International Journal of Research (IJR)
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Vol. 8 Issue 5
May 2021

CYBER SECURITY AWARENESS BY USING SOCIAL MEDIA PLATFORMS AMONG STUDENTS

A Descriptive Study

Jeffy Varghese Bino

Catholicate College, Pathanamthitta, Kerala

Abstract

The internet is not a secure place because of limited regulations. The unawareness of users about threats that can face them in cyberspace, can cause the successful execution of such threats. Users should establish a culture of awareness before entering the workforce. Therefore, academic institutions should engage in the process to enhance cyber security awareness (CSA) among students. In order to communicate effectively on CSA, the medium of communication should be familiar to the user and the user has to engage with this medium on a regular basis.

Students at a higher academic institution reveal that they engage with social media platforms at least once a week with Facebook and YouTube the most popular. They also use communication media like websites to pursue material about CSA.

This study found that there is a lack among students to engage with CSA initiatives that are available. It is suggested that academic institutions can contribute to the awareness of students by providing CSA material on a regular basis to them. Institutions can make use of social media platforms (Facebook and YouTube) and also communication mediums (institutional website and e-mails) to communicate CSA material with the students.

Keywords: *Cyber Security Awareness, Social Media Platforms, Awareness Behaviour*.

1. INTRODUCTION

Today, the world is so connected that a person from one region can see or video chat with another person in another region, people connect to the internet using their phones, computers, even employees come to connect with the outside world in their workplaces. Organizations' operations are performed remotely nowadays as contractors can communicate a thousand miles away. All these are possible and it makes life more easy and enjoyable but at the same time if there is no control over the devices the infrastructure of the workplace is in danger of any cyberattacks. People now connect to public Wi-Fi to do their business anytime and a huge amount of personal data are being processed over the unprotected medium. The organization

is most vulnerable to cybersecurity attacks because employees might compromise the network of the organization through the connection to the internet.

The purpose of the research study was to determine students' attitudes, awareness, and perceptions of personal privacy and cybersecurity of social media sites. Within the context of this study, social media is defined as forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas or personal messages. Privacy is defined as "freedom from unauthorized intrusion" and the ability to control one's personal information so that only those the owner wishes to view their information are allowed.

This includes both control over what information is viewable in social media as well as who can view it. According to Heiten (2016) digital literacy is defined as having three categories that include "1) finding and consuming digital content; 2) creating digital content; and 3) communicating or sharing it" . The authors believe that a fourth category that should be included in the definition of digital literacy is creating awareness of privacy/security risks and countermeasures. To that extent, a paper-based survey was administered to students enrolled in summer classes at a campus of a major university in western Pennsylvania. A paper-based survey was chosen in lieu of administering the survey online to increase the sample size

2. OBJECTIVE OF STUDY

- To evaluate whether universities should be providing better education regarding cyber security.
- To identify if the cybersecurity awareness program is needed or not.
- To understand the purpose of using social media among students.

3. LITERATURE REVIEW

The use of social media is prevalent in both the general society and on college campuses. The increasing popularity of the use of social media sites has brought to the forefront a new set of problems and issues facing the 21st century. Today's college generation is facing an emerging risk to reputational harm or financial loss much more so than prior generations since social media is their main form of communication. According to Moallem (2018), "users' understanding of risks and how to protect themselves from cyber-attacks is therefore fundamental in modern life" (p. 80)." According to a study done by the Pew Research Center (2019), 69% of US adults use Facebook and 73% use YouTube. The percentage of users using Instagram, Pinterest, Snapchat, LinkedIn, Twitter, Reddit, and WhatsApp is considerably lower. Among the 18-24-year-old age group 80% use at least one social media site. More specifically 94% use YouTube, 80% use Facebook, 78% use Snapchat, 71% use Instagram, and finally 45% use Twitter. Richardson (2017) in her study reported 90% of the participants

were using Facebook and Snapchat and 70% were using Instagram. Most users check their accounts multiple times a day (Pew Research Center, 2019).

