FACTORS FOR MINIMIZING CYBER HARASSMENT AMONG UNIVERSITY STUDENTS: CASE STUDY IN KINGDOM OF SAUDI ARABIA (KSA)

[1]FAHAD ABDULLAH MOAFA, [1]KAMSURIAH AHMAD, [2]WALEED MUGAHED AL-RAHMI, [2]NORMA ALIAS, [3]MAHMOOD ALI MOQBEL OBAID

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

[2]Ibnu Sina Institute for Scientific &Industrial Research (ISI-SIR), Faculty of Science, Universiti Teknologi Malaysia, 81310, UTM Skudai, Johor, Malaysia

[3]Faculty of Computer Science and Engineering, Hodeidah University, Al- Hodeidah, Yemen

E-mail: [1]fah171393@hotmail.com, [1]kamsuriah@ukm.edu.my [2]waleed.alrahmi@yahoo.com, [2]norma@ibnusina.utm.my, [3]eng_mahkah192@yahoo.com

ABSTRACT

This study 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. In this research were employed two theories the first Theory of Planned Behavior (TPB), the second selected Technology Acceptance Model TAM. However, based on TPB, the researcher has identified eight factors, to minimize cyber harassment, which is: technological support, attitude, subjective norms, social pressure, the influence of the mass media, perceived behavioral control, regulatory support and the role of the government, and security awareness. 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: *Factors, Cyber Harassment, Behavioural Intention, Saudi Arabia (KSA)*

1. INTRODUCTION

In the Information and Communication Technology (ICT), emergence utilization of computer technology [1][2], cybercrimes and computer base offences, has become a significant challenge worldwide[3]. Cybercrime refers to the crime conducted using computer networks or devices at any phase [4]. 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 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 [5][6]. Cybercrimes is defined as crimes committed with the aid of a computer[7][8]. They further divided these crimes into four categories. Firstly, crimes where computers or networks are the target of a crime, such as the denial of service attacks. Secondly, crimes where computers are used as instruments to commit crimes, such as fraud and cyber harassment. Thirdly, crimes where computers are incidental to the crimes, which happen with or without the use of computers, such as money laundering. The fourth and last category covers crimes due to the prevalence of computers. Examples of these cybercrimes include intellectual property violations, counterfeiting, and identity theft[8]. Cyber harassment (CH) is part of cybercrimes. It involves an action conducted by groups of persons, or individuals, using digital means to cause harm. It is capable of causing emotional distress to other persons. Cyber-stalking goes beyond the annoyance caused by un-solicited e-mails to include CH activities used to harass or stalk another person through email and telecommunication device utilizing internet medium [9][10] .Like many other countries around the world, including USA [7], European countries, such as Portugal and Saudi Arabia are suffering from the phenomenon of CH [11]. In Saudi Arabia (KSA), for instance, one of the reasons why young people are afraid to combat CH is because the Saudi society is a conservative Muslim society. Saudi is seeking to preserve its customs and traditions, and fearful of hacking issues[12]. The Saudis are at risk of cyber harassment, as it is an issue confounded by the minimal knowledge of how to minimize the risk. Therefore, to reduce the young people attraction to cyber offences in the KSA, the influential factors that motivate them, need to be identified [14]. It is noted that the self-efficacy in IT and ICT is highly risky due to the lack of awareness in combating cybercrimes in the KSA. The purpose of this article is to investigate the factors influencing anti-cyber harassment in Saudi Arabia. To do so, this study will employ the DTPB model which was developed by Taylor and Todd (1995).The Decomposed Theory of Planned Behavior (DTPB), takes into account attitudinal, social, and control factors to explain technology usage. Indeed, this model can be extended to help account for the factors influencing compacting anti-cyber harassment in the KSA by Saudi youths. This could be the first attempt of doing so in the KSA [66]. 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 [61].

2. CYBER HARRASMENT

It was argued by [15] that any crime conducted involving computer based technology, or trace of possibility that computer was utilized significantly in the conduct of the offence, is regarded as a cybercrime . According to[16], CH acts are those activities that typically harass, annoy, terrify, offend or threat a person, through e-mail, social media chat or other forms intended to harm the person involves. Furthermore, reviews, conducted by [3] 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 CH. This study concentrated on three aspects of CH: cyber-stalking, cyberbullying, and minimizing harassment.

2.1 Cyber-stalking

The increasing use of the cyberspace by 'criminals' prompted a rush of legislation and other interest. however, in spite the number of high-profile cases appearing in print media and other means of communications as the Internet, the topic has yet to get appropriate systematic analysis against a proper theoretical framework that must include a combination of an understanding of Internet crime, an understanding of the psychological phenomenon of stalking. However, certain people argue that our rights such as of privacy are "socially constructed," meaning that they, over time, change under the influence of human forces such as culture, law and technology. For this reason, Saudi Arabian government, in 2007 introduced the anticrime act. For example, the penalty for Hacking, Net Extortion, and Website Defacement is SR 5,00,00 or 1 Year or both in jail[67]. Cyber-stalking is synonymous to the stalking conducted offline, in which the intent of the perpetuators was to forcefully influence their victims, willy-nilly[18]. Cyber-stalking can take different forms, including threatening e-mails, spamming the victim, and harassing through live chats [19]. The main distinction between cyber harassment (CH) and cyberstalking lies in the duration of their occurrence. To explain, CH may occur just once, and for a limited period of time. However, in the case of cyberstalking (loving), the harassment can continue for a longer time and may last for weeks, months or even years [20].

