Internet Governance & Cyber Crimes In UAE

Ayesha Al Neyadi, Alia Al Kaabi, Laila Al Kaabi, Mariam Al Ghufli, Maitha Al Shamsi, Dr. Muhammad Khan

Abstract: Most people in UAE don't feel safe while they are use the Internet, because most internet users have been a victim for cyber crime. Cyber crime threat rate has increased which has targeted on citizen privacy, property and governments also the reputation problems. There are many criminal activities such as indecent acts, Copyright issues, Terrorist Acts, State security and Contempt of religion. Cyber crimes due to several reasons, such as they have lack of social intelligence, they are being greedy and not being content also some of them have financial troubles, these reasons usually exploited by criminals. Thus, the decree will be a punishment or criminalizes formally on any person who using any kind of information technology and any other's private life to blackmail or to threaten others online. In addition, at the present time, with the most detailed new cybercrime law that can be used to prove found guilty. As well, the author discusses that the new cyber-crime law provides protection of personal information including banking information, credit cards and electronic payment information.

Index Terms: Internet Governance, Cyber Crimes, UAE Cyber Crimes, UAE Internet Governance, Cyber Crime Law

1. INTRODUCTION

Internet governance (IG) concentrates on the application of new information and communication technologies and techniques to traditional or new practices of government also identifying opportunities and constraints on deployment with governmental authority. (What is Internet Governance and Where Does it, 2005). The Internet governance was introduced in the World Summit on the Information Society (WSIS) process and the development of principles, norms and programs that shape the evolution and the uses of the internet. The complexity of implementing Internet Governance regime that is issued, which involve five dimensions to internet issues such as infrastructure, Legal, Economic, Development, and Socio-cultural. Thus, many actors play a role in each these dimensions both in the private and public sector, which includes civil society activities and etc. However, with new cognitive tools that can reduce the complexity and help to introduce or create common approaches system with guiding principles. (Internet Governance issues, Actors and Divided, 2005). The cyber crimes cover any criminal act dealing with computers, networks and Internet. Regularly, most of cyber crimes involved the use of a specific malware system that controls computer networks in the region. Most of the perpetrators of cyber crime are from outside the United Arab Emirates so to reduce the cyber crimes; we must cooperate with other international agencies from all over the world. (Menting, 2015)

1.2 RESEARCH PROBLEM

There is a large segment of internet users in UAE still falling on cyber crimes, despite several awareness campaigns. (Abu Dhabi Police say people are still falling prey to "indecent" cyber crime , 2014). Nowadays, the number of users of social networking sites between UAE citizens has increased specially in Facebook, LinkedIn, and Twitter. According to the UAE Social Media Outlook 2014, the number of Facebook users in the UAE between 2010 and 2014 has increased from 1.67 million to 5 million. (2014 UAE SOCIALMEDIA OUTLOOK, 2014). This increasing in the number of users not only in Facebook but all over social networks. Furthermore, this has led to an increase in the number of cyber-crimes in United Arab Emirates. "According to the latest Norton Cybercrime 2012 report, 46 per cent of the UAE's social networking users have fallen victim to cybercrime on social networking platforms." (Cherrayil, 2012).
Additionally, they do not have adequate awareness and knowledge about the use of the internet and social networking.

1.3 RESEARCH GOAL

Aims:

- What is Internet governance, cyber-crimes?
- Identifying the factors of cyber-crimes
- Identifying how to prevent cyber-crimes
- How Internet used as a policy action?
- What are the acts or contributes of Internet government to fight cyber crime?

Objectives:

- Identify internet governance and cyber crimes implications.
- Analyses the law and policies of internet governance in the country.
- List types of risk that can a person get into by breaking the roles or using Internet without knowledge and not using the Internet wisely.
- Identifying the factors of cyber crimes

1.4 RESEARCH SIGNIFICANT

Our research provides an important sensitization about avoiding cyber crimes for threaten UAE citizen. Moreover, it will decrease the number of users, who are falling at any type of cyber crimes. Furthermore, the user will be aware of the risks could get into by breaking any policies roles or using the internet without enough knowledge. Our research will provide basic principles, opportunities and any challenges of cyber crimes, which it will improves the users knowledge to avoid all types of risks could fall in it in the future.

