RESEARCH ARTICLE OPEN ACCESS

Security Analysis of Social Engineering Attacks in Social Media Messaging Applications

Fahad Almuawi*, Mahjoub Hammad**
** (Department of Information Systems, Bishah University, KSA*
*** (Department of Information Systems, Bishah University, KSA*

ABSTRACT
The use of social media applications is a necessary component of modern life. Users of these applications are exposed to a variety of attacks for a variety of reasons. WhatsApp is a popular app in Saudi Arabia that allows users to share and exchange text, documents, and photographs with friends, family, and even workplaces. The researcher's goal in this work is to determine the prevalence of WhatsApp attack incidences and study how these attacks occur. The researcher prepared a study tool, which is an electronic questionnaire consisting of 13 questions. The questionnaire was sent to a large population of WhatsApp users in Bishah Province of which return the responses of 311 participants. The research assesses users' understanding of how to follow WhatsApp security rules, as well as the most well-known methods employed by attackers. The study concluded with several recommendations that should help to lower the risk of security threats using social media applications. One of the most important conclusions reached by the study is that in some cases, security notifications should be mandatory rather than optional, and that the notification given when a request to transfer a user account from one device to another should be improved.

***Keywords* -** Breaches, Instant Message, Social Engineering, Social Media, WhatsApp

Date of Submission: 20-06-2021 Date of Acceptance: 05-07-2021

I. INTRODUCTION

Relationships and conversations between people are part of human nature. Meeting and talking was the old way of communicating between people. Technology and modern means of communication have changed the way we communicate. Today we have many ways of digital communication. We can use Facebook to keep in touch with our friends and family and share them with posts, pictures, and links. We have Twitter for micro-blogging, WhatsApp for instant messaging. There are many other sites and applications. Using social media, we have instant access to millions of peoples, and we have new ways of interaction. [9]

One of the common problems on social media is the threats or attacks that a hacker uses with a specific goal, [28] usually to destroy something and obtain it illegally. [27] Social engineering is a technique used by cybercriminals to convince them to download malware from the internet or fill out their details under pretences. Moreover, the WhatsApp application is considered one of the most popular instant messaging applications. [5] Therefore, the paper will study breaches incidents related to this application. The purpose of this paper is to examine social media security risks, specifically the WhatsApp application and current mitigation techniques, [14] to gather insights and develop best practices to help individuals and organizations address social media security risks more effectively. [4] The researcher conducted an anonymous questionnaire and asked Whatsapp application users to fill in the questionnaire.

Finally, this paper concludes with some suggestions/recommendations regarding WhatsApp's social engineering attacks to reduce WhatsApp's security threats:

- Security notifications should not be optional. i.e., The user should not have the ability to disable security notifications.
- Going through some security notifications, they appear to be some more technical and therefore are not understandable to regular user. This makes them less useful for the user to take the appropriate action because he does not understand the message of the notification, or it is not clear for him what action he should take. It is recommended that the notifications contain some choices that the users are advised to take to help make the most appropriate action.
- Require two-step verification on transferring accounts from one device to another.

II. LITERATURE REVIEW

The literature review is executed to several practitioners and academic papers and books and defines Social Engineering, the Social Engineering attack and analysis Attacks on Secure Messaging Applications. Also, the researchers discuss issues such as user awareness and, finally, pay tribute to the effort expended to create methods that will help assess social media security.

2.1 Social Engineering definitions

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. [24] Social engineering is the exploitation of human error to obtain private information, access, or valuables. By doing ways to entice unsuspecting users to divulge the data. [1] [16]

Many information security practitioners and academia define social engineering, as described below:

The Team of Security Through Education:

We define it as, "Any act that influences a person to take an action that may or may not be in their best interest." [26]

2.2 Awareness of social engineering and counter-measures

Social engineers use a variety of persuasion strategies to persuade people to do what they want. Cyber-attacks can affect universities, hospitals, and educational institutions. To protect them from such attacks, we must boost social engineering awareness among students and other vulnerable populations. [12]

According to one of the study reports, [3] The researcher suggested a threat analysis approach based on graphs for social engineering and technological attacks. The most effective path for the attacker can be defined using mathematical equations. The researcher used a systematic method to clarify the situation, channel, attacker, and related principles and the effectiveness of the proposed strategy in preventing attacks. [3] Authority, obedience, and lying are all traditional methods of coercion. According to the author, robots will be able to search online, collect the desired information, and then process the data to extract behavioural patterns in a specific time. Similarly, the author stressed the importance of informing people about information security and social engineering attacks in various studies.