2.2 Cyber bullying

Cyber bullying is different from cyberstalking in that it usually occurs between minors, and it takes on a subtler quality [21]. The forms of cyberbullying include harassment through instant or text messaging, password stealing, and digital pictures. However, other forms of cyberbullying are less intense with no involvement of incriminating acts, while some forms of the bullying are indeed risky and severe, subjecting the victims to real danger. For instance, a proxy cyberbullying is that in which the victim was impersonated, by which the perpetuators used the victim profile to conduct prohibited act like posting into a paedophile domain. In a study by [22] who identified four types of cyberbullying: i) Angels of vengeance, ii) Revengeful nerds, iii) Miserable girls and iv) Careless cyberbully. Cyberbullying and cyber-stalking will likely become bigger problems as technology continues to advance. Law enforcement agencies are advised to be diligent, proactive, and innovative in their response.

2.3 Minimizing Cyber Harassment

The main theme of this study was minimizing harassment. Due to the social and psychological effects of harassment, it was necessary to find the minimizing methods used by victims. Moreover, [22]. have identified three major sources of harassment, which are; i) Parents and Care-custodians; ii) Peers (age group) and; iii) others. In a study reported by Kathleen et al. (2016) [23], majority of the respondents said they are not communicating with their parents or care custodians. This is due to a form of harassment suffered from them, with some victims citing electronic harassment, despite the consolidated roles performed in nurturing children and their development by parents, guardians and other caregivers. Some of the respondents went ahead to expressed a kind of overreaction shown to them by their care custodians in form of mobile phones confiscation or banned from using internet[23].Among the theories supporting reduction in cyber harassment is Decomposed Theory of Planned Behaviour (DTPB), originated from two theories, thus; Theory of Reasoned Action (TRA) and Theory of Planned Behaviour (TPB). The TPB theory was developed by [20] who took a step further to decompose behavioural, attitudinal and normative believe manipulation. The theory suggests that attitude, perception, norms and subjective behavioural management, will discourage the motivational intent to use technology. DTPB model denotes ideal comprehension of the connection between intent and behaviour, provides researchers with accurate factors that explains at best the determination to absorb innovation by breaking the beliefs structures. Additionally, it was discovered that the model is capable of recognising specific noticeable beliefs that inhibit IT utilization, and also, it has upper predictive ability in comparison to the traditional TRA, TPB and TAM [20].

3. CYBER HARASSMENT KINGDOM OF SAUDI ARABIA (KSA)

Cyber Crime Law showed that the aim of this Law is to combat cybercrimes by identifying the crimes and determining their punishments to ensure: the Enhancement of information security, the Protection of public Interest, morals, and common values, the Protection of rights pertaining to the legitimate use of computers and information networks and the Protection of national economy. This law was enacted and approved in the year 2012 [69].

3.1 Cybercrimes statistics in KSA

Nearly 3.6 million people were estimated to be victims of cybercrimes in the KSA with 12 calendar months, losing in a direct finance, approximately on the average of one hundred and ninety five US dollars [70]. Moreover, in approximation on daily basis, an average of 18 people fell victims of cybercrime in the KSA, resulting to over 1,500,000 victims globally. In terms of monetary loses, an estimated one hundred and ninety seven US dollars per victim occurs across the globe; the lost equal the cost of a week's nutritional food need of a family of four members. In addition, the KSA, only 20% of those exposed to cybercrime have sufficient technical awareness or technical support. In a survey of 1,000 people in the KSA to test the security of consumer electronic crime, Consumers lost nearly a day to fix the fallout from crime on the Internet [78]. In the report showed that, it also costs approximately SR 3,230 a person, ending up the provider losing more than 21 billion SAR in total [71]. Moreover , cybercrimes cost the KSA SR 2.8 billion annually, which means that there are 1.5 million victims each day around the world exposed to cyber crimes [79]. Also, In KSA, only 20% of those exposed to cybercrime have sufficient technical awareness or technical support. Accordingly, major problems in Saudi Arabia are the need to educate people about cybercrime and to push the state to tackle it. indeed, more effort is required to raise awareness, and to show the weakness of the measures to tackle security breaches in Saudi society [Almadinah, 2015. Electronic crimes cost the Saudi 2.8 billion SAR annually [71]. According to a report issued by Casper Spybot company in mid-2011, Saudi Arabia is within the high-risk group according to their risk of exposure to and 1.33% for each of (GCC) states. Thus, Saudi Arabia is the highest in being exposed to Internet crime in the GCC states. Additional, a study of cybercrime in the KSA showed that 14.2% of Saudi websites have been infiltrated, while only 8.9% for non-Saudi sites. Moreover, it was shown that 15.1% of Saudi Internet users mail have been targeted: 11.8% Saudis and 3.3% foreigners. Bearing in mind that from 11 million Internet Saudi users one million people have been targeted which reflects the how troubled Kingdom is with regards to cybercrime [71]. Oother statistics produced by the Saudi Interpol showed:

1. E-mail breaches were with 27%,
2. Financial breaches 12%,
3. Child sexual exploitation cases with 14%,
4. Electronic deception and fraud 5%.
5. Libel and defamation 13%,
6. Malicious programs 6%,
7. Terrorist threats across sites with 4% [82]

