International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol.10 No.1 September – October 2022

SECURITY AND INTERNET PRIVACY

Shashi Bera
Assistant Professor, Arka Jain University, Jamshedpur, Jharkhand.
Corresponding Author - Shashi Bera
Email- shashi.bera@arkajainuniversity.ac.in
DOI - 10.5281/zenodo.7312461

Abstract:

Social networking sites have emerged in recent years to enhance social connections over the internet while altering how an individual engages with the components of the internet and also with other individuals. The basic functions of a social networking site are interaction and sharing, which come under the paradigm of communication and establishing a profile online.

However, in today's world, social networking sites are considered a prime facet of technological phishing and other illicit activities. Individuals present on these networking sites are also not feeling safe anymore as they feel their data is at risk and might be gathered without their knowledge and used against them.

Data security and privacy are two of the most important fundamentals in cyber security, and they are actively researched and worked on to improve the overall user experience on any social networking site.

One of the most iconic features in the most popular social networking site, called integral, is the feature to "report" any data which the user feels is inappropriate, pretending to be them, hurting sentiments, or is causing overall unrest on the internet.

This feature has also been established on other social networking sites like Twitter and Facebook to safeguard the individuals present there.

Another feature that has gained recent attention on social networking sites is "two-factor authentication." With the help of this feature, the user can link their account to their cell number, which is, of course, protected, so when the user tries to login into their account, in addition to the login credentials, the user will have to put in a security code which they will receive as a text message on their cell number. This feature was first tried out by Google, and later all the social sites integrated it.

Keywords: *Social Medium, Social Network Sites, Internet Users, Social Platforms, Access Control.*

Introduction:

Nowadays, social media sites have become very useful for useful to connect with old friends like school times and families those stays at far and some of them at foreign countries.

Now we all know that all social apps have privacy setting but in spite of these safety hackers will crack that privacy and take your data's. As we aware that many regulation have been control to protect user's data. This is extremely important for any particular person, organisations and anyone one who uses the networks.

Why social security and privacy is more important than other data, because now days we all are 24/7 online working or using social media as much as users increases same time hackers also increased. Internet scams are continually evolving the normal public, recently the FBF documented recorded $3.5 billion in

losses due to internet crimes in 209 and just right now its increases on unbelievable numbers.

Phishing, this is most common online scam as we all know, how well it works essentially the truth is that while social media websites advertise themselves as being free, there is a hidden cost that comes with using them. Social media sites have direct partnerships with advertising services. Information collected from users is sold off to these advertising partners so they can show users tailored ads on social media channels. Most often, there is no way to opt-out of seeing ads. And even if you do opt-out, it doesn't necessarily mean you will not be tracked anymore. The bottom line is that many social media platforms make money by selling their users' data to third-party advertisers.

Social media accounts are left unattended or no longer used are a target for hackers. Once they gain control, they can post flatulent content misinformation about your id and virus infected links or malware.

There have been instances where hackers present over the internet have been successful in breaking into these layers of protection to extract and exploit the data, but the developers of these sites are working continuously to improve the protection and safeguard every individual present.

Social networking sites have been a great invention in terms of building connections and improving communication, but one of the major cons is that they have exposed data and made it vulnerable to an exponential level. The intensity of protection needed today is beyond imagination. That's why it has been recommended to use the internet consciously and safely.

Even though all information shared on public platforms like social media sites is free and open, it is mandatory to ask for the user's consent before using that information for any other purpose. Since advertisers use personal data without the user's consent, it is unethical and a violation of privacy.

Many social platforms offer users a safe environment to talk about their emotional or health issues. When that information is collected by third parties for promotional purposes, it is a breach of personal space and privacy.

Leakage of Personal Data:

This is another method used to violate web privacy and harvest personal data. Facebook is most infamous for leaking users' personal information. Facebook apps leak personal data and identify information about users to third parties such as advertising companies without the user's consent.

