The Effect of Social Media User Behaviors on Security and Privacy Threats

ASLIHAN BANU CENGIZ, GULER KALEM, and PINAR SARISARAY BOLUK

1Department of Information Technologies, Bahcesehir University, Istanbul, Turkey 34349 (e-mail: aslihanbanu.cengiz@gmail.com)
2Department of Software Engineering, Attilim University, Ankara, Turkey 06836 (e-mail: guler.kalem@atilim.edu.tr; gulerkalem@gmail.com)
3Department of Software Engineering, Bahcesehir University, Istanbul, Turkey 34349 (e-mail: pinar.sarisaray@eng.bau.edu.tr)

Corresponding author: Guler KALEM (e-mail: guler.kalem@atilim.edu.tr; gulerkalem@gmail.com).

ABSTRACT  The number of online social network (OSN) users is increasing daily and attacks and threats against over the time spent on online networks has been increasing equally. Attacks against OSN users exploit not only system vulnerabilities but also user-induced vulnerabilities, which naturally affect the hacker’s attack strategy as well. This study is designed to investigate the effect of social media user behaviors on their vulnerability level in terms of security and privacy. The study was conducted survey methods, which was applied to social media users in two countries - Turkey and Iraq. This study documents and analyzes the behaviors of 700 OSN users in two countries. This study examines the behaviors of social media users from two nationalities, investigating whether there is a relationship between social media users’ behaviors and security and privacy threats. Research findings demonstrate that there is a significant relationship between OSN users’ behaviors and their attitudes towards security and privacy. Additionally, Turkish social media users pay more attention to their behaviors in terms of privacy and security awareness than Iraq users.

INDEX TERMS  Cyber Attack, Cyber Security, Online Social Network (OSN), Social Media, User Online Behavior

I. INTRODUCTION

Online Social Networks (OSN) have become an integral part of the lives of billions. People from different regions of the world and from different age groups visit these networks, which have achieved remarkably widespread penetration, and continue to develop their prevalence. Social networks allow social media users to create user profiles, add other users, and see each other’s activities. Facebook (FB), Twitter, and many other Social Network users can do different types of activities on these sites such as post photos and update and comment on nearly anything every minute. Emerging through the Internet, these have started to spread over the so-called social network sharing sites. In a sense, this development has solidified and stabilized in the form of the modern communication channel we understand as “Social Network Sites”, networks operating through channels which enable interaction between people using multi-media data sharing. In the second quarter of 2019, Internet, social media, and mobile user statistics were published on the ‘We Are Social’ and ‘Hootsuite’ websites. In the report stated that 4.38 billion Internet users in the world make up 56% of the world population, while 45% of these (3.48 billion) are reported to be social media users. In 2018, Kemp found that 42% (3.19 billion) of 4.02 billion Internet users were social media users. Nielsen’s social networks report “Global Faces and Networked Places” observed that two thirds of the world’s Internet population spends time on social networking sites, an amount of time that corresponds to 10% of total Internet time. Social media is an integral part of our lives. With the widespread use of social networks, however, security problems that users may face in these networks have become important. Cranor et al. research into online privacy attitudes showed that social media users express a high level of concern about privacy on the Internet. Also, users are concerned with the way their data will be used. The best example to cite in support of their claims is Facebook. In 2010, Facebook made all kinds of information in all user accounts...
available to application developers (NGOs, academicians, analysis companies, software developers, etc.). In 2014, on the other hand, a personality test application was launched on Facebook via the Global Science Research Company. This application enabled Facebook developers to access the data of their Facebook friends in addition to their personal data. In this way, approximately 50 million Facebook users’ profiles were hacked. Facebook provided the following explanation after the incident: “People knowingly shared their information and there was no entry to any system; passwords and sensitive information were not stolen or hacked” [6]. Here, it is clear that the behaviors of users of Online Social Networks (OSN) have a big impact on information security. In this context, this study analyzes the behavior of social network users in terms of information security and privacy. We aim to determine the relationship between the behaviors of OSN users and security/privacy. In this context, users belonging to two different cultures (Turkish and Iraq) are included in the study. Hence, the effect of the different cultures is also investigated in terms of security and privacy awareness. The rest of the paper is organized as follows: Section 2 introduces related work. Section 3 describes our work. Section 4 presents our results. Finally, conclusion and future work is given in Section 5.

II. RELATED WORK

Christofides et al. [7] studied awareness of users’ privacy on social networking sites and how this awareness is reflected in their attitudes, observing that although users have some awareness of privacy issues, they still reveal a lot of information about themselves. The reason for this was reported as being their desire to build their own identities. O’Brien and Torres [8] subsequently supported these findings with their 2012 study on the awareness of OSN users on privacy and how their behavior was affected by this awareness. In the study, they observed that the level of trust in social networking sites was low. In particular, they found that users older than 30 years of age were the least trusting group. However, they also observed that low trust levels did not affect what OSN users shared on social media. The youngest group (those between 18 and 21 years of age) was the one divulging the highest amount of information about themselves. Although users between the ages of 26 and 29 spent less time on social media compared to others, the number of their friends on social media accounts was found to be higher. At the same time, the 26 - 29 age group was found to be more cautious in using protective security tools, with a rate of 92.3%. On the other hand, a major finding of the study was that OSN users neglect security issues to ensure social interaction. The authors additionally remarked that both social media tools and OSN users are responsible for the protection of privacy.

