International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 13, Issue 7, 2020

Social Media Networks Security Threats, Risks and Recommendation: A Case Study in the Kurdistan Region

Subhi R. M. Zeebaree[a], Siddeeq Y. Ameen[b], Mohammed A. M. Sadeeq[c],
[a,b,c]Duhok Polytechnic University, Duhok, Iraq, Email: [a]subhi.rafeeq@dpu.edu.krd, [b]siddeeq.ameen@dpu.edu.krd, [c]mohammed.abdulrazaq@dpu.edu.krd

It is well known that social media networks have a rapid growth in the number of users, since it is widely adopted as a way of communication, sharing knowledge, sharing thoughts, photos, videos, forming networks and many other features that attract more and more people worldwide. This increase raises the threats and risk consequences because of the lack of cyberculture among users. Moreover, the widespread use of the smartphone with such interesting applications, even for children, raises more problems and an urge for research to be conducted locally to avoid risks. Thus, the paper objective is how to increase the social media sites cyberculture in using social networking and deals with an electronic device such as the smartphone, since the investigation shows that the smartphone is the most widely used compared to others. The paper presents a review on social media sites and their usages together with threats and risks raised by such use. The paper also investigates the awareness of the people in the Kurdistan region about threats and risks through a questionnaire designed and conducted for such purposes. The results show that there is a threat to using social media networks with the need for training to avoid it. Finally, the paper put some recommendations for social media networks on how to reduce threats and risks when individuals share their information on the social media such as Facebook, Twitter, Instagram, snap chat…etc.

Key words: *Social Networking sites, Security, Privacy, mitigation techniques, Cyber Threats in Social Networking, Risks Prevention in Social Networking sites, Cyberculture, threats, risks.*

Introduction

Recently, the most common technology with daily usages by almost everyone is the Internet. With Internet technology, each person around the world even with very limited information technology experience, can communicate, information share, play, and many other uses of the Internet in an easy way and semi-free (D. Chaffey, 2019), (Zebari et al., 2018,Zebaree et al.,2019). One of these applications is used daily by almost all people in social media. Social media is a collection of Internet-based websites. The aim and function of social media are to promote the personal and business-focused interaction of individuals around the world (Edosomwan et al., 2011). Social media is a service that allow users to share contents. The contents are various types of information (messages, documents, videos) on a variety of topics. Moreover, the service also allows users to share new ideas, opinions, and thoughts with many people (McCarroll & Curran, 2013). There are many types of social media networks and services available today such as Facebook, YouTube, Twitter, Instagram, LinkedIn, and snap chat (A. Smith and M. Anderson, 2018).

In the last decade, social media networks, such as Facebook, Twitter, snap chat, YouTube, Instagram, have had a rapid growth in the number of users (E. Ortiz-Ospina,2019). This is because it is widely adopted, especially with the use of smartphone, as a way of communication, sharing knowledge, sharing thoughts, photos, videos forming networks and many other features that attract more and more people worldwide. Social networking sites can be valuable sales and marketing tools, as well as fun diversions. This is very clear from the global digital report of 2019 that shows that the number of internet users worldwide in 2019 was 4.388 billion, whereas is the number of social media users worldwide in 2019 was 3.484 billion, and the number of mobile phone users in 2019 was 5.112 billion. One of the interesting things found by the global digital report was that the social media users raised by 9% year-on-year whereas the number of internet users raised by 9.1% year-on-year. However, the study shows the differences in the level of usage in different countries and demographics. A study on the usage of social media in the state shows that the majority of USA social media users use Facebook and YouTube whereas the majority of the adults use snap chat and Instagram (D. Chaffey, 2019).

It worth mentioning here that social media networks have a constructive and destructive impact on users. One of the main constructive issues is social networking linking individuals and groups. The other most important constructive issue is the sharing of knowledge and can be considered as one of the valuable ways of learning and enhancing the culture of individuals, provided that the users' intention and awareness is looking at and targeting the right information (Abbas et al., 2019). Social impact is also worth mentioning here as it provides an easy way and almost all the time availability of websites one can access to improve users' psychology and avoid depression.