When you install any Facebook app, you are urged to accept certain terms and conditions. When you click 'Allow', the app gets an 'access token'. It has been found that certain Facebook apps leak these access tokens to advertising services, giving them access to personal user data like photos and messages. This is done without the consent of the user because no disclaimer says personal data is shared with third parties. Social media apps invade your privacy in this and other similar ways.

Social networking sites such as Facebook, Twitter, Instagram, and SnapChat have become very popular among internet users. People love sharing their personal views, news, photos, and all about what's going on in their lives.

But if you think about social media privacy for a moment, This information—some of which is very personal—is going up on the internet. Outside of your trusted circle of friends and relatives, who else is viewing what you post? Could you make yourself more vulnerable to social media scams? What types of scams?

Here are some tips and hints to help you protect your social media privacy and make your social networking a more rewarding experience. Read the social media site's terms.

Your personal information is valuable. You wouldn't just hand out your bank account information, so why would you give away your privacy rights on social networking sites? Pay attention to what information you are agreeing to share when you sign up for a social media account.

Take a moment to wade through the legal information contained in the Privacy Policy and Terms of Service before you click "Accept." You may find that some of the terms are in the best interest of the platform but may not be the best for your privacy.

Some of the conditions may exceed your comfort limit. For instance, some free sites may gather and sell data related to what you look at to third parties for marketing purposes. Make sure your permission choices are right for you.

Don't share private information like your full name and address:

Keep your full name and address to yourself. The same advice also applies to posting your children's or grandchildren's full names. As innocent as it may seem to share people's full names, you never know how a stalker or cybercriminal might use that information to their advantage.

For instance, with a combination of your first name and last name, cybercriminals may be able to guess your email address or purchase your email address from the dark web. With this information, they could send you a phishing email that could potentially lead to injecting malware and collecting data from your devices.

Remind the teens in your life to adopt the same practices, as they may be more likely to share personal information. Your kids may not be thinking about privacy on social media when giving their name and address or other personal details when entering an online contest. It's a good idea to keep social media privacy top of mind.

Be careful about posting photos on social media sites:

Think twice about posting photos. Even if you don't post a child's name, you may be revealing too much information in what you thought was a harmless photo.

Consider this scenario: You want to post a digital photo of your grandchild in their new sports uniform at the big game. What's wrong with this, you ask? If the photo contains the school's name, either on the uniforms or in the background, a stranger wouldn't have too much trouble tracking down your grandchild's location and identity. Consider blurring or cropping such revealing details, if you know how. If not, maybe that isn't the best photo to share.

And what about that picture of your expensive new TV? Advertising its location could make your home a tempting target for thieves. When in doubt, just share your photos privately with a trusted few.

Adjust the social media platform's privacy settings:

Each social media platform has a different process for controlling privacy settings. Always consider who can see, react to, or comment on your post or photos before sharing them.

Carefully decide whether you want your social media posts and pictures to be visible to everyone, only friends, or friends of friends when reviewing your privacy settings for each platform. You can also make a custom list for each post.

Tagging friends can be a lot of fun, but it can also be an invasion of privacy. Also, you don't want to be tagged in something inappropriate. Always opt to

review when somebody else tags you in a post before it is published. Keep in mind, however, that just because you may not approve the post to be published on your social media page, it may still be visible on theirs, publicly.

Learn what types of personal data social media sites store and share:

Upon signing up for a social media site, most users willingly give their name, gender, date of birth, and email address. Some social media sites don't stop at that. They go on to collect other information, like an IP address or the types of things you have liked, shared, or commented on.

Sometimes you're given the choice to use your Facebook credentials to log in to other third-party apps. While this may be convenient, you could unwittingly allow other apps to access more of your personal information than necessary.

One way to make sure that you are not over sharing information is to always read the fine print. When modifying your privacy settings on any social media platform, look for the "Apps and Websites" option under "Settings." Carefully review which websites are using your information.

Research Methodology:

Information that could have adverse consequences or maybe damage their financial standing and other factors like employability, insurability, or reputation should be properly protected from any public disclosure, fraud, theft, loss, or unauthorised use.

