Exploration of Cybersecurity Vulnerabilities and User Awareness on Social Media Platforms

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Samantha Jade Chiang

Spring, 2020.

Technical Project Team Members

Hana Kontrec

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Yixin Sun, Department of Computer Science

Mohammad Mahmoody, Department of Computer Science

Exploration of Cybersecurity Vulnerabilities and User Awareness on Social Media Platforms

Samantha Jade Chiang
University of Virginia
sjc2gg@virginia.edu

Hana Kontrec
University of Virginia
hk5gc@virginia.edu

ABSTRACT

The topic of our literature review is going to be the security and privacy and users' awareness of it on social media. We aim to answer some central questions with our literature review: Are users aware of how their information is being used and collected on social media platforms? What is the impact of social media awareness of cybersecurity practices and will it help users be better equipped to protect themselves on social media? What can be done to raise user awareness on social media? What can be done in the future to keep social media platforms accountable? The rationale of our literature review is to answer the above questions. We are going to review existing literature and try to find gaps in the research in order to propose possible future research or solutions to security on social media platforms. The significance of these findings will help analyze current practices and determine the best way of spreading this information in the future to those who may not be well versed in the subject.

1 INTRODUCTION

A lot of the literature surrounding cybersecurity in connection with social media deals with the ways that bad actors can use these platforms in newer methods of attacks. This becomes a much larger issue than previously, as the use of social media is at an all time high, and continues to climb. With this rise, there is a new pressing need for users to be more conscious of the threats that exist in the online space. Previously, there could be reliance on the social media platforms to keep their users safe, but as new, more complicated forms of attacks develop, it becomes crucial for a user to know how they can best protect themselves and their information. There has also been a lot of exploration into how users interact with social media platforms and their awareness of the impacts security vulnerabilities could have on their information. In this review, we will examine many papers pertaining to both subjects in order to analyze the imminent threats that users might face when delving into social media, as well as ways users can mitigate these risks.

2 BACKGROUND

As stated previously, there has been an emergence of cybersecurity attacks that have never been seen before. Of course, there is a difference between attacks that target the social media platform itself and those that aim for the users of that platform. The aim of each could range from an intent to steal a user's information, damage to the platform's reputation or infrastructure, and many more purposes.

The type of attack that is most typically seen on the user side is a social engineering attack, which is the elicitation of private information from users using a variety of methods. This can be through building trust, such as through impersonation or catfishing. This information can also be gathered through methods such as tricking the user into thinking they are giving their information to a reputable source, like through phishing. Sometimes, however, cyber attacks do not aim to steal information or cause financial trouble, but are used as just another form of harassment. Cyberbullying and doxxing are examples of this intention to cause emotional distress and harm to their targets.

On the other hand, attacks that target the social media platform tend to be more technology-driven. There are a wide variety of methods to attack such a large target. XSS attacks target web applications with malicious code, while DDOS attacks focus on overloading the server, and many, many more. What these all have in common, however, is the increase in their frequency. With the amount of people on social media and the rapid advancements in technology, attacks are easier and quicker to execute than before. Attacks can happen within seconds, which stresses the importance of prevention, so that bad actors do not have the chance to do so in the first place.

3 USER AWARENESS ON SOCIAL MEDIA

As social media platforms are becoming more ingrained in our society it is important to analyze and explore the stakeholders of this fast-growing technology. As of April 2021, the total number of active social media users is 4.33 billion which makes up about 55% of the total global population. The last year has seen an almost 14% increase in social media users which equates to around 520 million new users in the last 12 months [5]. As the number of social media users grows, the more important it is to explore their understanding and perception of social media platforms and how their data and information can be put at risk as a result of engaging in this technology.

3.1 User Perceptions vs Behavior on Social Media

The vast amount of users on social media makes social media platforms an ideal target for cybersecurity attackers. A study of awareness and privacy on Facebook, showed that a large majority of users in the study are not actually aware of how social media platforms use their data and are not aware of the privacy policies issued by the platform. About 70% of participants revealed that they were unaware of Facebook's ability to combine data about them from other sources and 56% that Facebook shares their data with third parties. Moreover, 77% claimed to have read Facebook's privacy policy, however, it was shown that those who claimed to have read it are not necessarily more knowledgeable about Facebook's activities [2]. This sentiment is consistent with other literature and there might be several important explanations for this result. Social media platforms are not very transparent with their data privacy practices and the information they do disclose are contained in long and obfuscated privacy policies and end-user license agreements (EULA). Therefore, it is not hard to imagine why the majority of users often do not read these documents. Moreover, user's usually agree to privacy policies when they are first creating a social media account. If they read the policy and do not agree with the terms, they have no power of negotiation with the social media platform meaning their only option is to not participate at all. Given how ingrained social media has become in our social lives, many users are often not willing to do this and decide to create a social media account regardless of the risks involved.