- *Authors; Ayesha Al Neyadi, Alia Al Kaabi, Laila Al Kaabi, Mariam Al Ghufli, Maitha Al Shamsi, Alumni Al Ain Womens College, Higher Colleges of Technology, UAE*
- *Research Supervisor & Co Author; Dr. Muhammad Khan, Faculty Computer and Information Sciences, Al Ain Womens College, Higher Colleges of Technology. UAE. Email: Muhammad.khan@hct.ac.ae*

1.5 RESEARCH QUESTIONS

WHAT ARE THE FACTORS THAT LED INTERNET USERS FAIL ON CYBER CRIMES?

1. How Internet governance deal with cyber-crimes?
2. What are the types of cyber crimes threaten UAE citizen?
3. Do Internet users have full awareness about cyber crimes?

1.6 RESTRICTION

- **It does not:**
  - Cover all the types of cyber crimes in UAE (social political, legal implications).
  - Address the failure or success factors of using all kind of laws and policies of the internet governance in UAE.
  - Attempt to resolve the failure causes of internet governance in control the cyber crimes.
  - Address the general public view of the project.
- **But:**
  - It will cover the types of cyber crimes that threaten UAE citizen.
  - It will address and analyze the success and failure factors on a broad view based on the UAE internet governance of using laws and policies.
  - It will analyze the factors that make the users falling in the cyber crimes and rank them according to their importance in the internet governance.

1.7 RESEARCH METHODOLOGY

In our research we will do survey using survey monkey site. In order to collect more information from people, which will help us to find out the factors that led people to fall in these problems. Moreover, we will search for journals and articles from newspaper and e-books to get more information related to Internet Governance and cyber crimes.

2. LITERATURE REVIEW

According to Enzer (2011), most internet users in the UAE have been a victim for an online crime. Hasbini (2014) says that the cyber crime threat rate has increased which had targeted on citizen privacies, property and governments also the reputation problems. Further, these online crimes are very difficult to prove and criminals are usually targeting the UAE citizens because of the economic status worldwide also the high rate of using mobile phone. Now days, everyone communication and commercial activities through out online. Also BISSON (2014) mention the clearly, the Cybercrimes growing severity of different forms as fraud, threat and abuser and some of the worst threats, as well as what we can do to defend against them. In addition, Berger (2012) mentions that most people don't feel safe during using the internet, which is an international instead of local problem. Moreover, the reason cyber crimes happen is that there are bad people who plan to steal and phishing the organization, which they must focus on stopping cyber crime. Also Enzer (2011) said that there are 2.55 Million of internet users in the UAE, which they become a victims to cyber-crimes, "because of a lack of education in the region about cyber-crime" (Enzer, 2011). Furthermore, it's important to educate the users who use and depend on the internet for their work to avoid falling in any trap of cyber-crimes, which they can do their work in the internet safely without any troubles. As GaskellPublished (2015) mentions that the "children online" found that more than half of young users in the UAE come across adult content, over 22% visit and use websites dedicated to gambling. Additionally, Enzer (2011) said that the users have to learn the main steps to protect their personal data in any web in the internet, which they found that "84% of cybercrime victims in the UAE found an online attack". There are many types of cyber crimes the criminals use it to attacks the users in the UAE, such as: "Computer viruses or malware 65%, Online scams 54%, Phishing messages 53%" of attacks in the last 12 months. Moreover,"20% the number of mobile phone attacks in the UAE", which occurs through using the mobile internet in the country. Furthermore, "56% of mobile phone users in the UAE access the internet via their mobile phones", Taufiq said. (Enzer, 2011). He also mentions that we are all live in open society where Internet services are available to all that it seems that we need to follow up children, and follow the evolution of technology. “But it is not just children who are naive when it comes to cyber security. The report also found that more than half of UAE respondents use free public Wi-Fi, with only 31 per cent of them taking precautions” (Al Bustani, 2015). Where most users do not take heed when using public networks, which all public networks considered as a hotbed of viruses and cyber crimes if the users did not take their precautions will be in danger. Al Bustani (2015) says that there are some of amateurs who can install and run scripts that it can attack and redirecting them to malicious websites to steal other people information. Besides to that, most of users trust store their passwords and personal data on the devices. Where there is a danger that threatens them, which is all files and data will encryption and they cannot be accessed, and they have to pay a ransom to restore their files and information. Not only that, but there is another attack for the smart phone. The user will receive a SMS that have a link to a website. Most of the SMSs are advertising massage that tempts the users to press the link. “This link then installs a certain application that starts monitoring all your traffic, stealing all your photos, all your data, all your passwords, and then these will be used in many bad activities” (`Despite in Wam (2012) in his article , there are criminal activities that are forbidden and illegal with different aspects online, which the most comment are Indecent acts (attempt to threat anyone or insult them with any other indecent acts), Copyright issues (the intention to engage illegal trade and publishing any ideas to build out the hates and racism to damage national unity), Terrorist Acts (encourage some people to do unlicensed bodies with funds such as making of explosives or any devices used in terrorist acts), State security (Mocking about the state and publishing any information that likely will affect the security of the nation and the threats of the state), Contempt of religion (insult or display any of the Divine Religions and holy symbols). According to Berger (2012) the most evidence confirm that cyber crimes are a variety of illegal activities such as: "online scams, phishing, hacking and unleashing computer viruses" (Berger, 2012). As Barakat (2015) mention, people fall in cyber crimes due to several reasons, such as they have lack of social intelligence, they are being greedy and not being content also some of them have financial troubles, these reasons usually exploited by criminals. But they don’t wait for the victim to report the crime, but rather they monitor the Internet and deal with the situation