[7] [8] [12] The authors of the study studied into the dangers of human attacks before suggesting ways to safeguard against them. The authors also looked into the various methods of human manipulation and the mediums utilized in social engineering attacks (phone, web, and physically). Finally, the authors presented a number of techniques for protecting against attacks.

2.3 Moral principles and social engineering studies

Mouton et al. addressed the ethical consequences of social engineering research in their study [2]. To begin, researchers clarified that ethical considerations must be taken into account when conducting social engineering research. The researcher also explored concerns about performing social engineering in public relations.

2.4 About Whatsapp

WhatsApp is a mobile messaging program that allows users to exchange messages without having to pay for SMS. It was founded in 2009 with the tagline "Simple. Personal. Real-time messaging." Brian Acton and Jan Koum launched the WhatsApp messenger in 2009 with the goal of making communication and the sharing of multimedia message easier and faster. [21] WhatsApp relies on internet connections to keep users in touch with friends and family on their contact lists. It not only allows users to communicate with one another, but it also allows them to form groups and send unlimited photos, video, and voice messages. [14] [17]

According to studies, WhatsApp is the most popular instant messaging app among today's young. Because WhatsApp uses internet data, its popularity among adolescents has resulted in a large profit for service providers. WhatsApp's popularity among young people stems from the fact that it allows them to send limitless texts to their friends and family members at no cost other than the internet data plan that they already have on their phones. After downloading, the application is really simple to use. It displays you who in your contacts is using WhatsApp and also assists them in inviting their friends who have yet to download and use the app. They can then begin communicating, sharing audio and video files, updating status, etc. [22] [23]

2.4.1 Definitions

WhatsApp is a messaging app that allows you to communicate It's a common mobile instant messaging (MIM) app that lets users send text messages, images, links, and photos, as well as make voice calls [32]. It's also used to keep online communities together, thanks to features like groups and multi-party chat. [25]

WhatsApp provides free messaging and calling that is quick, simple, and safe, and is available on phones all over the world. [20]

2.4.2 Privacy and security in WhatsApp

WhatsApp began as a text-messaging service. It now allows you to send and receive a variety of media, including text, images, videos, documents, and location, as well as audio, video, and conference calls. [13] End-to-end encryption covers WhatsApp messages and calls, ensuring that no third party, including WhatsApp, can read or listen to them. [11] [31]

WhatsApp have several key features that provided both positive and negative use considerations. WhatsApp eased communication among MMs and supported participation in group activities despite differing schedules and geographic locations. [30] [32] Challenges encountered with WhatsApp included:

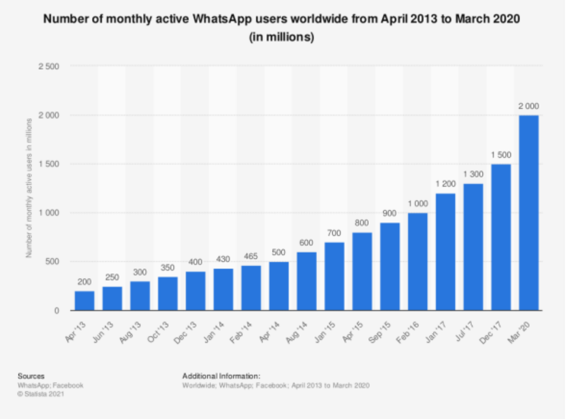
- Financial restrictions to data storage and continual access.
- Self-confidence using technology.
- Security and privacy concerns. [6]

2.4.3 End-to-end encryption (E2EE) in WhatsApp

End-to-end encryption is described as communications that remain encrypted from the sender's device to the recipient's device, with no third parties, including WhatsApp and our parent company Facebook. [11] [20]

The use of E2EE in common instant message (IM) apps like WhatsApp, Viber, Telegram, and Signal was investigated in a study [33]. Although IM apps are used by billions of people worldwide, offering functional encryption is a challenge. E2EE in group chats and various device support are two of these challenges [33]. Supporting E2EE in group chats on multiple devices linked to the same account, such as a smartphone and a laptop, goes beyond trivial, according to study [33]. Although both WhatsApp and Viber, which are both proprietary, have made E2EE the default setting for all conversations. If the communication channel is compromised, Signal Protocol supports forward secrecy, which prevents previously transmitted messages from being decrypted and read. [19]

