Science and Technology Publishing (SCI & TECH)
ISSN: 2632-1017
Vol. 8 Issue 1, January - 2024

Social Media Platform Attacks and Prevention Techniques: A Review

Akpasam Joseph Ekanem
Department of Electrical and Electronic Engineering,
Akwa Ibom State University Mkpat Enin, Akwa Ibom State

Abstract **Cybercrime on social media platforms is on the rise at the same time that usage of social media networks and internet users both rise daily. Hackers are creating new tools and strategies to access social media networks and gadgets for nefarious purposes. To stop and reduce the risk of cyberattacks in this area, more security measures are required. This paper examines social media platform hacks and attacks as well as risk-reduction strategies. Three prominent social media platforms—Facebook, Twitter, and LinkedIn—are used in the paper as case studies, but the same strategies apply to all other social media platforms as well.**

Keywords— Social Media, Cyber Security, Attacks, Threats, And Hackers

1.0 INTRODUCTION

In the current digital age, where information based on computer networks is essential to all types of enterprises. Information destruction through computer networks is a target of increasing threats and attacks. [1] explains that a threat is a potential security breach that arises whenever there is a situation, ability, action, or event that could compromise security and result in damage. In other words, a threat is a potential risk that might take advantage of a weakness. An attack is a deliberate attempt to undermine the security of a system. Attacks that are based on threats employ a variety of methods to access users' online environments. The infected file that was downloaded from spam or another online source is also a component of the thread-based assault. Typically, it seeks out system weaknesses and tries to exploit them. By paralleling several varied attacks, an attacker can use one attack to exploit multiple points of entry.

Social media is a platform that allows people to interact and communicate with one another without regard to distance [2]. Users can share content through social networking [3]. Also, [4] outlined seven categories of social networks that can be found online, including e-mail services like Gmail, Yahoo Mail, Microsoft Outlook, Hotmail, etc., instant messaging services like WhatsApp, Twitter, Yahoo Messenger, Instagram, Telegram, Snapchat, etc., blogging platforms like Blogger, Tomblr, Wix, Linda, etc., social networking sites like Facebook, TikTok, Quora, LinkedIn, etc., multimedia sharing services like YouTube, Skype, Flikr, etc., and These platforms have grown significantly over the past ten years due to their popularity as instruments for communication and information sharing. Over 500 million IoT devices were deployed globally in 2003, 12.5 billion in 2010, and 50 billion in 2020, according to a report in [6]. There are over 3.5 billion users on social media, and it is estimated that cybercriminals make over $3 billion a year from attacks on these users [7]. Facebook and other online social networking sites have a number of features like product and service sales and advertising that make them relevant to practically all internet users, whether they are using the internet for business or for personal use. Additionally, this has enhanced the activity of cybercriminals on the platform. A recent study by the Computer Emergency Response Team (CERT) found that the frequency of cyberattacks has been doubling annually [5]. Threatening security issues are present for online social networks [4]. The most well-known social networking platform is Facebook. It was introduced in February 2004 [8] and as of the second quarter of 2021, there were approximately 2.89 billion monthly active users. Cybercrime, which is expected to increase by

15% yearly over the next five years and reach $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015, would have the third-largest economy in the world after the United States and China.

In addition to being exponentially larger than the damage caused by natural disasters in a year, this is the largest transfer of economic wealth in history and poses a risk to the incentives for innovation and investment. It will also be more profitable than the global trade in all major illegal drugs put together [9]. The estimated cost of damage is based on historical data on cybercrime, which includes recent year-over-year growth, a sharp rise in organized crime gang hacking activities sponsored by hostile nation-states, and a cyberattack surface that will be orders of magnitude larger in 2025 than it is now [9]. Costs associated with cybercrime include data loss and damage, financial loss, lost productivity, intellectual property theft, theft of financial and personal data, fraud, disruption of business operations following an attack, restoration and erasure of compromised data and systems, forensic analysis, and reputational harm [9].

2.0 SOCIAL MEDIA PLATFORM ATTACKS

A social media threat is something that puts the social media accounts of a person or an organization in danger. Since so many social media users disclose or share personal information online, attackers looking to utilize that information for money or extortion can simply take advantage of them [10]. This section examines a few attacks on social media.

2.1 The Risk from Social Engineering threats

Social engineering is currently a pretty well-known hazard for online criminals. It enables attacker to gather the personal information of anybody. Attackers are carrying out this by utilizing data from databases or internet sources, creating false accounts, and gradually earning confidence. After earning the user's trust, the attacker begins to solicit the victim for personal details. Information includes the title of the project people are working on, the name of the server they are using, and the URL they use to access a backdoor into their computer [11, 12].

2.2 Identity Theft

Anyone who has published photographs or personal information online is at risk of identity theft or physical impersonation on social media. Here, the attacker creates a false internet profile to appear to be the victim or to take on a completely different persona using images and publicly available information about the target.

If the imposter has access to your financial accounts or manages to con people into transferring them money, identity theft can be quite dangerous. Accessing your social media accounts and submitting information to shady websites are further examples of identity theft [10, 14, 15, 16]. These actions expose other users to danger of fraud.