In addition, the rate of profile updates shows that OSN users do not feel uncomfortable about privacy. On the other hand, [9] observed that most of social media users are aware of security settings, but they do not change the default privacy settings. Madden [10] observed that half of social media users have difficulty in managing their privacy settings. In all, 48% of OSN users have difficulty managing the privacy controls on their social media accounts while 49% OSN users say that it is “not difficult at all”. However, [11] reached analyzing the threats related to user activities, they observed that 68.90% of the users updated their privacy settings against threats and dangers that may come from the social media environment. They concluded that users generally are aware of and think about privacy settings, in addition to the fact that young users post more information at a higher rate than all other age groups. The authors observed that young online social network users are concerned about the confidentiality of information. In particular, 90% of them keep their privacy settings up to date. Nonetheless, a review of the literature suggests that a definitive judgment has not yet been reached on the variable observations of user behaviors regarding security settings. Within the context of technology developing at breakneck speed and ever easier access to the Internet, use of social media and the time spent on social media increase constantly. Ellison et al. [12] considered the time OSN users spent on social networks, observing that users who spend 10 to 30 minutes a day on social media have between 150 and 200 friends in their social media profiles. They also found that the users preferred to be friends on social media with their existing friends, people living with them, neighbors, or classmates, rather than meeting and being friends with new people on social media. However, [13] reached results in their study different from those of Ellison, Steinfield, and Lampe. They observed that 31% of social network users are using it to get to contact with new people, otherwise 21% of users using it to keep in touch with their beloved friends and only 14% of them using it for general socializing as given in Fig. 1. A Secure Life published the results of a 500-person survey conducted in September 2019 via Pollfish. According to the results of the research, 26% of social media user have created a fake social media profile. Ghafari et al. [14] have completed a broad analysis on trust prediction and presented challenges faced during the trust prediction process in OSN, addition to this the state-of-the-art have been classified in pair-wise trust prediction in OSN.
popular web application attacks. The main concept of XSS
attacks is to exploit the security of the web-client in the web
application through executing malicious code to aggregate
sensitive data and users' cookies [24]. XSS can attack OSNs
and separate among users as a viral worm [25]. In April
2009, the XSS based worm, Mikeyy, rapidly transmitted
through tweets across Twitter and infected many users’
profiles [26]. Phishing attacks, the final threat to users
handled here, are a type of social engineering used to
obtain users’ private and sensitive data by representing a
legitimate TP. A survey [27] revealed that those users who
interacted on OSN web pages are more likely to fall for
phishing scams because of their social and trusting nature.
For example, the phishing attack on FB drew users to fake
FB login pages. Then, it propagated itself through users by
asking friends to click on a link posted on the main user’s
profile page [28]. As OSNs allow their users to publicly
exchange and share personal information with others easily,
users become a good target for attackers. The leakage of
personal and sensitive information, naturally, might have
negative implications for the OSN users, however. The
OSNs allow Third Party Application (TPA) providers to
design applications for the OSN, and to run them on its
platform, such as the Application Programming Interface
(API) in FB. These TPAs are extremely common through
OSN users. Since the users connect and permit TPAs to
access their privacy information, these apps can reach user’s
information automatically. In addition, TPAs are able to
post on users’ profiles or a user’s friend’s profile, or may
be able to reach other users’ data without those users’
knowledge [29]. This causes security and privacy breaches
and exposure to many kinds of attacks. Although different
models and a variety of types of solutions are proposed
to improve the users’ privacy and security, these solutions
couldn’t help users in protecting themselves from hackers
and other threats [30], [31]. This is because most theories
and models suggested by researchers require OSN users to
have skills and experiences in the security field. This lack
of awareness among users decreases the usability of the
suggested models and doesn’t have an impact on reducing
the effect of OSN based threats. Although many studies
[32] have analyzed the behavior of OSN users from different
perspectives, the issue of their relationship with security and
privacy threats that may be caused by user behavior is still
a relatively new one. In this study, the behaviors of users
that might cause privacy and security attacks are analyzed.
In addition, data on the behaviors of users from different
cultures were collected by a questionnaire. The collected
data were analyzed in relation to security-privacy threats. In
order to reach users from different cultures, we administered
surveys to social media users living in Turkey and Iraq with
different demographic characteristics.

### III. OUR WORK

In this study, we first use our previous study [33], which
collects common user behaviors affecting each user’s level of
security and privacy vulnerability. Some common behaviors

VOLUME 4, 2016
of OSN users that make them easy prey for hackers [34], [35]. These behaviors may include trusting friends or strangers, spending more time on OSNs, tagging, Check-In places, downloading unknown files, playing online games, downloading apps, joining many groups, adding, accepting, and making friends with unknown users, sharing too much personal information and too many photos, clicking on links and attractive videos and photos, and chatting, calling, and exchanging data through OSNs. Then behaviors belonging to the specific attack are identified to measure user OSN usage characteristics for different kind of threats. After identifying these behaviors, we prepared a questionnaire to collect data from different cultures.

A. INPUT DATA PREPARATION

In order to collect data on user behavior, we applied the field research method in the study and obtained data using the questionnaire technique. The population, sampling, data collection tools, data analysis, and research hypotheses were determined within the framework of this methodology in the study. The population of the study consisted of social media users from different cultures, Turkey and Northern Iraq. Due to the large population of the research and time and cost constraints, we were able to reach a total of 1000 social media users – 500 Turkish and 500 Iraqi OSN users selected by simple random sampling. This number is thought to represent the population of the study. We prepared a questionnaire as a data collection tool. Including 30 questions in total, the questionnaire consisted of three sections: user characteristics, privacy, and confidentiality. Two different data sets were obtained from the questionnaire and they were identified as (30x343) KR and (30x357) TR. The questionnaire was prepared according to scenarios for an attack or a vulnerability. However, the questionnaire data of 343 Iraqi and 357 Turkish users were used in the study after excluding the forms in which questions went answered, clear answers were not obtained, or questions were answered incorrectly. In total, 700 questionnaires were recorded. Research findings can be generalized with a ± 5% sampling error within a 95% confidence interval. The questionnaire items, on a five-likert type scale, indicated the relevance of the expressions in the questionnaire on a scale from 1 to 5. The range of the scale was calculated on the basis of the following formula: (a = array width/the number of group interviews) and the scale was formed accordingly. In the five-point Likert scale, the items are ranked as “completely disagree (1,00-1,80)”, “not agree (1,81-2,60)”, “uncertain (2,61-3,40)”, “agree (3,41-4,20)” and “completely agree (4,21-5,00)”.

