Social Engineering Attacks on Facebook – A Case Study

Abdul Shareef Pallivalappil [1, 2], Jagadeesha S. N. [3], Krishna Prasad K.[4]

[1] Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India.

[2]Assistant Professor, Department of Forensic Science, Jain (Deemed-to-be-University), JC Road, Bangalore, India.

ORCIDID: 0000-0001-6221-7078; Email ID: shareef.abdul777@gmail.com

[3]Research Professor, College of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India.

ORCIDID: 0000-0002-5185-2233; Email: jagadeesha2012@gmail.com

[4]Associate Professor & Post-Doctoral Research Fellow, College of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India

ORCIDID: 0000-0001-5282-9038; Email ID: krishnaprasadkcci@srinivasuniversity.edu.in

Area of the Paper: Computer Science
Type of the Paper: Research Case Study
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed In: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.5765883
Google Scholar Citation: IJCSBE

How to Cite this Paper:

Abdul Shareef, Pallivalappil, Jagadeesha, S. N., & Krishna Prasad, K., (2021). Social Engineering Attacks on Facebook – A Case Study. *International Journal of Case Studies in Business, IT, and Education (IJCSBE),* 5(2), 299-313. DOI: https://doi.org/10.5281/zenodo.5765883

International Journal of Case Studies in Business, IT and Education (IJCSBE)
A Refereed International Journal of Srinivas University, India.

Crossref DOI : https://doi.org/10.47992/IJCSBE.2581.6942.0135

Disclaimer: The scholarly papers as reviewed and published by the Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the S.P. The S.P. disclaims of any harm or loss caused due to the published content to any party.

Social Engineering Attacks on Facebook – A Case Study

Abdul Shareef Pallivalappil.[1, 2] Jagadeesha S. N. [3] Krishna Prasad K.[4]

[1] Research Scholar, College of Computer Science and Information Science, Srinivas University, Mangalore, India.

[2]Assistant Professor, Department of Forensic Science, Jain (Deemed-to-be-University), JC Road, Bangalore, India.

ORCIDID: 0000-0001-6221-7078; Email ID: shareef.abdul777@gmail.com

[3]Research Professor, College of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India.

ORCIDID: 0000-0002-5185-2233; Email: jagadeesha2012@gmail.com

[4]Associate Professor & Post-Doctoral Research Fellow, College of Computer Science and Information Science, Srinivas University, Mangalore, Karnataka, India

ORCIDID: 0000-0001-5282-9038; Email ID: krishnaprasadkcci@srinivasuniversity.edu.in

ABSTRACT

Background/Purpose: *Facebook is an American business that offer online social networking services. Facebook was founded in 2004 by Harvard University freshmen Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes. Free access to Facebook enables new users to create profiles, upload photos to existing groups, and start new ones. Every user's profile page has a Timeline area where they can upload material and their social network connections may reply with messages and Status updates informing them of their current location or condition. Additionally, Facebook includes a function called News Feed that notifies users of updates to their friends' profiles and statuses. Users can communicate with one another and exchange private messages using Facebook Messenger. Additionally, Facebook users may express their approval of a type of content by clicking the "Like" button. Every day, more than a billion people use Facebook, making it the most common social network on the planet. Menlo Park, California, is where the company's headquarters are located.*

Objective: *To analyse how Facebook is misused and turned into an attack platform, in order to get sensitive information that can be used to create an attack profile against an individual.*

Design/Methodology/Approach: *SWOT framework is being used to analyse and display information gathered from scholarly publications, web articles, and other sources.*

Findings/Results: *Social Engineering Attacks using Facebook help the attackers to steal sensitive private information from unaware users. Using a false profile is one of the most frequent techniques to execute a large-scale data harvesting attack. Cyber Criminals use Facebook as the main target for social engineering attacks because of its high number of users and popularity.*

Originality/Value: *This paper study gives a brief overview of Social Engineering Attacks on Facebook based on a variety of data collected.*

Paper Type: *Case study-based Research Analysis*

Keywords: Social Engineering Attack, Facebook, Social Network, Data Privacy, Fake Profiles, Attacks on personal Data, COVID-19, SWOT analysis

1. INTRODUCTION :

Facebook is a social networking and technology business based in the United States that was created in 2004 by Harvard classmates Mark Zuckerberg, Chris Hughes, Eduardo Saverin, Dustin Moskovitz, and Andrew McCollum. When the site was originally released on college campuses, it allowed users to create profiles and post updates with their peers around the time of it's with the addition of chat, photo and video sharing, it rapidly became renowned for colloquialisms such as "Making friends." however Facebook is now a authoritative advertising platform, driving projects to offer internet availability in poor nations, and advancing into virtual reality (VR) artificial intelligence (AR). Mark Zuckerberg who is leading Facebook paved its way to have more than a daily average of billion active users, with maximum number of users from them accessing the network via its mobile application. While Messenger app of Facebook has grown into a highly used platform on its own and due to the popularity of Instagram and the acquisitions of Oculus VR (in 2014), Facebook's reach and impact as a social network has grown significantly. Though Facebook has incorporated several safety features, cyber criminals are finding new method to steal data of users by initiating several social engineering attacks that is technical and also non-technical in nature. This paper will aim at understanding Facebook and its features along with different type of cyber-attacks through which cyber-criminal is targeting users to retrieve vital personal information and misuse them.

