Collaborative Learning on Satisfaction Through the use of Social Media on Malaysian Higher Education. Research Journal of Applied Sciences, Engineering and Technology, vol. 9, no. 12, pp. 1132-1142, 2015.

[40] A. Brunstein Klomek, F. Marrocco, M. Kleinman, I. S. Schonfeld, and M. S. Gould, 'Bullying, depression, and suicidality in adolescents', J. Am. Acad. Child Adolesc. Psychiatry, vol. 46, no. 1, pp. 40–49, 2007.

[41] R. S. Lazarus, 'Folkman. S.(1984). Stress, appraisal, and coping', New York pringer, 1986.

[42] J. A. Mora-Merchan, R. Del Rey, and T. Jäger, 'Cyberbullying: Review of an emergent issue', JA Mora-Merchán T. Jäger Cyberbullying a cross-national Comp. Verlag Empirisische Pädagogik, Landau, 2010.

[43] T. M. Group, 'The Global Diffusion of the Internet Project – The Internet in the Kingdom of Saudi Arabia'. 1999.

[44] S. T. Company, 'Consolidated Financial Statements for the Year ended'. 2017.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[45] [45] H. A. Alshahrani, 'A Brief History of the Internet in Saudi Arabia', TechTrends, vol. 60, no. 1, pp. 19–20, Jan. 2016.

[46] H. Khashan, 'Saudi Arabia's Flawed "Vision 2030&quot';, Middle East Q., Jan. 2017.

[47] L. Panetta, 'Remarks on Cybersecurity to the Business Executives for National Security', Speech given Oct., vol. 11, pp. 1947–1952, 2012.

[48] M. O?Moore and C. Kirkham, 'Self-esteem and its relationship to bullying behaviour', Aggress. Behav., vol. 27, no. 4, pp. 269–283, Jul. 2001.

[49] B. Mohamed and E. Elnaim, 'Cyber Crime in Kingdom of Saudi Arabia : The Threat Today and the Expected Future', Inf. Knowl. Manag, vol. 3, no. 12, pp. 14–19, 2013.

[50] A. Horbury, 'cybercrime-takes-its-toll @ www.symantec.com', symantec, 2013. [Online]. Available: https://www.symantec.com/connect/blogs/cybercrime-takes-its-toll.

[51] A. Alarifi, H. Tootell, and P. Hyland, 'A study of information security awareness and practices in Saudi Arabia', 2nd Int. Conf. Commun. Inf. Technol. Digit. Inf. Manag., pp. 6–12, 2012.

[52] A. AlKaabi, 'Strategic framework to minimise information security risks in the UAE', University of Bedfordshire, 2014.

[53] K. Almarhabi, 'Adherence to ICT Security and Privacy Policies in Saudi Arabia', vol. 147, no. 4, pp. 13–18, 2016.

[54] FBI, '2014 Internet Crime Report', Internet Crime Complain. Cent., pp. 1–48, 2014.

[55] A. Obaid and S. Alkaabi, 'Combating Computer Crime : An International Perspective', no. October, 2010.

[56] T. H. E. Yearfigures et al., 'KASPERSKY SECURITY BULLETIN 2014', 2014.

[57] Aboubekeur Cherif and Abdulnaser Rachid, 'overview of data mining concepts and algorithms with national security applications contents', in overview of data mining concepts and algorithms with national security applications Contents, 2009.

[58] E. F. G. Ajayi, 'The impact of cybercrimes on global trade and commerce', SSRN, no. Part 1, pp. 1–25, 2016.

[59] T. T. Ojanen, P. Boonmongkon, R. Samakkeekarom, N. Samoh, M. Cholratana, and T. E. Guadamuz, 'Connections between online harassment and offline violence among youth in Central Thailand', Child Abuse Negl., vol. 44, pp. 159–169, 2015.