WhatsApp had two billion monthly active users in March 2020, up from over one billion in February 2016. In February 2014, Facebook bought the service for 19 billion dollars, making it one of the world's most popular mobile messaging applications. The chart below shows how common it has become in recent years. [18]



Sources
WhatsApp; Facebook
© Statista 2021

Additional Information:
Worldwide; WhatsApp; Facebook; April 2013 to March 2020

Figure 1: Growth of WhatsApp users 2013 to 2020

III. METHODOLOGY

3.1 Introduction

WhatsApp is a popular smartphone app that allows users to send and receive IM. It enables Internet services to send and receive various types of text and multimedia messages among users or groups. A questionnaire-based research method was used to extract information about the respondents' characteristics regarding their level of use of WhatsApp. A questionnaire conducted targeting the most significant possible number of social media users in the Bishah governorate. The study asks about the most important reasons users disclose their data or fall victim to attackers. A sample size of 311 was used in this study and administered randomly amongst residents of Bishah so that it reaches different ages, genders and educational levels.

3.2 Data Analysis

In this section, we present an analysis of participants' responses to the questionnaire. The researcher did analyzed responses from 311 participants.

The questionnaire was performed an internet-based questionnaire using Google Forms and obtained responses. The study group of the research consists of 49 females (15.8%), 262 males (84.2%); a total of 311 persons should represent the society of Bishah (Table 1).

Table 1: Gender of Participants

Demographic Details		Frequency	Percent
Gender	Male	262	84.2 %
	Female	49	15.8 %
	Total	311	100 %

Out of 311 participants responded to the question of age, 3 less than 15 years, 43 were between the ages 15 and 25, 245 were between the ages of 26 and 50 and 20 over 50 (Table 2). Most of the participants were in the 26-50 age range.

Table 2: Age of Participants

Demographic Details		Frequency	Percent
Age (years)	Less than 15	3	1 %
	15 - 25	43	13.8 %
	26 – 50	245	78.8 %
	Over 50	20	6.4 %
	Total	311	100 %

We asked the participants about their level of education. The result is available in (Figure 2). However, education is a core demographic question because participants in different education levels may answer differently based on their background in security and protection, as the researcher will try to analyze the respondent's awareness.

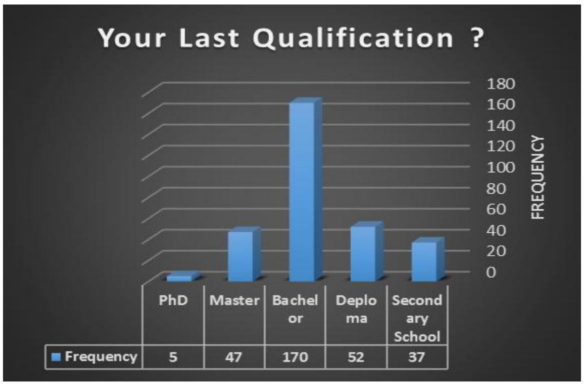


Figure 2: Types of Qualification

WhatsApp allows anyone to talk with their friends and family in a social environment. Based on these features, the researcher collected the data by asking the question, "Do you use WhatsApp?" Determine the prevalence and use of WhatsApp in the Bishah culture. The response rate was 100% with approval.

After testing it since November 2016, Facebook provided two-step verification in February 2017 to improve WhatsApp message protection significantly. One of the questionnaire's goals is to determine the level of consumer knowledge and enforcement of the company's policies to protect customers' privacy from unauthorized individuals. We are going to ask a question to find out the answer to this simple question. Have you allowed two-factor authentication?

The following were the responses: Two-step verification was not enabled by 45 of the 311 respondents. As shown below in (Figure 3).