2.3 Online harassment

Cyberbullying is the sharing of hurtful and damaging posts, messages, or content, either privately or publicly. Anonymous cyberbullying also occurs [10, 16].

2.4 Phishing Scams

Phishing is a technique used by con artists to get personal information via fake websites, emails, links, and online messaging. These messages provide the impression that they were sent by a reputable organization, such as a bank or credit card provider.

Phishing mails are sent by hackers to deceive the recipient into submitting personal information, such as passwords or credit card account information. These messages could include dangerous links that allow hackers to infect the target's computers with viruses or other malware [10, 11, 13, 16].

2.5 Data Breach

A data breach is a damaging cyberattack that takes place when a hacker has access to private data. Any size, style, or type of business or organization can be impacted by data breaches.

For people, this means having access to their credit card accounts, and medical records. This may contain client lists or personnel health data for larger firms [10].

These kinds of data access could result in major legal issues for the target entity. The impacted organization may face fines and legal action if the data breach results in a violation of any compliance requirements. Depending on how serious the breach was, the business can possibly lose its license to operate.

2.6 Malware

Malware is created as a piece of code or a file that gets transferred onto a user's computer in order to infect it or steal sensitive data.

Malware can appear in any form, but false news stories and videos are a particularly common place for it to appear. The fraudster wants the user to click on the fake news article because it contains malware that can harm the user's computer or social network account.

Additionally, malware may appear on phony websites or domains. You could be required to download a file in order to visit the website, but by doing so, you are granting the malware (and its creator) access to your computer [10, 16].

Consider a website that provides a video that "requires" a software update in order to play it. Before downloading anything, make sure the website is legitimate. To avoid any risk of virus, it's preferable to abandon the website if you're unsure.

2.7 Impersonating a brand

Even businesses face threats from social media. In order to imitate a brand and contact clients pretending to be the real business, scammers may set up a social media account.

The attacker wants to spread statements that damage the reputation of the company [10, 16] or get personal information from victims, such as account login information.

2.8 Affiliate Fraud

In order to hire social media influencers, some businesses set up affiliate programs. In return for posting material about the business, the influencers are paid a percentage on any goods or services they sell via their affiliate link.

Businesses utilize affiliate marketing to increase website traffic and generate income. However, it's likely that you will encounter fake affiliate marketing content.

In order to acquire a free gift card, scammers may post content that looks to be an advertisement and requests consumers' personal email addresses. But the user instead receives an endless stream of spam emails, some of which might even contain malware [10], in place of the gift card.

2.9 Keylogging attack

This type of attack employs malicious software to secretly record or log the keys that a user of a computer or mobile device presses on the keyboard in order to get sensitive data about the user. Passwords, addresses, debit/credit card information, and other details may also be stolen [17,18,19]. Keyloggers can be purposefully installed in systems for harmful intentions. Keyloggers can also be remotely installed on computers by cybercriminals without the owner's knowledge.

Despite the fact that many anti-spyware programs can identify some Software-based keyloggers and can quarantined, removed, or otherwise dealt with them, but no method can be said to be 100% successful [18].

2.10 False Freebies

Many businesses are using social media to advertise their goods and services. With boosted posts, giveaways are more affordable and can reach a larger audience.

Brands frequently advertise giveaways of their items to followers in order to increase exposure. [20] claims that approximately 93% of the firms studied use giveaways on social media to increase traffic and website hits.

Even while these offers can sound unbelievable, they occasionally are. Scammers will make fictitious brand profiles that advertise freebies and ask followers to provide their personal data. Over 148,000 cases of prize, sweepstakes, and

lottery fraud were reported in 2021, according to [21] [10].

2.11 Likejacking

Hackers utilize the cunning fraud known as "likejacking" to trick people into clicking the "like" button on a post or website without their knowledge.

Users might, for instance, want to click on an intriguing image or video to discover more details after they have already seen it. The user can't see themselves clicking an image or video since fraudsters [22] are hiding behind it, which is what they are unaware of. The number of these photographs will then increase and clog up your social media newsfeed [10].

2.12 Brute force attacks

Hackers rapidly modify their strategies to be successful in light of advancements in password security. The threat of brute force assaults can take many different forms, including simple brute force attacks, password spraying, dictionary attacks, credential stuffing, reverse brute force attacks, and hybrid brute force attacks, according to [23]. [24] stated that social media attackers employ well-known brute force programs to crack user passwords, including Hashcat, John the Ripper, Brutus, Wfuzz, THC Hydra, Medusa, RainbowCrack, OphCrack, L0phtCrack, and Aircrack-ng.

2.13 Sim Cloning Attack

Users frequently hunt for a SIM card clone app while switching between smartphones. A SIM duplicator can utilize another device on the same network in addition to transferring their data files. Users can switch to another device in this fashion without encountering any problems with authentication. To clone a user's sim card for illicit purposes, some hackers employ well-known sim cloning applications as MOBILEDIT [25], Magic Sim [26], USB Cell Phone SIM Card Cloner [27], SIM Explorer by Dekart [28], and Mister SIM [29].

