International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Digital Social Engineering Threatens Cybersecurity

Hassan Mustafa

Abstract*: This study aims to explore the role of social engineering in threatening cyber security by clarifying the concepts related to social engineering and its seriousness due to unlink to devices and equipment in general and its dependence on addressing the human psychic mechanisms known for curiosity. The study is based on the descriptive analysis studies that were based on the survey methodology using the questionnaire as a data collection tool, which was distributed to 98 respondents. The study found that the majority of the respondents had no idea about social engineering, and many of the females were rapidly clicking the links.. The study found that m these links can be attractive. The study found that there are significant differences between digital social engineering and hacking of phones and computers..

Keywords: Social Engineering - Cyber Security - Social Networking - Hacking - Interactive Links- digital social engineering.

I. INTRODUCTION

A new digital media, which were the result of a huge technical and technological revolution, impersonate one of the channels that create Social Networks for users. The world became as a small village. Not only, Northern People can meet easily with Southern People, but also, Eastern People can meet easily with Western People. Social networks became such as fruit of the information revolution, and one of the faces of the new media that is consistent with the paths of development and progress. Social networks shall meet the requirements of the modern digital age, which became available to all after the spread of smart phones and multiple applications that vary and be different in characteristics. But, human beings are familiar with different trends in how to use Social Networks in evil and good. This study aims to uncover the role of social engineering in threatening cyber security through the exploitation of human motivation to achieve illegal aims. So, we are focusing here on social networks as the easiest in the technical hacking needed by the hacker to reach the victims' devices.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Dr. Hassan Mustafa*, Dean, Department of Mass Communication, Al Falah University, Dubai, UAE.

II. METHODOLOGY

2.1 The theoretical framework:

The theoretical framework is a number of procedures and steps that the researcher study a group of hypotheses or theories and the researcher depends on it in his studies. This will be in a logical and sequential framework, in order to understand the study, and analyze the results that he has been obtained. It is known that there are many theories and models that related to the study of communicative thought and the relationship between variables. Theories and models reveal the impact of the media, and the satisfaction and needs that achieved by media. In this study we depend on satisfaction and needs entrance, for its importance and its role in the field of media research in general, whereas the interest to disclose satisfaction and needs began by the recipient through (traditional) media since the beginnings of experimental researches in the forties. The experimental researches extended to the impact of new digital media possible.

Original Approach for Uses & achieved Gratifications is considered as one of the approaches and theories that emerged in the 1940s as an extension of media theories about selective influence when the idea of the limited impact of the media is cleared to public. Researchers and scientists focused on identifying knowledge motivations of the public, and monitoring the capacity and potential of different media. In order to meet the needs and Gratifications of the public, according to what mentioned above; Original Approach for Uses & achieved Gratifications is created to rely on measuring the degree of interaction between media and public. Those means choose the public in a selective way, regardless Random exposure. Whereas, in digital media, there are many communication tools such as WhatsApp, Face book, Tweeter and other communication applications that are used geometrically and technically to penetrate devices. Original Approach for Uses & achieved Gratifications appeared for the first time in 1944, through an article entitled "Motivations and Gratifications for listening to the daily series" by the Sociologist HARZOG, through which she conducted a number of interviews with a number of listeners of the daily series, whereas, listeners reach to 100 listeners. In 1959 G, Sociologist HARZOG concluded that there is a group of Uses & achieved Gratifications. Furthermore, Researcher Katz raised the importance of changing the patterns of communication research, and looks forward to study how the public people deal with the means of communication instead of talking about the means of communication's effects.

Researcher Katz ensures the importance of researchers' changing to study variables that play an intermediary role. Moreover, in 1974, through the book "The use of public means of communication " by researchers ELIAHU KATZ and J. BLUMLER, where the idea of the book revolves around two axes; the first axe is functions and roles that have been played by the means of communication and its contents. The second axe; the individual motives of the recipient of exposure to the means of communication (MURAD, 2011).

2.2 The Importance of Study

The importance of this paper comes from the importance of social networking sites, applications, cyber security and various cyber-attacks received by cyberspace, which has become today the first threat on the personal and national level of States, especially the cyber-attacks, fraud and abuse led to increased risks of theft the world today. As people around the world increasingly rely on modern technology, they are increasingly vulnerable to cyber-attacks such as corporate security breaches, phishing, extortion, fraud and social media fraud. We observed that Cyberspace and its underlying infrastructure are vulnerable to a wide range of threats from electronic threats and physical hazards. Electronic authorities, as well as powerful states, exploit the weaknesses of their opponents to steal their information and money and develop capacity to disrupt, destroy or only threaten the opponent's ability to meet basic services. Moreover, there are a wide number of traditional crimes are now being committed through cyberspace, including the production and distribution of child pornography and juveniles, conspiracies of exploitation, banking and financial fraud, intellectual property violations, most recently crypto currencies and other crimes, all of these crimes have significant humanitarian, economic and legal consequences. The threat of cyber security leads to economic breakdowns and the creation of international conflicts. Cyber security today is an essential part of any international defense security policy. Every country around the world has dedicated cyber war departments and facilities within national security teams to reduce cyber risks.