Nonetheless in spite of these hacks, complaints of suspicious contacts did not exceed 1%, Asaf said that the society's awareness of the system of combating cyber-crime helped to raise this type of issue in the indicators of the Ministry of Justice, stressing that this is healthy for the society to reduce the number of crimes. However, according to him, the region of Makkah topped the list of the 13 regions of the Kingdom, in terms of filing cases to courts with a total of cases in the area of Mecca 207 cases related to cybercrimes. In fact, the eastern region was at the top of the list during the last two years 1435, and 1436. Anyway, the courts in the Najran region have not received any cases related to cyber-crimes during the past two years. However, this year, 15 cases were witnessed. The courts of the Tabuk region received cases of electronic crimes for the first time during the past year with four cases. No cases of the same kind were received during 1435 [85]. Furthermore, 776 cases of cybercrimes were addressed by the KSA courts in 2016 in ten months. This was higher in 2016 than the preceding two years, where there were 164 cases in the Kingdom in the year 2015, and 573 cases in the year 2016 [80]. However, the rise in cases reflects the community’s awareness, the effectiveness of the information from the Ministry of Justice and the Ministry of Interior [71]. See table 1.

Table1: Comparison of study in Saudi Arabia and other countries

No	Study in Saudi Arabia (KSA)	Other countries
1	Nearly 3.6 million people were estimated to be victims of cybercrimes in the KSA with 12 calendar months, losing in a direct finance, approximately on the average of one hundred and ninety five US dollars [70].	Approximately on the average of one hundred and ninety five US dollars [70].
2	In Saudi Arabia (KSA), for instance, one of the reasons why young people are afraid to combat CH is because the Saudi society is a conservative Muslim society. Saudi is seeking to preserve its customs and traditions, and fearful of hacking issues[12].	Cyber-stalking goes beyond the annoyance caused by un-solicited e-mails to include CH activities used to harass or stalk another person through email and telecommunication device utilizing internet medium [9][10] .Like many other countries around the world, including USA [7],
3	Reduce the young people attraction to cyber offences in the KSA, the influential factors that motivate them, need to be identified [14].	European countries, such as Portugal and Saudi Arabia are suffering from the phenomenon of CH [11].

3.2 Ethical, social and financial influence of cyber harassment on Saudi Community

Cyber harassment influences the Saudi community's ethical, social and financial aspects. Firstly, cyber harassment creates some ethical reflections among society such as illegal relationships, pornography, stealing, lying and other ethical effects in societies [24]. Secondly, on the social side, cyber harassment leads to the disintegration of the family such as the divorce of couples and education leakage from schools and universities. Finally, on the economical and the financial sides, these crimes give rise to individual and social problems [3]. As mentioned earlier, Saudi Arabia is one of the countries that has been most affected by this dilemma due to its socially conservative culture [26]. Furthermore, if students and researchers have a positive attitude and intention to use social media for educational purposes (i.e. have high levels of interactivity and perceived usefulness), this will have positive effects on their academic performance [13, 17, 25].

4. STUDY DESIGN

The aim of this paper is to explore and account for factors influencing the behavioural intention towards CH among citizen in the KSA, and to investigate possible solutions to minimise their influences. However, even though previous studies focused on several theories for explaining the influence of the usage or the adoption of technology such as TAM, DOI, TRA, UTAUT and TPB, our study concentrates on the DTPB as an integrated model to minimize the behavioural intention towards cyber harassment (MBICH). This is due to the fact that this model takes into account attitudinal, social, and control factors to explain technology usage. [66] In addition, this study tried to identify factors that can be used as guidance to stakeholders and academics in minimizing the behavioural intention towards cyber harassment (MBICH) which are, namely: technological support, attitudes, subjective norms, social pressure, the influence of the mass media, perceived behavioural control, regulatory support, the role of the government, and security awareness, that have an influence on the intention to engage in cyber harassment among Saudi youths.

4.1 Reason for adopting DTPB

This study has adopted and employed DTPB framework due to the following reason:

1. Its completeness in providing ways of understanding individuals, perceived behaviour and attitudes, norms and behavioural manipulations [27].
2. Various studies demonstrate predictive ability of DTPB based on its constituent's multidimensionality [27] [30].
3. It is recommended by Taylor and Todd and among researchers when investigating perceptions of intention [31].
4. Other models such as TAM theories have neglected see figure 1. social, attitudinal, and control factors to explain technology usage [64, 65, 66].

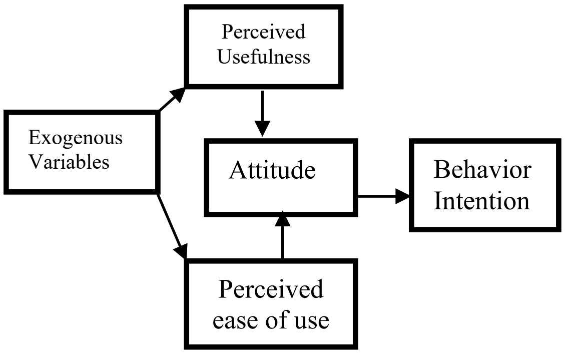

Figure 1: Technology Acceptance Model TAM

According to this model, attitudes, subjective norms, and perceived behavioral control are the constructs elements that help to understand the reasons or factors explaining individual actions, even if the intention is considered as the best indicator of behavior (Herrero Crespo & Rodríguez delBosque, 2008). However, from the proposed model we were able to identify the following significant factors see section 5.