B. USER PROFILES: DEMOGRAPHY

In this section, we give the OSN user properties of the participants in this study. Specifically, we provide their main profiles in terms of demography, OSN usage frequency, and number of friends on social media. The nationalities of the 700 individuals who participated in the study are shown in Table 1, while their demographic information including gender, age, and educational status is given in Table 2.

The study comprised 51% Turkish, and 49% Iraqi, participants. This distribution showed that the research sample was based on an equal distribution in terms of nationality. Table 2 shows gender, age and educational level of the participants. In addition to demographic questions, the participants were asked how many hours they spend on social media and how many friends they have on their accounts.

Table 3 shows the frequency distribution of the number of hours a day OSN users spend on social media.

As can be seen in Table 3, 250 (35.7%) participants spend 1 - 2 hours on social media per day, 214 (30.6%) participants spend 2 - 4 hours, 139 (19.9%) participants spend 4 – 6 hours, 52 (7.4%) participants spend less than 1 hour, and 45 (6.4%) participants spend more than 7 hours. Table 4 shows the frequency distribution of the number of OSN users' social media friends.

Table 1: Distribution of OSN Users by Nationality

| Nationality | Frequency | Percentage | Valid | Cumulative |
|-------------|-----------|------------|-------|------------|
| Turkish     | 357       | 51         | 51    | 100        |
| Iraqi       | 343       | 49         | 49    | 100        |
| Total       | 700       | 100        | 100   | 100        |

Table 2: T-Test on Internet Usage Levels of OSN Users by Nationality

| Gender | Male | Female | Percentage | Valid | Cumulative |
|--------|------|--------|------------|-------|------------|
| Male   | 120  | 193    | 237        | 150   |
| Female | 280  | 72     | 76         |       |

| Age     | School | High School | Undergraduate | Master’s Degree | PhD |
|---------|--------|-------------|---------------|-----------------|-----|
|          | 258    | 0           | 94            | 3               | 2   |

Table 3: Frequency Distribution of How Many Hours a Day the OSN Users Spend on Social Media

| Frequency | Percentage | Valid | Cumulative |
|-----------|------------|-------|------------|
| Less than 1 hour | 7.4 | 7.4   |
| 1 - 2 hours     | 35.7 | 35.7  |
| 2 - 4 hours     | 30.6 | 30.6  |
| 4 - 6 hours     | 19.9 | 19.9  |
| 7 hours and more| 6.4 | 6.4   |
| Total           | 100  | 100   |
Leakage attacks and Threats Targeting Children attacks include Fraud attacks, Phishing, XSS. Modern Threat Information channel(s) toward the victim. In this paper, we consider three OSN users. Through these channels, attackers can victimize OSN to find open channels to access or to connect with OSN. The attacker uses different techniques to breach the users' confidentiality. The attacker uses different techniques to breach the users' confidentiality. The attacker uses different techniques to breach the users' confidentiality.

In this study, due to their behavior identification common usage, we selected three types of classical attacks used by the attackers. We investigated the behaviors of these attacks to identify the channel or the process that an attack pursues to penetrate systems. In most cases, attackers try to find open channels to access or to connect with OSN users. Through these channels, attackers can victimize OSN users. Each attack has its own policy to find an open channel(s) toward the victim. In this paper, we consider three main group of attacks which are Classic Threat (Internet Fraud attacks, Phishing, XSS), Modern Threat (Information Leakage attacks) and Threats Targeting Children attacks (Cyber Bullying attacks).

1) Internet fraud: The phrase of internet fraud, refers to any access by using internet to fraud or obtain advantage of online users, and also recognized as "cyber fraud". The attacker uses social engineering techniques to attempt to trick OSN users into making strong friendship or installing software that can spy on what the user type. In the earlier period, fraudulent utilized traditional in person social networks, such as weekly group meetings, to continuously promoting sturdy relations with their possible victims. Recently, according to the North American Securities Administrators Association [36], 2011 by the growing publicity of OSNs, scam genius have overturned to OSNs to set up a trust relationships with their OSNs victims, and then they get advantages of private information that are shared in the online user’s profiles. In the latest years, for instance, scammers have been hacking into the accounts of FB users who journey in a foreign country. Once they handle to log into a victim’s account, the fraudulent cunningly ask the user’s friends for assisting to transmitting money to the fraudster’s bank account.

2) Phishing is another method that attackers use to steal the user’s ID and password. Attackers may drop an interested link that direct users for another re-logging [27], [30]. Once the re-logging is done, the user credential “ID and password” is not confidential any more, since the attacker has a copy of them (Phishing).

3) Cross-site scripting (XSS) attacks: Cross-site Scripting (or XSS) is one of the most popular web application attacks. The main concept of XSS is to exploit the security of the web-client in the web application through executing malicious code to aggregate sensitive data and cookies of users. XSS can attack OSN and separate among users as a viral worm [25]. During April 2009, the XSS based worm, called Mikeyy, rapidly transmitted through tweets across Twitter and infect the profile of many users [26]. Setting and managing cookies are another issue that opens channels for attackers. Through existing cookies, an attacker can find or learn the type of cookies that are accepted by the user’s browser. Then, the attacker can design such cookies and use them maliciously. Such a scenario is related to the Cross-site Scripting and Cross-site request forgery attacks [24], [37].