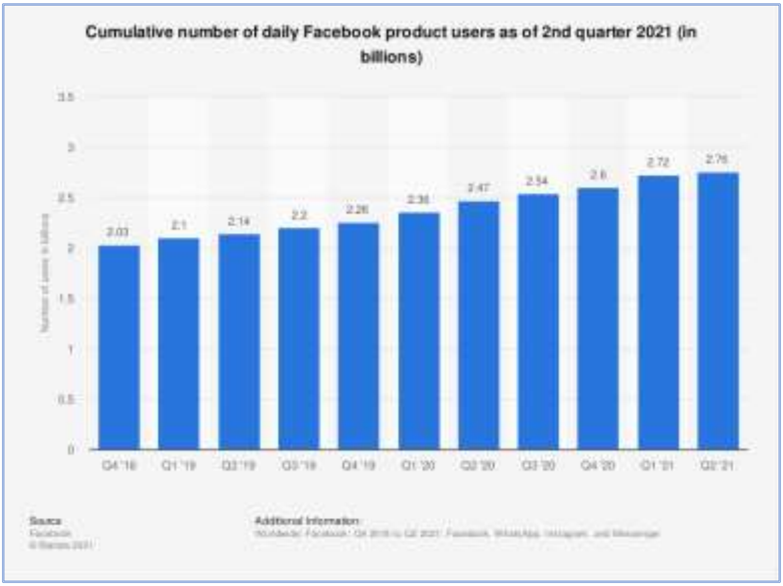

Fig.1: shows number of daily Facebook users as on 2nd Quarter 2021. (Source: statistica.com)

2. OBJECTIVES OF THE CASE STUDY :

These are the main objectives of the case study;
1. To understand the history of Facebook.
2. To study the strategy and business model of Facebook.
3. To understand the impact made by social engineering attacks on Facebook.
4. To investigate how the COVID-19 pandemic impacted the rise in cyber-attacks.
5. Use SWOT analysis for Facebook's performance evaluation.

3. RELATED WORKS :

Several research have been carried out in order to analyse and minimise the attack vector on social media and particularly prominent platforms like the Facebook. These studies have been successful in creating a high level of public awareness and preparedness for social engineering attacks. These connected works have given an understanding of the same by influencing security lapses that made it easier to carry out social engineering attacks such as security, sustainability, motivational factors, etc.
Table 1 summarises relevant research on various sorts of social media and Facebook privacy, as well as the study's area, topic, and citations.

Table 1: Related Works

Sl. No.	Area of study	Topic	Reference
1.	Facebook Security.	An explanation of the immune system architecture and issues faced by Facebook.	Stein et al., (2011). [1]
2.	Sustainability.	The fraudulent identities on Facebook	Krombholz et al.,

		are studied from the perspective of privacy considerations.	(2012). [2]
3.	Privacy concerns.	A study that elucidates that the least essential aspect for Facebook users are privacy preferences.	Garg et al., (2014). [3]
4.	Taxonomy of social engineering attacks.	As the decline in personal interaction and the abundance of communication facilities (such as email, instant messaging, Skype, Dropbox, LinkedIn, and Lync), social engineering attacks have new attack vectors.	Krombholz et al,. (2015). [4]
5.	Source credibility dimensions.	Intends to find out if source features affect how vulnerable Facebook users are to social engineering attacks.	Algarni et al., (2017). [5]
6.	Motivational factors.	According to the findings, information sharing, social engagement, and self-expression are all linked to a person's willingness to be open and honest about their feelings and thoughts.	Ajis, (2020). [6]
7.	Facebook users' data security and awareness.	Adults, who have a greater stake in Facebook privacy settings, have done so more diligently than young people, who tend to overshare on the social networking site.	Calbalhin, J. P (2018). [7]
8.	Protection Motivation Theory (PMT) framework.	According to the findings, the most important benefit driving privacy management was meeting social needs.	Vishwanath et al., (2018). [8]
9.	*in situ* identity.	This study suggests using continuous authentication to detect attacks in a situation where the same account, computer and IP addresses are same as their victims.	Wu et al., (2014). [9]
10.	Privacy Protection Behaviours (PPB)	Consumers are compelled to adopt specific habits in order to safeguard their privacy despite Facebook's noble purpose of connecting people.	Alkite et al., (2019). [10]

4. METHODOLOGY :

Explanatory study is carried out to ascertain the size and type of Facebook affect correlations in order to evaluate the effects of prescribed rules, diverse procedures, and so forth. Journals, conference papers, media articles, and public records were used to gather material and data for this case study.

5. FACEBOOK – AN OVERVIEW :

Facebook lets anyone above the age of 13 to open a free account [11]. It facilitates messages and status updates to be able to be sent between friends and relatives. In addition, it may exchange a variety of material, including images and links. As opposed to other forms of online communication, sharing anything on Facebook is a little bit different. Once a message or photo is posted, it can be viewed by public unless proper privacy settings are applied [12]. Also, users can create profile which contains complete names, telephone numbers and e-mail addresses, as well as information about jobs and social networks, photographs and records of activities [13].

5.1 Facebook Security Features:

Facebook Groups: Facebook allows to group friends lists into different categories such as public, custom, and friends. When sharing a photo or a post, users can choose a group to share such posts or photos. The information of a public group will be viewable to all who have access to the profile. The posts or photographs in the friend's option are only available to the user's list of friends. Users have the option to create individual groups to exchange the information, such as co-workers, college friends, and classmates [14].

Keeping the Contents of Profiles Private: The information on a Facebook user's profile can be controlled by the user. Facebook allows users to share information with particular individuals or make it completely public. Users can, for example, make their phone number available to family members and their date of birth visible to friends. Friends of users can also submit a relationship or photo tag request, which will show in the user's profile. The users can either accept or reject the request. As a result, harmful posts can be prevented from appearing in the profile page. The user can again limit the information on their profile, based on the groups they belong to.

Managing the Privacy of Posts: A user has the ability to specify which groups are permitted to view a particular post. This security feature enables users to exchange confidential information with family and friends without revealing it to the world or sharing it with others in their list of friends.