2.14 Attack using cloned phones

With the help of a cloning tool like "Dr.Fone," social media attackers may now replicate iPhone and Android phones[30]. Data transfers across iOS, Android, and Windows devices are possible with the Dr.Fone toolbox. It is also capable of cross-platform transfer. Every significant version of the Mac and Windows operating systems can execute the application, which has an easy-to-use interface. It can directly transfer data from one device to another, including contacts, call logs, messages, images, videos, music, and more. It also offers an intuitive user interface. It offers a simple, one-click method for easily cloning phones.

2.15 Spyware attacks

Spyware is a type of malicious software that has the ability to collect private data from internet users without their consent. Without the information owner's permission, the information it gathers is then forwarded to a third party [17, 46, 47]. The four basic categories of spyware are Trojans, adware, system monitors, and tracking cookies. Spyware is mostly used to track a user's internet activity and provide perilous pop-up advertisements. Smartphone users risk contracting spyware by visiting specific websites, clicking on pop-up messages requesting the download of a program or application, exploiting security flaws in the browser or other software, etc. Spyware is typically concealed and challenging to detect. When a spyware infection begins to use up their system's resources and slows it down, people may become aware of it.

2.16 Threats from software vulnerabilities

Software security flaws must be found and avoided by users in order to protect themselves, their reputation, and their brands. Users must first be informed of the many categories of security flaws and how to prevent them in order to accomplish this. Bugs, the exposure of sensitive data, injection flaws, buffer overflows, security misconfigurations, broken access control, unsafe deserialization, and broken or missing authentication are some of the most prevalent forms of software vulnerabilities. Hackers attack and destroy a system by taking advantage of security flaws in software, which can lead to

financial losses and tarnish the reputation of the companies they target. The success of these attacks is due to software flaws. Attackers occasionally exploit security flaws to steal and get access to a person's personal information, including bank accounts, in order to steal money [48].

3.0 PREVENTATIVE MEASURES

Because of the popularity of social media platforms, hackers are continuously coming up with new ways to access users' social media accounts and utilize them for their own evil ends [31]. Users are vulnerable to risks such as identity theft, sim cloning, brute force, phishing, information leakage, impersonation, and others as detailed in section 2.0 [32] [33] [34] as a result of the hackers' activity. This section uses three well-known social media platforms (Facebook, Twitter, and LinkedIn) to demonstrate preventive measures based on current best practices to safeguard social media accounts. Any social media platform can be used to implement the concepts offered. Also presented are the general preventive actions.

3.1 Safeguarding Your Facebook Account

This study will examine Facebook's privacy and security settings in more detail [38] because it is currently the most widely used online network [35, 36, 37]. It will then provide 10 additional precautions that one can take to be secure online.

3.1.1 Access Facebook's settings

As shown in Figure 1, select Settings from the drop-down menu in the top right corner of the screen to access Facebook account settings.

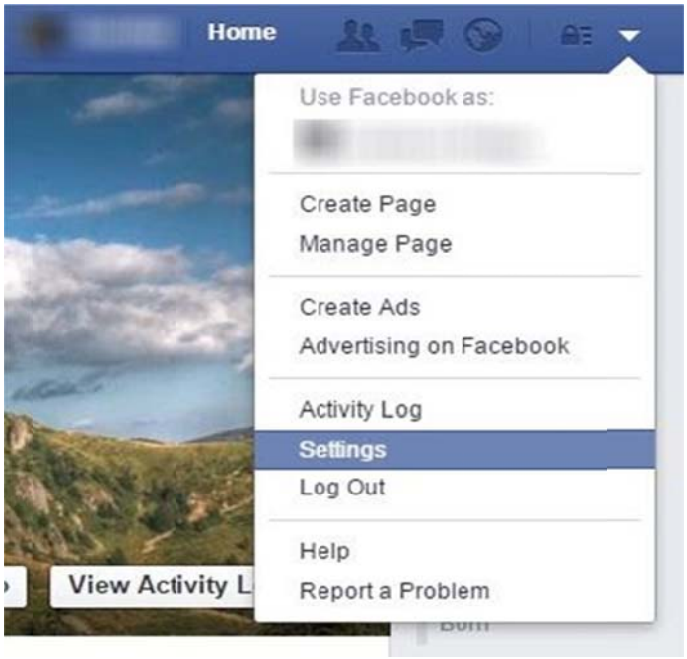


Figure 1 Accessing Facebook Settings

3.1.2 Standard Account Preferences

The General Account Settings are displayed in the sidebar on the left side of the page when you click the Settings button, as illustrated in Figure 2. Users can update their Facebook account password and download a copy of their Facebook data from this page.

