IJARASEM

ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 1, January 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.421

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

ISSN: 2395-7852 | www.ijarasem.com | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 1, January 2023|

Social Media Role in Cyber Crime

Manoj Kumar Tatwal

Assistant Professor, Dept. of Maths, Govt. College, Bundi, Rajasthan, India

ABSTRACT: Social media platforms are the success story of the century, certainly as far as numbers of users go. To give you an idea of the popularity of this type of software here are some of those numbers:

- Facebook – 2.45 billion monthly active users
- Twitter – 300 million monthly active users
- Instagram – 1 billion monthly active users

Popularity like this means that social media is like honey to a wasp where cybercrime is concerned. Fraudsters see social media users as a captive and trusting audience, that can be manipulated into performing acts they would normally be more vigilant about. Social media has effectively built a platform, not just for sharing ideas and cat pictures, but as a playground for cybercrime.Here, we look at some of the ways that your social presence is being used to commit cybercrime.

KEYWORDS: social media, cyber crime, fraudsters, facebook, twitter, instagram, software, audience, manipulated

I. INTRODUCTION

In a report from security vendor Bromium, "Social Media Platforms and the Cybercrime Economy"[4] they describe this conduit for cyber-attacks as "platform criminality". The social media platforms that many of us love and use daily are a portal that opens new opportunities for cybercriminals to exploit. The nature of social media means data sharing is an inherent part of the apps. Trust is also a crucial part of the social media engine. These two things align to create a perfect cyber-storm.[1]The Bromium report explains how cyber-attacks are facilitated by social media platforms; it concludes:

- A "global distribution centre for malware": The report explains that 20% of organizations have been infected by malware via social media.
- Specifically, the spread of cryptomining malware: Simply clicking on a YouTube advert could end in cryptomining malware infection.
- The boundary between the darknet and social media is blurring across social platforms, such as WhatsApp and Instagram, which are being used to promote and sell the tools of the hacker.[2]

Social media is also a deep pool of personal data. People feel safe to share personal details on social media platforms; a sense of safety is an important part of being on social media, that is designed to be used between friends and family.[3] However, without due care, personal data, such as name, phone number, address, and even your location can be stolen and used for identity theft or the creation of synthetic identities.Social media is not all bad. It offers a way to keep in touch with family and friends and generally communicate. Professional versions of social media, such as LinkedIn, are an important way to keep up with industry intelligence. But using them safely requires some effort. Here are some ideas of using your social media account, safely.Privacy has been in the news a lot over the last couple of years. Regulations such as the EU's GDPR, have resulted in privacy becoming mandated[4]. In 2019, Facebook, one of the worst privacy violation offenders, ended up with a fine of $5 billion (approx. £3.9 billion) for the Cambridge Analytica debacle because Facebook sold user data without consent.[5] In another Facebook case, the company was accused of storing hundreds of millions of passwords in plain text, accessible by Facebook employees.[6]When using social media, you should always ensure you are comfortable with the privacy settings on the platform. Each platform is different, but some general rules of thumb are:

- Do not overshare – avoid putting highly sensitive information on a social platform, especially those such as Twitter which are essentially public.
- Know the audience – some platforms allow you to set granular controls over who can see a post, e.g., only friends, use these settings wisely.

- Control your public profile – if the platform allows this, control who can view your account details.[5]
- Control your data – do not place data such as birthday or phone number on a platform that is public. Avoid these types of data even in more private settings too.

Some social media platforms are more insecure than others.Twitter: This is essentially an open social platform. Your profile is public, or it is private, there is no granularity. Private profiles mean that only those who follow you can see your tweets. Twitter asks for your date of birth during profile setup. If you add it (this is optional) then the world can see it unless you set your profile to private.

Facebook: Because of privacy violations, Facebook has been forced to make changes to improve overall privacy on the platform. Groups are now public, private, and private and hidden. The platform has also updated its "Privacy Check-up Tool" to help you decide if your privacy settings are robust enough.[7] Other privacy settings have been improved too.[6]

LinkedIn: This professional social platform has good levels of privacy granularity. You can choose which degree of connection can see various profile settings, such as email address. There is even a level of control over who can see your last name.