In summary, social networks' positive or constructive influences can be reflected on individuals', organisations' and even governments' development processes. An example of such positive influence is in Duhok Polytechnic University and even other universities around the world or schools; social media can develop and support the following:

- support, learning and educational processes,
- provide communication and collaboration to enhance the academic performance for both students and academics.
- Form communication groups in the university with certain issues such as a course team, programme team, project team, management team, between both students and academics.
- Form social networks as online learning platforms (LMS—learning management system such as Moodle.
- Many other applications that enhance higher education.

In spite of these constructive issues and many more, there are destructive effects. These include wasting time which might cause failure in school and universities, and social life such as marriage, employment, and many more destructive issues that need urgent investigation by researchers around the world to put solutions and reduce or eliminate such destructive issues (Abbas et al., 2019).

The increase in using the social media sites makes it a pool by cybercriminals and cybercrime. According to previous studies, there are several threats and security risks facing the users of social media or maybe the victims are organisations; among those most vulnerable to attack and threats, are those who do not have Internet usage culture (Alguliyev et al., 2018). This suggests that almost all social media sites have security risks.

Since the goal of social networking sites is to share personal information with each other, it will become a source of hackers. Those hackers or criminals are using shared information and connection to place an attack on users' accounts. With such an attack they used such sensitive and personal information, and user profiles through many ways that harm the user. They benefit from unaware poor cyberculture users together with user-friendly social media applications (Alguliyev et al., 2018). These risks can harm the individual or make trouble and problems to an organisation by compromising the organisation or stealing vital organisation information. The risks can also affect governments through its national security and economics. Therefore, everybody should have a certain level of Internet usage culture to be aware of illegal usages, threats and protection. It means using Internet applications with efficiency and not using it erroneously (Kumar & Somani, 2018). Every user of the Internet should know that any device connected to the Internet has an address known as IP address; by this address the hacker can access to devise data (Gupta et al., 2018). One of the most usages of the internet by people is social media (D. Chaffey, 2019). This can apply by determining

the risks and security threats that target the organisation. (Gupta et al., 2018). Furthermore, how to use these sites as an end-user in a safe way is essential with knowledge on documented policy that have been signed with the account establishment, and is very essential. This needs to be spread in communities, organisations and universities by a well-informed user that will work to educate the others on these issues and establish best practices that can be standardised and updated as applications (Oxley, 2011).

The study presented in this paper will investigate the threats and risks of using social media and their related factors. The aspects of this investigation are very serious and need to be investigated from different points of view, since its consequences are very serious to an individual, organisation and even country because of the number of users using these applications and social media nowadays. It can be said that almost all Internet users are social media users. Furthermore, governments around the world need also to pay attention to this serious problem and conduct forums with those responsible for the development of such applications to assure safe and secure usages. Finally, people living in the Kurdistan region need also to be aware of using such applications. Therefore, the study accomplished in this paper will also highlight social media usage in the Kurdistan region in Iraq and will show the difference from another part of the world such as Europe and the USA. Understanding these differences in popularity of different social networks is really important when targeting specific audiences.

Social Media Access and Usages

Generally, users can access social media services through web-based technologies using their personal computer or their mobile devices (smartphones) (D. Chaffey, 2019.). These accesses to social media websites require users to have an account or create their own accounts through certain verification and policy agreement. The verification requires special information about a person such as a phone number, email, address, current location …, etc. On the other hand, the goal of the social media policy is to set expectations for appropriate behaviour and ensure that users will not expose the social media providers to legal problems or public embarrassment. Such policies include directives on using the social networking website, as well as rules for what types of information can be shared (Taha et al., 2017). Almost all social media policies include restrictions on disclosing confidential or proprietary business secrets or anything that could influence others (Lough & Fisher, 2016). The incorrect use of social media could be facing the user to attacking or hacking, especially, the users who have no or limited cyberculture (Elm, 2008), (Chan & Virkki, 2014).

There are now more than 3.48 billion active social media users, which makes social media an unavoidable part of the life strategy. Users of social media networks can share various pieces of personal information with others as users upload their images, share their date of birth,

show their phone number and write their current address (Fire et al., 2014). Sharing personal data like this can contribute to data misuse. Some individuals, for example, share profile information including their full name, gender and telephone number and other sensitive information. . Hacking uses the social network account of one of the users, and the hacker can misuse details to blackmail the user (Norman et al., 2017).