4) Information Leakage attack is another popular type of OSN attack, in which the attacker tries to collect information to breach the users’ confidentiality. The attacker uses different techniques to breach the user’s privacy and get them to disclose individual information. This process occurs when the user does not change his/her privacy setting, and on daily bases he/she shares many sensitive data over OSNs [38]. OSN allows their users to publicly exchange and share personal information with others easily. Therefore, users become a good target for attackers.

Table 4: Frequency Distribution of the Number of Friends of the OSN Users in Social Media

| Frequency | Percentage | Valid Percentage | Cumulative Percentage |
|-----------|------------|------------------|-----------------------|
| 1 - 100   | 54         | 7.7              | 7.7                   |
| 101 - 200 | 108        | 15.4             | 15.4                  |
| 201 - 300 | 158        | 22.6             | 22.6                  |
| 301 - 400 | 202        | 28.9             | 28.9                  |
| Over 400  | 178        | 25.4             | 25.4                  |
| Total     | 700        | 100              | 100                   |

As can be seen in Table 4, 202 (28.9%) participants have social media friends in the range of 301 - 400 friends, 178 (25.4%) participants have 400 and above social media friends, 158 (22.6%) participants have 201 - 300 social media friends, 108 (15.4%) have 101 - 200, and 54 (7.7%) have 1 - 100 social media friends.

C. RESEARCH HYPOTHESES

In order to inspect the attack behavior performance results based on nationality, we used the following hypotheses. Our aim is to explore the effect of the cultures on user behaviors in terms of security and privacy awareness.

- H1: There is a significant relationship between the nationality of OSN users and the frequency of Internet use.
- H2: There is a significant relationship between the nationality of OSN users and the frequency of using pseudonyms in their social media accounts.
- H3: There is a significant relationship between the frequency of OSN users’ use of social networks and their use of protective security tools.
- H4: There is a significant relationship between parents’ follow-up of their children’s activities on OSN and their nationality (Iraqi/Turkish).
- H5: There is a significant relationship between the time spent on the Internet and the number of followers.
- H6: There is a relationship between the behaviors of OSN users and their attitudes towards privacy/security.

D. CONSIDERED ATTACKS BASED ON USER BEHAVIORS

In this study, due to their behavior identification common usage, we selected three types of classical attacks used by the attackers. We investigated the behaviors of these attacks to identify the channel or the process that an attack pursues to penetrate systems. In most cases, attackers try to find open channels to access or to connect with OSN users. Through these channels, attackers can victimize OSN users. Each attack has its own policy to find an open channel(s) toward the victim. In this paper, we consider three main group of attacks which are Classic Threat Internet Fraud attacks, Phishing, XSS), Modern Threat (Information Leakage attacks) and Threats Targeting Children attacks (Cyber Bullying attacks).

1) Internet fraud: The phrase of internet fraud, refers to any access by using internet to fraud or obtain advantage of online users, and also recognized as "cyber fraud". The attacker uses social engineering techniques to attempt to trick OSN users into making strong friendship or installing software that can spy on what the user type. In the earlier period, fraudulent utilized traditional in person social networks, such as weekly group meetings, to continuously promoting sturdy relations with their possible victims. Recently, according to the North American Securities Administrators Association [36], 2011 by the growing publicity of OSNs, scam genius have overturned to OSNs to set up a trust relationships with their OSNs victims, and then they get advantages of private information that are shared in the online user’s profiles. In the latest years, for instance, scammers have been hacking into the accounts of FB users who journey in a foreign country. Once they handle to log into a victim’s account, the fraudulent cunningly ask the user’s friends for assisting to transmitting money to the fraudster’s bank account.

2) Phishing is another method that attackers use to steal the user’s ID and password. Attackers may drop an interested link that direct users for another re-logging [27], [30]. Once the re-logging is done, the user credential “ID and password” is not confidential any more, since the attacker has a copy of them (Phishing).

3) Cross-site scripting (XSS) attacks: Cross-site Scripting (or XSS) is one of the most popular web application attacks. The main concept of XSS is to exploit the security of the web-client in the web application through executing malicious code to aggregate sensitive data and cookies of users. XSS can attack OSN and separate among users as a viral worm [25]. During April 2009, the XSS based worm, called Mikeyy, rapidly transmitted through tweets across Twitter and infect the profile of many users [26]. Setting and managing cookies are another issue that opens channels for attackers. Through existing cookies, an attacker can find or learn the type of cookies that are accepted by the user’s browser. Then, the attacker can design such cookies and use them maliciously. Such a scenario is related to the Cross-site Scripting and Cross-site request forgery attacks [24], [37].

4) Information Leakage attack is another popular type of OSN attack, in which the attacker tries to collect information to breach the users’ confidentiality. The attacker uses different techniques to breach the user’s privacy and get them to disclose individual information. This process occurs when the user does not change his/her privacy setting, and on daily bases he/she shares many sensitive data over OSNs [38]. OSN allows their users to publicly exchange and share personal information with others easily. Therefore, users become a good target for attackers. The Leakage...
Table 5: Correlations between the Scales

| R       | Correlation |
|---------|-------------|
| 0.00 - 0.25 | Very Weak |
| 0.26 - 0.49 | Weak       |
| 0.50 - 0.69 | Medium     |
| 0.70 - 0.89 | High       |
| 0.90 - 1.00 | Very High  |

Table 6: T-Test on Internet Usage Levels of OSN Users by Nationality

| Nationality | N  | X   | SS  | Sd  | t   | p   |
|-------------|----|-----|-----|-----|-----|-----|
| Turkish     | 357| 3.20| 1.230| 669.436| -3.849| <0.05*|
| Iraqi       | 343| 3.52| .958 |       |     |     |

