Nathaly Flores

CYSE 600

Long Analytical Paper 6

Old Dominion University

Social Media and Cybercrimes Awareness

Introduction

Cybercrime, frequently comprehended as computer crime, is the prohibited usage of a computer for scams, romance scammers, Trafficking in children/adults and intellectual property, stealing's identities through social media, and invading privacy. Since the era of the computer has evolved it has been crucial to businesses, entertainment, and government, cybercrime has increased in volume, primarily using the Internet (Gillespie, 2019). It has been declared that cybercrime has significantly skyrocketed at an astounding speed and has been counted to be well over eleven percent each year (Decker, 2020). Numerous cybercrimes have occurred because phishing has been growing as the public and companies resume being used, unsettled by the lack of essential cybersecurity awareness. This occurs when a hacker impersonates an authentic person and persuades the victim to obtain an email, instant message, or text message and social media (Hong, 2012). The only way to fight this battle is to bring awareness to companies and the public.

Cybercrimes Achieved via the usage of social media.

The number of social platforms and applications has grown into a broad range. In the world of Information technology, the social platform is said to be a tool that creates a simple way for individuals to invent and publish content to people. For instance, Twitter emphasizes short text messages, and Instagram and TikTok are indicated to be straightforward in conveying pictures and videos to family and friends. Social platforms are a few proven mediums and are mainly uncontrolled for content. Meaning social platforms have more irregular restrictions than conventional papers of public transmission, like newspapers and radio stations, concerning what

individuals can post (Marttila, Koivula, & Räsänen, 2021). Many cybercrimes are committed by using social media, majorly for financial gain. Several crimes are committed through social media, including spam emails, cyberbullying, identity theft, online child pornography, phishing, and virus distribution, among others (Marttila, Koivula, & Räsänen, 2021).

Black-hat hacking techniques, strategies, and approaches are employed as an enlisting tool for individuals curious about comprehending and discovering more information (TTP) (Marttila, Koivula, & Räsänen, 2021). Facebook has been promoting the larceny of credit cards as a type of cybercrime continually being committed. Malicious actors, also known as threat actors, are people using consumers' stolen credit cards to buy and deal them off; these hackers bragged about what they have done and exposed CVV2 information to other hackers. These hackers/cybercriminals groups have their own general social platform accounts. They encourage others to use hacking lessons and security holes on YouTube to learn how to hack.

Cybercrime on social platforms is here to stay and will not disappear soon. Social media threat actors/hackers are using progressive ideas. Our nation has done its best to install the latest security updates and patches to try to overcome the persisting threat of these hackers attacking daily. Cybercrime has been rising; network defenses have been doing their best to keep their systems up to date from cyber criminals. These cybercriminals have discovered new ways of bypassing security standards. Security awareness is one of the main tools needed in social media to bring awareness of scams and frauds that are occurring daily. Hackers/scammers will keep raising the use of social media as their primary objective, as well as using platforms/blogs to show others how to hack a specific site or platform (Marttila, Koivula, & Räsänen, 2021).

Dating applications through social platforms

Individuals seek love and contentment; people turn to date applications to pursue finding 'the one; these applications have become well-known. These love applications ask for private information like end-users' location and exact area, identity to know if the person is genuine, occupation information, and statistics trends. The problem with these dating websites and applications is that they keep the information provided permanently and are constantly divulged to other social media platforms and the government. As a result, this violates an individual's privacy and ethical principles. For instance, tinder and Grindr, Bumblebee, Facebook dating application, etc., are modifying dating rules to their unlimited support of geolocation and real-time dating or phone dating applications (Murphy, 2015). Dating application characteristics are from traditional dating websites that highlight picture-based options, which allow for a small portion of self-description and then, depending on the person's social media account, like a Facebook profile for information. These applications can also influence end-user privacy views because they constantly enclose confidential dialogues and information based on location. End users are more willing to message the person in private through an application rather than use their people skills to engage (Hjorth & Lim, 2012).

Moreover, the definite reasons people use tinder, and such applications are hooking up, building friendships, seeking relationships, and leisure. Rejection increases with social relations and unable to manage problems confidentially, although egocentricity reduces it. It has significantly affected social confidentiality problems, excluding systemic concerns.

Catfishing

Another phenomenon that scammers use to trick users is Catfishing. Catfishing has been around for a few years and comes with online dating websites, social media, and applications, and it has increased significantly over the past years. What is catfishing, and why is this important to know? Catfishing is someone that creates a profile pretending to be someone they are not; in other words, using fake identities through deceitful actions on social networking platforms and typically selecting a particular victim. Catfishing is the same meaning as scammers/hackers because they are after one thing financial gain and get information that can benefit them when using dating applications or social media platforms.