When comparing the most popular social networks, it is best to review them by active account usage, not just by the number of user accounts. Studies have shown that some social networks are growing more rapidly than others while some are now in decline. Common examples of social media sites are Facebook, Twitter, Instagram, Snapchat and others (Rosen et al., 2013).

Facebook

Today Facebook is one of the most active social networks used worldwide. Facebook revealed in April 2019 that they have more than 2.38 billion active monthly users (C. Menlo Park, 2019). The network allows users to create profile pages where they can introduce themselves, sharing pictures and whatever they think about. Facebook also enables the use of different applications within the network, ranging from fortune cookies to messenger (Forkosh-Baruch & Hershkovitz, 2012), (Sarapin & Morris, 2015), (Sturgeon & Walker, 2009).

Twitter

Twitter is a website for Microblogging. The user can post up to 140 characters of short messages on his or her account. Other users can then subscribe or follow that person's page and receive their updated messages (M. Ahlgren, 2020). In the middle of 2017 Twitter handled around 750 messages per second, or around 65 million messages per day, with a steep growth rate (M. Ahlgren, 2019). Twitter reached 336 million monthly active users. This means that there are 6000 tweets every second. There is also 23 percent of the internet population on Twitter (M. Ahlgren, 2020).

Instagram

Instagram is a classic social media network service. In such media networks messages and ideas are exchanged between people. Mainly photo and video are shared in such a media network. It offers easy integration with video and hence is often used by any independent user to present their own idea (McCarroll & Curran, 2013).

Snapchat

Snapchat is a social media application used globally. One of the principal features of Snapchat is that pictures and videos are usually only available for a short time before they become inaccessible to their recipients. The application has evolved from originally focusing on person-to-person photo sharing to presently featuring users' stories of 24 hours of chronological content, along with discovering (G. Felix, 2014).

Social Media Cyberculture

At any instant, there will be huge number of social media users using the social media sites. Absolutely, those users have different levels of knowledge, skills and behaviour on using the social media sites (Kumar & Somani, 2018). In other words, not all of them have the same cyberculture. In this case, it is expected the threats that they face will be also different. Thus, it is essential to consider this in the review paper. There are attempts to classify the social media users according to many criteria since these criteria have an impact on social media threats of users (Alguliyev et al., 2018). In this review, we can classify the social media users and their cyberculture that depend on age, education qualification, civilisation or location.

Social Media Users' Ages

Social media is nearly used by each one in civilised countries, children, teenagers, youth, adults and the elderly. An example of such investigation shows that Facebook use is relatively common across a range of age groups, with 68% of those ages 50 to 64 and nearly half of those 65 and older saying they use the site. Other investigation shows that the largest demographic group of Twitter users are between the ages of 18 and 29 (37%). 25% of users are between 30 and 49 years old. LinkedIn is the social media network for professionals. It is expected that the level of threats will be different from each category as the following review shows (A. Smith and M. Anderson, 2018).

Adults are not interested to spend their time on social media because they enjoy traditional life. Some of them share all their information with each other without knowing who will see their information. Roughly two-thirds of U.S. adults (68%) now report that they are Facebook users, and roughly three-quarters of those users access Facebook on a daily basis. This category of users is facing threats and security risks (E. Ortiz-Ospina, 2019).

The youth category is the most frequent user's category of social networking sites and spends most of their time on the network as they do a lot of their work through social sites; also they use it for entertainment (E. Ortiz-Ospina, 2019). This category is more familiar with site policy and knowledge of how social sites are used. This category is targeted by hackers and

attackers because it is considered an important source of information; but they have the ability to save themselves (A. Smith and M. Anderson, 2018).

Teenager users are the most used to the reality of social media and they are the most vulnerable to hacks and threats because they do not have the information and culture sufficient to use these sites (E. Ortiz-Ospina, 2019). They may face many problems, especially girls, because they are an important source of information, especially in Eastern societies (AARON SMITH et al., 2018).

Children also use the social networking sites in a random way because they do not have the knowledge of how to use these sites and thus this causes problems that may lead to penetration of the device through which information can be obtained which may be a source of threats to parents (C. Menlo Park, 2019).