Instagram: Owned by Facebook, this platform has suffered from inherent security vulnerabilities like its parent, putting data at risk. The platform has also been used as a way to recruit Money Mules.[7]

One of the reasons that social media can be so useful to fraudsters is that, currently, it is fairly easy to set up a fake account. Facebook has recently had to delete 5.4 billion fake accounts across its platform.[8] Fake accounts are used to trick legitimate users, socially engineering them into clicking malicious links or even giving away sensitive information.The fake account method can also be used to spoof a real user account, using photos of that person. The fraudster then posts offensive material in an attempt to extort money from the target.As well as being a target for malicious account access via phishing emails and texts, social media is being increasingly used to deliver phishing. The combination of wide reach and elevated trust levels is making social media an attractive way for cybercriminals to use social engineering tricks against their targets.Cybercrimes on social media include "Romance Scams" where a fake account is used to groom a victim, eventually tricking them into handing over money. Another scam type is the offer of free vouchers and giveaways. The fraudster provides a link in a post that goes to a malicious website.[8]

II. DISCUSSION

There's no denying that social media has forever changed how we interact with one another. Social media has been more important than ever in the past year, with many of us stuck in our homes waiting out the seemingly endless COVID-19 pandemic. Whether we've used our social media feeds to pass the time or connect with friends and family, it's helped us all feel connected, informed us, or just given us a good laugh. Unfortunately, it's also been weaponized to spread disinformation, promote scams, and, more recently, steal information from COVID vaccination cards. These examples only scratch the surface of how threat actors can take advantage of us on social media. In this blog, we'll explore social media-linked cybercrime, focusing on three different aspects:

- Cybercrime targeting social media users
- Cybercrime facilitated by social media platforms
- Cybercrime advertised on social media platforms[9]

Our social media accounts have become somewhat safer over the years, with significant improvements in privacy and security usually coming in the wake of some sort of social media disaster (I've lost count of how many times Mark Zuckerberg has appeared in front of Congress to explain "what went wrong"). The increased adoption of two-factor authentication (2FA), for instance, has helped avoid many of the single points of failure. However, just because you checked all those little boxes in your security settings to make you feel bulletproof, it doesn't mean that your account is invincible in the face of an opportunistic threat actor. Social media account credentials are often leaked in database dumps, opening the door to account takeover. And 2FA isn't a guarantee of protection: We've seen attackers advertising services for bypassing 2FA on cybercriminal platforms. In some cases, cybercriminals freely share knowledge on how to bypass or hijack 2FA.[10] Ideas may include a loophole found in a given application's security apparatus or a more elaborate scheme that requires a bit of finesse. For example, a user on one Russian-language cybercriminal forum advertised a method for "dominating" an Instagram account. The tactic entailed hijacking an Instagram account (presumably with leaked credentials) and stealing it from a user by taking advantage of the connection between Facebook and Instagram. The method ultimately allowed the attacker to enable 2FA on their own device, giving them full control over the victim's Instagram account. [11]You've probably heard terms such as "bots," "zombies," and "botnets" in recent news stories about data breaches and other cybersecurity risks. These bots are also being sold on cybercriminal platforms to target social media accounts. Unlike traditional botnets that directly infect computers to create networks, social botnets use social media platforms to create a network of fake profiles linked together to spread malicious links and content. On one Russian-language cybercriminal platform, users can be found advertising botnets for Telegram and TikTok that can reveal personally identifiable information (PII) about users.Checkers and brute-forcers are also popular tools sold and shared on cybercriminal forums. By using credentials leaked from database breaches, attackers can employ checkers and brute-forcers to conduct credential-stuffing attacks. These attacks attempt automated login requests against websites to determine the validity of credentials and, if successful, gain unauthorized access. Gaining access to a victim's social media account might provide a password that could be used to try and log into accounts on other sites if the victim has re-used their password. In this sense, gaining access to a social media account might be the first step in a two-stage attack.[12]