Furthermore, users being aware of how their data is being used online does not necessarily result in safer online behavior. One study tested user attitudes toward ownership, privacy, and control of data by people who closely followed events leading up to the 2016 Facebook/Cambridge Analytica (CA) scandal and those that followed a year later and those who did not. While both parties exhibited an overall "reduced sense of ownership and control" over their data, those who claimed to have paid the most attention to the CA scandal generally seem to be more "more polarized" in their views of data privacy and are "more aware that their data is being used as a means of profiling" by social media platforms. An important takeaway from this study is that "an event and its outcome may change attitudes without changing actual behavior," however, "norms do eventually guide actual behavior" [8]. Those who are more aware of highly-publicized stories on the topic are not any more likely to change their behaviors than those who don't. As with blindly accepting privacy policies, this could be the result of a feeling of helplessness and lack of power to do anything about it. However, there is still hope for the future as norms are slowly but surely changing. For instance, as a result of the CA scandal and related highly-publicized scandals, people seem to be more aware of their data being collected online for the purpose of personalized advertising. Awareness of these types of practices does change user behavior but it could lead to changing norms which could, in turn, affect user behavior in the future.

3.2 Student Attitudes, Awareness, and Perceptions

In 2020, a survey conducted on students, aged 18-45, on their perceptions of their security on social media platforms. Before this study, however, a literature review was conducted in order to gain a better understanding of the knowledge that has been collected on cybersecurity in social media. This brought up several key points, emphasizing how social media becomes a major factor in many people's lives. This can be seen through the fact that approximately 80% of 18-24 year olds use social media, often checking these sites multiple times throughout the day. [3]

Though social media seems to be omnipresent in many people's lives, these same users may not have the strongest grasp on the cybersecurity implications that come with having and interacting with such a platform. As a result of news coverage tending to use eye-catching and provoking headlines, real information becomes distorted, presenting a false narrative to whoever happens upon the story. The typical user will most likely get their information from these sources and trust them by taking them at their word without doing much research. It is important not only to understand the risks that one faces when using social media, but also how to protect themselves and their information.

There is a lot of trust put into these platforms to protect their users to the best of their abilities by leaving them in charge of encrypting passwords and databases, banning suspicious accounts, and monitoring public information. However, as so many people join these networks, it becomes easier and easier to slip through the cracks. This is why users must take their security into their own hands and do everything they can to protect themselves and their sensitive information. This study conducted on student attitudes, awareness, and perceptions provides an important service. Being able to get a lot of insight into the viewpoints and knowledge of students on cybersecurity in social media versus the typical population provides useful information on the types of people most affected by it. Of the 107 of respondents, approximately 93% used at least one form of social media, making them more likely to than their non-student counterparts. Through a series of questions, it becomes clear that, as a whole, students had a better understanding of the risks associated with social media, and used the privacy options provided to them by social media platforms, such as making their account private. The study also showed that those who had previously been a victim were much more likely to be vigilant and aware of their online presence. Most students also pointed out a need for training in cybersecurity and social media, through either a school or college program.

While students are aware of risk on social media, more than half answered that they would be willing to sacrifice privacy in order to use social media. This indicates that, even though students tended to be lower risk than non-students, there is still a gap in knowledge that needs to be filled. There are many aspects of social media, and within that, many levels of cybersecurity which need to be taught and presented to all those who intend to use the platform. [3]

Through a series of questions, it becomes clear that, as a whole, students had a better understanding of the risks associated with social media, and used the privacy options provided to them by social media platforms, such as making their account private. The study also showed that those who had previously been

a victim were much more likely to be vigilant and aware of their online presence. Most students also pointed out a need for training in cybersecurity and social media, through either a school or college program.