Social Media Users According to Qualification

As we explain there are many social media users, but not all of them have enough information to use social media. Some of them do courses or still studying in school, institute or college and others are uneducated (Kumar & Somani, 2018), (Gupta et al., 2018). In this case, we can classify according to qualification as the following:

Uneducated users with no qualifications at all or limited education such that they do not even obtain the primary school qualification: This kind of user may be labour workers in certain countries but now have the ability to use social media with the availability of the smartphone, especially the easy use and access of such devices and services.

Primary school qualification kind of users are usually children. Therefore they do not have cyberculture of using the Internet and social networking sites and have no cultural awareness. Perhaps it is an adult, but he/she did not complete their studies; they also are considered to not have the full electronic culture of the use of social sites and therefore are the most vulnerable to attacks on the communication sites of social media (Kumar & Somani, 2018).

Secondary school qualification categories are the most who use social media and have an interest in using social networking because they are teenagers (AARON SMITH et al., 2018). All the time they could be online; for these reasons they are faced with threats on social media and the hacker has targeted them (Gupta et al., 2018).

The university qualification have enough information about how to use the internet, and also should have a knowledge of cyberculture (C. Menlo Park, 2019). When they use social media

they know how to keep their accounting safe and any messages which may include a virus. The hacker and attacker have difficulties in threatening this kind of user (Gupta et al., 2018).

Social Media Users According to Location

Civilisation is different from one place to another. Therefore, the culture and behaviour of users are different from one place to another. Thus we can classify the users of social media depending on their location which represents the way to access and deal with the information on social media. In this case, we can divide this type of users into categories as illustrated below:

Civilised regions means all countries and cities that have all type of services like the internet and other technology (Chan & Virkki, 2014). It is well known that there are certain differences in cyberculture between users in different countries or even cities. Users in this civilised region should have full access to social media more than other locations and even their level of information literacy is much better than others. Users in this area are spending most of their time online and using most of the services available on the internet through social media networks. Therefore, they face threats and risks more than other ones (Chan & Virkki, 2014).

Remote region users mean the country or city that have limited access to all services of the internet or other technology. This kind of user may have two problems. The first, they do not have the cyberculture to use social media (Chan & Virkki, 2014). The second is that they have do not have an online service all the time and therefore they don't know anything about their accounts on social media when they are offline. For these two reasons, this kind of user is threated more than other ones (Chan & Virkki, 2014).

Social Media Sites' Threats and Risks

Social networks deal heavily with private information related to people, organisations and even governmental information. This makes such networks an interesting place to hackers, criminals and intruders to place their threats. A threat is a possible danger that might exploit a vulnerability to breach the security of users and therefore cause possible harm to users. Thus, privacy should be one of the major concerns with social media sites, of developers, governments, organisations, and even social media users. The aim of this threat, especially in social media, include stealing identity and personal information theft, from social media sites. Getting your computer or social profile hacked leads to loss or corruption of data or physical damage to the hardware and/or infrastructure. Knowing how to identify computer security threats is the first step in protecting computer systems.

Generally, the threats could be divided into two forms; the first one is the input form where the users share their information which represents personal culture; much of that personal information give attackers a clear picture of everything about a person and the information required to perform other attacks such as credit card fraud or identity theft. The posting about daily actions like a vacation and the current location, gives the attacker more control (Adu Michael & Adewale Olumide, 2014).

The second form of threats that the user will be unable to understand, is the policy of social sites or if one does not have the knowledge of cyberculture of using websites. In this case, the user may be exposed to violations and threats. This form of threat is raised because of what is called misuse of an application or system. An example of such form of threat can be found when creating an account for any social site requires the introduction of some personal information such as phone number, e-mail, personal picture, address and birthday; this information may not be hidden to friends or anyone visiting the personal account (C. Menlo Park, 2019). With this information, a stranger may be able to connect to the telephone number and mail and cause the user to be intimidated. Sometimes the poor user may visit some of the undesirable sites in the community or publish his own images in these sites. There also may be a threat by people who exploit the abuse of sites. However, in an an east community especially in the Kurdistan region, they are most vulnerable to these threats because the site language maybe not understood by them.