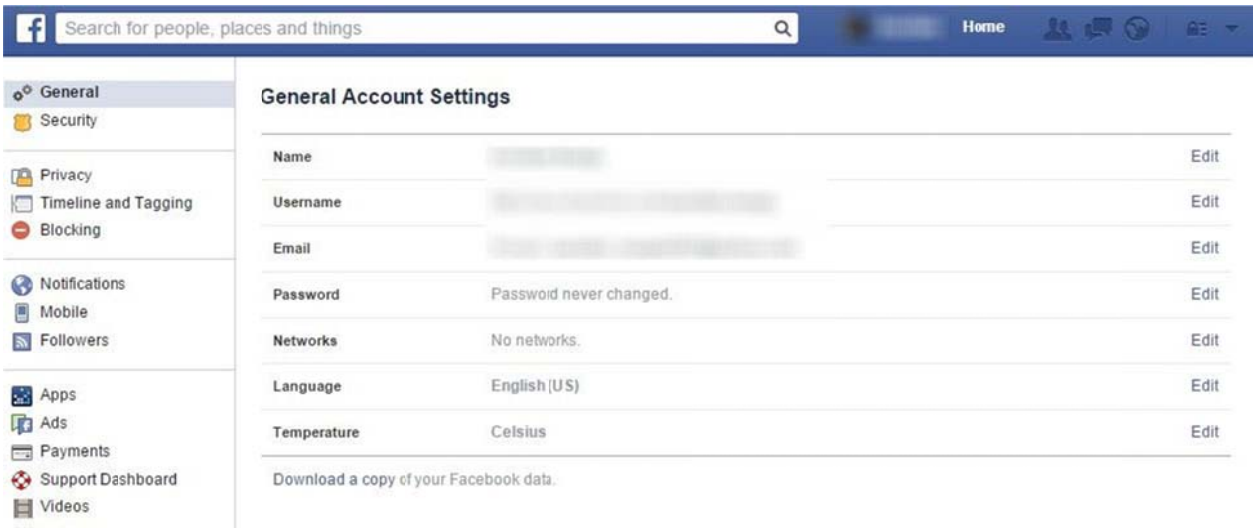


Figure 2 General Account Settings

3.1.3 Security Options

Numerous options are accessible when looking at the Security Settings on the left side of the screen, as seen in Figure 3, and are explored in more detail in this section.

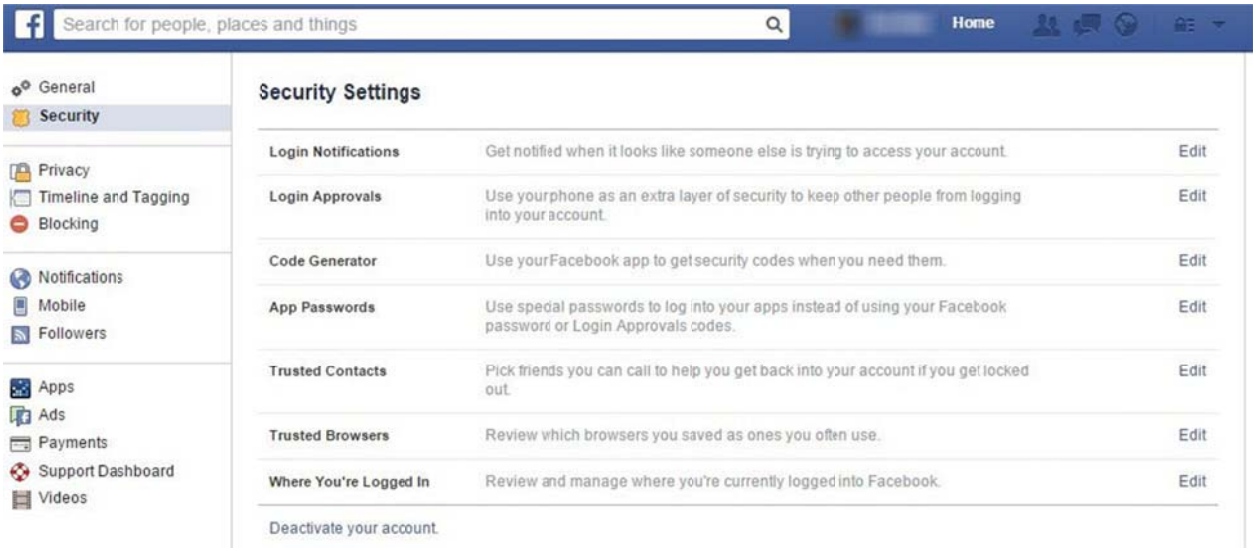


Figure 3 Security Settings

a. **Notifications for Login**

The user can choose to receive text and email messages when their accounts are accessed from an unidentified computer or mobile device by checking this box. In the event that a hacker tries to access an account, this is incredibly helpful. To prevent keylogging, brute force, and data breach assaults, the setting should be enabled.

b. **Approvals for login**

A security code must be produced after activating this option in order to access the account on a different browser. There are three possibilities:

• get a security code via SMS to a mobile device; generate a security code using the Facebook mobile app's Code Generator (requires an Internet connection); pre-generate 10 codes that the user may print out and use when they don't have their phones with them;

Another goal of this layer of protection is to prevent unauthorized users from accessing user's Facebook account.