While students are aware of risk on social media, more than half answered that they would be willing to sacrifice privacy in order to use social media. This indicates that, even though students tended to be lower risk than non-students, there is still a gap in knowledge that needs to be filled. There are many aspects of social media, and within that, many levels of cybersecurity which need to be taught and presented to all those who intend to use the platform.

3.3 Public Trust

A study on the US public opinion on governing AI revealed that the public has an overall "lack of trust for most actors to develop and manage AI" and the most trusted actors to do so turned out to be university researchers and the US military. Greater trust was shown towards tech companies and intergovernmental research organizations while trust in the U.S. government was at the bottom of the list. This trust, or lack thereof, seems to center around the user's perception of an organization's motives and incentives. The reason the public has a distrust of government is because they have a general distrust of politicians while they have distrust of tech companies due to their "power and influence in the U.S. economy." However, even though this study showed that the public has more trust in tech companies than the government, this does not mean that they are opposed to government regulation of tech companies in some cases. The paper emphasizes that the public "prefers government regulation if they trust the government more than they do major companies." The entities the public puts most of their trust in seems to come down to the entities whose interests best align with their own [9].

Another aspect of trust also comes down to familiarity. As mentioned above, the public has more trust in tech companies as a whole than intergovernmental organizations. Tech companies are often household names such as Apple and Microsoft while intergovernmental organizations like CERN and AAA are lesser known entities. Therefore, there is a possibility that people rated intergovernmental organizations less trustworthy than tech companies simply because they were less informed about them. Moreover, another interesting finding in this research, specifically relating to social media platforms, is that out of all the actors presented to the participants, the participants trusted Facebook, as a singular entity, the least, even less than tech companies in general. The researchers mentioned that at the time of the study, the Cambridge Analytica scandal was widely publicized. I think this is a significant detail. There might be a possible link between information and knowledge publicized in the media and how that affects the public's attitudes and trust towards different entities. For instance, another part of the study examined different issues with Artificial Technology (AI) and their importance to participants. They were, in order of importance to the people surveyed: data privacy, cyber-attacks, surveillance, and digital manipulation. On the other hand, Critical AI systems failure, China arms race, and criminal justice bias were at the bottom of the list [9]. Cases relating to the former topics, such as the Facebook/CA scandal, seem to be more publicized in the media than the latter and this can definitely have an impact on public opinions towards these topics. In short, people are more likely to deem more important the issues they are more familiar with.

4 CYBERSECURITY

While the threat of cyber attacks is certainly not a new one, the frequency at which they occur grows as technology advances. More people can now be targeted that might not have been at risk before, either because they did not use social media, or because systems that protect their information are no longer secure. With such a large portion of the population owning at least one social media account, it is important not only to be aware of the threats online, as discussed in the previous section, but take an active role in one's own protection.

4.1 On Cybersecurity, Crowdsourcing, and Social Cyber-Attack

Not all cyber attacks aim to gather private information or achieve financial gains. Some attacks are meant to cause harm and distress. One of the most dangerous ways that this can be achieved is through social cyberattack with the intent to manipulate not just one person, but an entire crowd. [7]

The spreading of disinformation is a problem that existed long before social media. The internet provides quick and easy access to information with just a few clicks, which presents both good and bad impacts on those who might access this content. On the one hand, this can be used in a positive way, spreading information about volunteer opportunities or fundraising campaigns. On the other hand, the question of whether the information is true allows for the reach of the internet to be used for malicious intent, like spreading hate speech or inciting chaos. Anyone can own a website and put whatever they want on it, without being checked on the veracity of its contents.

The paper points to, specifically, an incident that occured in July 2021, where photos and information were being spread about a conflict between a Hindi tribe and Muslim immigrants in Assam, Inida. This resulted in many arrests and deaths from the skirmish and riots. In reality, no such incident occurred, though the material had been rapidly spread through social media as users who received this information often forwarded it to their family and friends. The information was completely fabricated and the alleged photos had been photoshopped from riots that had occurred previously in other countries.[7]

Though one person was arrested for sending over 20,000 messages propagating this false information, it is undoubted that others had aided in this attack. There were also many who were complicit by failing to check the information that had been sent to them. The paper brings up the topic of the role of the government in both keeping platforms accountable in their security, as well as ensuring that incidents such as this, and other cyber attacks do not occur or have as far of a reach. Challenges arise, however, as attacks can easily cross borders, highlighting a need for a global effort to heighten cybersecurity efforts. This ties into a call for more research into these types

of attacks. The questions of who and why remain unanswered, which could give a better understanding of the situation at large.