Threats in social media can be broadly categorised into: privacy related threats, SNS variants of traditional network and information security threats, identity-related threats and social threats to groups (Al Hasib, 2009). Privacy-related threats can be further divided into subgroups such as digital dossiers of personal information, face recognition, content-based image retrieval, image tagging, and cross-profiling and difficulty of complete account deletion. SNS variants vulnerabilities group can be further divided into cross-site scripting, viruses and worms, and SNS aggregators (Rathore et al., 2017). On the other hand, identity-related threats can be divided into phishing, information leakage, profile squatting through identity theft. Finally, social threats can be also further divided into stalking and corporate espionage.

Investigation of the above threats shows the following (Al Hasib, 2009):

- Most of the users run the risk of over-disclosure and privacy invasions due to this underestimation of extent and activity of their social network.
- Users fail to properly manage the privacy preference due to the complexity and ambiguity of the interface.
- legislation and policy are inefficient.

One of the serious problems with social networks is threats can take advantage of a user's personal information published in the social network to attack users and their friend as it occurred in classic threats. These classic threats can take the form of malware, phishing, spammer, Internet fraud and cross-Site Scripting (XSS). On the other hand, modern threats are typically unique. Usually, these threats specifically target users' personal information as well as the personal information of their friends. The form that modern threats taken are combination threats and threats targeting children (Al Hasib, 2009).

Privacy concerns with social networking services have become controversial and a much-publicised topic. This is caused because of the huge harms that have been recorded in recent years over those sites to people, organisations and even governments. Privacy threats occurred over social sites sometimes because of the sites themselves and sometimes are related to the users. Thus, these causes include user limitations, design flaws or limitations and implicit flows of information. As mentioned above, when a user threatens their friend, they are also threatened too. This is because such type of threats is passed through the internet from one server to the other, provided an individual or company is connected to the internet (Alguliyev et al., 2018), (Abraham, 2012).

Risks associated with social networks can be classified into two risks; one is associated with organisations and another is associated with people. In the first category, some organisations are using those social networks for official or personal reasons. It is expected that they are vulnerable to any one of the major attacks and are expecting failure (Alguliyev et al., 2018), (Kumar & Somani, 2018), (Delerue & He, 2012).

Social Media Threats and Risk Assessment in the Kurdistan Region Case Study

A questionnaire has been designed to assess the usages, threats, and risks of social media sites at Duhok Polytechnic University. The university is a public university with six colleges and eight institutes. The most interesting about the university is that it covers Duhok city, Zakho city and some other towns such as Shekhan, Akre, Amedi, and Bardarash. It also covers a rural area around these towns. The sample considered for the questionnaire is 350 users. The majority of the sampled users are students but there are a member of academics holding masters and doctorates and even administrators working at the university in different jobs. Thus, the age will be not less than 18. Other investigations need to be conducted in the future that involve primary and secondary schools and even uneducated people. The majority of the sample of users living in the district is 55%, whereas 40% are living almost equally in the city and the sub-district. Only 5% are living in a rural and remote areas.

The questionnaire samples involve males and females almost equally with ages between 15 to 63years. 21-30 forms almost 65% of the samples, whereas 15-20 form almost 25% of the

sample of users. The others are above 30 years and form around 10% of the sample. The results show that less than 10% of the sample did not use social media whereas almost 15% used social media sites more than 5 hours daily. The majority of the sample (57%) used social media sites for more than one hour and less than 3 hours daily. The other 25% used social media sites for less than one hour and more than three hours equally. The investigation shows that almost 80% access social media via mobile devices, whereas 10% access social media via a laptop computer, with 10% access to the media sites via both mobile and laptop computers and even tablets. This result shows that almost all have access to social media and have smartphones which are a good sign of the level of living compared to the civilised countries. It means that they have Internet access daily and can communicate and use social media for constructive applications if recommended by the university. Furthermore, the investigation support this when it shows that the majority (75%) access social media at home. Less than 5% use an Internet cafe to access social media and even less than 5% use the offices to access social media. In this aspect, since the majority of the sample are students, it reflects that the people in Kurdistan rely heavily on the home Internet to access the Internet and social media. However, some other universities around the world especially private universities, might provide free Internet. In this case, students might use university and home to access social media. This is also of benefit to the positive sign in using social media. In this aspect, it is worth investigating the worker's access to social media in offices and homes to show the waste of time with using social media in any organisation.