immediately. Therefore, Hasbini (2014) says that the most dangerous had attack on user is bank malware in UAE. In this case, Most of them don't aware the cyber fraudulent activities when it comes online payment and e-services, because of the wide smartphones availability of unprotected that has tented to target users with malware and phishing attacks affecting all types of devices. In Emirates 247 (2015) has identify the internal procedures, and implementing training and awareness programs. In order to solve this problem UAE police have established cybercrime and organizational security units, also they have computer forensics teams who specialize in examining and presenting electronic evidence that store on computers or on other electronic devices. Were their roles includes "investigating all types of crimes committed against and by means of computer data and systems". (Emirates 247, 2015). Also, Moyenorient3 (2014) says that they have a specialists use a cyber-police power to oversee the Internet, including its use by human rights activists. Abu Dhabi's State Security Apparatus and the Department of Anti-Electronic Crimes has also been created within the Criminal Investigation Department of the Dubai police, has created a unit specialized in cyber crime to spy in the internet and its users. As Berger (2012) according to his words, is an important to change the policy of any company, which they need to change their technology always to make sure the company system is secure tightly. In addition, GaskellPublished (2015) mention that the user must also be aware of threats aimed at exploiting mobile games, some games carried within it spyware functionality to record sounds, process calls and steal SMS information. According to Wam (2012) article, the "Sheikh Khalifa bin Zayed Al Nahyan has issued Federal Legal Decree No. 5 for 2012 on combating cyber crimes". Within new decree that coverage online activity and generate information regard to information that is published online, whether it's personal or ongoing activities. In this decree provide on legal protections of privacy which include all information credit card numbers, bank account numbers any other online details and also electronic payment methods. Therefore, there will be protects the individual privacy from anyone who duplicates of credit cards. Thus, the decree will be a punishment or criminalizes formally on any person who using any kind of information technology and any other's private life to blackmail or to threaten others online. Also, for anyone who did criminal activities, they will have consequences of jail and would face any other punishments in order of judicial or administrative authorities. (Wam, 2012)

As Moyenorient3 (2014) mention that the regulation authority has categories of websites that are blocked in UAE:

1. Content conflicting with UAE ethics and morals, including indecent acts and dating.
2. Content containing material that expresses hate of religions.
3. Content conflicting with UAE Laws.
4. Content that allows or helps users to access blocked content.
5. Content that directly or indirectly poses a risk to UAE Internet users, such as phishing websites, hacking tools and spyware.
6. Content related to gambling.
7. Content providing information about purchasing, manufacturing, promoting and using illegal drugs.