Modify Previous Posts: Users have the ability to edit their previous postings. In actuality, two factors contribute to the change of earlier entries. Users may now alter what they've previously typed on Facebook. Users can also change the privacy settings for previous postings at any time with Facebook's new security feature. For example, if user have posted something publicly and now wish to make it available to a select group of friends. They can modify the privacy settings for that individual post and share in this situation.

Blocking Doubtful Accounts: Facebook automatically checks new accounts for identity verification. It examines the user's profile information, the frequency of friend requests made by the new user, the volume of friend requests replied to, the posts, and the replies of friends during a certain time period. If a user's account has a lot of random and large outgoing friend requests, Facebook will notify him or her and restrict him or her from sending friend requests for a specific amount of time. Furthermore, if a new or existing account has been flagged as dangerous or suspicious by a large number of people, Facebook will block it. Before every user attempt to create an application, Facebook will verify his or her identity by asking an SMS verification or a voice call. Malicious applications will be less likely to send automated friend requests as a result of this.

Account Snooping Logs: If someone logs into a Facebook account without the user's consent. Users can find the activity logs by going to Facebook Settings > Security and Login and searching for "Where You're Logged In". Users may discover all active Facebook log-ins from desktop and mobile devices, as well as across applications such as Messenger. It will offer information on the user's current location, browser, and device. If anything doesn't look right, user can log out of individual devices or all devices at once. This is useful if a user forgets to log out of a friend's laptop or a public computer [15].

6. DIFFERENT TYPES OF CYBER ATTACKS TARGETING FACEBOOK :

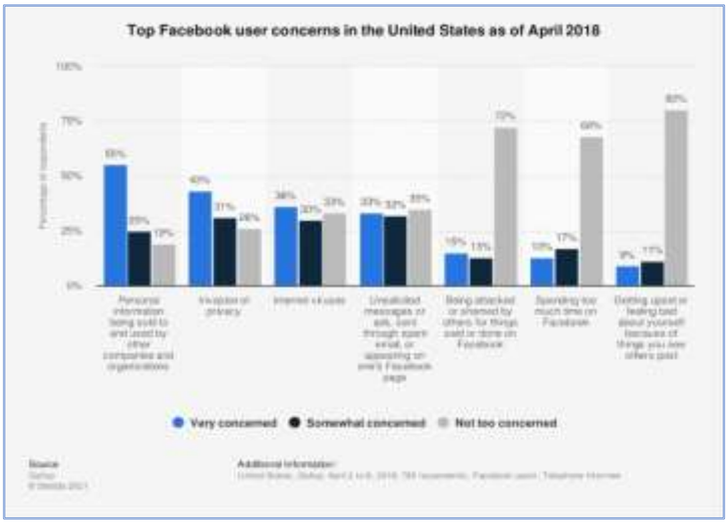

Fig.2: Explains about Facebook users concerns in US. (Source: statistica.com)

Intellectual Property Theft: Facebook users post images, videos, and music with the aim of sharing them with their friends. In Facebook, they might easily become victims of intellectual property theft. This sort of violence can be perpetrated by both known and unknown individuals. When a user shares his or her information with only his or her friends, but they misuse this intellectual property, such as a photo or video, because there is no stringent copy write legislation for these types of data, a threat arises from known persons [16].

Identity Theft: Facebook users may be unaware of the security of their personal information and, as a result, publish it on their profile, making it easy for someone to steal their identity. The opponent can use such information to search up the person's identity and use it for unlawful reasons. Furthermore, some users provide their exact location and address, which an assailant might use to physically assault them [17].

Breach of Personal Information: Many Facebook users accept friends they've never met face to face. An attacker may simply become friends with the users in this circumstance, providing him or her access to personal datalike date of birth, email, and mobile number. An adversary's capacity to phish information and spam email poses a threat. A malicious script can also be used to invite friends [18].

Viruses, Cross Site Scripting (XSS) and attack initiated using computer worms: Because of third-party apps, Facebook is also vulnerable to XSS attacks. This sort of attack allows the proprietor of a third-party programme to inject malicious code into the user's profile, allowing the account to be compromised and therefore making phishing attacks easier [19].

Attacks targeting friends list: If an attacker is able to add someone as a friend, he or she can gain access to that person's friends list and send harmful links or requests to those friends. The attacker has the ability to propagate rumours and/or harmful software to everyone on the friend list. Users are inconvenienced, and the network and server are overburdened with unnecessary data. Clickjacking is also a problem for Facebook users. Users unwittingly click on a link and transmit malware throughout the network as a result of this assault. Attackers generally post some fascinating or harmless news on people's Facebook pages, along with a like button or a link to read more. When someone clicks on that link, the malicious application spreads to all of his or her friends, who all receive the identical link. As a result, this malicious programme propagated from a single person's wall to tens of thousands of people.

Social Engineering on Facebook: Not only is Facebook the most popular social network, but it's also a hotspot for social engineering cyber assaults [20]. Social engineering attacks occur when individuals are duped in order to exploit a target. Phishing attacks, Trojan software, and Internet scams are all examples of social engineering assaults [21]. According to ISACA's up-to-date statement, State of Security 2021, Part 2, social engineering is the foremost reason of organisational compromise, whereas PhishLabs' Quarterly Threat Trends and Intelligence Report indicated a 22% rise in the number of phishing assaults in the first half of this year against the same period last year. Similarly, Breach Investigations Report of Verizon's 2021 Data identified social engineering as the furthermost main method of data breach attack, noting85 percent of attacks target in some way on the human element of cybersecurity. Gemini's recent research also demonstrates how cybercriminals can commit payment fraud by utilising social engineering methods to circumvent specific security rules such as 3D Secure [22]. At the moment, social engineering attacks are the most significant threat to cybersecurity [23], they can be detected but not prevented. Hence, further details are mentioned as follows;