Scammers know that the likelihood of achieving a successful attack is a numbers game – the more individuals they target, the higher the chances of success. Attackers behind email phishing attacks know this, and that's why they often use mass mailing techniques. But the same is also true when attempting to scam users on social media platforms. Unfortunately, these platforms have become victims of their own success, particularly in comment sections and personal messaging interfaces. These convenient tools can be a cesspool for scams promoted by fake personas and botnets. After being advertised on cybercriminal forums, mass commenting and private messenger spammers are syndicated across social media.Social engineering skills also come into play – attackers are known to craft comments that contain malicious links coupled with a promotional slogan or clever message. For instance, a targeted attacker may monitor a social media user (aka target reconnaissance), [13]observe they are enthusiastic about Minecraft, and then leave a comment with a link offering "freebies" for Minecraft. This link would redirect to a phishing page designed to steal the user's credentials.More technically sophisticated threat actors use their knowledge of tradecraft to spread malware across social media platforms. On one Russian-language cybercriminal forum, a user shared a method for disseminating an executable file in which an attacker would download a popular YouTube video, encrypt it with a remote access trojan (RAT), and then re-upload the video to their personal YouTube channel with a link to download the RAT in the video description. Social media impersonation is another tactic that can be pretty effective. Successful impersonation scams have made headlines, especially when the person being impersonated is well known.[14] Some of the more infamous scams have been fueled by the increasing popularity of cryptocurrency. In these scams, attackers impersonate celebrities on social media platforms and promise to provide unsuspecting victims "more" cryptocurrency in exchange for a small deposit. Of course, the fraudsters ultimately take the money and run, and they never make good on their promise. Adding to Facebook's security woes, its subsidiary messaging platform WhatsApp has been the victim of recent impersonation scams. At the onset of the coronavirus pandemic in 2020, threat actors engaged in Business Email Compromise (BEC) increasingly used WhatsApp and Facebook messaging services in BEC attacks by impersonating high-level executives, lending an air of authenticity to their requests for wire transfers.[15]

Finally, we can't talk about cybercrime and social media without taking a closer look at the syndication of cybercriminal advertisements across social media platforms. Just because your personal feed of cat memes and snack foods isn't reflecting these ads, that doesn't mean they aren't out there. This begs the question: Why would cybercriminals advertise their illegal activity on legitimate platforms? Well, there's really not just one single answer. But we know that many financially motivated threat actors won't shy away from a scheme if the reward outweighs the risk (in their mind).One type of cybercrime commonly advertised on Facebook is credit card theft. This includes users buying and selling stolen credit cards, offers of carding as a service, threat actors exchanging carding methods, and even some braggadocious fraudsters boasting about leaked CVV2 data – maybe trying to get some skin in the game.We have observed cybercriminals advertising YouTube videos that teach hacking or advertise vulnerabilities. Some cybercriminal forums even have their own dedicated channels on social media platforms that are publicly available. These are not only effective for sharing hacking tactics, techniques, and procedures (TTPs),[16] but they also serve as somewhat of a recruiting tool for anyone on the Internet who wants to learn more about black-hat hacking. Social media platforms also have fraud-dedicated groups whose users could care less about hiding their criminal activity. In Russia, fraud-dedicated groups operate primarily on two platforms – VKontake (VK) and Odnoklassniki (OK). The types of information openly shared in the groups include compromised financial information such as credit card numbers with PII and authorization codes, cybercrime tutorials, and commercial offerings like malware. Just as cybercriminal platforms ban users for defrauding other members,[17] the VK and OK admins try to shut down pages, groups, and profiles that promote fraudulent content. However, many scammers continue to use fraud-related terms like cashout, carding, and selling CCs when naming their groups and profiles.We've just highlighted a few here, but there are endless other examples of social media fraud, suggesting that cybercrime on social media won't disappear any time soon. In fact, it seems that fraud has only accelerated during the pandemic, with network defenders trying to catch up with cybercriminals' innovative new methods.[18] Despite security updates and patching that help ward off future threats, threat actors on social media continue to find ways to be creative and use our naivety against us. For this reason, security awareness is one of the best tools at our disposal when we are using social media. Because social media is such an accessible attack vector, scammers will continue to weaponize it going forward, and coordination on cybercriminal forums will almost certainly continue. If you are interested in learning more about detecting fake social media profiles, check out some of our existing research here. If you are interested in how Digital Shadows SearchLight^{TM} can help you detect threat actors impersonating your social media handles, you can take Searchlight for a 7-day test drive or contact us for a customized demo.[19]