2.3 Goals of the Study:

- Identify the role of Social Networks as a bridge to penetrate the various devices.
- Access to the most important forms of cyber security threats of Digital Social Engineering.
- Identify Social Networking Applications and websites most vulnerable to cyber-attacks.
- Identify the impact of cyber-attacks.
- How to raise the level of knowledge awareness.

2.4 Study Approach

The study requires the use of the descriptive analytical strategic approach to start with describing the problem to diagnose and then clarify it to be understood and then interpreted and finally guidance in the proper framework, in practice, follow-up, observation and practical experience of the researcher.

2.5 Study Society

The Society of the study consisted of a random sample consisting of (102) respondents, which included mostly university students due to their young age and that they are the most used groups for these platforms.

2.6 Data Collection Tools

This study is based on the Questionnaire as a data collection tool, in addition to conducting a number of personal interviews. The researcher also analyzed the contents of some messages in social media platforms through personal experience and practical experience in the field.

III. LITERATURE REVIEW

3.1 Social networks (Origin and Development)

During the information revolution that spread in all over the world, and the technical and technological development that made smart phones and small media tools easy to use and able to bring all the news from all over the world in your hands, this information revolution, has been brought major changes, and created a new communication environment, consisting of a number of contexts, paths and transitions to serve the receiver.

Researchers define social networks as a system of electronic networks that appeared on the global information network in 2004 G, which appeared as a result of the need for the nature of the knowledge age and Globalization, and intellectual exchange between different parties and peoples, and to meet the need of individuals in the acquaintance and exchange of experiences, cultures and perspectives points of view with users from different countries of in all over the world may participate in the desires, hobbies and interests, all of these things are listed under the word of (Al Wasl), which means communication, collection, passion and non-abandonment (Ibrahim Mustafa et al.: 2004 G). The Internet and these interactive pages (including but not limited, WhatsApp, Face book, and Tweeter) provide a huge amount of ideas that can be converted to stories, news, advertisements and other templates and forms of media and information, which may be a part of life for individuals and groups that could be employed, and the most important topics to a specific public to explore his desires and what interests this specific public. And then these topics are exploited to gain Illegal money.

3.1.1 (Face book):

Face- Book application was founded by young man called (MARK ZUCKERBERG), Face- Book is a website where a group of individuals meet for the purpose of networking individuals in the acquaintance and exchange of experiences, cultures and perspectives points of view with users from different countries of in all over the world, and this site started from the Harvard campus when (MARK ZUCKERBERG) designed a website that serves university students to exchange information and acquaintance. The latest Statistics of the World Digital Report in 2018 G show that the number of Face- Book users reached more than 2 billion (Global Digital Report: 2018).

3.1.2 (Twitter):

Twitter is one of the most popular social networks and social media in the world, offering a Micro blogging service that allows to its users to send tweets that will get a re-tweet and / or admiration for other tweets, up to a maximum of 280 characters per one message. This shall be made directly throughout Twitter or by sending an SMS, instant messaging programs, or applications provided by developers such as Face- Book and others. These updates appear on the user's page, friends can read these updates directly from their homepage or visit the user's profile.

Users can receive responses and updates throughout an e-mail, RSS feedback and SMS messages using four service numbers in the United States of America and Canada and India in addition to the international number that all users around the world can send through it in the UK. Twitter has been available in Arabic since March 2012, and (tweets) are plural of (tweet).

Twitter was founded in March 2006 G by JACK DORSEY, NOAH GLASS, BIZ STONE and EVAN WILLIAMS (Wikipedia: 2019) and was actually launched in July of the same year (2006 G). The site has become very popular in all over the world, by 2012 the number of users exceeded 100 million users publish more than 340 million tweets per day, while the search query service reached to 1.6 billion per day and increased its popularity significantly during the United States of America presidential elections 2016 where the site proved Indeed, which it is the source of urgent news, where more than 40 million tweets related to the elections were published until 10 pm Eastern Time. The number of participants according to the latest statistics about 330 million users (Global Digital Report: 2018).

3.1.3 (WhatsApp):

WhatsApp is a multi-platform instant messaging application for smart phones, in addition to basic messages users can send pictures, voice messages, video and multimedia.

WhatsApp was founded in 2009 G by American BRIAN ACTON and UKRAINIAN JAN KUM (also CEO), and both former Yahoo employees, it is located in Santa Clara, California.

WhatsApp is competing with a number of Asian messaging services such as KAKAO TALK, LINE and WE CHAT. Furthermore, one of the advantages of using whatsApp, there are ten billion daily messages were sent to WhatsApp just in 2012 G. It also increased 2 billion in April 2012 G and 1 billion last October. Moreover, WhatsApp announced on Twitter on 13 June 2013 that their new daily records had reached to 27 Billion messages. Face- Book Company bought WhatsApp on 19 February 2014 for 19 billion USD. (Wikipedia 2019).The number of users of WhatsApp application until 2018 exceeded 1.5 million users in about 180 countries to be the most used application of instant communication applications (Global Digital Report: 2018), which has some features that can be summarized in the following:

free

Diffuse

Easy to use

Can use multimedia (Texts - Images - Audio - Video - Drawings - Emoji - Stickers).