Any person "subjected to abuse, insult or defamation on social networking sites" could open a complaint with the unit, which would immediately take care and deal of the site after verifying the complaint. (Moyenorient3, 2014). However, as Mustafa (2012) mention that at the present time, with the most detailed new cybercrime law that can be used to prove found guilty. As well, the author discusses that the new cyber-crime law provides protection of personal information including banking information, credit cards and electronic payment information. In addition, as GaskellPublished (2015) written in article the authorities alerted users about malware transported through politically-oriented news or social networking forums using social engineering strategies to gain full entree and control over the victim's devices and files. According to BISSON (2014) that, the anti-cybercrime will defend on particular measures from authentication and awareness. Therefore, the authentication is to strengthen the companies' authentication protocols of security control, which include two-factor authentication is to protect the wealth of data behind a user's account and reduce the risks threatening critical data with this option can involve in using mobile applications and hardware marks. Thus, In this authentication have beneficial on prevention, which include the adds Houmann can record who did/ said what and who in authentication protocols with this tool can address the rising status of cyber bullying and child abuse on online. However, organizations should ensure they have full awareness of what's on their network with security solutions as user has to know the security applications to reduce the danger for the users, their systems and data assets. Moreover, for the children, need to educate them about the cybercrimes and to watch out the suspicious activity online. (BISSON, 2014). Because UAE society is an advanced society and everyone can access to the internet Hasbini confirms that parents and users need to be fully aware of the attacks that threaten them. "We need more awareness on how to deal with online threats, because it's the internet and we don't know who is hiding behind the internet." (Hasbini, 2015).

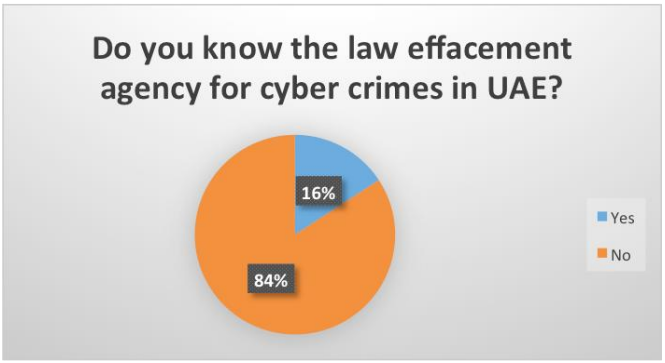


Chart5: *Shows the number of people who know the law Effacement agency for cyber crimes in UAE and who are not.*

There are serious consequences for cyber crimes as some of the crimes continue into real life. The real danger is when children are exposed to blackmail and threats they are afraid to tell their parent the truth which exposing them to depression or even suicide. "The worst part of these numbers is that 98 per cent of these incidents go unreported" (Shaheem, 2015). Thus, GaskellPublished in his article paper (2015), that the families need mutli-platform solutions that integrate a full

range of features and tools that allow them to provide and mange their device and children privacy, the solution enables full, multi layered security across a range of devices allowing real time protection and observing of the cyber activity. To help parents better protect their children the solution comes with a parental control feature that can limit the number of hours children spend online in addition to monitoring activity online and on social media platforms. (GaskellPublished, 2015).

3. METHOD SECTION

Study type

In our research, we used exploratory and descriptive methods.

3.1 Exploratory Research

In this research our aim is to clarify the concepts and better understanding of specific problems or questions in literature search which tends to be qualitative data by posting survey to a social networking, which takes the form of open-ended questions where can leave responses in the format of open text comments. Thus, mostly the result of quality data is useful to identify our purpose of the research and understanding of specific target respondents of opinions and behavior. (Wyse , 2014)

3.2 Descriptive Research

In this research are more like guideline, which describe the people, and situations based on our research questions. Moreover, the data, descriptive research may be qualitative or quantitative on a specific group of people to evaluate the survey and describes the situations and provide the statistically conclusive of data. For example, knowing the statistic result about how well people know the cyber crimes and law effacement in UAE. (The Research Process, n.d)

3.3 Methods

In the research, we use a mixed methodology of collecting information and data which they are:

Quantitative data: is more structured as numerical data which useful for measurements and analysis of target concepts to answers based on particular age of the group which included an online survey to gather the information from respondents.

Qualitative data: are used to gain an understanding of the objectives and a literature review to provide and develop an ideal about the research, such as resource data which include online reports, books, journals and documents. (Wyse, 2011)

Sample/Population: The Population of our research includes males and females criticize of the UAE. We took a random simple around 100 people's females and males were 75 % students, 17 %Employed and 13 % Unemployed from age 7% under age, 79% 18- 25 and 14% above 25 were answered the questionnaires opinions and comments through an online survey at UAE.