One of the most interesting results of the questionnaire shows that almost 65% of the sample uses Instagram, Snapchat, and Viber whereas Facebook and Twitter is used only by 42% and 8% respectively. These interesting results reflect that students in Kurdistan are somehow different from other parts of the world in the way they use social media. The other interesting results show that 52% have an idea about social media threats and risks whereas the other 48% have no idea. This suggests the need for training and awareness programs to be conducted by the university IT department to educate the students and staff members on using social media safely. This is also found when almost 65% of the sample of users requested such training.

The results also show that 80% of the sample of users did not suffer from any threats. However, only 65% indicate that there are some outside the university in the region that have been threatened, whereas 35% have not heard about anyone being threatened in the region in using social media. Thus, it is essential to have some form of incident reporting in the region that informs social media users about any incident to avoid any risk in the future. In spite of the majority of 80% of users sampled used the social media for operation such as learning process or groups communication that support higher education, since the university did not implement the LMS (Moodle) efficiently till now; there are 38% who did not know that such use might affect National security. However, 78% have some form of protection on their

devices from any threats, whereas almost 80% have private information in their devices that can be hacked. With the questionnaire, they show that they have some form of protection in their devices especially on private information. This is a good sign and needs to be strengthened more and used by the users. This suggests conducting a forum at the university to publish and widen the spread of social media protection. It is well known in these aspects that passwords are the most used to provide user authentication. The results show that 25-30% use very strong passwords (numbers, characters, and symbols) whereas only 48% used numbers and characters in their passwords. The other used very weak passwords from numbers only.

Recommendation on Social Media Usages

This section is very vital for any social media users since it shows how we can protect users in the Kurdistan region and in other parts of the world from the threats and risks of using social media sites. This information has been achieved via the analysis conducted on the investigation performed at Duhok Polytechnic University and via the collection of recommendations on social media site's safe usages.

The risk of using social media can be reduced. There is much research in this area that needs to be considered and implemented by users, and organisation and government levels.

Research shows that many organisations can easily review their security policies to cover social media. Therefore, organisations do not need to issue security policies and guidelines specifically, for social media. The research shows also that a good overall security awareness program, along with and technical and administrative safeguards, need to be considered by organisation, and government officials (Hogben, 2007), (Hiatt & Choi, 2016). The investigation shows that governments should have a major role in providing secure use of social media sites. The reason for that is because any harm for users and organisations will be reflected on the community and national security. Since such data are the most wanted by criminals and un-aware users and information is continually leaked in ever-greater amounts as previous studies have shown. Furthermore, the government has the information, resources and control over people and organisations through legislation required and the operation of social media sites in the country. These efforts by governments will crack down on cybercriminals and reduce the destructive part of social media sites. This legislation must be implemented at both national and global levels to ensure that crimes and criminals cannot get away with their crimes. The legislation must ensure secure behaviour by users dealing with sensitive data and any criminal or offensive acts must face the right action to stop criminals and make users aware also. Therefore many recommendations were suggested by the researchers to increase the user's cyberculture and reduce threats and risks. These

recommendations include the following (Jabee & Alam, 2016), (Aljohani et al., 2016), (Gong, 2015),(Alguliyev et al., 2018), (Kumar & Somani, 2018):

- Keep the computer system, smartphone and any connected devices operating systems, up-to-date
- Understand security settings for each social media and seek consultation. This will assure that privacy and settings are in place.
- A computer system or smartphone must have a secure configuration with the help professionals.
- The password must be strong (numbers, upper- and lower case letters, and special characters symbols). Assure that the password is well protected. In this aspect make sure that you change passwords frequently to avoid being trapped by hackers.
- Building self-awareness about information disclosure.
- Do not publish sensitive information or any information that might be used by criminals.
- Add only the trusted to your contact list and do not trust people you do not know very well.
- Unexpected links that you do not know the source of, must be avoided.
- Install and assure that updated antivirus software is available on your device.
- Read the fine print on website privacy policies
- Remove unnecessary personal information or protect it using some secure algorithms or tools.
- Any attachment coming from an unknown source must not be opened since it a source of hacking.
- Arranging forums or educational workshops to raise security awareness in using social media sites
- Set network IP to the defaults to hide user identity from possible hackers.
- Use the social media sites option that limits post viewing to specific audiences.
- The block feature needs to be enabled and used when the situation requires it.
- Always log out when you are not using the media sites to make sure that other people won't use your social media profile and account.
- Do not open any message from a stranger or from an unknown website.