c. **Code Generator**

To generate codes that users can use to log into their Facebook account from a different browser, utilize this option along with Login Approvals. To prevent keylogging, malware, brute force, and data breaches, the code generator should be turned on.

d. **Passwords for apps**

This feature enables users to establish one-time passwords for third-party Facebook applications while protecting their primary Facebook password. The password is not remembered when a user exits the application. The user will need to create a new password once more in order to access the third-party application. Additionally, the app password option can be selected to protect against keylogging, malware, brute force, and data breaches.

e. **Trusted People**

A user can pick close friends from this option to call if they experience any difficulties logging into their Facebook account. This option can also be turned on to protect against keylogging, brute force, malware, sim cloning, and phone cloning attacks.

f. **Reliable Browsers**

A list of the stored (trusted) web browsers that Facebook users have used to access their accounts can be seen here. A user has the option to remove a browser from the list if they no longer use it, such as when they leave their place of employment and no longer use it there. Phishing attacks, data breaches, brute force attacks, malware, and other attacks will be avoided as a result.

g. **Your current login location**

Users can check their logged-in status here and End Activity (terminate the session) on locations and gadgets they don't recognize to prevent malware, phishing scams, data breaches, brute force assaults, and other threats.

h. **Make your account inactive**

Users can choose to cancel their Facebook account from this location. This is helpful if the user knows that they won't have access to their Facebook account for a while or just don't want to. Users can always reactivate their accounts. This can stop data breach attacks, brand impersonation, cyberbullying, and identity theft.

3.1.4 Setting up privacy

The Privacy Settings tab is where you should go next if you want to increase the app's general security. The options from this area are intended to assist users in reviewing fundamental privacy settings and ensuring that the audience requested or selected can read their profile and any shared items, as shown in figure 4. If these settings are implemented correctly, the user will be protected from cyberbullying, affiliate fraud, brand impersonation, identity theft, data breach, and malware assaults.

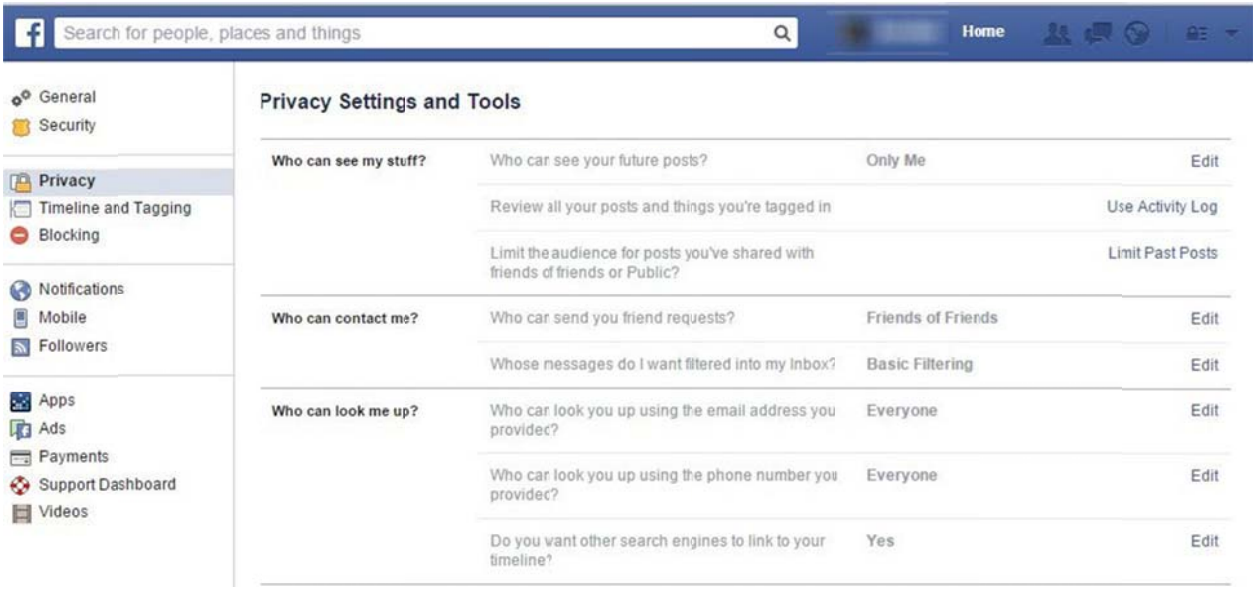


Figure 4 Privacy Settings

a. **Who can see my stuff?**

Decide who will read your posts. You can select from the following options: Public; Friends; Friends with Acquaintances; Only Me; or you can build a Custom audience.

It is advised that a user make Friends their default sharing setting.

Users can limit the audience for their posts from the past in the same place where they can review their posts and Facebook activity using the Activity Log.

b**. How can I be reached?**

Users can control who is allowed to send them friend invitations here. The user should set this to Everyone if they want to be found by people they once knew.

c. **Can somebody look me up?**

Users can decide whether they want to have their phone number or email used to search them up in this location. They can also decide whether they want anyone looking for them online to be sent to their Facebook timelines by search engines.