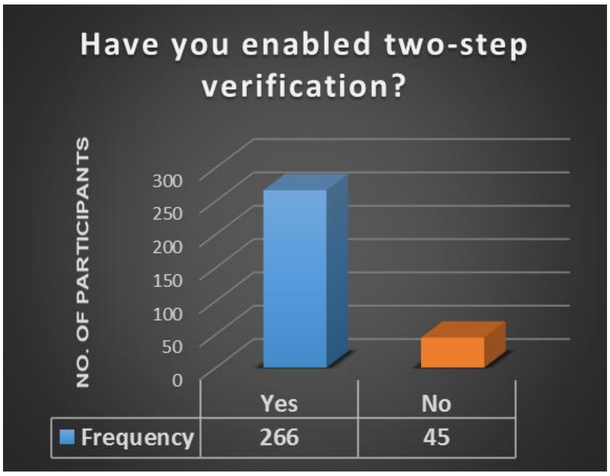


Figure 3: Participants Opinion about WhatsApp enabled two-step verification or Not.

Additionally, we asked the participants, have you been exposed to any Whatsapp scam or robbery attempt?

The study indicates that about 16% of respondents answered yes and reported having previously been defrauded, while 84% said they had never been tricked before. (Figure 4)

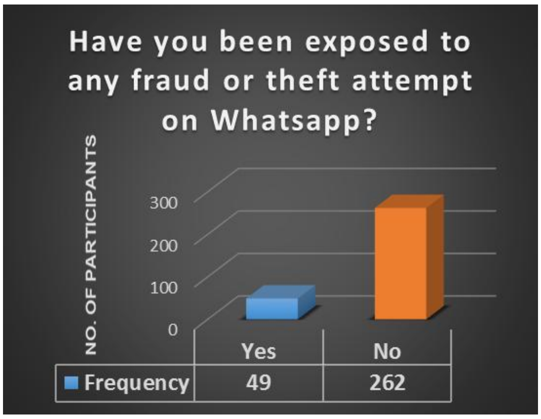


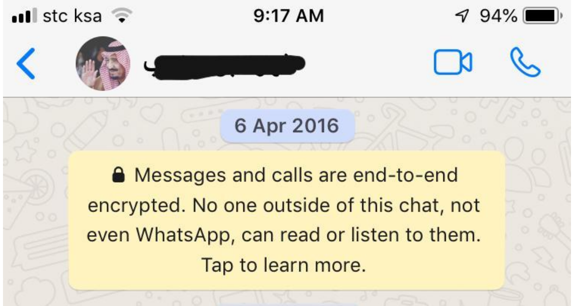
Figure 4: Participants Opinion about on whether they have you been exposed to any fraud or theft attempt on Whatsapp or Not.

Even with a significant development, such as WhatsApp rolling out end-to-end encryption, it ensures only you and the person you're communicating with can read or listen to what is sent, and nobody in between, not even WhatsApp. [11] (Figure 5) This is because, with end-to-end encryption, your messages are secured with a lock, and only the recipient and you have the unique key needed to unlock and read them. Surprisingly, despite WhatsApp's end-to-end security info messages and the high media attention, the majority of the participants were not even aware of encryption. A direct question is asked with multiple

answering options (Table 3). A straightforward question is asked with multiple answer options.
How did the attempted hack/fraud/data theft take place?

- I have received a link, and I clicked on it.
- I have been contacted by someone on the phone.
- I got a message from someone I trust, but his account was compromised
- I was asked to download an application to provide a service related to WhatsApp
- Other than that

The number of participants in this question was (49), and the highest share for selection was I got a message from someone I trust, but his account was compromised. With 29 frequencies (59%).



[redacted]

6 Apr 2016

Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

Figure 5: End-To-end Encryption

Table 3: The methods used to deceive the participants

How did the attempted hack / fraud / data theft take place?	Frequency	Percent
I have received a link and I clicked on it.	9	2.9
I have been contacted by someone on the phone.	5	1.6
I got a message from someone I trust, but his account was compromised	29	9.3
I was asked to download an application to provide a service related to WhatsApp	1	0.3
Other than that	5	1.6
No. of participants	49	15.8
The remaining participants are:	262	84.2
Total	311	100

To understand the reasons used to make the participants fall victim to the hacker is a straightforward question asked to the participants with multiple answer options including text so that people can write any other reason. Most of the participants gave multiple reasons but the majority chose (the other person (the attacker) asked for help and I was trying to help). (Table 4)