Federal Trade Commission recently mentioned the sum of funds American residents have conveyed they lost to romance scammers, which has soared by nearly fifty percent since 2019; Since 2016, it has grown more than four times. By 2020 Federal trade commission it affirmed that romance scammers/hackers surpassed the summit of over three million and upsurged than it was before in the previous year (Fletcher, 2022).

Scammers and Romance using applications

The other form of scamming is the traditional scam that happens online. Online scams have been going on since the 1990s. They are continuously growing due to the proliferation of smartphones and IoT (Internet of Things) and new devices connecting to the Internet. Numerous online fraud scams victimize innocent people. Romance fraud is a scammer used to gain individual bank data from their targets. The scammer will use a dating site or application to win over a target and embrace an online identity that does not portray who they are. The criminal's profile will usually display a person on business trips or in the military (Scams, 2022).

Furthermore, the delinquent will use the individual and steal their identity to acquire the victim's trust by forming a fantasy of a romantic relationship and inflaming intrigue from the victim. The so-called relationship will advance relatively fast, and the main objective of the scammer is to make the target fall in love with the fantasy they have created with the scammer. Once the scammers see that the victim has fallen in love with them, the next step will be to convince the victim that they want to meet in person. Once the scammer has the victim worked up about meeting, they will begin to liaise numerous obstacles for the same reason the scammer's intentions will be not to meet the victim (Sorell & Whitty, 2019). For instance, the scammer will ask the victim for help purchasing a plane ticket, customs fees for flying, even retrieving a package, a visa, or other travel documents, or medical expenses (Scams, 2022). The main objective of the scammer is to get money by requesting to transfer it through a Wire transfer or reload a card or a gift card. If the victim does what the scammer says, then the lover comes to the rescue, then the scammer uses that to express their upcoming meeting for the future, which will never happen (Sorell & Whitty, 2019). That is to say; the scammer will keep using that same strategy to pursue the victim into their scheme until the victim has lost so much money from these scammers or no longer needs the victim and moves on to the next target.

Must examine and investigate, not allow someone to become a victim of these scams. We should educate and periodically monitor the younger generation, such as teenagers and young adults, who can fall prey to these scams. In addition, we should check on the elderly because scammers constantly target them. Scammers and criminals know whom to dispute with. Cyber Experts recommend ways for people who fall into the young generation or the elderly category to protect themselves from scammers.

1. If using social media, lower the exposure of personal data posted online and only add people you know.
2. Withstand the scammer's wish to act quickly. Scammers are skilled in manipulating people's emotions and invent emergencies to convince victims to act without thinking.
3. Always search for the data the scammer is proposing and any contact data given by the scammer. Seek agencies or people that have experience with scamming; they will be able to help and confirm that the scammer is trying to be scammed.
4. Never give scammers money or personal information to the scammer or give out gift cards as payments.

They are being preyed on by cybercriminals and Cybersex trafficking. These criminals also use the Internet to draft their victims (Litam, 2017).

The use of Hi-Tech

The use of technology daily; makes our lives more straightforward, and the benefits are good in many ways. However, there are valuable ways in the use Technology there. Trafficking has been around for a while now. It also has been used for nefarious ways, one of them being trafficking. Traffickers are using technology to trap victims by promising them victims work, opportunities, and a better life. According to DHS, Trafficking uses trains, buses, planes, and ships to transport victims, hiding them in plain sight. These criminals have various tools to choose from. The Internet and social media make communication easy, and people can talk to others anonymously. The downside of the Internet and social media is that criminals can work as a team and do not require being in the same country where the victim resides. They can work remotely on the other side of the planet and target anyone about anywhere. Cyber Criminals try

to hide their tracks and remain anonymous. One person can be in Europe or America. The other person can be in South America or some island or America, making it challenging and mystifying to trap.

One of the reasons we should be careful in using technology online is because traffickers use technology to grow their operations and remotely identify and recruit people on a massive than what is feasible through traditional offline schemes. Social media is a widely known venue, as traffickers abuse these platforms to acquire insight into a person's life.
Understanding how a cybercriminal works using technology will help us not fall into their trap. These human traffickers are very smart in the way they convince their victims. A family friend's daughter was close to falling into human trafficking hands. She was talking to a man online whom she had never met through Facebook. The man gave her the story as he could make her the subsequent supermodel, which she was convinced of. Off she went to travel to Los Angeles, California, for a photo shoot but instead, the photo shoot did not take place, and she was being lured into taking a trip to the Middle east for a photo shoot. She was one of the few lucky people whom law enforcement could intercept this plane and return her to her family before letting her know she was in great danger with the person she was talking to was someone who did human trafficking.