Knight-McCord, Cleary, Grant, Herron, Jumbo, Lacey, Livingston, Robinson, Smith, and Emanuel (2016) had conducted a study to determine which social media sites were being used the most by students. They distributed a survey to 363 students both in-person and online. What they found was that like the other studies, Instagram was the most widely used site followed by Snapchat and Facebook. The ones that were not as much used were LinkedIn and Pinterest.

Rivera, Di Gangi, Worrell, Thompson, and Johnston (2015) stated that "…academics must consider how they prepare current and future college students to deal with the personal risks involved in using social media. News coverage has made everyone aware of some of the dangers of revealing personal information through social media, but most news stories sacrifice measured and helpful coverage in the interest of sensational headlines. As a result, it is fair to assume that most social media users have a distorted view of the personal risk associated with using social media". This creates a compelling reason for gaining a deeper understanding of students' attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media sites. Moallem (2018) established the importance of awareness to cybersecurity threats and cited prior studies that found the issue is not with awareness but action.

Sharma, Jain, and Tiwari (2015) found that 84% of students felt that sharing of personal information on social networking sites (SNS) was risky. Moallem (2018) investigated students' cyber security awareness at two California State Universities in Silicon Valley. An online survey was administered to students enrolled in three classes. The survey consisted of ten questions, but none of them focused on social media or privacy. One of the conclusions drawn was that students were "…not very aware of how to protect their data".

Goh, Di Gangi, Rivera, and Worrell (2016) discussed that social media risks can be classified in two areas: social risk and technology risk. They identified social risk to include topics such as cyberbullying, cyberstalking, and identity theft. Technology risk, on the other hand, includes malicious software or malware, hacks, unauthorized access to social media account, and service interruptions.

In summary the studies referenced in this section provided evidence that the use of social media is prevalent in both the general society and on college campuses. The literature further defined a list of commonly used social media platforms and their rate of adoption by different generations of users. The studies did not provide coverage of the topics of security and privacy within the use of social media indicating an opportunity for this research study.

4. RESEARCH METHODOLOGY

- **Research design**

  Research design used for this study is descriptive.

- **Secondary Data**

  Secondary data are collected from text book, journals, Websites and also refer previous research studies.

CYBER SECURITY HAZARD AWARENESS

Cyber security awareness refers to how much end users know about the cyber security threats their networks face and the risks they introduce. End users are considered the weakest link and the primary vulnerability within a network. Organizations allot funding to protect their networks from outside threats and reduce vulnerabilities. Being that end users are a major vulnerability, technical means to improve security are not enough: organizations must also provide training for a personal awareness of cyber security. They should educate employees on current threats and how to avoid them.

Threat-agents normally look for the easiest way to gain access into a network, which is often the human element. Specific attacks are designed to be most inviting to the users. A popular attack is to trick users into clicking a link within an email that contains malware, divulging sensitive information over the phone or through email. Spear phishing or social engineering are two of the most common attacks.

Other forms of cyber threats in the 21st century and beyond will be the Internet of Things (IOT) based attacks, which are installed almost in everything eg; cars, refrigerators, smartphones, and much more. Ransomware is another cyber threat where attacks are carried out on the computer system, ransomware paralyzes the whole computer system. Cyber-threats can be mitigated as well.

Social_engineering is when someone uses a compelling story, authority or other means to convince someone to handover sensitive information such as usernames and passwords. An end user who is trained in cyber security awareness will have the ability to recognize those types of attacks and avoid them.

The internet has revolutionized managing life tasks, enabling connections with new people through social networks and opening new economic horizons for transactions via mobile devices both for individuals and organizations, including radical change in the higher education system and teaching methods. Even so, many people still face information security risks from a vast array of threats. These threats range from simple to catastrophic attacks. The first may consist of primitive spam e-mails, while the second may involve organized cyber-crime groups that use malicious software to steal, corrupt, and destroy data on a significant scale. A major

factor in information security risk is level of individual cyber security awareness, which can be usefully described as low, medium, or high. Low awareness behaviors include not paying attention or neglecting security alerts, provided in most cases automatically by applications, such as when accessing free open networks (such as Wi-Fi) with mobile devices and laptops. A medium awareness level may be characterized by negligence expressed in improper technology operation. Finally, high awareness involves knowledge of cyber threats and capable actions taken in their prevention.