Another important solution is also proposed, that aims to educate social media users with training videos proposed by social media sites developers before signing up. When signing up for an account, it requires all new users to view a short video that discusses Internet security topics, personal identifiable information, and instructs users on privacy settings for that network. The button for an account to be submitted should not appear until the video has been played. Like the ethical disclaimers that people accept only automatically, this way it cannot be bypassed. Any existing users would also be required to watch the video the day it goes online to continue using their accounts. The video might be expected to be watched once

a year to remind users of its significance in building on the concept of annual training often used in the military. Such an idea is fairly easy to implement with today's technology. It will also help to avoid or at least reduce the harm and risks from threats by providing better education. It can be considered as a precaution suggestion for the problem. Moreover, as a case of the Kurdistan region, this video or other useful information related to the threats, risks, and privacy needs to be translated to the Kurdish language to assure safe and secure usages. This is the responsibility of government officials working on information technologies such as CIO, IT admin, security admins, etc.

Finally, as the problem is obvious and can be considered as a worldwide problem, it is essential to establish an organisation or office that is responsible for recording all the threats and incidents that occurred in Kurdistan. The organisation or offices will work with other organisations or offices around the world to report on accidents of threats and to publish awareness to their people immediately. This will definitely reduce or even eliminate threats and risks.

Conclusion

The paper shows how social media sites become essential in the life of people and their usages increased dramatically to cover almost all ages and education levels. However, such increase by the government, organisations, and people should avoid the increased threat and reduce the risks from such threats that might harm people, organisations and governments. This paper reviewed the usages, threats, risks and the type of social media sites used to enhance the cyberculture of people using such media sites. The paper investigation through a questionnaire conducted at Duhok Polytechnic University, shows the constructive and destructive side of using social media sites in the Kurdistan region, Iraq. This step is essential to compare with other studies conducted around the world and to put some recommendations on such usages, threats, and risks. This investigation reaches the conclusion that the people in Kurdistan need training on using such social media sites to increase the cyberculture and to reduce the risks raised. Finally, the research paper put some recommendations to parents, organisations and governments to be aware and put in place polices and training programs via special offices controlled by the government chief information officer, since the government is responsible to give tips to people by sent messages or give training in schools, universities and clubs to reduce risk and educate people about using social media sites correctly.

REFERENCES

Aaron Smith, Monica Anderson, S., & Inquiries, D. 20036USA202-419-4300 | M.-857-8562 | F.-419-4372 | M. (2018, March 1). Social Media Use 2018: Demographics and Statistics. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2018/03/01/social-media-use-in-2018/

Abbas, J., Aman, J., Nurunnabi, M., & Bano, S. (2019). The impact of social media on learning behavior for sustainable education: Evidence of students from selected universities in Pakistan. *Sustainability*, *11*(6), 1683.

Abraham, A. (Ed.). (2012). *Computational Social Networks: Security and Privacy*. Springer-Verlag. https://doi.org/10.1007/978-1-4471-4051-1

Adu Michael, K., & Adewale Olumide, S. (2014). Mitigating Cybercrime and Online Social Networks Threats in Nigeria. *Proceedings of the World Congress on Engineering and Computer Science*, *1*.

Al Hasib, A. (2009). Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, *9*(11), 288–93.

Alguliyev, R., Aliguliyev, R., & Yusifov, F. (2018). Role of Social Networks in E-government: Risks and Security Threats. *Online Journal of Communication and Media Technologies*, *8*(4), 363–376.

Aljohani, M., Nisbet, A., & Blincoe, K. (2016). *A survey of social media users privacy settings & information disclosure*.

C. Menlo Park. (2019, April 25). *Facebook Inc (FB) 8-K Material Event Wed Apr 24 2019*. Last10K. https://last10k.com/sec-filings/fb

Chan, C. K., & Virkki, J. (2014). Perspectives for sharing personal information on online social networks. *Social Networking*, *2014*.