7. SOCIAL ENGINEERING ATTACK TYPES ON FACEBOOK :

Social networking engineering crimes are easy to disseminate, hard to trace to the culprit, and cost very little per victim. They are very well threats wherein the offender seeks to influence the victims into acting on his or her behalf. Typically, the attacker's objective is to mislead victims into giving sensitive or vital information. Traditional e-mail hoaxes and phishing, as well as its more complex targeted versions, such as spear phishing, are examples of these attacks. Pretexting [24] is used in the majority of online social engineering assaults. To bootstrap the attack, the attacker makes communication with the victim and sends some first requests. This strategy, although effective since it reaches a huge number of prospective victims, has the drawback that unsolicited contact requests are becoming increasingly suspicious among Internet users. Previous research has indicated that impersonating an existing friend of the victim or inserting the attack into current chat discussions might increase trust levels [25]. Another important characteristic of social networks is their assistance in making new acquaintances. For example, one frequent method is to detect similar friends in cliques automatically and then promote new connections with messages like "You have 4 common friends with Kumar." Do you want to make Kumar a new friend?" In addition, data about users' actions is frequently gathered, analysed, and linked in order to assess the likelihood that two users know one other. When a prospective acquaintance is discovered, the social networking site may offer a new friendship recommendation when the user checks in [25].

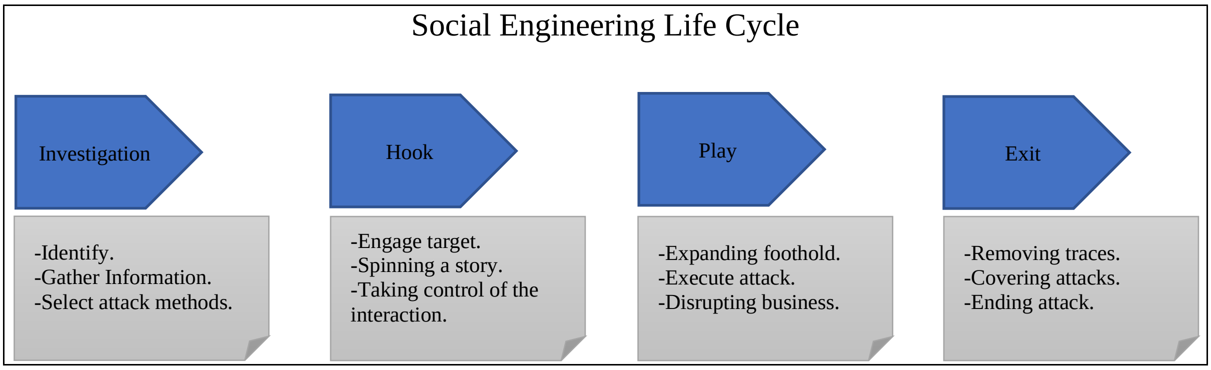

Fig. 3: shows Social Engineering Life Cycle. (Source: social-engineer.org)

7.1 Different techniques used for Social Engineering Attacks:

Social engineering operations take many forms and may be conducted out anywhere there is human connection. The following are a few of the most common forms of digital social engineering attacks. [26].

Pretexting: It is a technique in which an attacker finds information by describing a succession of well-crafted falsehoods. The culprit may initiate the trick by stating that he or she requires sensitive data from the target in order to accomplish a tricky project. The attacker often begins by mimicking as co-workers, law enforcement officials, banking sector officials, officers from tax department, or other parties having a legitimate interest in knowing in order to acquire the victim's trust. The pretexter offers questions ostensibly to verify the victim's identity, but are really meant to get sensitive personal information. The fraudster acquires a range of sensitive data and records using this approach, including the victim's personal addresses, Aadhaar Details, phone numbers, vacation details, details about bank account, and sensitive information about a physical set-up.

Spear phishing attacks: Here, the offender targets specific individuals or companies using publicly available information on Facebook. They then tailor their messages to their victims' characteristics, job titles, and contacts in order to disguise their attack. Spear phishing [27] requires substantial effort on the attacker's behalf and may take many months to execute. They are far harder to detect, and when performed properly, have a greater success rate. In a phishing attack scenario, an attacker can send a chat message to one or more employees over Facebook Messenger while posing as an organization's IT expert. It is phrased and signed identically to the consultant's emails, giving recipients the impression that they are receiving a real message. The letter asks recipients to change their passwords and contains a link to a fake website where the attacker obtains their personal information.

Phishing scams: They are email and SMS operations designed to inspire victims with a sense of desperation, curiosity, or fear, are among the most prevalent forms of social engineering assault. Individuals are then persuaded to divulge personal information, access hazardous websites, or download malware-infected files. A chat message is delivered to a Facebook user of an internet platform notifying them of a rule violation that requires immediate attention on their part, such as changing their password [28]. It provides a link to a malicious website that appears very much alike to the legitimate version and invites the unsuspecting user to provide their existing login details and a new password. Whenever the form is submitted, the hacker receives the information. Also, phishing efforts transmit identical or almost identical communications to all users, email services equipped with threat detection and prevention systems have a far simpler time identifying and preventing them.

8. IMPACT OF SOCIAL ENGINEERING ATTACKS ON FACEBOOK :

Because Facebook is among the most popular social networking site in the world, its success spawned a black-market sector that takes advantage of the trust connection that exists between users to provide illicit services such as purchasing Facebook likes, comments, and shares. All of these harmful actions entail the establishment of a large number of false accounts in order to carry out online assaults on the site [29]. Fake accounts are categorized into duplicate and fraudulent accounts by Facebook. False accounts are classed as either user-misclassified or undesired and a duplicate account is one that an individual maintains in addition to their primary account.