Although, TPB introduced one variable, perceived behavior control, as an answer to all uncontrollable elements of behavior, the beliefs behind the perceived behavior control were aggregated to create a measure for it. This aggregation has been criticized for not identifying specific factors that might predict behavior and for the biases it may create. Furthermore, Taylor and Todd (1995) suggest that TPB model still requires individuals to be motivated to perform ascertain behavior.

5. FACTORS FOR MINIMIZING THE CYBER HARASSMENT

5.1 Technological Support

According to previous studies, technological support positively affects the flexibility of technology and Internet services. This was supported by [30], who observed that the connection between technological aid and perceived attitudinal control is vital and affirmative for a number of students at government institutions in Malaysia depending on the availability of the technological assistance, which determine the adoption of online education services by those students. In the KSA, only 20% of those exposed to cybercrime have sufficient technical awareness or technical support. Accordingly, major problems in Saudi Arabia are the need to educate people about cybercrime and to push the state to tackle it. Indeed, more effort is required to raise awareness, and to show the weakness of the measures to tackle security breaches in Saudi society [71] [76].

5.2 Attitude

Attitude towards using technology is defined as the overall affective reaction of an individual to using a system [72]. In fact it appeared that attitude can affect behaviour directly, and is a more accurate predictor of behaviour than behavioural intention [31]. However, Al Amro pointed out that cybercriminals are personally highly motivated in the KSA by achieving wealth and some other benefit through:
Revenge which is considered a harmful and dangerous motivation for cybercrime. demonstrating technical capabilities to show ability to carry out piracy, entertainment with no particular motives or goals.
political motivation targeting government sites, or to express different political opinions [71]
These all can be linked to risk, trust and awareness and must be considered as of the most attitudinal intention to be concerned about towards minimizing cyber harassment in the KSA. In this regard, for example the infrastructure of the KSA post does not reach to e-Commerce standards, and this is because of the no Adequate security specially in the delivery process Which clearly leads to a losing confidence [74]. In fact, several researchers have suggested that high levels of perceived risks are considered to be a barrier that prevents the adoption of innovation [32]. In addition, [33] opined that the risk factor compose of a number of measures that affect the victim's attitudes, as well as behavioural and social viewpoint, in addition to the time wasted. Additionally, a lot of previous studies looked at the influence of the potential risk factor affecting individual's behaviour towards the acceptance of a new technology. The outcome of the study found that the potential risk had a significant pessimistic influence on the behaviour of students in handling cyber harassment. According to the literature, this construct is considered to be significantly relevant to this study because an important characteristic of cyber harassment is privacy. Hence, observing others in order to minimize cyber harassment may prove to be difficult unless one makes a conscious effort to do so. On the other hand, several previous studies tackled the importance of the concept of trust in the adoption of new technological services. For example, [34]pointed out that the trust factor is one of the most significant factors influencing the attitude of potential Internet users towards the use of e-legal services in Hong Kong. One more researcher [32] have shown that reliability has an important and positive influence on the attitude towards the adoption of Internet banking. Another study discussed the trust factor and its influence on the attitude of graduate students in the USA and Australia [35].Thereafter, trust is a major issues in several social activities involving uncertainty and reliability [37]. Moreover, it is cardinal to any economic processes, whether carried out in a retail outlet in the real offline sequence or online. The acceptance or rejection of emerging technological innovation begin with the person awareness of the technology [20]. So many researchers have shown that awareness/knowledge of emerging technology is among the important factors encouraging the acceptance of new product. For instance, Christa (2006) recommends that consumers must be informed with new brands before they actually adopt them. In addition, a number of studies have discussed the issue of the awareness of new technological services. These studies focused on the importance of this factor and its influence on the attitude towards the adoption of new technology [20]. For instance, [38] tackled the role of awareness with regard to the influence it has upon the actual usage when it comes to e-banking in Australia [38]. However, according to Besbes and Legohérel, Muslims, in the KSA, in this regard, tend to adhere to Islamic teachings which instil fear and trust of God. Therefore, there would be nothing left to fear instil in them but the awareness of law and potential imbalance between Internet Usage & Awareness program in Kingdom[66] Khan claimed that crimes in the KSA are more likely to be more avoided due to Islamic law and fear of God. Indeed, he assured how crucial this could be as technology in cyber world is considered a challenge to all of us as it is capable of leaving no trace or evidence to cyber-crime [67].

5.3 Subjective Norms

Subjective norms means an individual's understanding of social negativism to accept innovation or not. Social influences determine individuals conformation to expectations of others [39]. This study identified two social factors, namely, social pressure and the influence of the mass media. Many behavioural researchers consider social pressure, such as from the family, as one of the subjective behavioural norms that have an influence on an individual's behaviour [40]. While other researchers consider the use of social media have a positive impact on collaboration and engagement among students [28, 29, 36].

With regard to the behaviour of clients towards IT usage, especially towards the adoption of new technological services, two previous studies confirmed that family influence is one of the determinants of subjective norms when it comes to the minimizing of cyber harassment on the part of the individual. For example, discussed the influence of the family as a subjective norm in the behaviour of a number of bank clients in Taiwan. The results showed that the family significantly and positively affects subjective norms [41]. Also, [43] conducted a study in Malaysia on IBS [42]. The researcher confirmed that the family plays the most important role in the behaviour of a number of college students in Malaysia. Moreover, social media sites also allowed the public to share information, which can pose an intended or unintended risks 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 [51, 52] 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 [81].