III. RESULTS

"Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm." — Anna Maria Chavez….The term cyber is a prefix which denotes a relationship with IT (information and technology), in other words, anything related to computers such internets, cloud storage, etc. falls under the category of cyber. Whereas the term crime refers to an illegal act which causes harm either to person physically, mentally or in any other way; or it harms the reputation of an individual. When these two terms cyber and crime meets and forms a single term "cybercrime" it is deadliest combination.[20] Now-a-days cybercrime is the most reported crime in the country and we often see that not only teenagers but people of almost all age groups are present and connected on social media. People usually use social media to share their pictures, videos, thoughts, wishes, etc. with the friends staying far away and to get in touch with their friends with whom they have lost their touch years back and this is the purpose for which it is meant. But the people with evil mind anyhow manage to find that how they can misuse it and do the mischief.[21] The people who either put spam comments or comments defaming others on social media or create fake accounts or follows any person or texts any person uselessly for the purpose of fun, but they seriously don't know that they are committing serious crimes and can be prosecuted and punished under either the Indian Penal Code, 1860; or the Criminal Procedure Code, or; the Information Technology Act, 2000; or under any other law as per circumstances and facts of the case.For any person or any organization, his/her reputation is utmost important as an individual or an organization is recognized after its name or goodwill only, but if that goodwill or name only gets spoiled then the value of that thing often falls, trust of people gets migrated and many such things happens. For example if we think of clothing brand, then suddenly names like Adidas, SuperDry, Wrangler starts coming to our minds;[22] if we think of mobile brand, then names like Apple, OnePlus, Xiaomi, etc. starts flashing into our minds, why is it so? This is because they have very good reputation in the market and their goodwill is very high because people have trust on them, and in case, if they breaks the trust of even a single customer, it's pretty sure that no one is going to come back to them.[23] But in case, if any person knowingly tries to spoil either the name of any person or any organization in the market on the false and ruthless basis, then under law, it is termed as defamation and it is illegal. The term defamation has been defined under section 499 of the Indian Penal Code, 1860. In short, if any person who by either by writing, or speaking, or by making gesture tries to publish or do any act which harms the reputation, then that person will be charged for act of defamation.[24]Now-a-days, we often get to see good number of cases of defamation on social media platforms such as Facebook, Instagram, Snapchat, Twitter, etc. But no one is interested in taking action as they enjoy it and feels it's a good time pass and let it go on. But the person who is being defamed for an unnecessary cause only knows through which time he is passing. Some people are enough brave that have no effect on what people are saying about them but there is a majority of people who are very delicate and starts thinking of future consequences of it. This social media defamation has a very negative effect on each and every person who is being defamed especially on people who are very delicate, as starts suffering from diseases such as severe depression, overthinking, stress, etc. and some people thinks that they now they can't face the society and there is now is worth of living more and at the end they take their own lives by hanging themselves to death.[25]Social media defamation is one of the most common crimes now-a-days that we see. Now the question is what is it exactly and where we see this? The answer to this question is very simple, lets understand with the help of an easy example:

There are two person namely Jatin and Yatin, both are very good very friends. One day Yatin clicked some funny pictures (in which he was made a girl with the help of an application) of Jatin on his mobile, and he posted that pictures on social media using hashtags suitable to the pictures, and that images got viral. Jatin was unaware of it and when he came to know, he was completely shocked to see them. He became totally upset after seeing the comments of the public on his pictures and decided to quit his life as his reputation was completely destroyed everywhere, in the eyes of his family, friends, university, etc. He feels that if he goes out, he will not be able to stand or face the people as they will laugh. Later one of his friend named Kunal stopped him to do so and said that it is defamation and instead of committing suicide, he should file a suit against Yatin for the same.[26]

From the above example, we can conclude how serious crime defamation is. No doubt, defamation is just a one word, but it has that power that any can take his/her life, if it comes to him. People will have to understand that there's a huge difference between defamatory statement and free speech. People also very well knows that have the Right of Speech, but they don't know that how to use it. There are various crimes associated with the case of social media defamation and the same are as mentioned below:

Basically the term 'stalking' refers to act of following a specific person from a long period of time whereas the term, cyber stalking refers to the act of the stalking that is done using internet. It includes harassment as well as threatening. In crime of cyber stalking basically there are two parties, where the person whoever do the act of stalking is called as the stalker or the attacker and the person on whom the attack is being made is called as the victim. Usually the under cyber stalking the stalker is the friend or known the person of the victim, he later starts following that person on his social media accounts like Facebook, Instagram, WhatsApp, etc. in order to view his profile and pictures and in some cases the stalker becomes so violent that he starts harassing or threatening the victim by sending inappropriate pictures or videos or messages which makes them feel uncomfortable.[27] Sometimes the stalking becomes so serious in nature that it even leads to murder or rape or some sort of physical assault on the victim. Now the question is how the act of stalking is dealt within the boundaries of the India? The answer to this question is very simple, in India, the act of stalking is governed under the Information Technology Act, 2000 and the Criminal Law (Amendment) Act, 2013. Section 67A of the IT Act, 2000 states that if any person circulates or publishes any restricted con tent on internet, then such act will be considered as crime of obscenity and if it committed for the first time then the same is punishable with the imprisonment which may extend to the period of 5 year alongwith the fine of amount upto Rs. 1,00,000/- and if the same person commits it for the second or subsequent time, in that case it is punishable with the imprisonment which may extend to the period of 10 year alongwith the fine of amount upto Rs. 10,00,000/-For the women who are the residents of Delhi and feels that they are being stalked, they can call 1096 and report the same whereas for women residing in the other parts of India[28], they can contact National Commission of Women by calling 011- 23219750. Women can also the report the case of cyber stalking by filing an online complaint on the portal of National Commission of Women (NCW) by visiting their website i.e. http:// ncw.nic.in/ and the same will taken by the commission with the help of cyber crime department and police of respective areas.[29]

"Sticks and Stones can break only bones. But words can kill you.Why is said so? This is because if you got hurt by sticks and stones you will recover within sometime and the wound will be healed, but the if you are hurt by the words of someone, it is more dangerous as it can cause severe depression and can also take your life too. They hurt caused by the words of someone can also destroy your inner confidence, your selfrespect, your spirit and you might not even be able to stand in group.[25] This was the blur picture of meaning of trolling, now moving to the actual meaning of trolling, it is somewhat similar to defamation, but is not exactly defamation. It is basically circulating the picture or video or message on famous and most surfed social media platforms such as WhatsApp, Facebook, Instagram, Snapchat, etc. which insults any individual or any group or any organization, or make them feel uncomfortable, or puts them under severe depression is known as social media trolling. Trolling also includes putting some text which is totally controversial in order to start unwanted debate, comments, etc. and the end result arising out of it always flags off the disputes between religions, genders, etc. Also sometimes this dispute crosses all the limits and becomes the spot of crimes. In short, we can say that trolling is the direct character assassination of an individual or any group or any organization, because it spoils the whole goodwill or reputation of the person or any group and they feels so insulted or gets so destroyed from inside that don't even feel comfortable to stand in some group or some public place. f Instagram – Suppose there's a video posted, now on every comment thread there are users who say something like "this video sucks,"[26] and these are those people who even don't know what the video is mentioning about or sometimes we see people fighting uselessly in comments just to gain the attention of the audience on their profiles, and to do this they forget all the standards or common sense and falls to such a level, that no one can expect. But now the question is how can we report this type of users or posts trolling someone? It very simple to report such users or posts that create nuisance on social media. In order to report a post or user, we simply have to click on option of 'more options' and then we have to choose report, after clicking report, we have to choose whether its spam or inappropriate, and then have to select the best matching options (like what sort of content is posted) from the options available and then we have to click.[27] It will directly be sent to the community, where they check that the post has actually adhered the guidelines or not, and then they take the appropriate actions against that particular post or user.Stealing of identity is also known as identity theft or identity fraud, so from its name itself i.e. identity theft we can presume the meaning. It is the combination of two words i.e. identity and theft, where identity means who or what a person is and theft means stealing, so, it's basically stealing of identity of some person. Now-a-days, stealing of identity is a very common crime but is very serious in nature as an identity of an individual is being robbed by some person and then it gets misused. It is commonly of two types i.e. true name and account takeover. The true name identity theft means that the thief will use the name or identities of another person and can get issued SIM Card, open bank account, get debit or credit card issued for himself, whereas incase of account takeover he will just use steal the already issued stuff such debit cards, credit cards, etc. In both cases, it's not going to cost him anything because the identity is of that another person and in case if he commits any subsequent crime, that person whose identity was originally used will be the accused once.[28]