Table 4: The reasons used to make the participants fall victim to the hacker

Why did you act like that?	Frequency	Percent
There was an exciting piece of news and I was interested in reading it.	12	3.9
I was promised a service, a discount, or a prize and I wanted to have it.	3	1
The other person (the attacker) asked for help and I was trying to help.	26	8.4
The other person (the attacker) asked me to do a specific procedure related to work/business	5	1.6
Other	3	1
No. of participants	49	15.8
The remaining participants are:	262	84.2
Total	311	100

Table (5) shows the number of breach attempts and the qualifications of the participants. Participants holding a Bachelor degree represents the majority of successful attempts with a percentage of (42.8%). Master degree holders comes second with a percentage of (22.4%). Almost equal to them, participants with diploma degree were (20.4%). Secondary-school participants represent (12.2%) of the total breaches.

Table 5: Shows the number of breach attempts and the qualifications of the participants

Your Last Qualification? * Have you been exposed to any fraud or theft attempt on Whatsapp?					
			Have you been exposed to any fraud or theft attempt on Whatsapp?		Total
			Yes	No	
Your Last Qualificati on ?	Secondary School	Count	6	31	37

	%	1.90%	10.00%	11.90%
Diploma	Count	10	42	52
	%	3.20%	13.50%	16.70%
Bachelor	Count	21	149	170
	%	6.80%	47.90%	54.70%
Master	Count	11	36	47
	%	3.50%	11.60%	15.10%
PhD	Count	1	4	5
	%	0.30%	1.30%	1.60%
Total	Count	49	262	311
	%	15.80%	84.20%	100.00%

Table (6) links between breach attempts and whether the victim has already enabled two-step verification. 41 out of 49 had their devices hacked while the installed version of WhatsApp had the two-step verification enabled. This represents 83.6% of the total successful breach attempts. The rest (16.4%) was not enabling this feature when the breach took place.

Table 6: linkages between attempted breaches and whether or not the victim has enabled two-step verification

Have you enabled two-step verification? * Have you been exposed to any fraud or theft attempt on Whatsapp?					
			Have you been exposed to any fraud or theft attempt on Whatsapp?		Total
			Yes	No	
Have you enabled two-step verification?	Yes	Count	41	225	266
		% of Total	13.20%	72.30%	85.50%
	No	Count	8	37	45
		% of Total	2.60%	11.90%	14.50%
Total		Count	49	262	311
		% of Total	15.80%	84.20%	100.00%

Table (7) shows the relationship between the number of breach attempts and how they take place. The first with the highest percentage (59.20%) is by receiving a message from someone the victim trusts and whose devise has been compromised. The second hacking method is that the victim received a link and he clicked on it with a percentage of (18.40%). The third happens when someone contacted the victim on phone (10.20%). Asking the victim to download an application to provide a service related to WhatsApp is the fourth hacking method with a percentage of (2.00%). Of the sample, (10.20%) preferred not to explain how the breach happen.

Table 7: Shows the relationship between the number of breach attempts and how they take place

How did the attempted hack / fraud / data theft take place? * Have you been exposed to any fraud or theft attempt on Whatsapp?					
			Have you been exposed to any fraud or theft attempt on Whatsapp?		Total
			Yes	No	
attempted hack / fraud / data theft	I have received a link and I clicked on it.	Count	9	0	9
		%	18.40%	0.00 %	18.40%

	I have been contacted by someone on the phone.	Count	5	0	5
		%	10.20%	0.00 %	10.20%
	I got a message from someone I trust, but his account was compromised	Count	29	0	29
		%	59.20%	0.00 %	59.20%
	I was asked to download an application to provide a service related to WhatsApp	Count	1	0	1
		%	2.00%	0.00 %	2.00%
	Other than that	Count	5	0	5
		%	10.20%	0.00 %	10.20%
Total		Count	49	0	49
		%	100.00 %	0.00 %	100.00 %

IV. RESULTS

From the findings, breaches still exist with a percentage of 15.75% of the total participants of the questionnaire. Security measures in WhatsApp application are not enough to prevent breaches from occurring. This does not mean that security measures such as: Two-Step verification and End-to-End encryption are not strong enough or that they are inadequate. The reason behind such high percentage in breaches may be linked to human factor.