5.4 Social Pressure

Many behavioural researchers consider social pressure, such as from the family, as one of the behavioural subjective norms that has an influence on an individual's behaviour [31]. With regard to the behaviour of people towards IT usage, especially towards the adoption of new technological services, two previous studies confirmed the influence of the family as one of the subjective norm determinants when it comes to the individual's minimizing of cyber harassment and other technological services. For example, [45] discussed the influence of the family as a subjective norm in the behaviour of a number of bank clients in Taiwan [44]. The results showed that the family significantly and positively affects the subjective norms. [45] conducted a study in Malaysia on IBS [45]. The researchers confirmed that the family plays an important role in the behaviour of a number of college students in Malaysia. According to this theory, our behaviour is guided by three types of considerations:

(Behavioural beliefs): this is about the likely results of the behaviour and their evaluations,

(Normative beliefs): it is about the normative expectations and motivation of others and to comply with the in perceived social pressure

(control beliefs): the presence of factors which facilitate performance of the behaviour and their perceived power

In combination, these lead to the shaping of a behavioural intention. However same literature assures that social influence is likely to be affected by age, gender, experience and voluntariness ; which are hypothesised to be stronger with regards to women, as they may have greater social pressure to conform [75].

5.5 Mass Media

It is highly agreed that cross media advertisements which may include brochures, newspapers, TV, messages and banners in public places, and seminars would increase the number of e-government users in the KSA or any other part of the world. Indeed, it will increase general acceptance, awareness, and therefore the usage of e-services among the public. [73] In deed, within the previous year's, number of young fellows frequenting social media has raised considerably. This applies to the KSA as well. [46], found that 22% of teenagers visiting social media outlets not less than times per day, and over half of adolescents checked social media at least once a day [43][46]. Individual identities are formed by connecting with others, and what drives online and mobile communications is the desire of young people to connect with their peers anywhere at any time. Social networking sites also allow for the public sharing of information [47, 57]. Sexing can also create unintended consequences such as harmed reputations, broken relationships, and shattered friendships [7] [48]. However, there are many different forms of precautions on using the internet. An example, Saudi Arabia's INTERPOL has warned of increasing fraud by online and offline sales, as well as job advertisements outside Saudi Arabia. In his address to Al-Iktissia, the director of INTERPOL called upon Internet users, both citizens and residents, to take all precautions as he warned people while using the Internet, not to go behind commercials and to drift behind false business opportunities to prevent fraud and fraud. Al-Zaben warned against not following the announcements and quotas of jobs outside Saudi Arabia, which require sending personal data, a copy of the passport, expertise and detailed information for completing the job procedures [76].

5.6 Perceived Behavioural Control

Perceived behavioural control is defined as individual beliefs about their power to influence a particular person's attitude. Internal and external issues affect these beliefs. The internal issues of attitudinal control show a person's self-confidence in his/her ability to behave. The factors outside behavioural control, which in [44] words, addressed as 'facilitating conditions', reflect the person's beliefs in respect of the money availability, time, and needed logistics to control the behaviour. The following paragraphs will discuss the effect of the two factors included in perceived behavioural control, namely, regulatory support and the role of the government with regard to the attitude of youths towards minimizing CH in the KSA. Support from government plays a vital role in the dissemination of innovation. Support from government refers to the creation of enabling environment to motivates clients and institutions to utilize a technology and to accept technological developments [49]. Government participation could contribute towards securing a good environment that encourages people to adopt IT projects [11][42][45]. As discussed by [46], the relationship between government support and the perceived behavioural control [46]. The results indicated that government support influences the perceived behavioural control of a number of Internet users in Singapore. The study also showed that the connection between support from government and potential behavioural control is vital and positive.Firstly, fewer than 10% cybercrimes are reported only, and not more than of the 2% reported incidences were prosecuted successfully [50]. Secondly, difficulties in cross-border law enforcement make it easy for the perpetrators to shield from the reach of local or international Internet regulations. This trend was further compounded by diverse moral values, decadence laws, and differed enforcement approaches in different countries [50]. Moreover, Baum (2011) reported that regulatory support means the role of government in promoting e-business adoption by establishing regulation and provision of incentives [7].

5.7 Regulatory Support and the Role of the Government

Internationally, internet regulatory laws are confronted by several challenges. At first, about 10 percent of cybercrimes and harassment were reported; also, fewer than 2% were successfully prosecuted [53]. Secondly, difficulties in performing law enforcement duties at cross border, subjected to regulation implementation to graveness, because the offenders find it easy to commence due to lack of common cross border enforcement framework. This gap further implicates laws and morale values in respect to cyber offences across various countries [54]. Moreover, [55] reported law and regulation support to mean the roles government plays in motivating the utilization of e-commerce avenues, by creating operating rules and provision of incentives [55]. Political, social and cultural factors, like rule of laws, political will and transparency, protection of property rights may influence the diffusion of information technology [37]. Goh (1995) [58]. defined government's support as the initiation of enabling environment to motivate clients and institutions to accept and utilize technology. Goh also indicates that government support plays an important role in transmitting innovations news and that of the existing technology [56][58]. Additionally, government involvement in promoting IT utilization, through the enactment of effective and sound policies that encourage technological development in the country, will definitely enhance the securing of ideal environment that motivates the adoption of IT programs [44]. In the KSA, Internet censorship is transparent and effective. Government carried its citizens alone, through disseminating of information regard to the censored contents and to it extent. The government operates a website that discuss content censorship including the processes of how the information content is censored, and the reasons why the targeted Internet content is censored. Among the censored internet content performed by Saudi government include those items marked immoral, illicit or illegal such as pornographic material, and websites related to " fire arms like bombs, alcoholic/liquor drinks, lottery/gambling and pages insulting the Islamic religion values or the KSA laws and regulations" [59]. The censorship regulation responsibility lies with Internet Services Unit (ISU) situated at the King Abdul Aziz City for Science and Technology in Riyadh. Websites are filtered for content based on their function or activities using proxy server. The proxy server used is checked to filter content of any information that is suspected to be immoral or inappropriate, as listed on the website of the ISU [60]The relationship between the support of the government and the perceived behavioural control is discussed by [61]. The results indicated that the support of the government influences the perceived behavioural control of a number of Internet users in Singapore. Moreover, indicated that the relationship between the support of the government and the perceived behavioural control is significant and positive. Although the system is good, increasing Internet crimes are occurring every day, which means that it needs adjustments to be done to the system to include new crimes and apply new punishments. Further, the Ministry of Interior poses the role of implementing the measures of cybercrime, which is difficult because of the difficulty of getting digital evidence to link to the perpetrators, either because of the ability to destroy evidences, or because of being external to the KSA as they may live escape to other countries. Thus, it remains difficult to have a suitable system to combat cybercrimes specially without international cooperation with the international community to avoid the abuse of all over the international networks [71] [77].