It is up to the user to keep themselves aware and informed. Perhaps in the future, the government could provide aid in squashing false information. But even with this possibility, the internet is too vast to be policed at all times, making it essential that users protect themselves and aid in shutting down disinformation and fear mongering where they see it.

4.2 Cybersecurity Vulnerabilities of Facebook and Solutions

Facebook is still one of the most used social media platforms and has been the subject of many technical reports and research papers. Being such a large platform with a large number of users, it is naturally prone to many cybersecurity attacks. One researcher splits these cybersecurity attacks into two categories: "platform related and user related". The biggest distinction between the two is that platform related attacks cannot be solved by the user rather the platforms itself while user related refers to attacks that users are aware of. Platform related attacks explored by the paper are SMS Verification Weaknesses, Social Authentication, Vulnerabilities from Applications and Puppetnets while user related attacks include fake profiles, Sybil, Identity Theft, and Accessing Blocked User Accounts [1]. This paper does a very good job describing the different vulnerabilities in detail but the main takeaway comes down to two things. First, platform related vulnerabilities are not often visible to users and it comes down to the social media platforms to mitigate the risks posed to their platforms, and, therein, their users. Second, user related vulnerabilities can be solved by the user if they are proactive in lessening their risk of being exposed to vulnerabilities by staying informed and understanding how the information they make public can be exploited. There is no one solution to eliminating all vulnerabilities on social media platforms, but staying informed on how to lessen the impact of these vulnerabilities can go a long way.

One case study of Facebook explored a specific vulnerability on the platform: photo tagging. Photo tagging enables one user to tag other active users, their "friends", in their photos. Photos paired with tags that connect a user to other users, may contain sensitive information not only about the places they like to frequent but also who some of their closest friends and family are. Moreover, a significant vulnerability with photo tagging comes down to the issue of content ownership. Users can tag their friends in a photo without their permission. Your friend, for instance, can be very informed on the topic of photo tagging and how that affects their security and choose not to post sensitive information on their profile. Regardless, you are able to post a photo of them on your account and tag their account. Your friend has the option to remove the tag after it has already been placed but there is no way to stop someone from tagging them in the first place. This is a problem since tags can be "used by third parties to breach one's privacy" [4]. Therefore, content outside of a user's hands can make them vulnerable to breaches of privacy. One possible solution comes down to the topic of content ownership. Who owns the right to your content? At the least, other users should need permission to tag your active account to their photos or social media platforms should enable a setting that allows a user to disable the ability of their account being tagged in other's content. Overall, users need to be aware of their vulnerability on social media so then they could make more informed decisions on how to expose and control their online information.

4.3 Cybersecurity in Social Media: Challenges and the Way Forward

There are many ways that a system can be attacked, to the point where information can never truly be fully protected. Attacks such as phishing, ransomware, malware, DDOS attacks, and botnets are just a handful of the methods that bad actors can use in order to exploit vulnerabilities and cause harm. As technology continues to advance, cyber attacks can be launched even quicker and easier than before. It can be done even in the matter of a few seconds, making the chances of falling victim to these crimes quite large. [6] Being such a broad field, many challenges are presented in trying to further prevent attacks. One such problem is that of balancing privacy and security. Many social media platforms rely on being able to connect with other users. Limiting such connections would defeat the purpose of the platform. This, and the many other issues faced by security in social media must be addressed before cyber attacks become more and more frequent.

Some of the most dangerous types of attacks are those anchored in social engineering. These types of attacks are prolific on social media, as the platform makes communication between users easy, even if one of the parties is a malicious entity. In addition to this, third party applications and games are often used to further a user's experiences on this platform, which introduces even more risk, as the third party is not subject to the same security policies as the ones the user is aware of when signing up for the initial social media network.

One oversight that is noted in a paper on cybersecurity in social media is the relationship between employees and social media security. [6] An employee's online presence can easily be linked to their company, and their actions will reflect on their employer, both good and bad. But in addition to this reputation aspect, there is that of cybersecurity. An employee account with a weak password can easily be compromised, or an employee could fall victim to a sort of phishing attack and lose information or account access. These are only a few examples of the ways that an employee could become a risk because of poor cyber safety. This highlights the growing need for companies to maintain a social media manager, not only to preserve their image, but to help inform and train other employees in the importance of safety when using social media.