*p < 0.05

Table 7: T-Test on the Use of Pseudonyms in Social Media according to the Nationality of OSN Users

| Nationality | N  | X   | SS  | Sd  | t   | p   |
|-------------|----|-----|-----|-----|-----|-----|
| Turkish     | 357| 1.98| 1.371| 467.411| 5.119| <0.05*|
| Iraqi       | 343| 1.58| .540 |       |     |     |

*p < 0.05

E. DATA ANALYSIS

We analyzed the data obtained from the study in two ways. First, we used Excel to analyze user behaviors in response to the three types of threats. Here, we classified user behaviors into three groups in terms of their robustness to the attacks: Secure, Moderate, and Insecure. We also investigated results based on nationality to analyze the effect of culture on user behavior data. We used SPSS 22.0 software to evaluate the data. In this context, seven research hypotheses are investigated. Descriptive statistical methods (Number, Percentage, Mean, Standard deviation) were used to evaluate the data. In addition, Chi-square analysis was used to compare the grouped variables. The results were evaluated at a 95% confidence interval and 5% significance level. Statistical techniques such as arithmetic mean (x) and t-test were used in data analysis. The relationship between the variables of the study was tested with Pearson’s correlation analysis. The correlation between the scales is given in Table 5.

This study adopts a Quantitative Research method to meet the research objectives. The aim of this research is to arrive at statistically-valid conclusions for our research questions in order to clarify the relationship between user behaviors and their security-privacy vulnerability status.

IV. RESULTS

A. EVALUATION OF HYPOTHESIS DATA

H1: There is a significant difference between the nationality of OSN users and frequency of Internet use. Table 6 shows the independent sample t-test results, which are used to determine whether there is a significant difference in the frequency of Internet use according to the nationality of OSN users, which is one of the sub-objectives of the study.

Analysis of Table 6 demonstrates that there is a significant difference between the attitudes of Turkish and Iraqi social media users about the frequency of their Internet use \( t(669.436) = -3.849, p < 0.05 \). In addition, the arithmetic mean values were examined to determine the group that had the highest average and it was observed that the social media usage frequency of the Iraqi OSN users (X = 3.52) was higher than that of the Turkish users (X = 3.20). The difference is considered statistically significant at the level of 0.05. Consecutively, it is understood that Iraqi social media users use social media more frequently than Turkish users.

H2: There is a significant difference between the nationality of OSN users and the frequency of using pseudonyms in their social media accounts.

Table 7 shows the independent sample t-test results, which are used to determine whether there is a significant difference between the nationality of OSN users and the use of pseudonyms in their social media accounts, which is another of the sub-objectives of the study.

Table 7 demonstrates that there is a significant difference between the Turkish and Iraqi social media users in terms of pseudonym use in their social media accounts \( t(467.411) = 5.119, p < 0.05 \). The arithmetic mean values were examined to determine the group that had the highest average, and it was observed that more Turkish OSN users (X = 1.98) used pseudonyms on social media than Iraqi users (x = 1.58). The difference is considered statistically significant.
at the level of 0.05. It can thus be understood that a higher number of Turkish social media users use pseudonyms than Iraqi users.

H3: There is a significant relationship between the frequency of OSN users’ use of social networks and their use of protective security tools.

Furthermore, we conducted analysis in this study to determine whether there was a significant relationship between OSN users’ frequency of social network use and their use of protective security tools, another of the sub-objectives of the study. Since Skewness and Kurtosis values are between -1 and 1 for these two variables, the data show normal distribution. We used Pearson’s correlation test to find the relationship between these variables. The results of the correlation analysis are given in Table 8.

As seen in Table 8, there is no significant relationship between OSN usage frequency and users’ use of security and privacy in browser settings (r = 0.057, p > 0.05). Accordingly, there is no relationship between OSN usage frequency and users’ checking security and privacy in browser settings. This result shows that usage frequency of the user does not have an affect on the knowledge of security and privacy setting in OSN.

H4: There is a significant relationship between social media users supports on parental follow-up and the nationalities of the users (Iraqi/Turkish).

This correlation analysis showed that there was a low level of positive correlation between the social media users views on parental follow-up and the nationalities of OSN users (r = 0.076, p < 0.05), at 0.05 significance level.

In addition, the results of the cross analysis in Table 10 showed that 17% of Turkish users strongly agree and 29% agree with the statement “parents’ should follow-up on their children’s OSN activities”. Iraqi OSN users (19%) mostly disagree with the statement “parents follow their children’s OSN activities”.

H5: There is a significant relationship between time spent on the Internet and number of followers.

One of the aims of the study was to determine whether there is a significant relationship between the time spent on the Internet and the user’s number of followers. Pearson’s correlation test was used to find the relationship between these variables. The results of the correlation analysis are given in Table 11.

According to the results of the correlation analysis, a significant and positive correlation was found between the time spent on the Internet of OSN users at a significance level of 0.01 and the number of followers (r = 0.426, p < 0.01). This can briefly be interpreted as follows: The number of followers increases as the time spent on the Internet increases.
of followers in the OSN may increase as OSN users spend more time on the Internet, or, vice versa, as the time spent on the Internet by OSN user’s decreases, the number of followers in the OSN may decrease.

H6: There is a relationship between privacy and security behaviors for OSN user.

The main purpose of the study was to determine whether there is a significant relationship between the behaviors of OSN users and their attitudes towards privacy and security. Pearson’s correlation test was used to find the relationship between these variables (privacy and security). The results of the correlation analysis are given in Table 12.