About 59% of the breaches took place when the attacker sends a message to the victim impersonating someone else. So, no matter what encryption the application uses or even whether it employs the two-step verification, users fall victims because they trust the other party then based on that they voluntarily do what the other party request them to do. And this has nothing to do with how strong the encryption is or how many security measures the application adopt. (Figure 6)

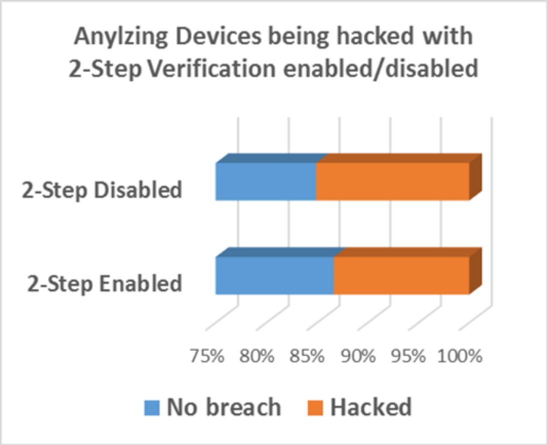


Figure 6: Statistics indicating how many people were exposed to risks dependent on whether two-step verification was enabled or not

After analyzing the responses to this question (Have you enabled two-step verification?), 266 participants out of 311 were enabling this feature which represents 85.5% of the total participants. 45 participants (14.5%) reports not enabling the feature (figure 7). This shows that the majority of the sample are aware of the risks and security threats that the use of the application has.

The researcher suggests that such a feature should be changed from being optional to being obligatory on users. Several actions in the application right now do not require the two-step verification to be set.

When a device linked to a specific account of a person changed, other contacts receive a notification that the key of end-to-end encryption has been changed and tells the user to ensure that key is identical with the other user who has changed his device. The problem with this is that if the user contacted the other one using the same application to do the verification, the other person could be an attacker. This security notice does not show how the user should do this step. The researcher suggests that this notification should be improved to give options for the user to do like making a phone call with the person to validate the encryption key. It should also warn the user against using the same application when doing the verification process.

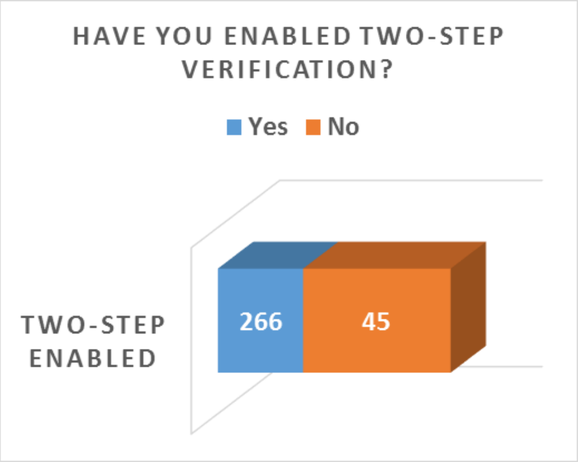


Figure 7: Participants Opinion about actively enabled two-step verification or Not.

The questionnaire shows that the most common way is when a user receives a message from someone the victim trusts and whose devise has been compromised with a percentage of 59.20% of all reported breaches. The human factor should be helped using various techniques to overcome ambiguity that is usually utilized in breach attempts.

Probably all breaches in Whatsapp starts with an attacker compromises the account of a user and has control over it then starts contacting other users in the contact list of the compromised device pretending to be the original user. (Figure 8)

The researcher thinks that current way of transferring an account which involves just entering a verification code (six-digit number sent in a SMS message to the phone number) is not secure enough. The researcher suggests hardening the transferring of an account from one device to another by applying some techniques:

- There should be a message sent from Whatsapp company to the device that the account was originally linked to. The message could be something similar to this " … There is an attempt to transfer your account from this device to another device. Do you start this request?".
- The message should also shows when this attempt happen in addition to any available info about the device being used like the operating system (android, iOS, …), make and model of the device, …etc. That should make the original user aware of the account transferring procedure rather than relying on a six-digit code.
- It could involve the usage of fingerprint in the procedure of account-transferring