There are two source of data collection techniques, Primary and Secondary. The Primary data collection as Surveys, Secondary data collection as Journals, News Papers, e-books and online sources. In our research paper we used both data source techniques to collect the data we need. In the Primary data which is a document or physical object which was written or created during the time under study. These sources were present during an experience or time period and offer an inside view of a particular event, we used Survey to collect some information we need in the research paper, the survey include nine questions, the first three question are personal which will help to know which type of audience is more knowledge about our research topic, then the other six questions will help us to know if either the audience have deal with cyber crime and how they react to solve it or they just ignore it and didn't deal with it. The secondary data collection is data used in research that has already been collected for another sources purpose to summarize and analyze original research. As for our research paper we used Journals, Newspaper, online sources and e-books, which we summarized in the literature review part. Data analysis is the method of understanding the meaning of the data we have collected and organized, and displayed in form of chart and line graph. Data will be collected and analyzed to get to a conclusion and the needed result. A survey was used to figure people knowledge about cyber crime and laws. The survey contain option and comment question, which will help us to get the data we need to select to reach our objective. We used Surveymonkey.com to make the survey, Microsoft Excel to draw the graphs and Microsoft office to write the Research paper.

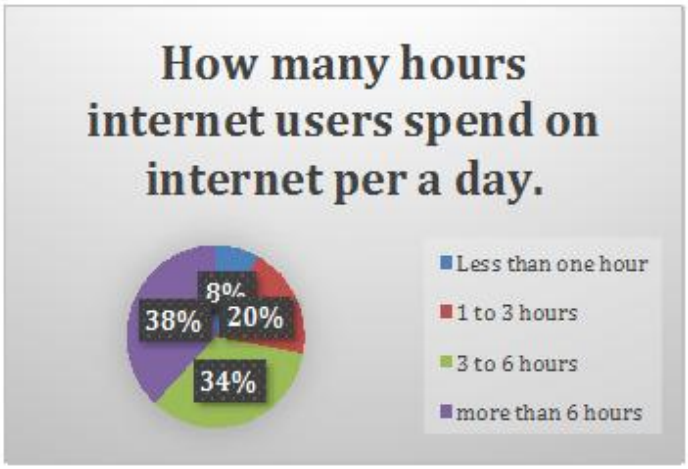
4. FINDINGS/ RESULTS

RQ 1. What are the factors that led internet users fail on cyber crimes?

To figure out this question, we used the literature review to analyze the data to answer this question. Which considered as qualitative data. From the literature review, we found some of the factors that led Internet users fail on cyber crimes. For instance, using a free public Wi-Fi without taking precaution which making its users at high risks. (Al Bustani, 2015). In addition, the lack of education let UAE user's victims to cyber crimes. (Enzer, 2011). Which mean that the lack of education and awareness about cyber crimes considered as one of the factors that let Internet users fail on cyber crimes. Based on the survey, from our sample we found that seven people are under 18 years old, 79 who are between 18 to 25 years old and 14 who are above 25 years olds.

Answer choices	Responses	
Under 18 years old	**7.00%**	**7**
Between 18 to 25 years old	**79.00%**	**79**
above 25 years old	**14.00%**	**14**

Table 1: *Shows the result of the age groups.*



We found that the highest percentage is the people who are between 18 to 25 years old. Which mean that the most Internet users in our sample who are between 18 to 25 years old.Based on the survey, we found that 16 people who are employees in different organizations, 69 people who are students and only 12 people who are unemployed as shows Chart1. From our survey we found that the most Internet users in ours sample are students in different majors and different educational organizations. Also the lowest groups who are unemployed.

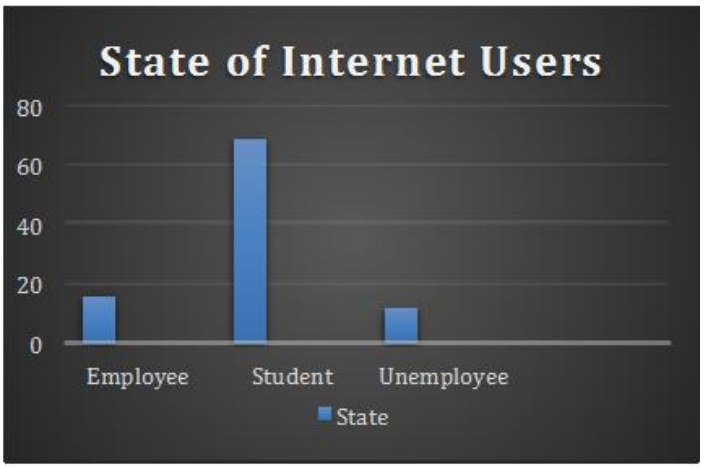


Chart 1: *Shows the percentage of the Internet users' state.*

Furthermore, based on our survey we found that only 8 internet users who spend less than one hour, 20 internet users who spend between one to three hours, 34 internet users who spend their time on internet between three to six hours and 38 internet users who spend their time on internet more than six hours. So, we find that there is a relationship between how old the Internet users is and between the states of internet users and between how many hours he spend in internet per a day. The highest percentage was the internet users who are between 18 and 25 years olds, which they are still students from different majors, which they spend more than 6 hours in internet per a day. So, we consider that the age of Internet users and the hours that they spend in internet user are some of factors that led internet users to fall on cyber crimes.