Possibility of text, voice and visual communication.

Groups system

Means of information (links)

Alerts and updates

These means have developed day by day and have become a pressing and urgent humanitarian need.

The new media or the new media reality, which imposed by the revolution of information, technically and technologically, is the product of the development and progress of the modern age. The new real life has produced a number of phenomena and challenges that had to be identified and analyzed before they worsen and be negative, until will be difficult to address in the future.

One of these transmissions is the following (ABBOUD, 2015):

The appearance of a number of professions and media jobs that are based on knowledge of the use of modern technologies and information networks portals for use in the purposes of penetration and digital blackmail.

The kind of spam links and penetrations.

Lack of monitoring on global Internet networks, which contributed to spread wrong information and false facts.

From this point of view, many specialists and researchers focused on monitoring the negative effects of the use of modern technologies and smart phone applications, especially social networking sites that have become a daily routine used by many of the most important of these effects are threats to cyber security.

3.2.1 Definition of cyberspace cyber security

There are several overlapping definitions of the concept of cyberspace cyber security, but we are use only what serve the purposes of research. One of these definitions is the International Telecommunication Union (ITU), which defines as systems and services that are directly or indirectly connected to the Internet, telecommunications and computer networks (FREDERICK WALAMA: 2012).

Some of people describe the concept of cyberspace cyber security as the fourth arm of modern armies next to the air forces, naval forces and land forces, especially that the Internet witnessed the beginning of talking about real battles that taking place in this virtual world (ABBAS BADRAN: 2010).

Some of people describe the concept of cyberspace cyber security as a hypothetical world that is overlapping with our physical world, which is complexly influenced by it, where the relationship between the two worlds is based on an integrative vision that contents with advantages and ongoing risks (DAVID BELL et al., 2004).

It is clear from these definitions that cyberspace cyber security is an operational field, which is the fifth field of modern warfare after the field of land war, air war, sea war, space and cyberspace, not only on the Internet, but also on other global and private networks such as: GPS / Acars / Swift / GSM / pstn.

We observe that both last definitions have focused on the risk of the negative use and exploitation of this cyberspace by threatening others.

3.2.2 Cyber security:

The overlapping of concept of cyberspace is similar to overlap the concept of cyber security, which includes a number of different definitions, including "cyber security largely consists of defensive methods that used to detect and frustrate potential hackers." (KEMMERER: 2003).

Amoroso (2006) defines it as the ability to reduce the risk of harmful; attacks on programs, computers and networks. This includes tools used to detect Disassembles process, stop viruses, forbidden access to malware, enforce authentication, enable and operate encrypted connections. "

International

Telecommunication Union (ITU) defines cyber security as a group of tools, policies, security concepts, security assurances, guidelines, risk management approaches, procedures, training, best practices, safeguards and techniques that could be used to protect the cyber environment and the assets of users. (International Telecommunication Union (ITU) 2009). We observe in this definition that it is not limited only to technical aspects, but even included policies and procedures, which is a broad, comprehensive definition.

Some people may confuse between the concepts of information security and the concept of cyber security, but there is a difference between the concepts of information security and the concept of cyber security because information security aims to protect computer systems from illegal access to them, or tampering with information during storage, processing or transport, which includes everything that may protect the ((information) that shall be in a computer system, or may not). It is concerned with huge areas, such as encryption, storage, physical insurance, security standards and information security and risk management. So cyber security is a part of information security.

The objectives of cyber security can be summarized in the following info graphic:

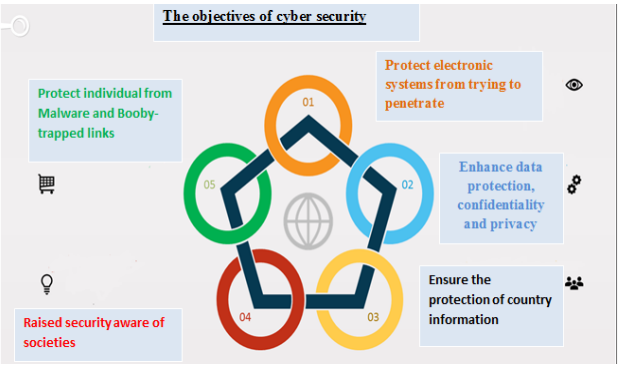


Figure (1)

IV. THE CONCEPT OF DIGITAL SOCIAL ENGINEERING

The term of Social Engineering basically related to the humanities and at the same time participates in the concepts of information security. The term of Social Engineering refers to the psychological manipulation of people in conducting business or disclosing confidential information. Deceiving trust for the purpose of gathering information, fraud, or access to the system the term of Social Engineering differs from the traditional "Deception" because it is often one of several steps in a more complex fraud system (Anderson, 2008). This definition may be summarized by using the art of extracting information (The art of debriefing) from people to get confidential information. This is the definition of the general concept of Social Engineering and added to my own concept, which is the digital part of the subject and I claimed the following definition: (the art of exploiting people's curiosity to obtain confidential information through electronic links in various forms through social media platforms to penetrate the target devices).