Due to the fact that users' Facebook timelines will show up in search engine results if they do a name search, this is a privacy setting that users should carefully examine.

3.1.5 Setting up the Timeline and Tagging

Users can change their Facebook account's privacy settings in this location. As shown in Figure 5, individuals can decide who can add items to their timelines, who can view the content

they share on their timelines, and how to handle tagging options. If done correctly, it will shield consumers against phishing, affiliate scam, malware, cyberbullying, and data breach threats.

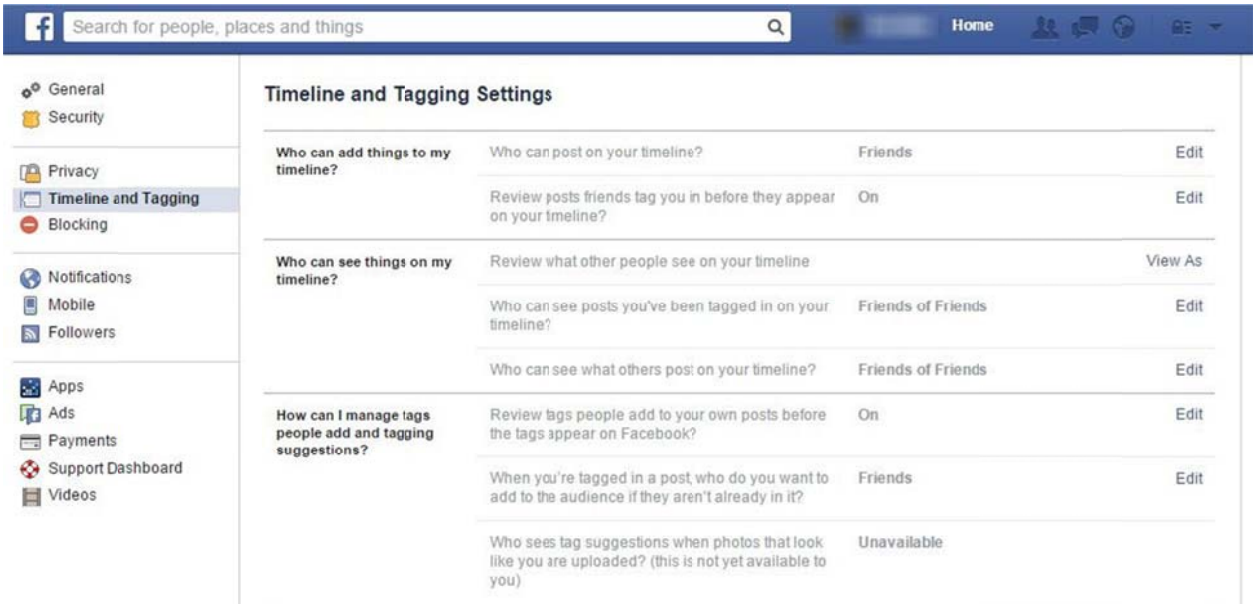


Figure 5: Timeline and tagging settings

a. **Who is able to add items to my timeline?**
This one is simple to understand. Users can decide whether to enable friends to publish on their timelines and can decide whether to appear publicly before being tagged in a post.

b. **Who is able to view items on my timeline?**
Users can check who else has access to what on their timelines by using this feature. A single person can be chosen by the user to see how they see their timelines. They can pick who can view posts that they are tagged in on their timelines as well as who can view what other people post there. Users should set these choices to Friends in the last two scenarios.

c. **How do I control the tags that other people add and the suggested tags?**
Users can review the tags their friends add to their images before they show by turning on this feature. It is a crucial privacy setting because if someone tags one of their posts, all of their friends will be able to see the post.

3.1.6 Blocking

Users can limit how other Facebook users, Facebook applications, or Facebook pages connect with them via the Blocking tab, as illustrated in Figure 6, which protects users from assaults such as affiliate scams, malware, cyberbullying, social engineering, and data breaches.