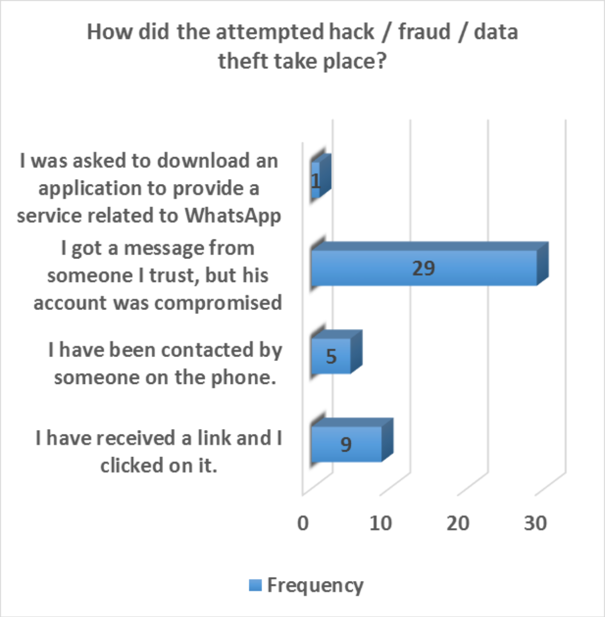


Figure 8: Participants Opinion about Hacking attempts

V. CONCLUSIONS

Surely WhatsApp is indispensable on the phone, anyone can use it to exchange messages, video calls and voice calls between two parties for free. Because of this fame, the application became vulnerable to piracy, espionage, and surveillance. So, when you use WhatsApp, you are vulnerable to penetration at any moment unless you take the basic security and protection steps recommended by the WhatsApp company. In this aspect, the researcher raised several questions by making a questionnaire that was presented to a sample of the residents of Bishah province to measure and know the methods of penetration and threats they were exposed to through the use of WhatsApp application and the extent of their commitment to apply the instructions for security and protection and update the application with security patches that WhatsApp LLC develops.

The percentage of attacks reported by respondents was 15.75% of the total respondents. This does not mean that security measures such as: two-step verification and end-to-end encryption are not strong or insufficient. The researcher believes that the cause of this high percentage of breaches is related to the human factor. Therefore, regardless of the encryption used by the app or even whether it uses two-step verification, users still fall victims because they trust the other party since they voluntarily do what the other party asks them to do. There are some other things WhatsApp users should do to ensure security. The first of which is to run the "Show Security Notifications" option. This will alert the user if a contact's security code has changed and is likely to be compromised. The researcher suggests that activating the alert should be mandatory and not optional, as well as to increase security in the event of an alert that the contact security code has been changed, and several ways are suggested to make sure that they contact the person to ensure his identity using different methods like sending a text message containing a code stating clearly that there is an attempt to transfer the user account to another device or usage of fingerprint in the procedure of account-transferring.

REFERENCES

[1]. Nastase, Lavinia. "Security in the internet of things: A survey on application layer protocols." 2017 21st international conference on control systems and computer science (CSCS). IEEE, 2017.

[2]. Mouton, Francois, et al. "Necessity for ethics in social engineering research." Computers & Security 55 (2015): 114-127.

[3]. Beckers K, Krautsevich L, Yautsiukhin A. Analysis of social engineering threats with attack graphs. DPM/SETOP/QASA, Vol. 8872 of Lecture Notes in Computer Science Springer. Springer; 2014:216-232

[4]. Weichbroth, Paweł, and Łukasz Łysik. "Mobile Security: Threats and Best Practices." Mobile Information Systems 2020 (2020).

[5]. Okereafor, Kenneth, and Rania Djehaiche. "A Review of Application Challenges of Digital Forensics." International Journal of Simulation Systems Science and Technology 21.2 (2020): 35-1

[6]. Guan, D. J., Chia-Mei Chen, and Jia-Bin Lin. "Anomaly based malicious url detection in instant messaging." Proceedings of the joint workshop on information security (JWIS). Vol. 43. 2009.

[7]. Parlakkılıç, Alaattin. "Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach." International Journal of Information Security Science 7.4 (2018): 172-178.

[8]. Bullée, Jan-Willem Hendrik, et al. "On the anatomy of social engineering attacks—A literature-based dissection of successful attacks." Journal of investigative psychology and offender profiling 15.1 (2018): 20-45.

[9]. Schrittwieser, Sebastian, et al. "Guess who is texting you? evaluating the security of smartphone messaging applications." (2012).