Cybercriminals use applications like Facebook, Craigslist, Instagram, and Twitter and dating applications like Bumble, Tinder, etc. End users should take cautious measures when using these social platforms. Sometimes see the person's face but do not know their intentions; since it is often used, people tend to let their guard down; that is where the person should not let their guard down but be vigilant. There has been a rise in online dating app fraud in recent years.

There has been an increasing extent of worried about online privacy, hackers, and security. People give out information willingly without knowing the threat and dangers they are getting themselves into (Schell, 2007). The US Government recently passed the Patriot Act to fight security in America. The Federal trade commission reported on its website during covid 19 in 2019 that American citizens had lost a good amount of capital due to romance scams. Since then, it has increased yearly, and the love of scams has grown worldwide (Ruggieri, Ingoglia, Bonfanti, & Lo Coco, 2020). These scams have increased by fifty percent more than in previous years. Nonetheless, the increase in romance scams has left many with broken hearts and no money.

The benefits of using social media

There have been various views on social platforms and applications, particularly internet-based social platforms, and their usefulness to society. Social media allows individuals to grasp every moment and make personal or skilled connections allowing them to use it for career purposes or friendship. Apart from the invasion of technology, it has imperiled conventional face-to-face communication, which causes individuals to spend an average of one hundred thirty-six times on social media accounts daily (Osborne, 2020).

Social platforms improve people's social skills in a way that improves them to manage their lives in a virtual and modern society. Individuals use social platforms to communicate with people worldwide by making informal or skilled connections. Social platforms have given individuals morals and increased their sense of belonging, significantly impacting their psychological happiness (Best, Manktelow, & Taylor, 2014).

Not only does it broaden people's social network, but it also strengthens social relations, which decreases feelings of loneliness, promotes friendship, and encourages identity probe in overall enhances people's well-being. Some advantages of using social media are communication and staying updated with family and friends worldwide, online socialization, improving learning prospects, and more extensive health information, which can also lead to mental health as a stress reliever. Social media suggests the younger generation the option to grow their social circle and make new friends. Another benefit of using social media is the growth of education through media, self-confidence, and social support and awareness for those to be conscious of what they publish on platforms like Facebook, Twitter, and Instagram.

The gloomy outcome of using social media

Social media has heightened rapidly, bringing numerous benefits concomitantly and creating severe social media cyber security situations. It also acts as a vulnerable platform to be exploited by hackers. Social media also brings cyberbullying, intimidating messages, and fiction that evolved familiar to people, particularly the younger generation. Hacking is the main problem with Facebook and Twitter accounts risking the security of people's personal information and reducing human interaction. Another problem associated with the use of social media is people's addictions and excessive time on social media. (Moate, Chukwuere, & Mavhungu, 2017) indicate that social media is one of the most outcomes made in the 21st century but can significantly harm users. Social media has impacted people's statuses, primarily children.

The leading cause is that adults poorly convey pictures on social media platforms with brutality and sex, which can significantly impact a child's behavior (Edge, 2017). These negative results are apparent in social lifestyles and cultural views (Mingle & Adams, 2015) argue that

social media changes learners' conduct and educational backgrounds. Besides these problems mentioned, another issue evolved in social media are the following:

- Privacy of information, End users share private information on social media, which causes privacy breaches that can also source personal information loss or prompt hackers to hold the exact cause for malicious motives. For instance, end-user data can be seen by everyone if the person uses their computer in a default location in public.
- Data mining means leaving an information trail behind while using the Internet. When someone makes a new social account online and gives details like birthdays, names, locations, and personal routines without the person's consent, this information is leveraged and then given to a third party for sharing the target market. It can lead to security problems as a third party can collect real-time updates on the end user's precise location.
- Virus and Malware Attacks, Malware and viruses are frequently found on a computer system through pesky ads. Once this malware and viruses access a computer network, the hacker steals personal information or provokes a total disruption to the person's computer system. This leads to the loss of all types of information like personal, professional, financial, and so forth.
- Problems are causing the use of 3rd Party Applications; Most applications now request approval from end users to access personal data. For instance, contacts, photographs, and recent geographic location before posting or installing applications operating in the background might download malware to the end users' phones or smart devices without their knowledge.

- Lawful Matters and legal threats related to social media, for instance, posting distasteful content towards anyone, society, or country. Those legal matters can be carried as offensive posts and uploaded by any person or company.