Individual profiles of users made for an organization, company, or pet are known as user-misclassified accounts. Undesirable accounts are user profiles formed with the intent of violating Facebook's terms of service, like spamming. In 2013, around 4.3to 7.9 percent of Facebook's monthly number of active users were duplicate accounts, as per an internal Facebook investigation of a small model of its accounts. The estimated number of user-misclassified profiles is between 0.8 and 2.1 percent of Monthly Average Users in the same year, while unwanted accounts was projected between 0.4 and 1.2 percent of MAUs [30]. Estimates based on recognising names that appear to be fraudulent or other false behaviour are used. The most typical purpose of a fake account is to amass unwarranted authority and influence inside a particular community [31].

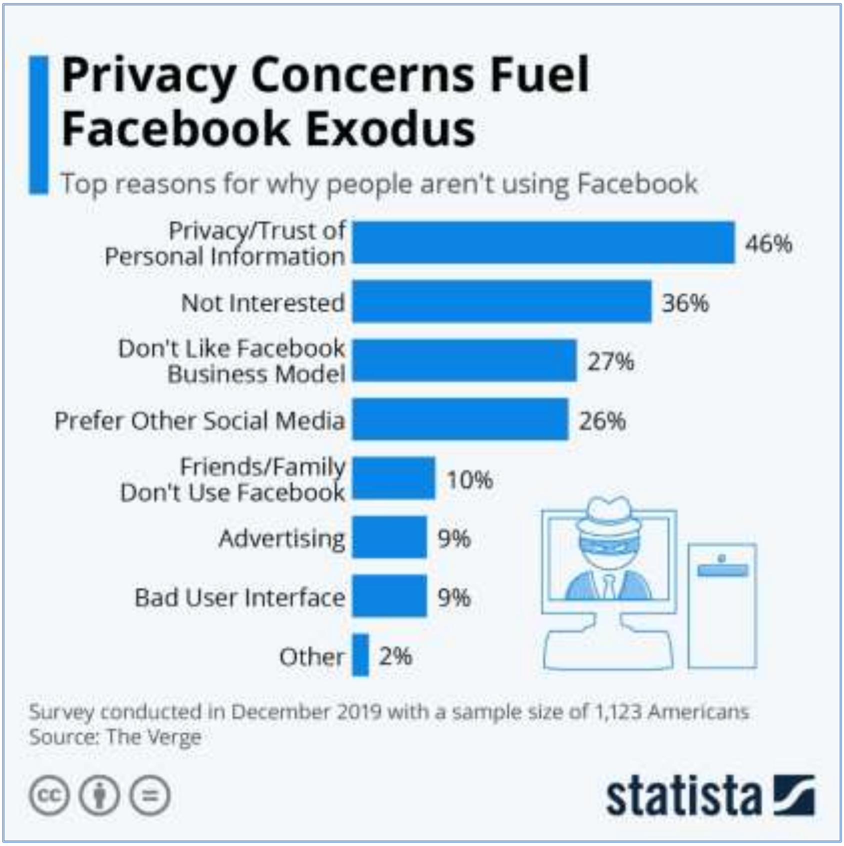

Fig. 4: Explains about the privacy concerns which is affecting Facebook users.

(Source: Statistica.com)

According to Facebook's own estimations, duplicate accounts account for about 11% of monthly active users, with fraudulent accounts accounting for another 5%. Others assert that the total is far greater [32] Despite this, Facebook is still bragging about its 2.45 billion monthly users, which is about one-third of the world's population., Lithuanian national Evaldas Rimasauskas, launched the biggest social engineering campaign in history against two of the world's top companies: Google and Facebook. Rimasauskas and his friends established a fake firm, purporting to be a tech giant with ties to Google and Facebook. Rimasauskas also opened bank accounts in the company's name. After that, the scammers sent phishing emails to particular Google and Facebook workers, billing them for legitimate products and services offered by the manufacturers but ordering them to pay cash into their fake accounts. Between 2013 and 2015, Rimasauskas and his colleagues robbed the two technological behemoths of more than $100 million [33].

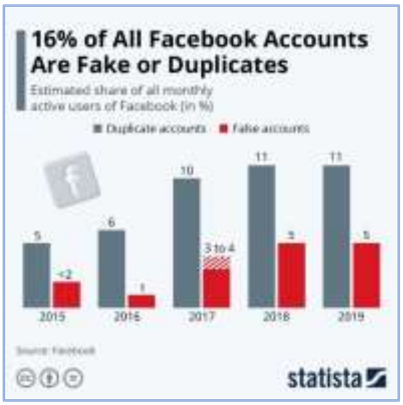

Fig. 5: Elucidates about Facebook duplicate and fake account. (Source: statistica.com).

9. SOCIAL ENGINEERING ATTACKS IN THE WAKE OF COVID-19 PANDEMIC :

The worldwide epidemic caused by COVID-19 and the subsequent lockdown measures enforced by various governments across the world have disrupted all critical activities. At the peak of the epidemic lockdown in April 2020, this was projected that a third of the worldwide people would be quarantined and socially isolated to different degrees.