[10]. Cai, Xiang, et al. "A systematic approach to developing and evaluating website fingerprinting defenses." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014.

[11]. Whatsapp, Website, online, About end-to-end encryption ttps://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=en.

[12]. Salahdine, Fatima, and Naima Kaabouch. "Social engineering attacks: a questionnaire." Future Internet 11.4 (2019): 89.

[13]. Sushama, C., M. Sunil Kumar, and P. Neelima. "Privacy and security issues in the future: A social media." Materials Today: Proceedings (2021).

[14]. Sutikno, Tole, et al. "WhatsApp, viber and telegram: Which is the best for instant messaging?." International Journal of Electrical & Computer Engineering (2088-8708) 6.3 (2016).

[15]. Conteh, Nabie Y., and Paul J. Schmick. "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks." International Journal of Advanced Computer Research 6.23 (2016): 31.

[16]. Aldawood, Hussain, and Geoffrey Skinner. "A taxonomy for social engineering attacks via personal devices." International Journal of Computer Applications 975 (2019): 8887.

[17]. Johari, Rahul, et al. "S2NOW: Secure Social Network Ontology Using WhatsApp." Security and Communication Networks 2021 (2021).

[18]. “Number of mobile phone messaging app users worldwide from
2016 to 2021,” https: www.statista.com statistics 483255 numberof- mobile-messaging-users-worldwide, 2018.

[19]. Weichbroth, Paweł,Łysik, Łukasz, “Mobile Security: Threats and Best Practices” in Mobile Information Systems, 2020.

[20]. WhatsApp, WhatsApp Encryption Overview. Technical report (2016). https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

[21]. Church, Karen, and Rodrigo De Oliveira. "What's up with WhatsApp? Comparing mobile instant messaging behaviors with traditional SMS." Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services. 2013.

[22]. Hadnagy, Christopher. Social engineering: The art of human hacking. John Wiley & Sons, 2010.

[23]. Long, Johnny. No tech hacking: guide to social engineering, dumpster diving, and shoulder surfing. Syngress, 2011.

[24]. Wikipedia, " Social engineering (security) " Wikipedia, 2020. https://en.wikipedia.org/wiki/Social_engineering_(security) [Accessed: 25-Feb-2020].

[25]. Katharina Krombholz*, Heidelinde Hobel, Markus Huber, Edgar Weippl, "Advanced social engineering attacks" Available online 24 October 2014

[26]. Security Through Education, Website, https://www.social-engineer.org/about/

[27]. Yasin, Affan, et al. "Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG)." Information and Software Technology 95 (2018): 179-200.

[28]. Heartfield, Ryan, and George Loukas. "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework." Computers & Security 76 (2018): 101-127.

[29]. Norton, Emerging Threats, Website: https://us.norton.com/internetsecurity-emerging-threats-what-is-smishing.html

[30]. ICT Report: Mobility in Saudi Arabia. (2019). In CITC. Retrieved from https://www.citc.gov.sa/ar/mediacenter/annualreport/Documents/PR_REP_015A.pdf

[31]. Whatsapp, Website, online https://faq.whatsapp.com/general/security-and-privacy/were-updating-our-terms-and-privacy-policy?ref-banner&lang=en

[32]. Rashidi, Yasmeen, Kami Vaniea, and L. Jean Camp. "Understanding Saudis’ privacy concerns when using WhatsApp." Proceedings of the Workshop on Usable Security (USEC’16). 2016.

[33]. Herzberg, Amir, and Hemi Leibowitz. "Can Johnny finally encrypt? Evaluating E2E-encryption in popular IM applications." Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust. 2016.

AUTHORS

Fahad Almuawi received his B.S. degree in Engineering Technology From the department of Computer Technology, Riyadh Technology, KSA. I am currently working as a trainer in the Computer Department and serves as a head of the Department of Admission and Registration at the Technical College in Bishah. His current research interests include Cybersecurity, Cloud Computing and Biometrics.

Dr. Mahjoub Hammad is an assistant professor of Information systems at College of Computing and Information Technology, Information Systems Department, Bishah University, KSA. Dr. Mahjoub currently serves as a head of Information Systems Department in Bishah University. Dr Mahjoub has many published papers in cyber-security and information systems areas. He also serves as a reviewer in many international journals. His current research interests include Cybersecurity, IOT and biometrics.