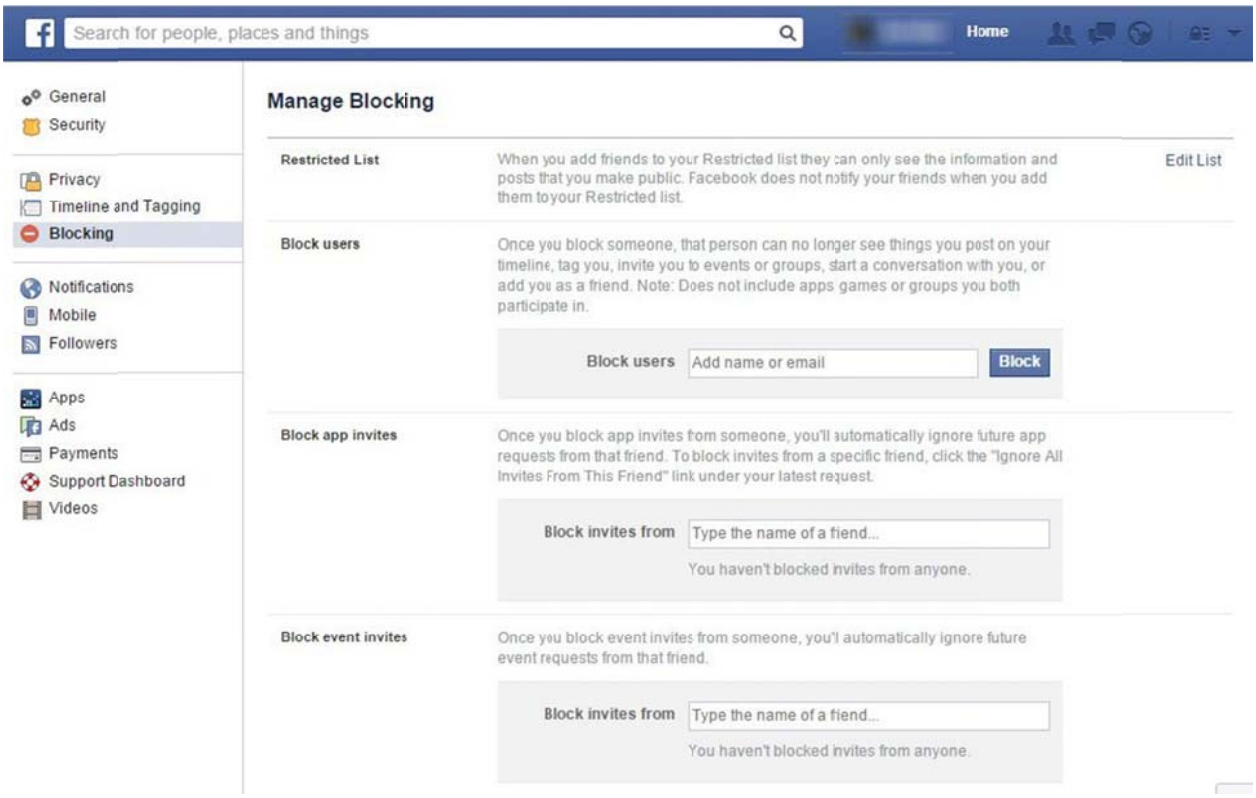


Figure 6 Manage Blocking settings

a. **Restricted List**

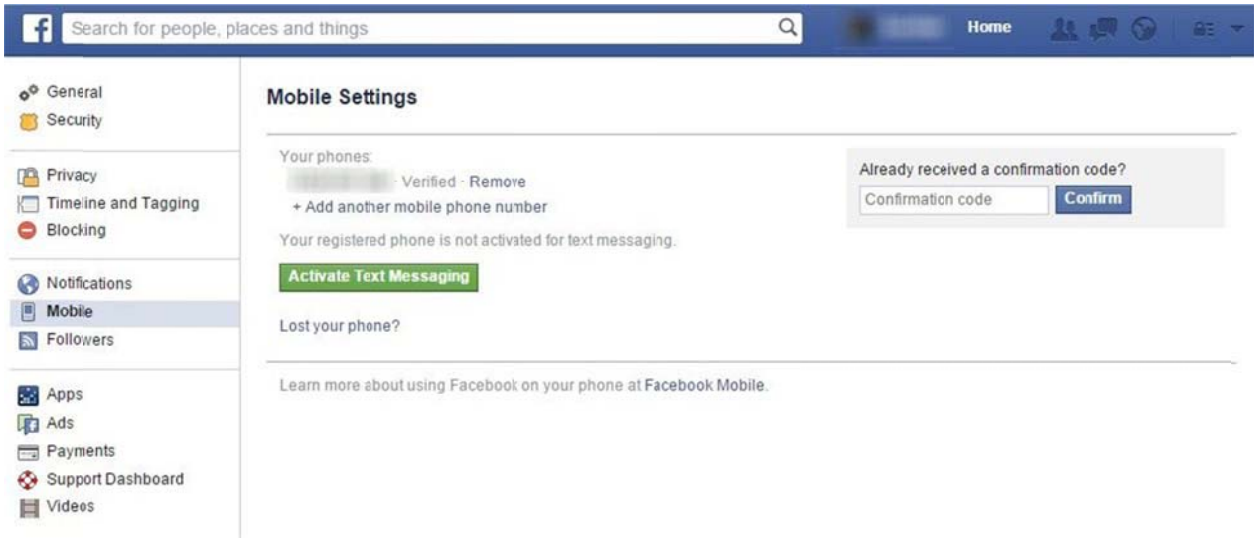
When you want to prevent a friend from seeing the posts you share on your timeline for other friends, you can use this list. That person can still view the stuff you make public, though.

b. **Blocking users**

Users can initiate conversations, send invitations, add people as friends, and add persons to the "cannot see your Facebook profile" list. Users may also add a buddy whose account has been compromised using this feature. Users can also choose to block someone's invitations to events or apps, as well as Facebook sites, in the same Blocking menu.