Designing new forms to get sensitive data

The hacker has developed unique ways of striking a social media account effortlessly. For instance, hackers can begin using phishing, which is a method of getting admission to critical and sensitive data of the end users' account information. These hackers make up simple strategies to create fake websites that can appear authentic. These websites can request the end user to provide personal credentials, which can give the hackers access to login into these end users' accounts. Malware programs are usually installed on the end users' devices without their consent. These applications generate viruses in the computer software, and hackers can use personal data to observe the end users' movements. Posting photos, status, and location check-ins give the hacker a degree of the end user's data in social media accounts. It is a typical threat. SingCERT statement indicates that the release of privacy settings discloses to end users the risks caused by cybercriminals, hackers, and scammers. As stated by this report, in April 2021, approximately five hundred thirty-three end users' accounts were leaked and exposed vital data to cybercriminals (SingCert, 2021).

Cybersecurity is a concern; therefore, various actions must be taken to protect information users using social media platforms. For example, users should ensure they have high-quality and robust antivirus to avoid malware caused by malicious websites. Additionally, educational and training programs should be initiated to create awareness among social media

users. Moreover, social networking sites should have security settings that help secure the user's account. For example, Facebook has login alerts that help to notify the user whenever someone tries to log in. Also, Facebook allows social media users to limit the number of people who can see their posts. Third party-authenticator is another strategy used by Facebook to authenticate any app belonging to a third party (Aldawood & Skinner, 2019). In this regard, social media users should understand how to protect their personal information when using social media.

Cybercriminals' primary area is social media for cybercrime; this occurs because they can quickly gain access to their end users' sensitive data. End users should be in the vanguard for securing their data. End users should constantly properly update bypass arising cyber threats. Educational training agendas are required to develop an awareness among the public on ensuring their data is secure.

Preventing from being scammed & bringing awareness

Scammers are not just someone who does not know what they are doing when scamming; they are trained and study their targets for profit (Johnson, Albizri, & Jain, 2020). A red flag should always be when someone asks for personal information. Always be careful when someone asks for sensitive personal information online, over the phone, or by email. Do not send pictures of family members or friends to someone you have never met but online. It would be best if the person is prudent and cautious when someone messages and asks for money, especially on dating or friendly application sites. This should be a red flag when scammers or hacker’s askes about money online; most of us will ask our family members or friends for that help, not ask the Internet online for help or money. Remember, sometimes family or friends will use information about someone they know in their lives and use it against them. Imagine what a

hacker/scammer can do with sensitive information given so quickly without ever knowing that person. Scammers/hackers do not care about anyone, nor do they have feelings or what will happen to the person if they are broke; scammers only care about destroying the person and even an organization if they can accomplish their goals.

These are the kinds of awareness we must spread about these types of scammers/hackers that people fall for more often than people think. Even huge Companies like Google and Facebook have been victims of these attacks. These companies face phishing sites pretending to be the actual site which can cause them to steal valuable information from a person. Spreading awareness will help people not fall for these cybercrimes. If people can see the dangers by showing commercials and billboard signs of how someone can use and steal information by using online dating sites or showing short descriptions of what type of method these scammers do to make people give out money to them. Bringing cybersecurity awareness will help someone who has fallen into the potential danger of being kidnapped by someone who is doing cyber trafficking with these applications or know someone which prevents them from being victimized. Having more cybersecurity awareness of these situations will potentially stop this. Hopefully, fewer people will fall victim to these situations and instead be alert and able to help others. This awareness should be made out to the public and all workplaces.

Safety Tips

Everyone should take a few straightforward steps when acquiring the Internet. Here are a few of them:

- Fund a vigor online safety agenda. Like Anti-malware brands, for instance, Norton, which delivers real-time security versus a broad spectrum of attacks/threats, like viruses, malware, and ransomware (Herath, Khanna, & Ahmed, 2022).

- Utilizing a solid password for daily usage, whether personal or work. Password should be at least ten different alphabetic and numeric symbols mixtures must be mandated. Please only use the same password all over again on different websites, and make sure to constantly change passwords to prevent them from ever being attacked and creating a challenge for hackers to acquire. If passwords cannot be remembered, utilize a password manager to keep all the login data secure.
- Regularly maintaining computer software current. Particularly for the CPU and internet protection software. For Hackers to acquire access to a system, there is an undisclosed flaw or a cyber-attack that occurs in the security software, which needs to be broadcasted. This can also reduce the possibility of a cyber-attack victim by securing their computer systems against susceptibilities and computer weakness (Herath, Khanna, & Ahmed, 2022).
- Posting sensitive information on social media applications and sites is a dangerous thing to do. Make sure to keep in charge of all the things being posted, specifically privacy the less that is being posted, the fewer hackers/scammers will be attracted (Herath, Khanna, & Ahmed, 2022).