On social media also the cases of stealing of identity are increasing day by day as people create fake accounts of some other person, sometimes to take revenge from someone or to make fun. The person who creates such accounts is very familiar with the person whose account they are creating because they have all information like date of birth, place of residence, religion, etc. which is 100% accurate, so that it pretends to be the original identity of that person only. And this is absolutely an invasion on the privacy of the public getting connected to that account. Let's clear this with an easy example. "Tanu is a student of BBA and is also very beautiful girl. Mandeep is one of her best friend. One day one some matter they had a fight in the college and itself and their friendship came to an end as Tanu slapped Mandeep in front of whole college, so at that moment didn't told Tanu anything but he felt he was insulted and in order to take revenge from Tanu, he one day created a fake account of Tanu on Instagram and started posting her pictures which depicts that her account was original. He started posting sexual content from her fake account and started sending obscenity contented messages to all her known, also at late in the night he as Tanu started chatting with boys and girls for long hours and asked for them their pictures and day by day the image of Tanu originally was getting spoiled and people started thinking she was a girl with bad nature. But in real life she was not.[29]

From the above example we can conclude that the privacy of all the people who were chatting with Mandeep (who was pretending to be Tanu) was completely invaded as Mandeep was having all the sensitive information and pictures of all those persons with whom he used to chat. And also the personal identity and her privacy of Tanu have been attacked badly and she in a moment has become a girl with bad character in the eyes of the people.So it rightly said that, "Think Once Before You Act, Twice Before You Speak and Thrice Before You Post on Social Media!Whenever we post something on social media, we have always have to be vigilant, it's not the matter that whether the user is a girl or a boy, he/she is wearing short length or long length clothes, he/she is fair or dark in complexion; instead the user should know the people on social media, who all are connected/ added with him on that platform. The government and the respective agencies are doing their piece of work, also, the Information Technology Act, 2000 is meant to deal with crimes such as cyber stalking, cyber trolling, phishing, hacking, etc. Moreover, we should also monitor ourselves that what type of content we are putting on social media and with all whom we are sharing the content such.We should also keep our accounts secure by the way of changing the passwords regularly, updating the security policies made the respective agencies, not adding unknown people to the list of your known, not sharing the personal details such as OTP, passwords, etc. and the most important thing if you ever feel that you are being stalked or getting into the claws of such traps then all the true information shall be reported to the nearest police station or cyber crimes department of the city[11]

IV. CONCLUSIONS

We love social media these days. Facebook, Snapchat, Twitter, LinkedIn, and many others can lead to lots of sharing and fun, but also carry significant risks. This is particularly true now that cybercriminals are collating data and using it against us for targeting phishing attacks.Online social networks may seem all in fun and harmless, but they are anything but that. Anyone participating in a social network online assumes some risk of becoming a victim of a con artist or other criminal. But this does not mean you should opt out of getting involved. It's part of our society, and in some cases an important part of doing business. Just be aware of the risks and take action to avoid being a victim of identity theft or another cybercrime.It's always important to remember that once you put something on the Internet, it is there… forever. It never disappears, you can't completely remove it, and there is nothing preventing your connections from sharing. Once that happens, you lose control of it. If someone in their network shares it, it will crawl even further into the Internet and there really is little to nothing you can do about it[15].Therefore, always know who you are giving access to your personal information and if you don't want them to share something, ask them not to or just don't post it. Also, keep in mind that what you post can reflect on your business relationships as well. Even if you don't connect with business contacts via social media, it can still get around and affect your business.Pay attention to who wants to follow, friend, or share with you. Often cybercriminals will try to connect with people to learn about them, bring them into confidence, and then scam them. This may come in the form of attachments or links passed on once you are "friends" with that person. It may come in personal requests, such as asking you to send money via wire transfer or even gift cards to help with an emergency.[20]