The term cyber security awareness as follows: "[The] degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks". They noted widespread lack of awareness of cyber risks, extending to app usage and information delivery on social networks and internet web pages. Importantly, they pointed out that hackers (individual or collective) tend to seek out the most vulnerable users, i.e. those deficient in information and network security awareness. Hackers are proficient at exploiting both software bugs and security gaps unintentionally created by users themselves

THE IMPACT OF INTERNET AND CYBER ON SOCIETY

The internet has revolutionized how people access data and utilize various applications for modern day-to-day tasks. I noted the huge impact of the internet on daily life: "In our technology and information-infused world, cyberspace is an integral part of the modern-day society. In both personal and professional contexts, cyberspace is a highly effective tool in, and enabler of, most people's daily digitally transposed activities. However, Coppers noted the rising impact of information security breaches on the economy, resulting in information loss estimated at $2.5 million per year. As noted, this loss can be only partly mitigated by protective tools since their functionality in most cases is controlled by individuals.

Individual cyber engagement, in general, and with cyber protection tools in particular, has motivated both academic scholars and practitioners to focus on individual attitudes and behaviors concerning cyber threats. An instructive example was given was who emphasized the existing gap between facto and ex post facto mitigation activities conducted by employees in cases of cyber security breach due to lack of sufficient engagement with cyber security protection tools. Other studies evaluated level of individual resilience with cyber security awareness as a cause of job stress. In addition, the relationship between individual personality and level of cyber security risk propensity has been researched. Yet the relationships between individual cyber security awareness, knowledge and behavior have never been studied in cross-country comparison. In fact, the comparative approach is considered by important stakeholders to be crucial for the creation of intervention programs.

CYBER SECURITY PROTECTION BEHAVIORS

Recognizing the severe cost of cyber hazards, research has increasingly focused on the measures taken and behaviors exhibited by netizens to protect their devices. However, most recent studies related to cyber protection behavior look at very narrow aspects of cyber security behavior. For example, I surveyed level of compliance with security polices among 416 employees in 4 Malaysian companies. They found that employee attachment to the firm does not have a significant influence on their attitude to adopt a desired cyber security compliance behavior. I looked at whether employee information behavior is correlated with personality

traits such as conscientiousness, agreeableness, emotional stability, and risk taking. They showed that a small significant gender difference exists related to phishing e-mails, such that women were found to be more susceptible than men. On my another study aimed at exploring the relationship between employee resilience and job stress and cyber. They used a sample of 1,048 working Australians, reporting that higher levels of cyber threat resilience translated into significantly better ability, knowledge, attitude, and behavior in cyber mitigation processes. Similarly, participants who reported lower levels of job stress also were found to exhibit significantly better attitude, knowledge, and behavior in mitigation of cyber hazards. I focused on the relationship between risky employee cyber security behavior and individual (such as age and attitude) and organizational factors in protective cyber security activities.

CYBER SECURITY KNOWLEDGE

Increasingly, individuals are in actuality dependent on internet technologies for their day-to-day tasks. Ease of use has facilitated participation in cyber-related activities on a mass scale. However, knowledge of existing tools needed for protection against cyber threats is correspondingly lagging. As I noted, even basic level cyber security awareness may not translate into sufficient or appropriate cyber security protection knowledge to mitigate cyber risks and hazards. As such, he suggested increasing cyber security knowledge through cyber security training programs using theoretical lectures and simulators to provide exposure to cyber security protection tools. These would focus on operational, usage, and process aspects of improving user knowledge translating into effective cyber security mitigation behavior.