Prior to the pandemic caused by COVID-19, the International Labour Organization estimated that 7.9 percent of the worldwide workforce worked permanently from home. Due to the pandemic's disruption of typical work patterns, the ILO forecasts that the number of individuals permanently working from home might reach 18 percent of the worldwide workforce. This group is largely comprised of craftsmen, self-employed, high-income earners, freelancers, and knowledge-based workers, according to an ILO report released in April 2020[34]. The epidemic of COVID-19 and accompanying social distancing measures hastened commerce's shift to the Internet. The United Nations Conference on Trade and Development and the Netcomm Suisse E-commerce Association performed a joint poll in October 2020 in nine representative nations to get information about the situation [35]. The outbreak and its related transitions in work and education to the internet environment may be regarded as a trigger for a rise in credential phishing attempts, corporate email compromise assaults, and social engineering attacks. Ransomware assaults have also exceeded malware attacks as a result of increased internet activity during the epidemic. While these shifts happened throughout the epidemic, the most significant difference is the shift of attack methods away from generic issues and toward pandemic-related topics. The public health emergency produced by the COVID-19 pandemic, along with widespread fear, worry, and uncertainty, as well as a demand for knowledge about the pandemic, creates an excellent opportunity for hackers to benefit from social engineering assaults. When word of the epidemic hit the press in the early months of 2020, the frequency of social engineering attempts based on an epidemic theme rose substantially [36]. Another analysis provided by the consulting company Deloitte found a 254 percent increase in the number of new COVID-19-related site and sub-domain registrations each day during the early stages of the epidemic [37]. This has resulted in several government agencies in the United States of America issuing warnings about the trend, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency.

10. SWOT ANALYSIS :

SWOT analysis is the most frequently utilized technique for auditing and assessing a business's entire strategic position and environment. Its major aim is to find ways for establishing a firm-specific business model that best matches an organization's resources and skills with the environment in which it works. SWOT provides the framework for assessing internal potential and restrictions, as well as possible external opportunities and threats. It takes into account all of the good and negative variables impacting the performance of the business, both internal and external [38]. SWOT analysis of Facebook includes identifying the company's strengths, weaknesses, opportunities, and threats. Despite several conflicts over the previous year, it continues to lead as the best social networking platform, with over 2 billion monthly active users [39].

10.1 Strengths:

- Facebook continues to remain as the most popular social platform on the planet. [39]. Facebook now contains profiles from individuals of different age category. Also, friends and family members share their daily activity information via status updates and comments. Businesses sell products through Facebook ads and sponsored posts [40].
- Facebook is the most commonly used social media platform in the advertising category on the Internet. Facebook's ad revenue surpassed $40 billion in the United States in 2017. Given Facebook's massive audience, it's natural that it's the most popular platform for advertising, as opposed to other social media platforms.
- Facebook also owns a number of additional platforms and applications, including Instagram and WhatsApp Messenger [40]. Each offers distinct advantages; Instagram is a social networking platform for sharing videos and images, whereas WhatsApp is a messaging and calling software with end-to-end encryption to safeguard communication privacy.

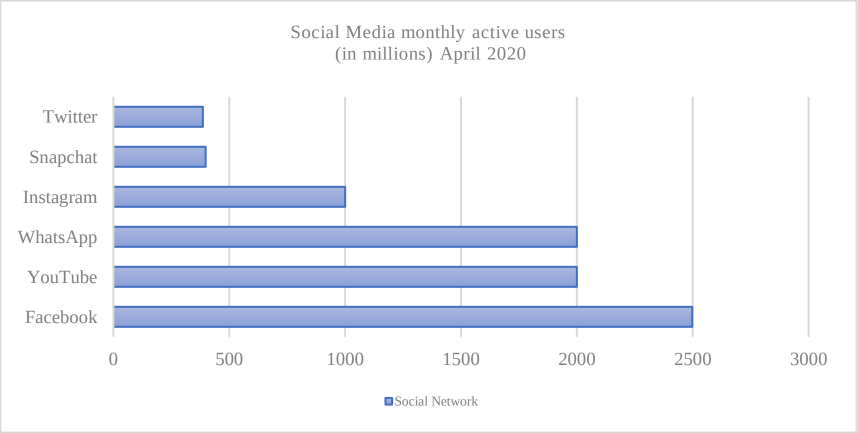

Fig. 6: Illustrates the detailed graphical representation of active monthly users of several social network in which it clearly states that Facebook dominates in terms of active monthly users.

(Source: Statistica.com)

- In 2019, Forbes rated Facebook as the world's fifth most valuable brand [40].
- Facebook has certainly understood the significance of diversifying its investments rather than concentrating them in a single sector. Diversification bolsters a business's stability by protecting its main financial personal assets that revenue from a particular industry decline [40].
- Facebook is renowned for attracting and keeping the best talent in the business according to Forbes [41]. Some of the rankings are;
  Ranked 147th as Best Employers for Diversity 2020.
  Ranked 144th in World's Best Employers 2019.
  Ranked 71st as Best Employers in America 2019.

- Mark Zuckerberg's excellent and innovative leadership is a characteristic that has paved for the success of Facebook.
- Facebook is a global leader in Research and Development spending.
- Facebook's marketing strategy is one of the best in the world as over 2 billion people uses their platform on a daily basis, it is a highly effective and powerful marketing tool [42].

10.2 Weaknesses:

- Security breaches and privacy issues are becoming increasingly prevalent across all technology-based organizations, and Facebook is no exception. [Fig.4].
- Facebook's business model is heavily dependent on advertising.
- Facebook has come under fire for spreading erroneous and false information [43].
- Attempt to disassociate from major scandals such as the Russia meddling scandal [44].

10.3 Opportunities:

- Facebook has the ability to reach a variety of audiences in a variety of ways by acquiring Instagram and WhatsApp [45].
- With billion active users in Facebook, it has the capability to expand its current services such as online shopping marketplace [46], Video on demand, etc., to compete with other big brands like Amazon, Netflix, YouTube and others.
- Facebook's platform could be opened up for integration with a variety of other applications, including blogs, podcasts, surveys, e-commerce, reviews, and games.
- Facebook has the monetary capacity to acquire promising start-ups.
- By providing new services, Facebook can expand its influence to new audiences, such as elderly generations and high-end business networks such as LinkedIn.