Digital Social Engineering focuses primarily on curiosity and surveillance for people by sending links in attractive forms such as images or texts that aroused feelings and provoke them to click on these links and then download the malicious files in the target machine. In this case, the device will link and communicate with the hacker's device to begin blackmail process and other processes.

This may be self-motivated and may be to achieve more dangerous aims for national security.

4.1 Methods and tools used in Digital Social Engineering

Digital Social Engineering could be used as a tool to achieve purpose that threats personal or public cyber security, including:

4.1.1 Internet Websites:

Victims are exploited through websites by exploiting their desire to spy on others, especially through the application of (WhatsApp) and the following image is a clear example of such sites (wt-spy, 2019) and using words and phrases that arouse the desire of the victims.

4.1.1.1 Site I: Spy on WhatsApp

Image No (1)

Through this site, the possibility of spying on any device with WhatsApp is announced through the number only and may be for personal or national purpose, the fraud is the victim, hacker seeks to spy by stealing the victim financial information or credit directly, or extorted later after clicking on the link Download the application on the victim's device and then hacker threats to publish private photos or financial information or extortion to provide sensitive information about the state or job or government institution that works or even private, leading to a threat to national security in such cases.

4.1.1.2 Site 2: know the identity of the owner of the phone number (hawiyyah, 2019)

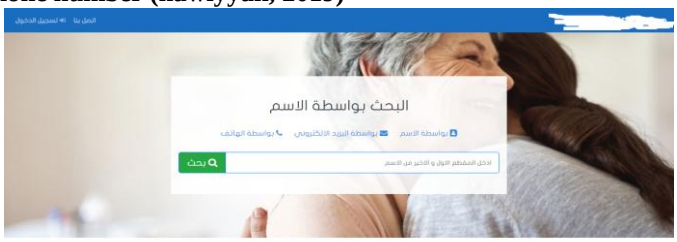


Image No (2)

This site claims that it knows the details of the identity of any person only through his phone number or name or e-mail, and after entering the data it will be considered as illusion that the search is underway and then a page with evidence is camouflaged and will not appear until after payment of a certain amount through Visa Card, and this will be a fraud as one of the methods threats to cyber security by the continuous access of the victim's financial card, and even if the victim had stopped the visa card, at least hacker has been taken the first amount, and if we collect the number of victims, the amount would be large.

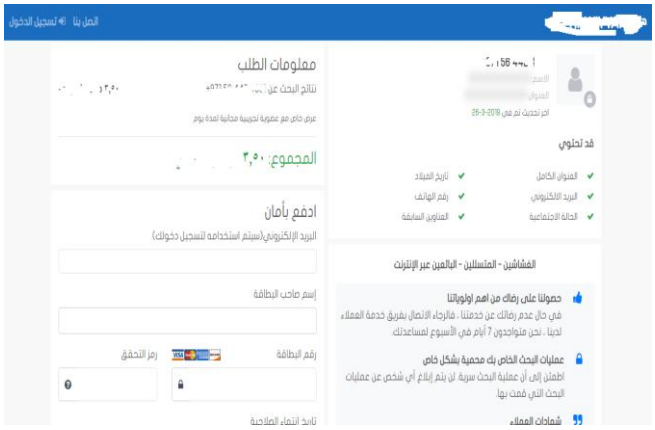


Image No (3)

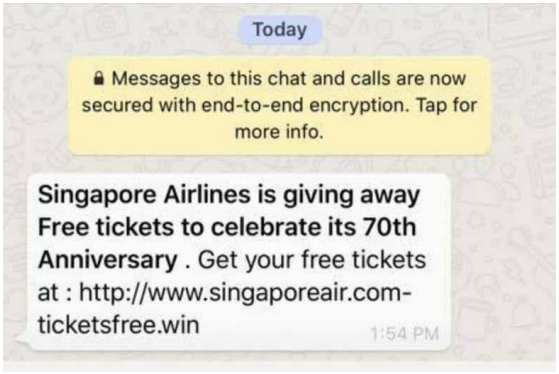
4.1.2 WhatsApp Messages:

It is the most general and the most dangerous among the social media platforms in the form of a fake message from the crook to your e-mail or your WhatsApp account bearing the identity of the WhatsApp in its form, color and address, reminding you that you have an unread voice message or the like topped by the application logo for more credibility. The message includes malware tracking that contains a file that installs itself after clicking on it without knowing where it was installed and how to delete to work in the background to continue what you do on the device to the moment when he can grab what important financial or personal data, he can blackmails you, and Extortion may be personal for money or other, and may be greater in relation to the security of States, such as seeking to get sensitive information about the employer or some other parties, and may also be through the recruitment of some terrorist organizations or even some countries and come in various forms Many of them are:

Winning cars, winning tickets, job applications, marriage applications, deciphering magic and work, expanding livelihood and many more as shown in the following pictures:

Image No (4) (YouTube 2017)

(**Image No (5) (Al Ittihad Newspaper, 2018**



(image no 8) (**2019 ، straittimes**)

(image no 7) (**Oman Network, 2018**)

4.1.3 Danger of Cyber Security Violation

The danger is not limited to members of society, but also to the national security of countries where these concepts have changed from just theories to practice. In 2011, the Defense Advanced Research Projects Agency (DARPA) announced a program to improve the Department of Defense's understanding of what is happening on social media sites, as well as Cyberspace attacks have increased in a variety of ways to threaten vital sectors in most countries, as part of their knowledge of the use of these sites to broadcast media messages that serve their strategic interests (Washington blog, 2011). In the report of the company (i.e. Free Eye) issued in 2019 that the Middle East suffered attacks, including sectors: Defense, Energy, Foreign Affairs, Justice Institutions, Media and Electronic Government Services.