[60] A. Shultz et al., 'Cholera Outbreak in Kenyan Refugee Camp: Risk Factors for Illness and Importance of Sanitation', Am J Trop Med Hyg, vol. 80, no. 4, pp. 640–645, Apr. 2009.

[61] B. C. M. Walker, B. R. Sockman, and S. Koehn, 'An Exploratory Study of Cyberbullying with Undergraduate University Students', TechTrends, vol. 55, no. 2, pp. 31–38, Feb. 2011.

[62] B. Dilmaç, 'Psychological needs as a predictor of cyber bullying: A preliminary report on college students', Kuram ve Uygulamada Egit. Bilim., vol. 9, no. 3, pp. 1307–1325, 2009.

[63] A. M. Schenk, W. J. Fremouw, and C. M. Keelan, 'Characteristics of college cyberbullies', Comput. Human Behav., vol. 29, no. 6, pp. 2320–2327, 2013.

[64] A. M. Schenk, C. Cooper-Lehki, C. M. Keelan, and W. J. Fremouw, 'Underreporting of Bestiality Among Juvenile Sex Offenders: Polygraph Versus Self-Report', J. Forensic Sci., vol. 59, no. 2, pp. 540–542, 2014.

[65] M. F. Wright, 'Cyber victimization on college campuses: Longitudinal associations with suicidal ideation, depression, and anxiety', Crim. Justice Rev., vol. 41, no. 2, pp. 190–203, 2016.

[66] 'Population Estimates | General Authority for Statistics', 2017. [Online]. Available: https://www.stats.gov.sa/en/43. [Accessed: 01-Apr-2017].

[67] F. A. Moafa, 'Classifications of Cybercrimes-Based Legislations : A Comparative Research between the UK and KSA', Int. J. Adv. Comput. Res., no. 2, p. 7970, 2014.

[68] W. M. Al-Rahmi, M. S. Othman, and L. M. Yusuf, "Using Social Media for Research: The Role of Interactivity, Collaborative Learning, and Engagement on the Performance of Students in Malaysian Post-Secondary Institutes. Mediterranean Journal of Social Sciences, vol. 6, no. 5, pp.536-546, 2015. http://dx.doi.org/10.5901/mjss.2015.v6n5s2p536

[69] W. M. Al-Rahmi, M. S. Othman, and M. Musa, "The Improvement of Students' Academic Performance by Using Social Media through Collaborative Learning in Malaysian Higher Education," Asian Social Science, vol. 10, no. 8, 2014.. Doi: http://dx.doi.org/10.5539/ass.v10n8p210

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[70] W. M. Al-Rahmi, A. M. Zeki, N. Alias, and A. A. Saged, "Use of social media and its impact on academic performance among university students in Malaysian Higher Education," Anthropologist, vol. 28, no. 1-2, pp. 52-68, 2017. http://dx.doi.org/10.1080/09720073.2017.1317962

[71] M. Abu-Fatim, 'Official on Introduction of Internet Into Kingdom'. Al-Riyadh, 1997.

[72] 'Security Firm: Cyberattacks Against Saudi Arabia Continue | Technology News | US News'. [Online]. Available: https://www.usnews.com/news/technology/articles/2017-04-26/security-firm-cyberattacks-against-saudi-arabia-continue. [Accessed: 09-Feb-2018].

[73] Freedom House, 'Freedom on the Net 2016: Silencing the messenger - Communication apps under pressure', Freedom House, 2016. [Online]. Available: https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf.

[74] F. A. Moafa, K. Ahmed, W. M. Al-Rahmi, N. Alias, M. A. Obaid "Factors for Minimizing Cyber Harassment Among University Students: Case Study In Kingdom Of Saudi Arabia (KSA)," Journal of Theoretical & Applied Information Technology, vol. 96, no. 6, 2018.

[75] M. Tan and T. S. H. Teo, "Factors Influencing the Adoption of Internet Banking," J. Assoc. Inf. Syst., vol. 1, no. 1, pp. 1–44, 2000.