According to the first result of the correlation analysis, a significant low and positive relationship was found between the behaviors of OSN users and their attitudes towards security ($r = 0.124$, $p < 0.01$) at a significant level of 0.01. This can be interpreted as indicating that the more social media users pay attention to their behaviors on the OSN, the greater their awareness of security attitudes on the OSN. According to the second result of the correlation analysis, a moderate and positive relationship was found between the behaviors of OSN users and their attitudes towards privacy ($r = 0.308$, $p < 0.01$) at a significant level of 0.01. In other words, the more OSN users pay attention to their social media behaviors, the more they increase their awareness of privacy. According to the last result of the correlation analysis, a significant, low level, and positive correlation was found between the behaviors of the OSN users and their attitudes towards privacy ($r = 0.082$, $p < 0.05$) at the significance level of 0.05. This can be interpreted as follows: As the OSN users’ awareness of security increases, their awareness of privacy increases as well. It is predicted that the reason for the weak level of relationship may be due to the other independent variables which affecting our independent variables and which we do not include in the scope of the research.

**Table 12: Correlation Test for OSN Users between Privacy and Security**

|          | 1   | 2   | 3   |
|----------|-----|-----|-----|
| 1-) Behavior | r   | p   | N   |
|           | 0.124** | 0.001 | 700 |
| 2-) Security | r   | p   | N   |
|           | 0.308** | 0.082* | 700 |
| 3-) Privacy | r   | p   | N   |
|           | 0.000 | 0.030 | 700 |

**p < 0.01 * p < 0.05. r: Pearson’s correlation coefficient p: Significance N: Number of OSN users**

In this section, we analyze the relation between each attack scenario and OSN users’ behaviors that may cause security and privacy treats. Our methodology starts with a comprehensive investigation of the most common threats and attacks that may prey on OSN users’ vulnerabilities. Our work has analyzed these attacks and threats in terms of user behavior. Then, survey questions are formulated to check the behavior of a user for a specific attack. For example, one of the attacks is malware. The literature demonstrates that malware bears a strong relationship with the duration that a user will be online [35]. Therefore, a suitable question to check the vulnerability of a user is “When finishing your activities on OSN, do you disconnect from the internet?” The answer of this question, as well as all others, has five levels: "strongly agree, agree, fair, disagree," and "strongly disagree". Through a number, the user will define the vulnerability level of him/her against a wide range of attacks. When a user asks thirty questions, the work gets thirty user reactions to three kind of attack types. All of the users attack related behaviors are collected and grouped into three ranges: insecure, moderate, and secure where the insecure range indicates the user behaviors are vulnerable to the attack, moderate range indicates unidentified user behavior for the attack and secure range indicates the user behaves more securely on social media compared to the other groups. We expect secure people may experience fewer attacks compared to the other groups. In this study, we focus specifically on three group of attacks: Classic Threat (Internet Fraud attacks, Phishing, XSS), Modern Threat (Information Leakage attacks) and Threats Targeting Children attacks (Cyber Bullying attacks).

Fig. 2 gives user behaviors considering to Internet Fraud attacks without differentiating nationality. It shows that for this kind of attack, 50% of users have reliable behaviors on social media while 42% of users have unreliable behaviors. Additionally, 8% of users have not identified in terms of security risk for this attack.

Fig. 3 presents user behavior distribution based on the
of users have not identified in terms of security risk for this attack.

Fig. 7 suggests that three vulnerability ranges for XSS (Cross Site Scripting) attack based on nationalities. It shows that 36% of Turkish users are vulnerable to this attack while 42% of Iraqi users are insecure. In the secure group, we observe once again a noticeable gap between these two cultures. 54% of Turkish users have reliable behaviors on social media while 45% of Northern Iraqi users have reliable behaviors on social media. According to this result, Turkish users have more secure behaviors than Iraqi users and Iraqi users have more insecure behaviors than Turkish users in terms XSS (Cross Site Scripting) attacks.

Fig. 8 shows general user behaviors for an Information Leakage attack. It shows that 40% of users present secure behavior for this kind of attack. It is also given that 55% of user presents more vulnerable compared to the other groups. Additionally, behaviors collected from 5% of users have not identified.
users have more insecure behaviors than Turkish users and Turkish users have more secure behaviors than Iraqi users in terms of Information Leakage attacks.

Fig. 10 shows general user behaviors for a CyberBulling attack. It shows that 30% of users presents secure behavior for this kind of attack. It is also given that 65% of user presents more vulnerable compared to the other groups. Additionally, behaviors collected from 5% of users have not identified.

Fig. 11 suggests that three vulnerability ranges for CyberBulling attack based on nationalities. It shows that 42% of Turkish users are vulnerable to this attack while 89% of Iraqi users are insecure. In the secure group, we observe once again a noticeable gap between these two cultures. 51% of Turkish users have reliable behaviors on social media while 8% of Northern Iraqi users have reliable behaviors on social media. According to this result, Turkish users have more secure behaviors than Iraqi users and Iraqi users have more insecure behaviors than Turkish users in terms of CyberBulling attacks.

V. CONCLUSION

In this paper, we aimed to analyze social media user behaviors in terms of security and privacy. In order to investigate user behaviors, we conducted surveys in two different countries: Turkey and Iraq. Then we analyzed data obtained from Turkish and Iraqi social media users so as to present the region and culture effect on user behaviors. Then, we identified the vulnerability level (insecure, moderate, and secure) of the two cultures for Internet Fraud, Information Leakage and Behavior, CyberBulling attacks based on their behaviors.

Our behavior analysis results show that Iraqi social media users use social media more frequently than Turkish users. Moreover, it was observed that a higher number of Turkish social media users use pseudonyms on social media than Iraqi users. We observed that the number of followers in the OSN environment increased as the time spent on the Internet by OSN users increased. This can be interpreted as meaning that social media users pay attention to and value the number of followers in today’s world, one in which the perception of popularity on social media is associated with the number of followers.