In 2018, the Middle East region saw a 17% increase in malware attacks to half a million attacks, according to Kaspersky Lab's KSN network.

We do not forget a vital factor in this increase, which is the growing interest in crypto currencies, which has become a more attractive target for cyber criminals in all over the world, especially the attempts to track them are very difficult, which led to a rapid increase in advertising and malicious links to crypto currencies, Kaspersky Lab recorded a four-fold increase Crypto mining attacks in the region, rising from 3.5 million in 2017 to 13 million in 2018 (Middle East Business, 2019).

4.1.4 The most dangerous types of cyber threats:

The following diagram from the famous Statist website (statista, 2019) reflects the different forms of cyber security threats in different forms but is essentially the same: putting a file in the target device for transmitting process.

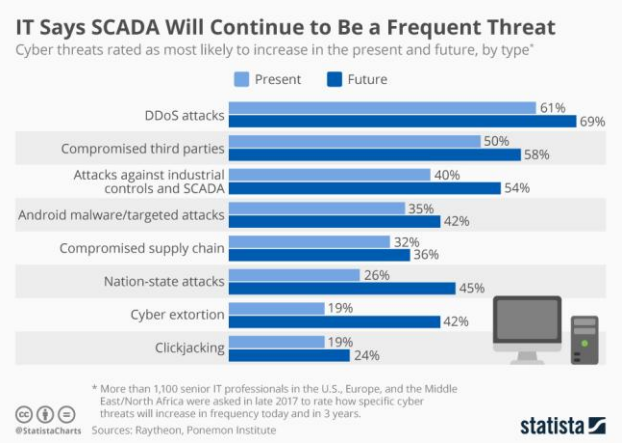


Figure (2)

We observe in the diagram of the total types (malware in Android devices), the operating system of mobile phones most widespread in the world, which confirms what we obtained to exploit Digital Social Engineering in the cultivation of these malware through the many booby-trapped links

Crypto jacking

I started with crypto jacking because of its seriousness and modernity as an emerging online threat as it began to explode by the end of 2017, crypto jacking became more active in 2018, especially with the rise in the value of crypto currencies. "It adopts a hiding mechanism in a computer or mobile device and uses the resources of the device to" extract "forms of funds throughout it. Crypto jacking can control to web browsers, as well as compromise all types of devices, from desktops and laptops, to smart phones and even network servers (malware bytes, 2019). Crypto jacking uses Digital Social Engineering and people's passion for getting extra money through advertising that aroused the reader to the possibility of making profits from home in one week or a month and then fill these links to malware, which hacking various devices and begin bargaining operations or destroy vital information.

V. RESULTS

- The majority of social media users are not sufficiently aware of the threats to cyber security in general, and Digital Social Engineering in particular.
- Social media platforms and instant messaging applications are the best place for Digital Social Engineering in implementing cyber-attacks.
- Pioneers of social networking platforms and applications of instant communication contribute in the spread of booby-trapped links by passing messages directly without verification, by adopting digital social engineering in the reliability of friends among them.
- Cyber-attacks are not limited to individuals only, but effect on countries and effect on the total economy.
- Awareness of cyber security remains weak compared to the recent spread of cyber threats.

VI. DISCUSSION

This study was based on a sample of users of social media platforms and the sample was 102 respondents.

Number of study sample individuals analyzed: 98

The actual Number of study sample individuals: 102 persons

Number of excluded questionnaires: 4 questionnaires

Reason for exclusion: The existence of incomplete data within the questionnaire, and the appropriate limit was reached for the sample frame.

sex	Number	Percent
Male	63	64%
Female	35	36%
Total	98	

Data refers to male respondents are more than female respondents, where males respondents percent are 63%, but females respondents percent are 36%

Distribute of sample individuals

Class	Number	Total Percent
(20-25)	29	30%
(26-30)	64	65%

More than 30	5	5%
Total	98	

Class represent from 26 to 30 age (ages of individual samples) the most percent, which is 65% "youth ", but persons, who older than 30 years old are the lest percent which is 5%

Distribute of sample individuals according to marital status

Class	Number	Total Percent
Single	29	%30
Married	68	%69
Divorced	1	%1
Total	98	

The results clarify that 69% of the respondents are married while 30% are single for only one divorced case. This is another indication, perhaps in other studies showing preoccupation with social media sites, but it is also an indicator of the passion for additional income, which makes this group vulnerable to digital social engineering attacks with advertisements for extra earning.