Any information found on the Internet may be used against you for nefarious purposes, so always think about what you post. And just because you use the highest privacy settings, doesn't necessarily keep you safe. Assume that whatever you post is available to anyone on the Internet. Hackers of all types troll social networking sites to put together collections of information on specific targets. The information may be used for something completely unrelated to social media, but can do a lot of damage. For example, if you work with financials in your company and you share it on social media, you could be targeted for wire transfer fraud.All of this may not only put you in physical danger, but it may also be used to create phishing messages and to send emails to people you know, including your co-workers. These email messages could contain malware. Once a link or attachment is clicked, it could unleash something nasty on the network. No one wants to be responsible for that[25].A good example where criminals will often go to learn important information about you is LinkedIn. This social networking site is a great way to form business relationships, but is also often used by criminals to learn more about an organization's personnel. For example, LinkedIn can provide a would-be criminal with the employee names, job positions, job responsibilities, and even how long an employee has worked at the organization. This information can then be used by criminals to target "high risk" employees or even be used as part of a larger social engineering campaign.Because all this information is now available to the public, you need to be even more diligent in detecting potentially malicious activity. From suspicious emails to phone calls, just because a person contacting you knows some personal information about you, does not mean they can be trusted. Don't be tricked into giving out even more information or opening links and attachments contained in emails. Always do an independent verification before disclosing any personal or sensitive details about yourself or your organization.Think about how you use social media and how much information you want to share with the world. Because even if you think it's just your "village" seeing the information, the reality is that it isn't. It's everyone, everywhere.Generally speaking, there are two ways in which hackers and cybercriminals use social engineering to exploit social networks.1. Attempting to get someone to install software on a computer or phone that will give them access to that device.2. Gain someone's trust in order to exploit personal connections and manipulate people through the social network.People are the weakest link in cybersecurity and the savvy hacker will take advantage whenever possible.[20] Following are a few tips to help you avoid becoming a victim of either of these:

Always use the strongest security settings possible on social media sites. For example, consider if you need to share your location. If it really isn't necessary (and it usually isn't), deactivate that option. Also be sure to limit who has access to your information. Don't make it public to the world, but instead make it viewable only to those who are directly linked to you, keeping in mind that even that information is vulnerable once one of them sends it on. Some sites will allow you to customize lists based on what you are posting. This may be appropriate for some content.Don't post personally identifiable information (PII) on social networking sites. This includes your birthdate, phone number, and address. If you want to exchange that information, do it via private messaging or email. Never ever post your social security number or any banking or other financial details, not even through the site's private messaging or email service.If you use your smart phone to post photos to your social networking sites, turn off location services for your camera. Leaving this activated will give away your location. While you may think it isn't a big deal to share your location, it can be[18]. When you're on vacation and sharing selfies with recognizable landmarks in the background, it would be a great time for someone to break into your house and steal all kinds of information.Be aware of unsolicited contact from strangers. Often, scammers will try to get to know you and then scam you. This happens often with online dating sites. They may use social engineering such as to convince you they need money to help them get out of a bind, but they also may use you to spread malware. It's reasonably easy to spoof someone's email address and often the criminals will do this to try to get your friends, colleagues, and other contacts to click malicious links. People are more likely to click a link if they trust the one posting it. Therefore, use caution even when clicking links on social media from those you do know.With the increase in popularity of private messaging services that are attached to the social media sites, such as Facebook Messenger, watch for private messages that arrive that include only a link, or have a vague description of what the link may contain. One that was seen recently was sent with text that addressed the recipient by name, "Bob, is this you?" Contained in the link was malware.[27]If a deal sounds too good to be true, it is. Cybercriminals use popular events and news stories as bait to get people to open infected email, visit infected websites, donate to fake charities, or purchase items that either don't exist or that are counterfeit. Recently, someone impersonated Iron Man star, Robert Downey Jr. and scammed people out of their money by "personally" asking them to donate to his favorite charity. Other stars were used in such scams as well, such as Brad Paisley, Hugh Jackman, and Elton John. All had to send pleas out to fans not to fall for it[28].Change your social networking passwords often. Studies have shown that even with all the password reuse issues and stolen credentials, 53% of social media users had not changed their passwords in over a year and 20% had never changed them. It's recommended to do it quarterly and when doing so, don't reuse one that you use on another site; especially one that you use for you financial accounts.The bottom line is just to use caution when participating in social networks. They can be fun and useful and are likely here to stay. However, just use good judgment and common sense when partaking so you are not or don't cause your company to be the next victim of fraud or identity theft.[29]