The Jamtara series was most famous for OTP frauds, looting huge amounts from gullible people, even though they cheated with very famous personalities. Connecting these basic security attacks are phishing attacks, vishing attacks, distributed denial of service attacks, and ransomware attacks.

What are the methods to be used to protect against hackers or any cybercrime? Here are some methods:

Use strong passwords, but OTP cannot be shareable.

Offers from banks that your debit card expired, winning tickets, so checking your bank's toll-free numbers is essential.

Be informed that the bank asks any OTP never to give messages for your debit card expiration and has never proposed any offers, so be alert.

Nowadays, one of the biggest scams going on is "Koun Banega Crorpati". In such frauds, the fraudsters send Whatsapp messages to unsuspecting victims from unknown numbers (most of them starting with the +92 code of Pakistan) claiming that their mobile number has won a lottery from Koun Banega Crorepati worth Rs. 25 lakhs and to claim that lottery they need to contact the same person whose number is provided in the Whatsapp message.

As the victim contacts the same number to claim the amount, the fraudster tells him/her that they need to pay the first certain refundable amount for processing the lottery. One victim paid a fraudster to block his contact.

Removable media is very easily lost, which could result in the compromise of large volumes of sensitive information stored on it. Some media types will retain information even after user deletion, placing information at risk where the media is used between systems (or when the media is disposed of).

Another major area that is also very dangerous is data mining and IP tracking; social networks are notorious for attempting to mine data and sell it to third parties.

Every time you create an account on a social network, you willingly give away some of your data. Like your name and address on social media. For example,

if we can search on Google, some sites ask for your email ID or phone number before opening the page. These are ways to collect data. Companies tend to mine more information about you, such as behavioural trends, social contacts, and your social interactions.

If you prevent data mining, then you might want to secure your business with a VPN. There's no denying that antivirus and VPNs can dramatically improve your security in the online world. Data privacy is an important issue.

What are social media users worried about? Are their concerns justified? Typically, these concerns stem from the universal presence of social media in people's lives. Forty-five percent of the world's population uses a social network, which means a shocking 348 billion people connect to some form of social media, according to data collected by Hoot suite.

Data Analysis & Interpretation:

Network analysis is its simplest definition. It involves the analysis of network data There is increasing pressure to protect computer networks against unauthorised intrusion, and some in this area are concerned with engineering systems that can be made invulnerable. Data analysis for network cyber security focuses on monitoring and analysing network traffic data to prevent or quickly identify malicious activity.

Such work involves the intersection of statistics, data mining, and computer science. Fundamentally, network traffic is relational, embodying a link between devices. As such, graph analysis approaches are a natural candidate. However, such methods do not scale well to the demands of real problems, and the critical aspect of the timing of communications events is not accounted for in these approaches.

Network security is a top priority for organisations that need to protect sensitive information and keep their data secure. To that end, security analysis involves the close inspection of a network's structure, data, and traffic to observe, detect, and eliminate positional data.

To execute an effective plan against cyber security threats, it's important to follow a set of guidelines. The following principles will help you formulate a winning strategy for analysing and protecting your network.

Network and system administrators spend an unacceptable amount of their time looking at traffic logs and traffic centers. They might spot an anomaly, reach out to peers, and then, over weeks or even months, either conclude that it was a legitimate threat or that it was just a random and relatively harmless programme that an employee was running.

Network security analysis has not traditionally been a team sport; to their detriment, security decision-makers rarely collaborate on data analysis with peers at other organizations. This can be due to a variety of reasons: fear of sharing sensitive information, understanding, a lack of training, or a lack of tools.

Future Prospects:

To keep pace in the current threat environment, network security must go beyond the basics. The future of network security, to be effective, requires implementing technological advances such as Al and machine learning. The importance of identity and access management cannot be denied. However, the same old tools cannot properly secure today's complex environments.

Today's online privacy issues and concerns are accelerating. Historically, you have been told that the companies you interact with online take steps to safeguard the privacy of their users and, while they

may sell data in anonymous or aggregate form, they do not share their users' personal information directly with other companies.