Ownership of identifiers (accounts) on social networks for all sample members:

The data indicate that the number of people who have identifiers (accounts) on social networking sites reached 100%, which is a predictable and accepted result, if not using social platforms, communication platforms such as WhatsApp and I do not think that one of us does not have such an application or other.

Class	Number	Total Percent
Yes	98	100%
No	0	0%
Total	98	

Second: Accounts Data

The percent to male and female that have accounts in social networks

Sex	Number	Total Percent
Male	50	51%
Female	48	49%

The results indicate a significant gender convergence in the use of social media platforms.

Applications that sample of individuals (respondents) are keen to use:

WhatsApp is the most used application by sample of individuals (respondents), which their percent reach 60%, followed by both Instagram and Twitter YouTube, while Facebook is the least among the proposals applications put forward in the questionnaire, perhaps this is because young people prefer Instagram more than Facebook because of the new features that Instagram offers, Note that citizens of the Gulf countries do not prefer to use Facebook applocation unlike residents in the Gulf. The sample of individuals (respondents) shows 18% of all sites, Snapchat in the first place. Note that WhatsApp is a communication platform. Note that the sample of individuals (respondents) has more than one account on different applications.

Network	Number	Total Percent
(Facebook)	25	26%
(twitter)	51	52%
(WhatsApp)	59	60%
(YouTube)	44	45%
(Instagram)	52	53%
Other	18	18%

Devices used by respondents to browse social networks:

The results of the study reached a number of samples of individuals (respondents) to use smart phones and mobile device to browse social networks by 90%, which is high but expected, and thus facilitate the use of Digital Social Engineering to spread the means used. Note that the samples of individuals (respondents) have more than one device for browsing.

Mean	Number	Total Percent
PC	30	34%
Laptop	28	31%
Smart phones and smart device	80	90%

The number of hours spent by the samples of individuals (respondents) daily to surf social networks:

Duration	Number	Total Percent
Less than an hour	10	10%
From one hour to two	39	40%
From three hours to 4	36	37%
From four hours or more	13	13%
Total	98	

40% of the samples of individuals (respondents) spend one to two hours per day to browse social media networks, 10% of the samples of individuals (respondents) spend less than an hour, 37% spend 3-4 hours per day and 13% of the samples of individuals (respondents) spend more than 4 hours per day. This is an indication of the addiction of these platforms, which increases the risk of cyber security and the need to raise awareness of it. The samples of individuals' (respondents) shall be aware of Digital Social Engineering Risks and cyber security threats:

It is clear from the previous schedule that the percentage of those who do not realize the seriousness of Digital Social Engineering and cyber security threats are the highest and most, followed by those who answered we don't know and it is also listed under the ignorance of the seriousness of these threats, which requires the need to intensify and increase doses of knowledge awareness.

Duration	Number	Total Percent
Yes	19	19%
No	42	43%
I don't know	37	38%

Click on links in Social Media Messages (Digital Social Engineering):
The samples of individuals (respondents) who clicked directly on the links in the messages in the different platforms were equal to the samples of individuals (respondents) who sometimes clicked, while the lack of direct compression was low, it is considered an indicator that reflects the great ignorance of the sample's cyber security. It is also linked to Digital Social Engineering, it cleared that the majority don't care about clicking on links under any particular name or form

Duration	Number	Total Percent
Yes	37	37.5%
No	24	22%
Sometimes	37	37.5%

The pursuit of attractive messages on the social networks of the respondents (Digital Social Engineering) .

Sex	Yes	No	Sometimes
Male	32%	45%	31%
Female	68%	55%	69%

We observe that females are the majority in the pursuit of attractive messages, and this means high instinct love curiosity, exploit emotion as well in such Booby-Trapped Messages and whether the attackers do through digital social engineering by sending curious messages such as what mentioned at the beginning of the study, or related to females Specifically like weight loss or cosmetic messages.
The samples of individuals (respondents) were exposed to some forms of cyber threats to the samples of individuals (respondents):

Number of Followers	Number	Total Percent
Male	78	80%
Female	20	20%

The percentage of persons that exposed to some forms of cyber threats reached 20%, while 80% of persons don't expose to some forms of cyber threats.
Topics covered by social media samples of individuals (respondents) (Digital Social Engineering):

Topics and Political issues	**14**	**16%**
Economic and marketing topic	11	12%
Educational topic	17	19%
Youth topic	16	18%
Social topic	12	13%
Technical and cultural topic	2	2%
Religious topic	14	16%
Sports and healthy topic	4	4%

Political, youth and social issues consists of the largest share of the concerns of the samples of individuals (respondents), while religious issues are the lowest by only 2%. Health, sports and economic and marketing issues accounted for 16% each.