10.4 Threats:

- The number of anti-Facebook legislation is rapidly increasing, spurred by recent incidents such as Cambridge Analytica [47].
- Facebook is prohibited in China, Iran, and North Korea in order to curtail freedom of speech. [48].
- Facebook's user base is under threat of eroding due to competition from both existing and new platforms.
- Russia has imposed strict restriction and monitoring on Facebook content in the country [49].
- The European Union and the United Kingdom enacted a new digital tax that will impose a higher tax on Facebook [50].
- 11% of Facebooks 2.5 billion Monthly Active Users globally in 2019 December might be duplicate accounts and 5% could be fake accounts [51]. Most cloned accounts originate in developing countries such as the Philippines, Vietnam, and Indonesia [Fig.4].

11. CONCLUSION :

Businesses advertise on Facebook; families communicate via Facebook Messenger and WhatsApp. Facebook is a prime target for cyber criminals, particularly social engineering attacks, and despite a slew of privacy scandals involving CEO Mark Zuckerberg, Facebook is still the world's most popular social media platform. While it is reasonable to believe that Facebook deserves to be the leading social media platform, the company continues to face threats. Facebook should prioritize innovation and cybersecurity in the future to ensure a superior user experience. The company's research and development investments must continue to grow in order to strengthen its abilities in countering cybercrime. Additionally, Facebook must continue to negotiate with governments to gain access to regions where it presently has a negligible presence.

REFERENCES :

[1] Stein, T., Chen, E., & Mangla, K. (2011). Facebook immune system. Proceedings of the 4thWorkshop on Social Network Systems, SNS'11, m.
CrossRef↗

[2] Krombholz, K., Merkl, D., & Weippl, E. (2012). Fake identities in social media: A case study on the sustainability of the Facebook business model. *Journal of Service Science Research*, *4*(2), 175–212.
CrossRef↗

[3] Garg, V., Benton, K., & Camp, L. J. (2014, March). The privacy paradox: a Facebook case study. In *2014 TPRC conference paper*.
Google Scholar↗

[4] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*(1), 113–122.
Google Scholar↗

[5] Algarni, A., Xu, Y., &Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687.
Google Scholar↗

[6] Ajis, A. (2020). The Core Elements of Motivational Factors that Influence Facebook Users to Self-Disclosure. *International Journal of Business and Management*, *4*(2), 1–11.
Google Scholar↗

[7] Calbalhin, J. P. (2018). Facebook User's Data Security and Awareness: A Literature Review. *Journal of Academic Research*, *3*(2), 1-13.
Google Scholar↗

[8] Vishwanath, A., Xu, W., & Ngoh, Z. (2018). How people protect their privacy on facebook: A cost-benefit view. *Journal of the Association for Information Science and Technology*, *69*(5), 700–709.
Google Scholar↗

[9] Wu, S. H., Chou, M. J., Tseng, C. H., Lee, Y. J., & Chen, K. T. (2015). Detecting in situ identity fraud on social network services: A case study with facebook. *IEEE Systems Journal*, *11*(4), 2432-2443.
Google Scholar↗

[10] Alkire, L., Pohlmann, J., & Barnett, W. (2019). Triggers and motivators of privacy protection behavior on Facebook. *Journal of Services Marketing*, *33*(1), 57–72.
Google Scholar↗

[11] Pavni Diwanji, V. of Y. P. (2021). How do we know someone is old enough to use our apps?, About Facebook. https://about.fb.com/news/2021/07/age-verification. Retrieved on 09/09/2021.

[12] Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108.
Google Scholar↗

[13] Facebook. (2021). Control who can see what you share, Facebook Help Centre. https://www.facebook.com/help/1297502253597210. Retrieved on 09/09/2021.

[14] Alsahafi, R. M. (2018). Case study of comparing security features of Facebook and google plus. *International Journal of Scientific and Technology Research*, *7*(12), 255–261. Researchgate↗

[15] Eric Griffith. (2021). 15 Hidden Facebook Features Only Power Users Know. https://in.pcmag.com/social-media/142565/15-hidden-facebook-features-only-power-users-know. Retrieved on 09/09/2021.

[16] Choi, Y. B. (2021). Organizational Cyber Data Breach Analysis of Facebook, Equifax, and Uber Cases. *International Journal of Cyber Research and Education (IJCRE)*, *3*(1), 58-64. Google Scholar↗

[17] Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. *International Journal of Computer Science and Network Security*, *18*(1), 43-55. Google Scholar↗

[18] Wallbridge, R. (2009). How safe is Your Facebook Profile? Privacy issues of online social networks. *ANU Undergraduate Research Journal*, *1*(01), 1-8. Google Scholar↗

[19] John Leyden. (2020). XSS vulnerability in 'Login with Facebook' button earns $20,000 bug bounty, The Daily Swig. https://portswigger.net/daily-swig/xss-vulnerability-in-login-with-facebook-button-earns-20-000-bug-bounty. Retrieved on 10/09/2021.

[20] Kim Crawley. (2017). Social Engineering on Facebook. https://blogs.blackberry.com/en/2017/10/social-engineering-on-facebook. Retrieved on 10/09/2021.

[21] Bradbury, D. (2012). Spreading fear on Facebook. *Network security*, *2012*(10), 15-17. Google Scholar↗

[22] Fruhlinger, J. (2019). Social engineering explained: How criminals exploit human behavior. https://www.csoonline.com/article/2124681/what-is-social-engineering.html. Retrieved on 10/09/2021.