For example, the “Phishing Simulator” is a popular training resource, designed as an effective training process to increase awareness of suspicious e-mails sent by hackers. Such e-mails often contain malicious software (“malware”) resulting in illicit data leakage. The simulator is also suitable for trainers, exposing them to practical protection tools to mitigate phishing e-mails and internet links and guiding them in how to attain optimal levels of protection against cyber security threats.

In my study, the influence of a cyber security awareness campaign for school youth, along with their existing knowledge related to cyber security hazards, was measured. He found that campaigns have a positive impact on improving cyber hazard awareness and knowledge. In my later study, explored “Cyber Hygiene” (i.e. level of cyber knowledge) in 268 computer and device users ranging in age from 18 to 55+. The survey focused on how they maintain system health and online security tools such as firewalls and anti-virus software, and was carried out using Amazon Mechanical Turk, a crowdsourcing marketplace. MTurk allows businesses (i.e. “requesters”) to allocate tasks to remote “crowdworkers”, a potentially rich source of data collection. They found that self-identified experts had less cyber hygiene knowledge than self-identified non-experts. This surprising finding could be attributed to the latter being more dependent and relying on external guidelines, hence investing greater efforts in acquiring the necessary cyber security knowledge for their tasks.

EDUCATION

Education Our research found that 80% of the students did feel that training should be offered on the concepts of risk to the use of social media and how to use the security settings to mitigate that risk. Our next concern was related to the timing of when that training should be offered. The research found that almost 85% felt training should be offered during the freshman year.

Most students did use the privacy settings in social media to mark their account private. Others wanted to keep their account public because they used their social media accounts for promoting their own small business and felt that security was a negative if it reduced their marketing reach.

Some students create fake accounts/pen names to provide anonymity of their activity on social media to manage their social media presence.

Based on the survey results, students do understand the risk of engaging in unsafe behaviors that compromises their privacy on social media platforms and do know what to do about it. As far as the question related to the need for formalized instruction and its implications on digital literacy in a university setting, the authors were biased in thinking that formalized instruction would be needed and focus on the need to increase awareness of privacy risks in the use of social media and in the use and configuration of security settings.

5. FINDINGS

From conducting the study all three research objectives were achieved satisfactorily and the following conclusions emerged:

• Students are aware of the risk of using social media and could provide good examples of issues that have occurred in the past to include account compromise and identity theft.

• A migration is occurring in the use of social media platforms by generation z students. The migration is moving away from Twitter and Facebook to the use of Snapchat and Instagram.

• When security settings were not used the most common reason was that they are hard to understand and use. They also indicated that it limited their online reach.

• Students do value the need for training on cybersecurity and privacy in the use of social media and feel this should occur in the students' freshman year.

From our research, the authors have formulated a maturity model (see Figure 1) based on a student's sophistication with the use of social media privacy and security behaviors. This model can serve as a guide for future research on the development of training topics and their optimum teaching modality. At the base of the pyramid, setting strong passwords is commonplace amongst the most commonly used social media providers. At the next level, privacy settings include setting an account to be either private or public. At the third level, a secure configuration could include the use of two-factor authentication and geolocation. Fourth is selfregulation, which from the human behavior perspective, determines how one chooses to control their online postings. At the top of the pyramid, the intentional design of the personal brand, otherwise known as their social media presence, is crucial to managing public personal perception such as in the case of hiring or firing decisions and to that extent students must also understand that there is a positive relationship between the use of LinkedIn and obtaining relevant work in their field of study. Richardson (2017) had suggested "social media provides the opportunity for students to create their own persona and branding, whether this is positive or negative. Students can have a true identity, a pseudo identity through social media, and possibly even an anonymous identity as they post and comment. Research that studies the affect

that social media has towards forming traditional relationships and identity development would also provide useful information".