Here, one can infer the possibility of exploiting such sensitive topics through digital social engineering in general as a trap for booby-traps.
The samples of individuals' (respondents) contribution to increasing the spread of cyber threats by passing messages (digital social engineering):

Method	Number	Total Percent
Direct exercise without verifying of message	80	82 %
Firstly, verifying of message	9	9%
I don't know	9	9%

This is clear by the direct passing of messages without verification, which contributes to the spread of these booby-trapped links, especially in different sets, and this is an important aspect in knowing the psychology of victims through Digital Social Engineering knowing their speed in passing without verification.
The extent of trust of the samples of individuals (respondents) in social networks

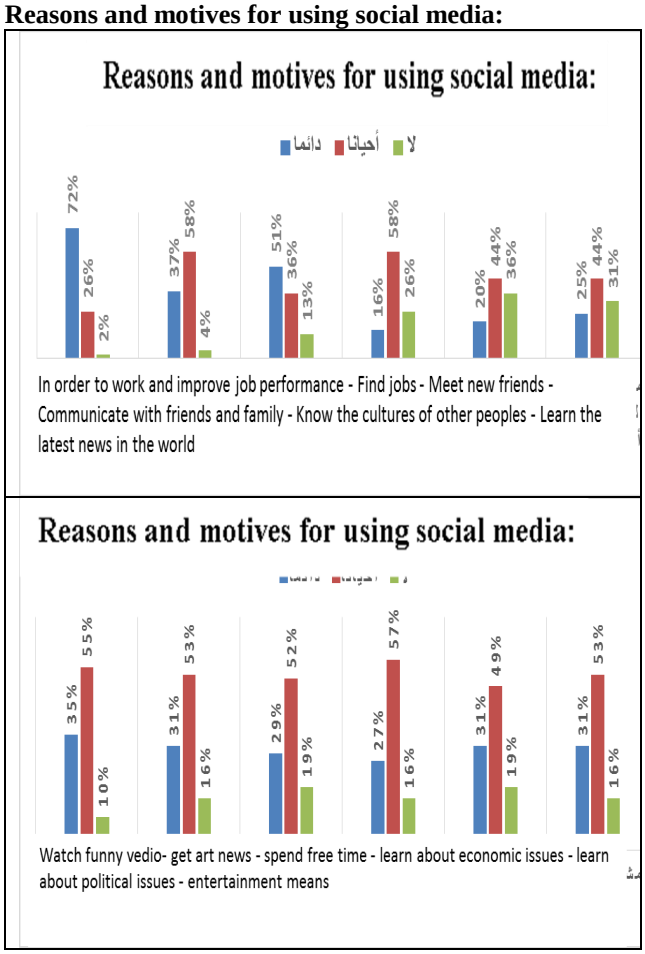
Answer	Number	Total Percent
Yes	9	9 %
No	14	14%
Sometimes	75	95%

There are 77% of the samples of individuals (respondents) sometimes trust in social networks, while only don't 9% trust in it. This small percentage may be the cause of poor participation, and it is considered as an indication that these networks are still suffering from security breaches, these security breaches do not make users of social networks trust in it The extent to which social networks contribute to enhancing awareness of the dangers of cyber security threats:

Answer	Number	Total Percent
Yes	43	44 %
No	12	12%
Sometimes	43	44%

Respondents were equally opinionated on the extent to which social networks contributed to enhancing cognitive awareness of the dangers of cyber security threats by 44% of those who said "**yes**" and 44% of those who said "**sometimes**", while 12% said "**no**". This large percentage of those who answered yes or sometimes reflect the respondents' belief that social networks can be a security fence, as well as a security gap, by positively beneficial awareness

Reasons and motives for using social media:



It is clear from these tables that the knowing news and developments comes first followed by communication with friends and family and then to identify different cultures and entertainment and entertainment, and that the pursuit of the job came in a significant proportion and all are exploited using Digital Social Engineering, such as links to identify the strange marriage habits in African or other countries, or by explaining what happened to a politician or celebrity, or electronic games.

VII. CONCLUSION AND RECOMMENDATIONS

Through the study's findings, the researcher recommends the following:

A. There is a lack of awareness about the cyber dangers in Arab countries..

B. There are many influencers being used by attackers through their accounts,.

C. The public opinion need more information and awareness messages,

D. The cyber Security is not only governmental responsibility and the private sector is not involved in the matter of national security issue,

E. Most of social media users are not updated about the cyber danger

VIII. RECOMMENDATIONS

a) Cyber security studies should be included in the curricula and systems of teaching in universities, and universities teachers shall encourage graduate students to research in this context, especially the concepts of Digital Social Engineering.
b) The necessity of enacting laws that are binding on Social Media Celebrities, even slightly limiting the use of their accounts in spreading threats.
c) Optimal exploitation of various media platforms and websites in order to enlighten Arab public opinion about the seriousness of cyber threats.
d) Encouraging the private sector to invest in safety systems.
e) Information about The need to follow the developments in the field of cyberspace.