In addition, when the views of social media users on parental follow-up are examined that Turkish OSN users believe that parents should follow the activities of their children on the OSN more frequently than Iraqi users. The data obtained in our study revealed, simply, that cultural differences affect social media usage habits. We conclude that Iraqi social media users have a higher level of vulnerability than Turkish users for all types of attacks that were included in this study. These results have verified the hypothesis that there is a significant relationship between behavior and exposed threat and their attitudes towards privacy/security.
Further, it seems that the more OSN users pay attention to their behaviors on social media, the greater their awareness of security and privacy will be. As security awareness among OSN users increases, a concurrent increase in their awareness about privacy increases seems also to take place. The boundaries of this study are made by considering 2 cultures (Iraq, Turkey) since we could only able to reach the data of these 2 cultures for this study. As a future work, we have a plan to include more cultures to be analysed and compare the difference. Additionally, we plan to investigate the effect of user profiles such as education, age etc. on user behaviors to deepen the analysis of our results. Our paper gives some new knowledge and insights to Security and Privacy Area in terms of user behaviors by considering different kind of security attack scenarios. Based on our resource findings, two different recommendations are obtained.

- It is quite essential that security specialists, software security coders should have well elaborated our results. Then, they should adapt new security and privacy solutions based on user behavior and treatment strategies after security attacks by considering our paper results.
- Both, governments (Iraq, Turkey) and private sector, are invited to set up, and keep renewing, the foundation and facilities for a competent system of social media communications by enhancing security and privacy rules.

References

[1] R. Gross and A. Acquisti, “Information revelation and privacy in online social networks,” in Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 71–80.

[2] J. Nagy and P. Pecho, “Social networks security,” in 2009 Third International Conference on Emerging Security Information, Systems and Technologies. IEEE, 2009, pp. 321–325.

[3] S. Kemp, “The state of digital in April 2019: all the numbers you need to know,” 2019.

[4] G. Faces and N. Places, “A nielsen report on social networking’s new global footprint,” The Nielsen Company, 2009.

[5] L. F. Cranor, J. Reagle, and M. S. Ackerman, “Beyond concern: Understanding net users’ attitudes about online privacy,” The Internet upheaval: raising questions, seeking answers in communications policy, pp. 47–70, 2000.

[6] “5 soruda facebook verilerinė ‘usulzu kullanmakla’ suclanan cambridge analytica,” https://www.bbc.com/turkce/haberler-dunya-43469094 2018.

[7] E. Christofides, A. Muise, and S. Desmarais, Privacy and disclosure on Facebook: Youth and Adult’s information disclosure and perceptions of privacy risks. University of Guelph, 2011.

[8] D. O’Brien and A. M. Torres, “Social networking and online privacy: Facebook users’ perceptions,” Irish Journal of Management, 2012.

[9] N. Aldhaiferi, C. Watson, and A. Sajeev, “Personal information privacy settings of online social networks and their suitability for mobile internet devices,” arXiv preprint arXiv:1305.2770, 2013.

[10] M. Madden, “Privacy management on social media sites,” Pew Internet Report, pp. 1–20, 2012.

[11] K. Williams, A. Boyd, S. Densten, R. Chin, D. Diamond, and C. Morgen-thaler, “Social networking privacy behaviors and risks,” Seidenberg School of CSIS, Pace University, USA, 2009.

[12] N. B. Ellison, C. Steinfield, and C. Lampe, “The benefits of facebook “friends”: social capital and college students’ use of online social network sites,” Journal of computer-mediated communication, vol. 12, no. 4, pp. 1143–1168, 2007.

[13] P. B. Brandtzæg and J. Heim, “Why people use social network sites,” in International conference on online communities and social computing. Springer, 2009, pp. 143–152.

[14] S. M. Ghafari, A. Beheghti, A. Joshi, C. Paris, A. Mahnood, S. Yakhchi, and M. A. Orgun, “A survey on trust prediction in online social networks,” IEEE Access, vol. 8, pp. 144292–144309, 2020.

[15] A. Beheghti, V. Mrave-ji-Hashemi, S. Yakhchi, H. R. Motahari-Nezhad, S. M. Ghafari, and J. Yang, “Personality2vec: Enabling the analysis of behavioral disorders in social networks,” in Proceedings of the 13th International Conference on Web Search and Data Mining, ser. WSDM ‘20, New York, NY, USA: Association for Computing Machinery, 2020, p. 825–828. [Online]. Available: https://doi.org/10.1145/3336191.3371865.

[16] V. Moustaoka, Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. An-thopoulos, “Enhancing social networking in smart cities: Privacy and security borderlines,” Technological Forecasting and Social Change, vol. 142, pp. 283–300, 2019.

[17] M. Tsay-Vogel, J. Shanahan, and N. Signorielli, “Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among facebook users,” New Media & Society, vol. 20, no. 1, pp. 141–161, 2018. [Online]. Available: https://doi.org/10.1177/1461444816660731.

[18] I. Sari, “Çocuk ve bilişim sanaldan gerçekle sorunlar: Çözüm önerileri ve iyi uygulama örnekleri. samer yayınları. erişim tarihi: 14 temmuz 2019,” 2013.

[19] M. Anderson, “Parents, teens and digital monitoring,” Pew Research Center: Internet, Science & Tech, 2016.

[20] A. A.-A. Mohamed, “Online privacy concerns among social networks’ users,” Cross-cultural communication, vol. 6, no. 4, pp. 74–89, 2011.

[21] M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: threats and solutions,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019–2036, 2014.

[22] J. Baltazar, J. Costoya, and R. Flores, “The real face of koobface: The largest web 2.0 botnet explained,” Trend Micro Research, vol. 5, no. 9, p. 10, 2009.

[23] Z. Mao, N. Li, and I. Molloy, “Defeating cross-site request forgery attacks with browser-enforced authenticity protection,” in International Conference on Financial Cryptography and Data Security. Springer, 2009, pp. 238–255.

[24] V. B. Livshits and W. Cui, “Spectator: Detection and containment of the largest web 2.0 botnet explained,” IEEE Access, vol. 8, pp. 144292–144309, 2020.