[23] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 2-5. CrossRef↗

[24] Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). The Art of Deception: Controlling the human element of security, *Foreword by Steve Wozniak*, (pp. 268-342). Google Books. Google Scholar↗

[25] Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). Reverse social engineering attacks in online social networks. *Lecture Notes in Computer Science*, *6739*(3), 55–74. CrossRef↗

[26] Imperva. (2021). Social Engineering Attack Techniques. https://www.imperva.com/learn/application-security/social-engineering-attack/. Retrieved on 13/09/2021.

[27] Burns, A. J., Johnson, M. E., & Caputo, D. D. (2019). Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 24-39. Google Scholar↗

[28] Shelke, P., & Badiye, A. (2013). Social networking: its uses and abuses. *Research Journal of Forensic Sciences*, *1*(1), 2-7. Google Scholar↗

[29] Reilly, I. (2018). F for Fake: Propaganda! Hoaxing! Hacking! Partisanship! and Activism! in the fake news ecology. *The Journal of American Culture*, *41*(2), 139-152. Google Scholar↗

[30] Yang, Z., Wilson, C., Wang, X., Gao, T., Zhao, B. Y., & Dai, Y. (2014). Uncovering social network sybils in the wild. *ACM Transactions on Knowledge Discovery from Data*, *8*(1). 8-17. CrossRef↗

[31] Gupta, A., & Kaushal, R. *Towards Detecting Fake User Accounts in Facebook. 1*, 1–6. CrossRef↗

[32] Elaine Mooreand Hannah Murphy. (2019). Facebook's massive fake numbers problem, Los Angeles Times. https://www.latimes.com/business/technology/story/2019-11-18/facebooks-massive-fake-numbers-problem. Retrieved on 13/09/2021.

[33] Tessian. (2021).11 Social Engineering Examples, Real Attacks. https://www.tessian.com/blog/examples-of-social-engineering-attacks/. Retrieved on 17/09/2021.

[34] ILO. (2020). Working from Home: Estimating the worldwide potential. *International Labour Organization Policy Brief*, (pp. 1-10). ILO Brief. Retrieved on 17/09/2021.

[35] United Nations UNCTAD. (2021). COVID-19 and E-commerce. *United Nations Conference on Trade and Development*, (pp. 4-6). UN-iLibrary. CrossRef↗

[36] Blank Rome. (2020). Flattening the Scam Curve: Be Prepared for Uptick in COVID-19 Social Engineering Cyber Attacks. https://www.blankrome.com/publications/flattening-scam-curve-be-prepared-uptick-covid-19-social-engineering-cyber-attacks. Retrieved on 17/09/2021.

[37] LORCA. (2020). Covid-19 Social Engineering Attacks. Threat Actors Are Capitalising on the Uncertainty That the Global Covid-19 Individuals, Organisations and Remote workers. Retrieved on 17/09/2021.

[38] Aithal P. S. & Kumar, P. M. (2015). Applying SWOC Analysis to an Institution of Higher Education. *International Journal of Management, IT and Engineering*, *5*(7), 231–247. Google Scholar↗

[39] Kiesha Frue. (2019). SWOT Analysis of Facebook: How has it survived for so long? https://pestleanalysis.com/swot-analysis-of-facebook/. Retrieved on25/09/2021.

[40] Kamil Franek. (2021). How Facebook Makes Money: Business Model Explained, Business Analytics. https://www.kamilfranek.com/how-facebook-makes-money-business-model-explained/. Retrieved on 25/09/2021.

[41] On Forbes Lists. (2021). Facebook (FB). https://www.forbes.com/companies/facebook/?sh =67cb1aba4193. Retrieved on 25/09/2021.

[42] Facebook SWOT Analysis. (2020). Business Strategy Hub.https://bstrategyhub.com/facebook-swot-analysis/. Retrieved on 25/09/2021.

[43] Mark Travers. (2020). Facebook spreads fake news faster than any other social website, according to new research. https://www.forbes.com/sites/traversmark/2020/03/21/facebook-spreads-fake-news-faster-than-any-other-social-website-according-to-new-research/?sh=65bde4986e1a. Retrieved on 25/09/2021.

[44] BBC News. (2018). Zuckerberg: Facebook is in "arms race" with Russia. https://www.bbc.com/news/world-us-canada-43719784. Retrieved on 25/09/2021.

[45] Prachi Juneja. (2021). The Whatsapp- Facebook-Instagram Merger. https://www.managementstudyguide.com/whatsapp-facebook-instagram-merger.htm. Retrieved on 25/09/2021.

[46] Cheikh-Ammar, M., & Barki, H. (2016). The influence of social presence, social exchange and feedback features on SNS continuous use: The Facebook context. *Journal of Organizational and End User Computing (JOEUC)*, *28*(2), 33-52.
Google Scholar↗

[47] Meredith, S. (2018). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html. Retrieved on 25/09/2021.

[48] Makeuseof. (2021). 3 Countries Where You Can't Use Facebook. https://www.makeuseof.com/countries-that-ban-facebook/. Retrieved on 25/09/2021.

[49] Apnews. (2021). Russia fines Facebook, Telegram over banned content.https://apnews.com/article/europe-russia-technology-government-and-politics-cea2b0203f13a2e6e17951f2eb570a31. Retrieved on 25/09/2021.

[50] Eshe Nelson & Michael J. Coren. (2018). The UK is going after Facebook and Google with a digital services tax: Quartz. https://qz.com/1442182/the-uk-is-going-after-facebook-and-google-with-a-digital-services-tax/. Retrieved on 25/09/2021.

[51] PTI. (2020). Facebook may have 275 million duplicate accounts globally - The Financial Express. https://www.financialexpress.com/industry/technology/facebook-may-have-275-million-duplicate-accounts-globally/1866916/. Retrieved on 25/09/2021.

****