5.8 Security Awareness

Information security can be described as the safeguarding of information as well as information systems from unsanctioned access, usage, disorder, leak, alteration, or damage so as to ensure confidentiality, veracity, and availability [62]. Cyber security is the competence to safeguard or shield the usage of cyberspace from cyber assaults (p. 22) (CNSS, 2010) [62]. These two definitions indicate that cyber security can be regarded as a subset of information security [62]. Awareness refers to the act of making users mindful of their functions and duties in offering security to a business entity's information as well as their own information shared in the cyberspace. The key objective of awareness is to offer information by providing an answer to the "what" element of information security. Users of social media surpass the security settings and put everything in the public domain by manipulating the default system settings. Several users face the risk of stalking, cyber-bullying and solicitation. Users also face abuse and defamation when some people create exact accounts to coerce particular people by tagging and posting imprecise information about other users so as to improve and dent their friendship or nobility. Impersonation is also employed to manipulate others for disclosing their security info and photos on social networking sites [63]. With increasing numbers of individuals using mobile devices, cyber threats are increasingly becoming prevalent among all ages. For example, One in four individuals have their mobile phone stolen, which exposed their sensitive information stored in their network accounts ass, social media and banking applications to be theft. Another report showed that, one in seven had their identity stolen, and one in six has been broken into one of their social media accounts, and one in four have one of their email accounts broken by pirates.

6. CONCLUSION AND FUTURE STUDIES

In conclusion, this study has identified and proposed eight factors for minimizing the cyber harassment such as technological support, attitude, subjective norms, social pressure, the influence of the mass media, perceived behavioural control, regulatory support, the role of the government, and security awareness in minimizing cyber harassment among Saudi youths. Therefore, these factors will help the administration and decision-makers in the KSA to formulate strategies that can significantly affect anti-cyber harassment among youths. Thus, this will help decision-makers in the KSA to formulate strategies that can significantly affect anti-cyber harassment among Saudi youths. In other words, this study has shown that there is an urgent need to develop a cyber-security strategy to strengthen the cyber ecosystem and enhance public-private partnerships. This study is expected to create a greater awareness among Saudi youths that may stimulate the fight against cyber harassment. Therefore, the Saudis will remain at risk of cyber harassment, as it is an issue confounded by the minimal knowledge of what is influencing anti-cyber harassment in Saudi Arabia and how to minimize Saudis attraction to cyber offences in the KSA. Indeed, this is not possible without identifying influential factors that motivate them so that we can investigate them. Indeed, this could be the first attempt of doing so in the KSA. The awareness of laws and potential balance between Internet Usage & Awareness program in Kingdom are more likely to avoid cybercrimes. This is very crucial as technology in cyber world is considered a challenge to all of us, as it is capable of leaving no trace or evidence to cybercrime. We recommend future studies extend studies in this field wherein other factors are included to commensurate with different educational environments around the world.

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] M. Mukred, Z. M. Yusof, U. A. Mokhtar, and N. A. Manap, "Electronic records management system adoption readiness framework for higher professional education institutions in Yemen," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 6, no. 6, pp. 804–811, 2016.

[2] M. Mukred and Z. M. Yusof, "The DeLone–McLean Information System Success Model for Electronic Records Management System Adoption in Higher Professional Education Institutions of Yemen," in International Conference of Reliable Information and Communication Technology, 2017, pp. 812–823.

[3] 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.

[4] N. Kshetri, "The simple economics of cybercrimes," IEEE Secur. Priv., vol. 4, no. 1, pp. 33–39, 2006.

[5] E. J. Appel, Cybervetting : internet searches for vetting, investigations, and open-source intelligence. 2015.

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

[7] K. Baum, Stalking victimization in the United States. DIANE Publishing, 2011.

[8] R. W. Taylor, E. J. Fritsch, and J. Liederbach, Digital crime and digital terrorism. Prentice Hall Press, 2014.

[9] K. Ahmad, T. S. F. T. Wook, and R. Samad, "Key based Approach for Integration of Heterogeneous Data Sources," vol. 48, no. 2, pp. 699–703, 2013.