RQ 2. How Internet governance deal with cyber-crimes?

To figure out this question, we used the literature review to analyze the data to answer this question. Which considered as qualitative data. Therefore, The United Arab Emirates Police have established cybercrime and organizational security units to mitigate the attacks and risks that internet users faced in UAE. (Emirates 247, 2015). In 2012, Sheikh Khalifa bin Zayed Al Nahyan has issued Federal Legal Decree that defends the privacy, which include the credit cars numbers, online information and the payment methods from anyone who duplicates their information. (Wam, 2012) In addition, for anyone who did criminal activities, they will have consequences of jail and would face any other punishments in order of judicial or administrative authorities. Anybody could open a complaint with the unit that would directly ensure and deal of the site or email after confirming the complaint. Now, with the most detailed new cybercrime law that can be used to prove found guilty and It has become easy to arrest and convict criminals. (Mustafa, 2012). In fact, there is a large interest of the government to control cyber crimes in UAE because the country become in sync with the technological revolution and the government want to protect their users from external risks.

RQ 3. What are the types of cyber crimes threaten UAE citizen?

To figure out this question, we used the literature review to analyze the data to answer this question. Which considered as qualitative data. Al Bustani (2015) says that there are some of amateurs who can install and run scripts which it can attack and redirecting them to malicious websites to steal other people information. Besides to that, most of users trust store their passwords and personal data on the devices. Where there is a danger that threatens them, which is all files and data will encryption and they cannot be accessed, and they have to pay a ransom to restore their files and information. What worries most users in the United Arab Emirates spying on people through CCTVs, Webcams and Telecommunication. Where criminals can capture images or video to use late to intimidate and blackmail users. The author added that there are online networks that allow users to sell drugs, assassination services, give access to websites that are blocked in certain countries. These online networks will never let anyone to track or know who you are deal with. Based on our serve, we found that five Internet users of our sample in UAE have been victim of any type of cyber crimes. Moreover, around 95 of Internet users was not as shows chart 3.

RQ 4. Do Internet users have full awareness about cyber crimes?

To figure out this question, we used the literature review to analyze the data to answer this question. Because UAE society is an advanced society and everyone can access to the Internet Hasbini confirms that parents and users need to be fully aware of the attacks that threaten them. "We need more awareness on how to deal with online threats, because it's the Internet and we don't know who is hiding behind the internet." (Hasbini, 2015). There are serious consequences for cyber crimes as some of the crimes continue into real life. The real danger is when children are exposed to blackmail and threats they are afraid to tell their parent the truth which exposing them to depression or even suicide. Despite the fact that Internet is a great source to gain knowledge and information whether it could be educational and entertaining information, we cannot turn a blind eye to the cyber crimes and the risks that threaten our children and us or even threaten the security of our country.

Chart4: *Shows that if the people have a good knowledge about cyber crimes or not.*

Based on our survey we found that around 47 person of our sample they don't think that people in UAE have a good knowledge about cyber crimes and around 48 person said yes they have a good knowledge about cyber crimes as shows chart 4. Based on our survey, we found that 19 people of our sample know about one of the law effacement agencies for cyber crime in UAE and around 80 person of our sample they don't know about any one of agencies that can report their problems as shows in chart 5. Taking everything's into consideration, we found that a high rate of internet users of our sample don't know where to report if they face a cyber crimes and there is a slight difference in the number who have knowledge about cyber crimes and that who are don't have a good knowledge about cyber crimes. Which mean the Internet users in UAE have a slight knowledge about the cyber crimes. Where it should intensify the educational programs and awareness to the social media users and students.

5. DISCUSSIONS

The purpose of this research is to know more about Internet governance and cyber crimes in UAE.

What are the factors that led Internet users to fail on cyber crimes?