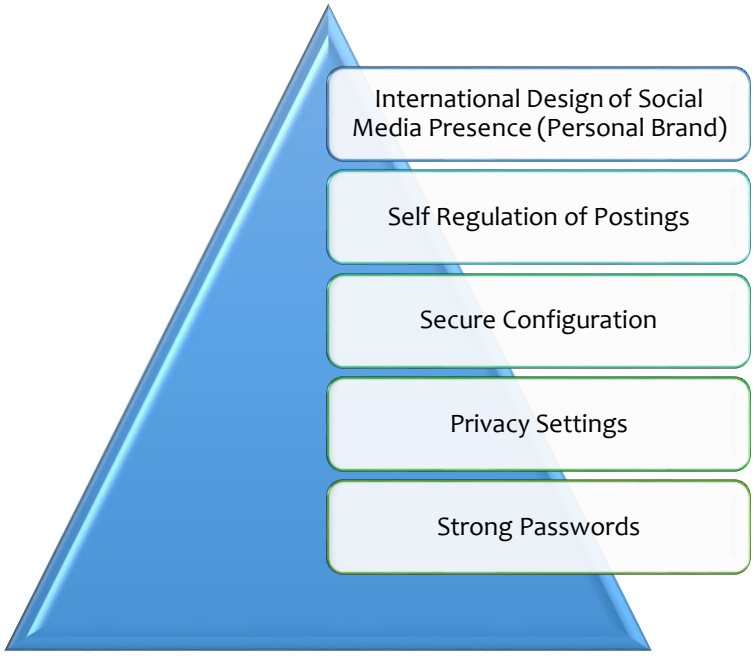

Figure 1. Social Media, Risk Awareness and Countermeasure Maturity Model (SMRA-CMM)

6. CONCLUSION

Through this research study a gap was discovered in the knowledge students had related to the importance of self-responsibility in managing their online social media activity. As self-reported by the students through the survey results, 78% had indicated that they were using the security features of their social media platform thus addressing the technological risk however 52% of students indicated they were okay with sacrificing their privacy for the opportunity to use the social media application indicating a need for additional awareness of training that expands from the technical risk but embraces the social risks as well. To this extent a definition of social risk that includes the influence of social media on future employers and job selection will require additional research. For the purposes of the SMRA-CMM the authors suggest that undergraduate education related to the students' risk to the loss of privacy and security online will require curriculum that first establishes the basis of cyber security basics to include the use of strong passwords and the use of a secure profile configuration to mitigate the technical risk and then further develops an understanding of the social risk that requires the regulation of online social media activity.

Our research has made a unique contribution to Information System education by addressing a gap that currently exists in that there is no formal structure to assess and develop privacy/cybersecurity awareness training for college students. This study proposes a maturity

model that will develop students beyond the use of simple security settings to active management of their online identity and personal brand.

Future research should be conducted on changing attitudes of digital natives with regards to their perception of accepted norms and benefits to loss of some privacy. An opportunity within academia lies in helping students understand the importance of reading and understanding the privacy policies of the sites they visit or applications they use. Additionally, a longitudinal study to understand students' perceptions on cyber-security would also prove to be beneficial.

7. BIBLIOGRAPHY

- Wikipedia-Cyber security awareness https://en.wikipedia.org/wiki/Cyber_security_awareness
- K. Njenga (ed.), ICICIS 2019 (Kalpa Publications in Computing, vol. 12), pp. 272–280
- ©2020 ISCAP (Information Systems and Computing Academic Professionals) Page 48 https://isedj.org/; http://iscap.info
- Cybersecurity Framework, National Institute of Standards and Technology. Retrieved from https://www.nist.gov/cyberframe work
- Pew Research Center. (2019). Social Networking Fact Sheet. Retrieved from https://www.pewinternet.org/2018/03/01/so cial-media-use-in-2018/
- International Journal of Advance Science and Technology Vol. 29 No. 10S, (2020), pp. 767-776
- Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin & Hamdullah Nejat Basim (2020): Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1712269 To link to this article: https://doi.org/10.1080/08874417.2020.1712269