REFERENCES

Arabic Reference
1. Ibrahim Mustafa, Ahmed Hassan Al-Zayat, Hamid Abdul Qader, Mohammed Ali Al-Najjar, 2004, the Intermediate Dictionary, Al-Shorouk International Library, 4th edition, p. 1037.
2. Shafik, Hassanein, 2007, the Journey of the News in Press and Visual News Agencies, Dar Al Fikr Al Arabi, Cairo.
3. Murad, Kamil Khurshid, 2011, Mass Communication and Media, Amman, Jordan, Dar Al-Masirah for Printing, Publishing and Distribution.
4. Abbas Badran, 2010 Electronic Wars: Engagement in a Changing World, Center for E- Government Studies, Beirut.
5. Aboud, Khalaf, 2015, Media and Migration to the Digital Age, Dar Al-Hamed for Publishing and Distribution, Amman, Jordan.
6. Mushtaq, Al-Naimi, 2018, fraud Information as one of Information Crimes, Halabi Legal Publications, Beirut, Lebanon.
7. Shloch, Noura, 2018, Cyber-piracy in the Cyberspace, "The Growing Threat to State Security," Babylon Center for Humanities Journal, vol. 8, no. 2, Algeria
8. Al Ittihad Newspaper, December 21, 2018
9. https://www.alittihad.ae/article/81471/2018/-%D8%A7%D9%84%D9%85%D8%B1%D9%83%D8%B2%D9%8A-%D9%8A%D8%AD%D8%B0%D8%B1-%D9%85%D9%86-%D8%B1%D8%B3%D8%A7%D8%A6%D9%84-%D8%A7%D8%AD%D8%AA%D9%8A%D8%A7%D9%84-%D8%B9%D8%A8%D8%B1-%D8%A7%D9%84%D9%88%D8%A7%D8%AA%D8%B3%D8%A7%D8%A8-

English Reference
10. Amoroso, Edward. 2006. Cyber Security. New Jersey: Silicon Press Global Digital Report in 2018, published on Jan 2019.
11. Dr. Frederick Wamala, THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE, 2011.
12. David Bell, Brain D. Loader, Nickolas Please and Douglas Sculer, Cyber Culture the key concept, first published 2004.
13. Kemmerer, Richard. A. 2003. Cybersecurity. Proceedings of the 25th IEEE, International Conference on Software Engineering: 705-715. http://dx.doi.org/10.1109/ICSE.2003.1201257
14. Internet websites
15. https://en.wikipedia.org/wiki/WhatsApp seen on 15 March 2019
16. https://en.wikipedia.org/wiki/Twitter seen on 15 March 2019
17. https://www.hawiyyah.com/en seen on 13 March 2019
18. https://middleeast-business.com/en/%D8%AA%D9%86%D8%A7%D9%85%D9%8A-%D8%A7%D9%84%D8%AA%D9%87% D8% AF% D9% 8A% D8% AF% D8% A7% D8% AA-% D8% A7% D9% 84% D8% A5% D9% 84% D9% 83% D8% AA% D8% B1% D9 % 88% D9% 86% D9% 8A% D8% A9-% D8% A7% D9% 84% D9% 85% D8% A7% D9% 84% D9% 8A% D8% A9 seen on 12 March 2019
19. https://www.malwarebytes.com/cryptojacking/ seen on 10 March 2019

20. https://www.statista.com/chart/17267/cyber-security-threats/ seen on 12 March 2019
21. https://www.straitstimes.com/singapore/courts-crime/singapore-airlines-warns-of-phishing-scam-promising-free-plane-tickets seen on 13 March 2019
22. https://twitter.com/OMN_4/status/995205570507563008 seen on 13 Mar 2019
23. http://www.wt-spy.com/homen.php?langar seen on 13 March 2019
24. https://www.youtube.com/watch?v=AkEJCebvGcY seen on 13 March 2019
25. Volume(issue), paging if given. Available: http://www.(URL)

AUTHORS PROFILE

Dr. Hassan Mustafa, Dean of Mass Communication at Al Falah University, Dubai, UAE
Publications:

- Books of (Introduction to Politics) ,(Introduction to New Media) ,(Digital Photography) , (Geopolitical in third Millennium and the role of New Media) , (Multimedia and Writing to New Media)

- ACADEMIC RESEARCHES AND CONFERENCES

2019

- The Efficiency of Communication Apps in enhancing Scientific Researches (peer review Researches Journal)
- THE ROLE OF STRICT LIABILITY IN CONSUMER PROTECTION AND THE NEED FOR ITS APPLICATION IN THE ADVERTISING FIELD (Social changes in the global world conference book), Macedonia.
- Impact of Artificial Intelligence on Smart Media Stations, Journal of Content, Community and Communication (SCOPUS indexed)
- Social Controller, AFU conference TASK 2019

2018

- Efficiency of Digital Marketing in growing Students small business Applied WhatsApp, AFU conference TASK 2018.
- THE Smart Techniques in Scientific Researches, Conference, Morocco.

2017

- Digital Citizenship, International Conference of Mass Communication, Morocco
- The Future Of Media (Smart Radio) – Presented at Media Studies Conference, Amity University, India

2016

- The Impact of New Media on Old Media, a Hournal of Bahry College, Sudan
- Information Technology in Education, Ajman Education & Training Conference

2015

- Using Multimedia in Education, The Gulf Teachers Forum Conference, University of Sharjah
- The Digital Technology in News – Sudan Radio Workshop
- The Informatics in Measuring the Public Opinion Workshop
- The New Media Technology Pre-Summit Workshop for Asia-Media Summit, Malaysia

2011

- The Digital Production and Archive in Sudan Radio, ABU Conference, India

2010

- The Digital Archive in Sudan Radio, ASBU, Tuni