[25] Z. Theodosiou, A. Vakali, A. Kounoudes, and L. G. An-thopoulos, “Enhancing social networking in smart cities: Privacy and security borderlines,” Technological Forecasting and Social Change, vol. 142, pp. 283–300, 2019.

[26] I. Paul, “Twitter worm: A closer look at what happened,” PCWorld, San Menlo Park, CA: USENIX Association, Jul. 2014, pp. 143–157. [Online]. Available: https://www.usenix.org/conference/soups2014/proceedings/presentation/das.

[27] Z. Chia, Y. C. Chiang, J. Guo, Y. H. Lin, and B. Lin, “Enabling the analysis of behavioral disorders in social networks,” in Proceedings of the 13th International Conference on Web Search and Data Mining, ser. WSDM ‘20, New York, NY, USA: Association for Computing Machinery, 2020, p. 825–828. [Online]. Available: https://doi.org/10.1145/3336191.3371865.

[28] I. Sari, “Çocuk ve bilişim sanaldan gerçekle sorunlar: Çözüm önerileri ve iyi uygulama örnekleri. samer yayınları. erişim tarihi: 14 temmuz 2019,” 2013.

[29] M. Anderson, “Parents, teens and digital monitoring,” Pew Research Center: Internet, Science & Tech, 2016.

[30] A. A.-A. Mohamed, “Online privacy concerns among social networks’ users,” Cross-cultural communication, vol. 6, no. 4, pp. 74–89, 2011.

[31] M. Fire, R. Goldschmidt, and Y. Elovici, “Online social networks: threats and solutions,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 2019–2036, 2014.

[32] J. Baltazar, J. Costoya, and R. Flores, “The real face of koobface: The largest web 2.0 botnet explained,” Trend Micro Research, vol. 5, no. 9, p. 10, 2009.

[33] Z. Mao, N. Li, and I. Molloy, “Defeating cross-site request forgery attacks with browser-enforced authenticity protection,” in International Conference on Financial Cryptography and Data Security. Springer, 2009, pp. 238–255.

[34] V. B. Livshits and W. Cui, “Spectator: Detection and containment of javascript worms,” in USENIX Annual Technical Conference, 2008, pp. 335–348.

[35] I. Paul, “Twitter worm: A closer look at what happened,” PCWorld, San Francisco, CA, USA, 2009.

[36] T. Amin, O. Okhiria, J. Lu, and J. An, “Facebook: A comprehensive analysis of phishing on a social system,” 2010.

[37] E. Mills, “Facebook hit by phishing attacks for a second day,” CNET News, pp. 8301–1009, 2009.

[38] D. Gunatilaka, “A survey of privacy and security issues in social net-works,” CSE571S: Network Security, pp. 1–12, 2011.
[30] A. Sadeghian, M. Zamani, and B. Shanmmugam, “Security threats in online social networks,” in 2013 International Conference on Informatics and Creative Multimedia. IEEE, 2013, pp. 254–258.

[31] S. Guha, K. Tang, and P. Francis, “Noyb: Privacy in online social networks,” in Proceedings of the first workshop on Online social networks, 2008, pp. 49–54.

[32] H. Saleem, J. Butt, A. Siddiqui, S. Saleem, A. S. Lalani, and M. Awang, “Behavioural tendency analysis towards e-participation for voting in political elections using social web,” International Journal of Management (IJM), vol. 12, no. 4, 2021.

[33] F. R. Abubaker and P. S. Boluk, “An intelligent model for vulnerability analysis of social media user,” in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). IEEE, 2016, pp. 258–263.

[34] S. Damen and N. Zannone, “Privacy implications of privacy settings and tagging in facebook,” in Workshop on Secure Data Management. Springer, 2013, pp. 121–138.

[35] I. Symantec, “Internet security threat report,” Mountain View, Vol. 19., CA:[sn], 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[36] “Informed investor advisory: Social networking,” http://www.nasaa.org/5568/informed-investor-advisory-social-networking/2011.

[37] M. Chi and R. Wanner, “Security policy and social media use,” ‘Reducing the Risk of Social Media to Your Organizations. Retrieved January, vol. 18, p. 88, 2011.

[38] N. N. A. Molok, A. Ahmad, and S. Chang, “Information leakage through online social networking: Opening the doorway for advanced persistence threats,” Journal of the Australian Institute of Professional Intelligence Officers, vol. 19, no. 2, p. 38–55, 2011. [Online]. Available: https://search.informit.org/doi/10.3316/informit.308417070681457

ASLIHAN BANU CENGIZ received her B.Sc. degree in mathematics from the Bahcesehir University, Istanbul, in 2016. She received the M.Sc. degree in information technologies from Bahcesehir University, in 2020. Her research interests include social media users behaviors.

PINAR SARISARAY BOLUK received the M.S. and B.S. degrees in Computer Engineering from Karadeniz Technical University, Trabzon. She earned the Ph.D. Degree in the Computer Engineering Department at Istanbul Technical University, Istanbul. She did postdoctoral training at the Computer Science Department of Southern Illinois University in 2013. Currently, she is serving as an Associate Professor at Software Engineering Department of Bahcesehir University; Istanbul. Her research interests are Wireless Sensor Networks, Network Security, Software Development, Analysis and Design, Emergency Management.

GULER KALEM received her B.Sc. and M.Sc. degrees from the Computer Engineering Department of Atılım University in 2003 and 2005, respectively. She studied at Medical Informatics Department of METU for her Ph.D studies. Later, she received her Ph.D degree from the Software Engineering Department of Atılım University in 2017. She is currently working as an instructor in the Department of Software Engineering, Atılım University, Ankara, Turkey. Her research interests include medical informatics, information systems, healthcare/mobile technologies, reasoning systems, network security and the semantic web technologies.