Irrespective of age and education, anyone can be a victim of cyber crime. According to Abu Dhabi Police they recorded about 33 online blackmail cases in six months, and that means people are still falling in cyber crimes, due to several reasons such as having a lack of social intelligence, they are being greedy and not being content, having a financial troubles and some of them become a victims to cyber-crimes, because of a lack of education about this problem (Enzer, 2011), these reasons usually exploited by criminals. Furthermore, because of the proliferation of the Internet and social networking sites, UAE found that most victims had an online attack, where people spend most of their time surfing the Internet. In addition, the survey that we have published indicates that most Internet users belong to the age group of 18 to 25 years, and a lot of them are students, which they spend most of their time online.

How Internet governance deal with cyber-crimes?

Because the internet is an open environment, all the cyber crimes that exist in the United Arab Emirates, are also found everywhere in the world, but what is different is the way to deal with it. In order to reduction of such crimes. UAE police have established cybercrime and organizational security units. Where Abu Dhabi's State Security Apparatus and the Department of Anti-Electronic Crimes has also been created within the Criminal Investigation Department of the Dubai police, has created a unit specialized in cyber crime to spy in the internet and its users. In addition, as Moyenorient (2014) mention that the regulation authority has categories of websites that are blocked in UAE.

What are the types of cyber crimes threaten UAE citizen?

Nowadays, the communication and commercial activities done through out online, however, most people don't feel safe during using the internet, because the cybercrimes growing severity of different forms as fraud, threat and abuser and some of the worst threats, as well as what we can do to defend against them. (BISSON 2014) There are many types of cyber crimes in the UAE, such as: Computer viruses or malware, online scams, Phishing messages and mobile phone attacks, which occurs through using the mobile internet in the country. On the other hand, money and blackmail are considered most common cyber crimes in UAE that due to ease of committed from anywhere in the world. Moreover, the criminals always target young people through social networking sites to portraying them, in order to blackmail later and take huge amounts of their money. As a result of the emergence of new technology the banking sector considered

the most targeted sector for cybercrime in UAE including ATM and Internet banking applications.

Do Internet users have full awareness about cyber crimes?

Although some of Internet user in UAE don't have any idea about cybercrime and what it is mean, however most of them know already about cybercrime. For those people who don't have a good knowledge about cybercrime, it's important to educate them, especially for those people who depend on the internet for their work to avoid falling in any trap of cyber-crimes, therefore they can do their work in the internet safely without any troubles.In addition, families need multi-platform solutions that integrate a full range of features and tools that allow them to provide and mange their device and children privacy. Furthermore, ADP advised them to monitor their children while using phones or computers, also they calls the public to not engage with strangers who may try to lure them into the chat rooms.

6. CONCLUSION

This research will provide an opportunity for people to know more about cyber-crimes in UAE. Which it will increase their awareness about the risks they may face while they are on the Internet or on social networking. Furthermore, the research paper aim to identifying what Internet Governs and cyber crime. Moreover, we identified the opportunities and constraints on deployment.

REFERENCES

[1] 7DAYS. (2014, August 10). Abu Dhabi Police say people are still falling prey to “indecent” cyber crime. Retrieved March 11, 2015, from http://7daysindubai.com/abu-dhabi-police-say-people-still-falling-prey-indecent-cyber-crime

[2] Amin Hasbini, M. (2014, June 23). The Rise of Cybercrime in Dubai and UAE. Retrieved April 7, 2015, from https://securelist.com/blog/research/63682/the-rise-of-cybercrime-in-dubai-and-uae/

[3] Berger, H. (2012, July 28). Vigilance key to reducing internet cyber attacks in UAE. The National. Retrieved April 6, 2015, from http://www.thenational.ae/lifestyle/personal-finance/vigilance-key-to-reducing-internet-cyber-attacks-in-uae#full

[4] Bisson, D. (2014, October 30). Authentication and Awareness: The Anti-Cybercrime Duo. Retrieved March 8, 2015, from http://www.tripwire.com/state-of-security/security-awareness/authentication-and-awareness-the-anti-cybercrime-duo/

[5] Ctb.ku. (2014). Collecting and Analyzing Data. Retrieved May 12, 2015, from http://ctb.ku.edu/en/table-of-contents/evaluate/evaluate-community-interventions/collect-analyze-data/main

[6] Emirates247. (2013, January 14). . ‘Banking is the most targeted sector for cybercrime in UAE’. Retrieved April 12, 2015, from http://www.emirates247.com/news/emirates/banking-is-the-most-targeted-sector-for-cybercrime-in-uae-2013-01-14-1.490928