Conclusion

The Internet is the key to globalization. Our society is developing daily, and scammers and fraudsters benefit from it. People/Society ought to see that criminals use the Internet as a vital tool (Yar & Steinmetz, 2019). Cybersecurity awareness is shown in the form of appropriate education for end users and teaching end users the legal and regulatory sanctions of cybersecurity information. Implementing the proper education and information to the end users will help companies and the public be cautious about what they do online. One way to help bring

awareness is to create a program for customers in which the end users are educated before using any social media platform services, allowing this to tackle consumers of all ages. Not only will awareness help end users fully understand the risks they may face when using social platforms. However, they will also be educated about cybersecurity risks, like love scams, human trafficking, stealing identities, and social media. Legal and regulatory sanctions have also affected the start of transparent policies and procedures for cybersecurity. The whole point of creating policies is prioritizing ensuring these policies are transparent and communicated and easy to understand for end users to comprehend quickly. Doing so will help end users feel that their private data is secure and protected. Social platforms will give consumers the capacity to make reports of any security situations they may encounter. This will give social platforms an understanding of cybersecurity practices they may face daily, which is vital for initiating the proper connection between social media platforms and their end users.

Works Cited

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *International Journal of Security*, 73.

Best, P., Manktelow, R., & Taylor, B. (2014). Online communication, social media and adolescent wellbeing: A systematic narrative review. *A systematic narrative review. Children and Youth Services Review*, 27-36.

Decker, E. (2020). Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score . *Journal of national security law & policy*, Vol.10 (3), p.1 .

Edge, W. (2017). Nursing Professionalism: Impact of Social Media Use among Nursing Students. *Journal of Healthcare Communications*, 3-28.

Fletcher, E. (2022, January 25). *Social media a gold mine for scammers in 2021*. Retrieved from Federal Trade Commission : https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2021

Gillespie, A. A. (2019). *Cybercrime: Key issues and debates.* Oxon: Routledge.

Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, 1-18.

Hjorth, L., & Lim, S. (2012). Mobile intimacy in an age of affective mobile media . *Feminist Media Studies* , 477-484.

Hong, J. (2012). The State of Phishing Attacks. *Looking past the systems people use, they target the people using the systems.* , No. 1, Pages 74-81.

Johnson, M. E., Albizri, A., & Jain, R. (2020). Exploratory Analysis to Identify Concepts, Skills, Knowledge, and Tools to Educate Business Analytics Practitioners. *Decision Sciences Journal of Innovative Education*, 90-118.

Litam, S. D. (2017). Human Sex Trafficking in America: What Counselors Need to Know . *The Professional Counselor*, 45-61.

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study. *American Journal of Criminal Justice*, 862–881.

Mingle, J., & Adams, M. (2015). Social Media Network Participation and Academic Performance in Senior High Schools in Ghana. *Library philosophy and practice*, 1.

Moate, K. M., Chukwuere, J. E., & Mavhungu, M. (2017). The impact of wireless fidelity on students? academic performance in a developing economy. *International Institute of Social and Economic Sciences*, 15-18.

Murphy, M. (2015). Swipe Left: A Theology of Tinder and Digital Dating. *The National Catholic Review. Retrieved from Loyola eCommons, Theology: Faculty Publications and Other Works.*, 1-3.

Osborne, I. (2020, January 25). *PI MEDIA*. Retrieved from Does social media improve or impede communication? : https://uclpimedia.com/online/does-social-media-improve-or-impede-communication

Ruggieri, S., Ingoglia, S., Bonfanti, R., & Lo Coco, G. (2020). The role of online social comparison as a protective factor for psychological wellbeing: A longitudinal study during the COVID-19 quarantine. *Personality and Individual Differences*, 171.

Scams, W. t. (2022, August). *Federal Trade Commission* . Retrieved from What to Know About Romance Scams : https://consumer.ftc.gov/articles/what-know-about-romance-scams

Schell, B. H. (2007). *The Internet and Society.* Canda: ABC-CLIO.

SingCert, C. (2021, May 03). *SingCert*. Retrieved from Social Media And Cybersecurity: https://www.csa.gov.sg/singcert/publications/social-media-and-cybersecurity

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood . *Security journal*, 342-361.

Yar, M., & Steinmetz, K. (2019). *Cybercrime and Society.* SAGE Publications Ltd.