In the past few years, that "Red Line" of privacy protection has been crossed.

More than 60 jurisdictions around the world have enacted or proposed postmodern privacy and data protection laws. As the public demands the protection of their privacy, but after using so many security passwords, hackers are successful.

Privacy protects the information we do not want to be shared publicly. Privacy helps protect our physical safety (if our real-time location data is private). Privacy helps protect our physical safety (if our real-time location data is private). Privacy helps protect us as individuals and our businesses against entities we depend on or that are more powerful than us.

"Privacy" is the ability to control who can access information about our private lives and our online activities. There are many ways you can improve your privacy, for example, by exercising caution before sharing private data online or with others.

Now the question is, how do I protect my privacy? There are many ways you can improve your privacy, for example, by exercising caution before sharing private data online or on call. You may also make minor decisions, such as paying in cash instead of using a credit card, encrypting your emails and backups, reading the terms of service before using a product, and reviewing how a website is tracking you.

To understand how a website is tracking you, use a tool like Backlight to check for privacy-threatening technology. If you see that a website is using something like Google Analytics, Companies to consider using a privacy-friendly and ethical alternative.

Now we can discuss Matomo to protect my privacy. Moto is a free and open-source web analytics application to track online visits to one or more websites and display reports on these visits for analysis.

When you use Matomo on your infrastructure, you control everything. All the data collected is stored only within your database, and no other business can access any of this information.

Even after a few years, the pace of transformation driven by digital technology jumps into hyper speed. We are currently living through one of these periods. With the explosion of data, people are increasingly becoming comfortable sharing digital devices that have become integral to our lives.

With consumers continuing to take a digital-first approach to everything from shopping to dating and investing, fraudsters are finding new and innovative ways to commit fraud.

Here are some of the fraud trends we will expect to see in the coming year:

Buy Now, Pay Later lenders will see an uptick in identity theft and synthetic identity fraud.

Beware of cryptocurrency scams now as these frauds will set up cryptocurrency accounts to extract, store, and funnel stolen funds, such as the billions of stimulus dollars swindled by criminals.

The trouble with ransomware attacks is that the fraudsters will not only demand a large ransom to return control to the companies they have hacked, but they will also steal and leverage data from the hacked company.

Love? Romance scams will continue to see an uptick, with fraudsters asking victims for money or loans to cover fabricated travel costs, medical expenses, and more.

While many types of internet fraud can target virtually anyone with access to a computer, many are crafted specifically with the elderly in mind. Seniors are often targeted for theft since they are perceived as being more susceptible to certain scams.

Whenever there is a problem, solutions are always there, so here are some solutions to protect yourself with trend micro security:

Turn on anti-phishing

When searching the web, scams and fake websites may appear in search results. Trend Micro's browser toolbar will show you which websites are safe to visit and which are not. It will also warn you of the security risks associated with websites before you access them.

Sharing too much information on social networks can put you at risk of identity theft. Let Trend Micro help you adjust the right privacy setting to ensure your information stays private.

The world was already undergoing tremendous digital transformation, and the outbreak of the pandemic accelerated its journey. Thoughts around threat landscapes commonly prioritise corporate and government network assets as high priorities, with personal networks and resources as lower-level threats.

Cyber-attacks have become more sophisticated than before. The first step that a business organisation must take to ensure security is to assess risks and how they can be managed. Depending upon the size and industry, organisations should create a robust strategy to strengthen their cyber security infrastructure.

The most interesting part is that hackers today use advanced techniques such as "Island Hopping" to attack enterprises via their more vulnerable business partners or tap into deep fake technology to fool user authentication mechanisms. Even nation-state hackers have moved beyond targeting huge corporations that operate industrial control systems, with information available on small companies.

References:

1. https://terranovasecurity.com/data-privacy-social-media-protect-your-information/,
2. https://www.oreilly.com/library/view/network-security-through/9781491962831/