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

[11] Z. A. A. G. Murshamshul Kamariah Musa and N. I. and M. S. N. B. M. Radzi, "Cyber Stalking: Social Issues of Harassment on Internet," vol. 15, pp. 9–17, 2015.

[12] F. A. Moafa, "Classifications of Cybercrimes-Based Legislations: A Comparative Research between the UK and KSA," Int. J. Adv. Comput. Res., 2014.

[13] 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.

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

[15] A. Alkaabi, G. Mohay, A. Mccullagh, and N. Chantler, "Dealing with the Problem of Cybercrime," no. October, pp. 8–9, 2010.

[16] F. Pereira, B. H. Spitzberg, and M. Matos, "Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents," Comput. Human Behav., vol. 62, pp. 136–146, 2016.

[17] 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

[18] H. Binsahl, S. Chang, and R. Bosua, "Identity and belonging : Saudi female international students and their use of social networking sites," vol. 6, no. 1, pp. 81–102, 2015.

[19] D. Felmlee and R. Faris, "Toxic Ties: Networks of Friendship, Dating, and Cyber Victimization," Soc. Psychol. Q., vol. 79, no. 3, pp. 243–262, 2016.

[20] C. Miller, "Cyber Stalking & Bullying: What Law Enforcement Needs to Know," Off. com, 2006.

[21] K. K.-J. Seo, J. Tunningley, Z. Warner, and J. Buening, "An Insight Into Student Perceptions of Cyberbullying Kay," Am. J. Distance Educ., vol. 30, no. 1, SI, pp. 39–47, 2016.

[22] B. D. Loader and D. Thomas, Cybercrime: Law enforcement, security and surveillance in the information age. Routledge, 2000.

[23] K. Van Royen, K. Poels, H. Vandebosch, and P. Adam, "'Thinking before posting?' Reducing cyber harassment on social networking sites through a reflective message," Comput. Human Behav., vol. 66, pp. 345–352, 2017.

[24] 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.

[25] 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

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

[27] H. Ajjan and R. Hartshorne, "Investigating faculty decisions to adopt Web 2.0 technologies: Theory and empirical tests," Internet High. Educ., vol. 11, no. 2, pp. 71–80, 2008.

[28] 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

[29] 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.

[30] S. Taylor and P. Todd, "Decomposition and crossover effects in the theory of planned behavior: A study of consumer adoption intentions," Int. J. Res. Mark., vol. 12, no. 2, pp. 137–155, 1995.

[31] S. Taylor and P. A. Todd, "Assessing IT usage: The role of prior experience.," Manag. Inf. Syst. Q., vol. 19, no. 4, pp. 561–570, 1995.

[32] S. N. Baraghani, "MASTER â€TM S THESIS Factors Influencing the Adoption of Internet Banking MASTER ' S THESIS Factors Influencing the Adoption of Internet," 2008.

[33] H. Nysveen and P. E. Pedersen, "An exploratory study of customers' perception of company web sites offering various interactive applications: moderating effects of customers' Internet experience," Decis. Support Syst., vol. 37, no. 1, pp. 137–150, 2004.

[34] 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 Abus. Negl., vol. 44, pp. 159–169, 2015.

[35] M. Al-Majali and N. K. N. Mat, "Modeling the antecedents of internet banking service adoption (IBSA) in Jordan: A Structural Equation Modeling (SEM) approach," J. Internet Bank. Commer., vol. 16, no. 1, pp. 1–15, 2011.

[36] 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

[37] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," CCS '03 Proc. 10th ACM Conf. Comput. Commun. Secur., pp. 62–72, 2006.

[38] I. Ajzen and M. Fishbein, "Attitude-behavior relations: A theoretical analysis and review of empirical research," Psychol. Bull., vol. 84, no. 5, pp. 888–918, 1977.

[39] P. M. Bentler and G. Speckart, "Models of attitude–behavior relations.," Psychol. Rev., vol. 86, no. 5, p. 452, 1979.

[40] [40] M. Mitchell and T. Pulvino, Characteristics of Risk and Return in Risk Arbitrage, vol. 56, no. 6. 2001.

[41] D. L. Amoroso, U. States, D. S. Hunsinger, and U. States, "Analysis of the Factors that Influence Online Purchasing," vol. 1, no. 1, pp. 1–16, 2008.

[42] P. a. Pavlou, "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," Int. J. Electron. Commer., vol. 7, no. 3, pp. 69–103, 2003.

[43] M. Sathye, "Adoption of Internet banking by Australian consumers: an empirical investigation," Int. J. Bank Mark., vol. 17, no. 7, pp. 324–334, 1999.

[44] K. Fang and Y.-Y. Shih, "The use of a decomposed theory of planned behavior to study Internet banking in Taiwan," Internet Res. Electron. Netw. Appl. Policy, vol. 14, no. 3, pp. 213–223, 2004.

[45] K. M. Nor, E. A. A. Shanab, and J. M. Pearson, "Internet banking acceptance in Malaysia based on the theory of reasoned action,"

JISTEM-Journal Inf. Syst. Technol. Manag., vol. 5, no. 1, pp. 3–14, 2008.

[46] G. S. O'Keeffe et al., "The Impact of Social Media on Children, Adolescents, and Families," Pediatrics, vol. 127, no. 4, pp. 800–804, 2011.

[47] 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.

[48] H. Beahviors, "Sexting behaviours among teens : Dating and romance in the digital age ?," vol. 11, no. 3, 2011.

[49] et al. Gardner, Dianne, "Predictors of workplace bullying and cyber-bullying in New Zealand," Int. J. Environ. Res. Public Health, vol. 13, no. 5, pp. 1–32, 2016.