D. Chaffey. (n.d.). *Global social media research summary 2019 | Smart Insights*. M. Retrieved February 1, 2020, from https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Delerue, H., & He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*.

E. Ortiz-Ospina,. (n.d.). *The rise of social media*. Our World in Data. Retrieved February 1, 2020, from https://ourworldindata.org/rise-of-social-media

Edosomwan, S., Prakasan, S. K., Kouame, D., Watson, J., & Seymour, T. (2011). The history of social media and its impact on business. *Journal of Applied Management and Entrepreneurship*, *16*(3), 79–91.

Elm, M. S. (2008). Panel Discussion II: Culture and Media Technology. Understanding and Studying Internet Culture (s). *Nordicom Review*, *29*(2), 85–90.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019–2036.

Forkosh-Baruch, A., & Hershkovitz, A. (2012). A case study of Israeli higher-education institutes sharing scholarly information with the community via social networks. *The Internet and Higher Education*, *15*(1), 58–68.

G. Felix. (n.d.). *Snapchat Settles Reggie Brown Suit, Credits Him With Original Idea—Bloomberg*. Retrieved February 2, 2020, from https://www.bloomberg.com/news/articles/2014-09-09/snapchat-settles-reggie-brown-suit-credits-him-with-original-idea

Gong, Z. (n.d.). *Towards Secure and Privacy-Preserving Online Social Networking Services*. 98.

Gupta, S. S., Thakral, A., & Choudhury, T. (2018). Social Media Security Analysis of Threats and Security Measures. *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 115–120.

Hiatt, D., & Choi, Y. B. (2016). Role of security in social networking. *International Journal of Advanced Computer Science and Applications*, *7*(2), 12–15.

Hogben, G. (2007). Security issues and recommendations for online social networks. *ENISA Position Paper*, *1*, 1–36.

Jabee, R., & Alam, M. A. (2016). Issues and challenges of cyber security for social networking sites (Facebook). *International Journal of Computer Applications*, *144*(3), 36–40.

Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. *International Journal of Advance Research in Computer Science and Management*, *4*(4), 125–129.

Lough, E., & Fisher, M. H. (2016). Internet use and online safety in adults with Williams syndrome. *Journal of Intellectual Disability Research*, *60*(10), 1020–1030.

M. Ahlgren,. (2020, January 4). *40+ Twitter Statistics 2020: Must-Know User Demographics & Facts*. Website Hosting Rating. https://www.websitehostingrating.com/twitter-statistics/

McCarroll, N., & Curran, K. (2013). Social networking in education. *International Journal of Innovation in the Digital Economy (IJIDE)*, *4*(1), 1–15.

Norman, A. A., Hamid, S., Hanifa, M. M., & Tamrin, S. I. (2017). Security threats and techniques in social networking sites: A systematic literature review. *Future Technologies Conference (FTC), Vancouver, Canada*.

Oxley, A. (2011). *A best practices guide for mitigating risk in the use of social media*. IBM Center for the Business of Government Washington, DC.

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y.-S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information Sciences*, *421*, 43–69.

Rosen, L. D., Carrier, L. M., & Cheever, N. A. (2013). Facebook and texting made me do it: Media-induced task-switching while studying. *Computers in Human Behavior*, *29*(3), 948–958.

Sarapin, S. H., & Morris, P. L. (2015). Faculty and Facebook friending: Instructor–student online social communication from the professor's perspective. *The Internet and Higher Education*, *27*, 14–23.

Sturgeon, C. M., & Walker, C. (2009). *Faculty on Facebook: Confirm or Deny?* https://eric.ed.gov/?id=ED504605

Taha, N., Al-Sayyed, R., Alqatawna, J., & Rodan, A. (Eds.). (2017). *Social Media Shaping e-Publishing and Academia*. Springer International Publishing. https://doi.org/10.1007/978-3-319-55354-2

Zebari, R. R., Zeebaree, S. R., & Jacksi, K. (2018). Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers. *2018 International Conference on Advanced Science and Engineering (ICOASE)*, 156–161.

Zeebaree, D. Q., Haron, H., Abdulazeez, A. M., & Zebari, D. A. (2019, April). Trainable Model Based on New Uniform LBP Feature to Identify the Risk of the Breast Cancer. In *2019 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 106-111). IEEE.