[7] Enzer, G. (2011, September 18). UAE faces high rates of cyber-crime: 1.4m UAE residents have been affected by online crime in 12 months. Retrieved April 6, 2015, from http://www.itp.net/586180-uae-faces-high-rates-of-cyber-crime

[8] Gaskell, H. (2015, March 18). UAE is top-two victim of regional cyber attacks: Country is second most hit victim in the Middle East and 15th worldwide. Retrieved April 8, 2015, from http://www.itp.net/602495-uae-is-top-two-victim-of-regional-cyber-attacks

[9] Gercke, M. (2012). UNDERSTANDING CYBERCRIME: Phenomena, Challenges and Legal Response. Retrieved March 12, 2015, from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime legislation EV6.pdf

[10] Malek, C. (2014, April 3). UAE calls for stronger cybercrimes laws. Retrieved March 12, 2015, from http://www.thenational.ae/uae/technology/uae-calls-for-stronger-cybercrimes-laws

[11] Menting, M. (2015). Academia.Edu. CybercrimePPT. Retrieved April 10, 2015, from http://www.academia.edu/217243/Cybercrime_PPT

[12] Moukhallati, D. (2014, April 28). Cyber crimes in Dubai nearly double in 2012. Retrieved March 11, 2015, from http://www.thenational.ae/uae/cyber-crimes-in-dubai-nearly-double-in-2012

[13] Moyenorient3. (2014, March 11). United Arab Emirates: Tracking “cyber-criminals” Telecommunications Regulatory Authority and cyber-crime units. Retrieved March 13, 2015, from http://12mars.rsf.org/2014-en/2014/03/11/united-arab-emirates-tracking-cyber-criminals/

[14] Mustafa, A. (2012, November 13). Cyber-crime law to fight internet abuse and protect privacy in the UAE. Retrieved April 13, 2015, from http://www.thenational.ae/news/uae-news/cyber-crime-law-to-fight-internet-abuse-and-protect-privacy-in-the-uae

[15] Mustafa, A. (2012, November 13). Cyber-crime law to fight internet abuse and protect privacy in the UAE. Retrieved March 13, 2015, from http://www.thenational.ae/news/uae-news/cyber-crime-law-to-fight-internet-abuse-and-protect-privacy-in-the-uae

[16] Noorhan, B. (2014, May 31). Most common cyber crimes in UAE are fraud involving money and extortion. Retrieved April 12, 2015, from http://gulfnews.com/news/uae/general/most-common-

cyber-crimes-in-uae-are-fraud- involving-money-and-extortion-1.1341312

[17] Nykodym, N. (2005). Criminal profiling and insider cyber crime. Retrieved March 12, 2015, from http://www.sciencedirect.com/science/article/pii/S1742287605000915

[18] Princeton. Education. (n.d.). What is a Primary Source?. Retrieved May 12, 2015, from http://www.princeton.edu/~refdesk/primary2.html

[19] Sagepub. (n.d.). The Research Process. Retrieved April 12, 2015, from http://www.sagepub.com/upm-data/44129_1.pdf

[20] UAECyber. (n.d.). UAE Federal Cyber Crime Laws. Retrieved March 12, 2015, from http://uaecyber.com/en/about/government-initiatives/uae-federal-cyber-crime-laws/

[21] VBTUTOR. (2013). Chapter 7: Data Collection. Retrieved April 3, 2015, from http://www.vbtutor.net/research/research_chp7.htm

[22] Wam. (2012, November 14). New UAE cyber crime laws: Jail for indecent posts. Retrieved March 17, 2015, from http://www.emirates247.com/news/government/new-uae-cyber-crime-laws- jail-for-indecent-posts-2012-11-14-1.482836

[23] Wyse, S. (2011, September 16). What is the Difference between Qualitative Research and Quantitative Research? Retrieved April 13, 2015, from http://www.snapsurveys.com/blog/what-is-the-difference-between-qualitative-research-and-quantitative-research/

[24] Wyse, S. (2014, October 29). Benefit From 3 Types of Survey Research. Retrieved April 12, 2015, from http://www.snapsurveys.com/blog/benefit-3-types-survey-research/

[25] Wyse, S. (2014, October 29). Benefit From 3 Types of Survey Research. Retrieved March 17, 2015, from http://www.snapsurveys.com/blog/benefit-3-types-survey-research/