Thus, it is up to the individual to protect themselves. This is not just simply having a strong password, but being careful of clicking on unknown links, watching where certain information is kept, or only talking to other trusted users. A user must realize that cybersecurity is not optional, and one must take an active role when it comes to their role in protecting their information. [6]

5 CONCLUSION

After analyzing these papers and studying the intentions behind them, a common theme begins to emerge in the relationship between social media users and the platform that they use. On the one hand, social media platforms do have an obligation to protect their users given that there are platform based cybersecurity attacks that are unable to be tackled by users themselves. Moreover, social media platforms are often not clear and transparent in their data and privacy policies and should do a better job of communicating them to their users so users have a clearer idea of how their information is being handled by the platform. On the other hand, the user also has a responsibility to be proactive with the risks that come with using these networking sites. Furthermore, changing norms has been shown to affect user behavior. Therefore, while user knowledge and awareness of data and privacy policies on social media does not necessarily change their current behavior online, it can, over time, change norms.

6 FUTURE WORK

While the papers and studies that exist currently are a good start, there are many other aspects of cybersecurity in social media that have little to no exploration within them. It would be both interesting and beneficial to see a study conducted on a larger variety of respondents, of different ages and backgrounds. From then, the study would continue by grouping the interviewees by similarities in order to see the trends that emerge from within such groups.

As for the actual method of testing to see the individual's perception of cybersecurity and procedure of protecting themselves, this could be conducted in multiple ways as well. A popular method that is used within networks of people is a phishing test. Though this is typically done within one's place of work or study, and in an unexpected way, research could be conducted on some sort of modified method. The study should conduct not only social engineering attacks such as phishing, but more technologically reliant tests as well. This could highlight the types of people most at risk and stress the importance of cybersecurity.

In terms of research on user awareness and behavior on social media platforms, one unexplored territory is that of the effect of highly publicized news and media. The research studies explored in this literature review seem to have a common theme. When users know more about a topic they are more likely to have a strong opinion about it. This is an interesting topic and further exploring it could lead to understanding how to shape user behavior on social media platforms in the future.

REFERENCES

[1] 2014. A survey of security vulnerabilities in social networking media: the case of facebook. (2014). DOI: http://dx.doi.org/10.1145/2656434.2656444

[2] Alessandro Acquisti, Ralph Gross, George Danezis, and Philippe Golle. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. (2006). DOI: http://dx.doi.org/10.1007/11957454_3

[3] Neelima Bhatnagar and Michael Pry. 2020. Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Information Systems Education Journal* 18, 1 (2020), 48–58. https://eric.ed.gov/?id=EJ1246231

[4] Diego Las Casa Joao Paulo Pesce and Gustavo Rauber. 2012. Privacy attacks in social media using photo tagging networks: a case study with Facebook. *Proceedings of the 1st Workshop on Privacy and Security in Online Social Media* (2012), 1–8. DOI: http://dx.doi.org/10.1007/s00779-014-0773-4

[5] Keipos. 2021. Global Social Media Stats. (2021).

[6] Thaier Hayajneh Kutub Thakur and Jason Tseng. 2019. Cyber Security in Social Media: Challenges and the Way Forward. *IT Professional* 21, 2 (2019), 41–49. DOI: http://dx.doi.org/10.1109/MITP.2018.2881373

[7] Lea Shanley Rebecca Goolsby and Aaron Lovell. 2013. On Cybersecurity, Crowdsourcing, and Social Cyber-Attack. (2013). https://apps.dtic.mil/sti/citations/ADA580185.

[8] Frank Shipman and Catherine Marshall. 2020. Ownership, Privacy, and Control in the Wake of Cambridge Analytica: The Relationship between Attitudes and Awareness. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), 1–12. DOI: http://dx.doi.org/10.1145/3313831.3376662

[9] BaoBao Zhang and Allan Dafoe. 2020. U.S. Public Opinion on the Governance of Artificial Intelligence. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 187-193* (2020), 187–193. DOI: http://dx.doi.org/10.1145/3375627.3375827