REFERENCES

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
2. ^ "cybercrime | Definition". Encyclopedia Britannica. Retrieved 25 May 2021.
3. ^ Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.
4. ^ Bossler, Adam M.; Berenblum, Tamar (20 October 2019). "Introduction: new directions in cybercrime research". Journal of Crime and Justice. 42 (5): 495–499. doi:10.1080/0735648X.2019.1692426. ISSN 0735-648X.
5. ^ "cybercrime | Definition, Statistics, & Examples | Britannica". www.britannica.com. Retrieved 14 December 2021.
6. ^ "BUFFETT: This is 'the number one problem with mankind'". Business Insider. Retrieved 17 May 2021.
7. ^ "Warren Buffett: 'Cyber poses real risks to humanity'". finance.yahoo.com. Retrieved 17 May 2021.
8. ^ "Cyber crime costs global economy $445 billion a year: report". Reuters. 9 June 2014. Retrieved 17 June 2014.
9. ^ "#Cybercrime— what are the costs to victims - North Denver News". North Denver News. 17 January 2015. Retrieved 16 May 2015.
10. ^ Lewis, James (February 2018). "Economic Impact of Cybercrime - No Slowing Down" (PDF).
11. ^ "The Global Risk Report 2020" (PDF). World Economic Forum. 15th Edition: 102. 15 January 2020.
12. ^ Gordon, Sarah (25 July 2006). "On the definition and classification of cybercrime". Journal in Computer Virology. 2: 13–20. doi:10.1007/s11416-006-0015-z. S2CID 3334277.
13. ^ Richet, Jean-Loup (1 January 2022). "How cybercriminal communities grow and change: An investigation of ad-fraud communities". Technological Forecasting and Social Change. 174 (121282): 121282. doi:10.1016/j.techfore.2021.121282. ISSN 0040-1625. S2CID 239962449.
14. ^ Lehman, Jeffrey; Phelps, Shirelle (2005). West's Encyclopedia of American Law, Vol. 3 (2 ed.). Detroit: Thomson/Gale. p. 137. ISBN 9780787663742.
15. ^ "Computer and Internet Fraud". LII / Legal Information Institute. Retrieved 1 November 2020.
16. ^ Parker D (1983) Fighting Computer Crime, U.S.: Charles Scribner's Sons.
17. ^ "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress". www.everycrsreport.com. Retrieved 5 September 2021.
18. ^ Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyberterrorism. Facts on File. pp. 52–53. ISBN 9781438110196.
19. ^ Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on 6 July 2011.
20. ^ Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Archived from the original on 25 September 2015. Retrieved 20 September 2015.
21. ^ "Kaspersky Security Bulletin 2016. The ransomware revolution". securelist.com. Retrieved 17 May 2021.
22. ^ "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021". Cybercrime Magazine. 19 October 2018. Retrieved 17 May 2021.
23. ^ Carback, Joshua T. (2018). "Cybersex Trafficking: Toward a More Effective Prosecutorial Response". Criminal Law Bulletin. 54 (1): 64–183. p. 64.
24. ^ "IJM Seeks to End Cybersex Trafficking of Children and #RestartFreedom this Cyber Monday and Giving Tuesday". PR Newswire. 28 November 2016.
25. ^ "Cybersex Trafficking". IJM. 2020.
26. ^ "Cyber-sex trafficking: A 21st century scourge". CNN. 18 July 2013.
27. ^ "Senator warns of possible surge in child cybersex traffic". The Philippine Star. 13 April 2020.
28. ^ "Duterte's drug war and child cybersex trafficking". The ASEAN Post. 18 October 2019.
29. ^ "Norwegian national, partner nabbed; 4 rescued from cybersex den". Manila Bulletin. 1 May 2020.

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)