[50] M. Bakhsh, A. Mahmood, and I. I. Awan, "A comparative analysis of cybercrime and cyberlaws in Islamic Republic of Pakistan , Kingdom of Saudi Arabia , and the United Arab Emirates," pp. 9–15, 2016.

[51] 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

[52] 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.

[53] Symantec, "Internet Security Threat Report 2011 Trends," vol. 17, no. April, pp. 1–52, 2012.

[54] R. Broadhurst and Y. Chang, "Cybercrime in Asia:Trend and challenges," Asian Handb. Criminol., no. FEBRUARY, pp. 1–26, 2012.

[55] B. Pudjianto, "Factors Affecting e-Government Assimilation in Developing Countries," Commun. Policy Res., pp. 1–14, 2010.

[56] A. T. C. Goh, "Modeling soil correlations using neural networks," J. Comput. Civ. Eng., vol. 9, no. 4, pp. 275–278, 1995.

[57] 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

[58] H. P. Goh, "The Diffusion of Internet in Singapore; A content analytic Approach," Fac. Bus. Adm. Natl. Univ. Singapore, vol. 96, 1995.

[59] K. A. City, "Internet Services Unit," 2010.

[60] K. M. Al-Tawil, "The Internet in Saudi Arabia." pp. 625–632, 2001.

[61] 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.

[62] S. N. N. I. A. Ia, "National Information Assurance Glossary," CNSS Instr. No. 4009, vol. CNSSI No., no. 4009, 2010.

[63] A. Dhami, N. Agarwal, T. K. Chakraborty, B. P. Singh, and J. Minj, "file:///C:/Users/Mac/Downloads/scholar (9).ris," Proc. 2013 3rd IEEE Int. Adv. Comput. Conf. IACC 2013, no. February 2016, pp. 465–469, 2013.

[64] G. Bin Huang, Q. Y. Zhu, and C. K. Siew, "Extreme learning machine: Theory and applications," Neurocomputing, vol. 70, no. 1–3, pp. 489–501, 2006.

[65] M. Afshar and K. Ahmad, "A new hybrid model for electronic record management," J. Theor. Appl. Inf. Technol., vol. 81, no. 3, p. 489, 2015.

[66] A. Besbes And P. Legohérel. "Using The Decomposed Theory Of Planned Behavior (Dtpb) To Explain The Intention To Book Tourism Products Online". International Journal Of Online Marketing, 4(1), 1-10,Pp:2. January-March 2014

[67] N. K. Khan. Taxonomy Of Cyber Crimes And Legislation In Saudi Arabia. International Journal Of Advanced Research In Computer Engineering & Technology (Ijarcet), Volume 1, Issue 8, October, 2012, 207

[68] A. Arabnews,. Cybercrime Costs Saudi Arabia Sr 2.6 Bn A Year, 2012online Available: Http://Www.Arabnews.Com/Saudi-Arabia/Cybercrime-Costs-Saudi-Arabia-Sr-26-Bn-Year (December 08-2013)

[69] Ksa. Anti-Cyber Crime Law, Kingdom Of Saudi Arabia (Ksa) Bureau Of Experts At The Council Of Ministers, Anti-Cyber Crime

Law, Royal Decree No. M/17 8 Rabi 1 1428/26 March, 2007. 1st Ed.; 2009. Available From: Http://Www.Saudiembassy.Net. [Last Accessed On 2014 Nov 2

[70] B. M. And E. Elnaim.Cyber Crime In Kingdom Of Saudi Arabia: The Threat Today And The Expected Future Information And Knowledge Management. Vol.3, No.12, 2013 14

[71] S. Al Amro. Cybercrime In Saudi Arabia: Fact Or Fiction? Ijcsi. International Journal Of Computer Science Issues, Volume 14, Issue 2, March 2017

[72] K.I. Al-Qeisi, . (2009). Analysing The Use Of Utaut Model In Explaining An Online Behaviour: Internet Banking Adoption.Phd Thesis, Brunel University

[73] Using The Utaut Model To Determine Factors Affecting Acceptance And Use Of E-Government Services In The Kingdom Of Saudi Arabia Mohammed Abdulrahaman Alshehri Griffith University Dec2012 Phd Thesis

[74] Y. Altaweel. E-Commerce In Saudi Arabia: Challenges And Obstacles. Alriyadh. , (2009)

[75] F. F. Alsharif. Investigating The Factors Affecting On-Line Shopping Adoption In Saudi Arabia. Phd Thesis. De Montfort University. England. 2013

[76] Http://Www.Aleqt.Com/2012/04/15/Article_647185.Html

[77] Almadinah, 2015. Electronic crimes cost the Saudi 2.8 billion SAR annually. Available at: http://www.al-madina.com/node/641706# [Online; accessed Oct 15,].

[78] A. Almadinah, 2015. Electronic crimes cost the Saudi 2.8 billion SAR annually. Available at: http://www.al-madina.com/node/641706# [Online; accessed Oct 15,

[79] A. Almadinah, 2015. Electronic crimes cost the Saudi 2.8 billion SAR annually. Available at: http://www.al-madina.com/node/641706# [Online; accessed Oct 15,].

[80] Alsakinah, 2016. Saudi Arabia: escalating cybercrimes. Available at: http://www.assakina.com/awareness-net/rebounds/90908.html [Online; accessed Dec 21, 2016]

[81] 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