3.1.7 Mobile settings

According to Figure 7, this is likely one of the most crucial security options users can choose for their Facebook page. Users must submit a mobile phone number here in order to enable Login Approvals. To prevent phishing attacks, data breaches, malware, cyberbullying, social engineering, brute force, sim cloning, phone cloning, likejacking, fake giveaways, and affiliate scams attacks, they will receive a code via text message to log in to their Facebook accounts in the event that their browsers are not recognized.



1)

Figure 7 Facebook Mobile Settings

3.1.8 Apps

The majority of Facebook users make use of third-party programs, which typically request users' consent before accessing their content and personal information. As shown in Figure 8, a user may see exactly what each third-party app has access to in this location and decide whether to remove it from the list if they no longer use it or find themselves dealing with a dubious program. If configured appropriately, the option will defend the user from assaults such as phishing, data breaches, malware, social engineering, keylogging, identity theft, and affiliate scams.

Figure 8 App Settings

3.1.9 Ads

The third option, Ads based on your use of websites or apps off Facebook, allows you to opt out of ads that are selected for you by Facebook, based on your behavior on a particular website, for example, a news website. If you want to opt-out from these two options, simply select No one to these two options.

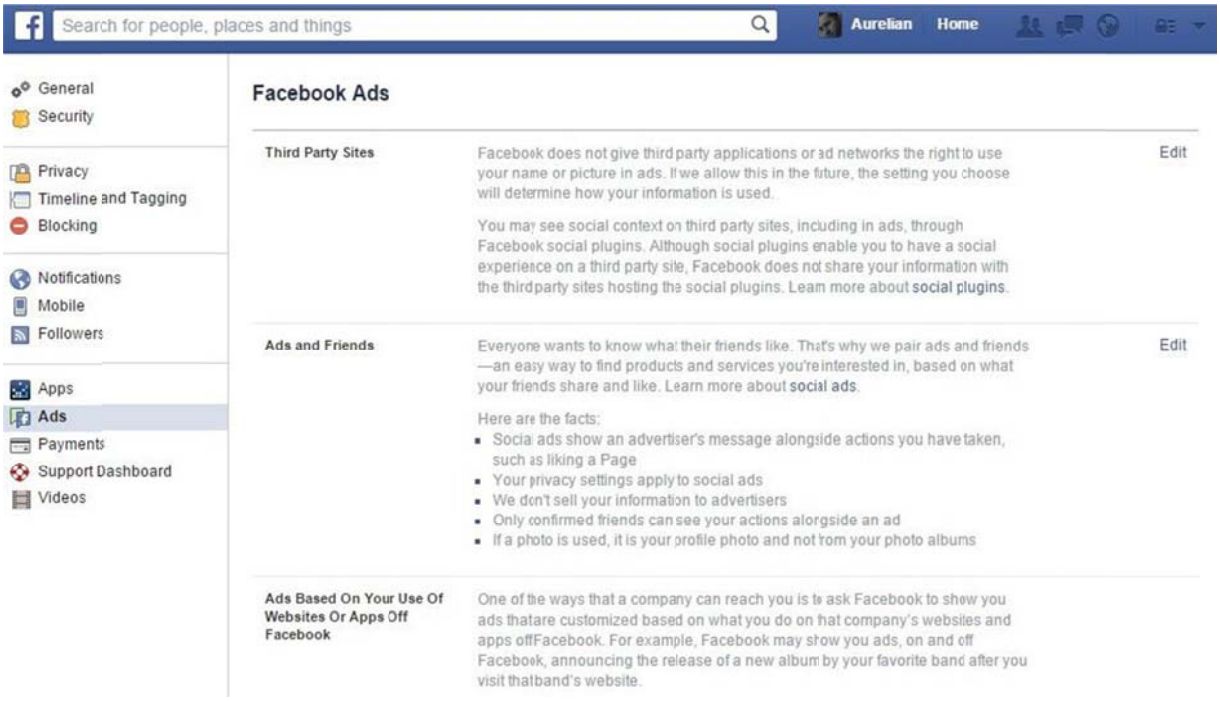


Figure 9: Facebook Ads Settings

3.1.10 Broad security improvements for Facebook [39, 40, 41]

i. Refuse friend requests from people you don't know. The creation of fictitious Facebook pages is one of the preferred techniques employed by online con artists to gather sensitive information and private data from consumers. Children and their parents should be aware of this potential threat to their privacy.

ii. Avoid giving other users access to your Facebook login information, including your email address, phone number, and password. Cybercriminals may exploit this information to gain access to personal information.

iii. Constantly update your browser with the most recent fixes. The most recent patches should be installed on browsers, other programs on computers, and the operating system. Users should avoid exposing their machine to cyber-criminal attacks and practice safety.

iv. Employ a reliable security program. You must rely on reliable security program that has real-time scanning engine. This implies that files acquired from web locations are quickly and thoroughly analyzed.

v. Protect yourself against phishing scams. Pay attention to the different communications you get from users you don't know asking for your personal information.

vi. Avoid using the same password for multiple online accounts, including your Facebook account. If you use the same password across many sites, you put yourself at risk of a hacker trying to access all of your accounts.

vii. Turn on login authorizations. Users are advised to consider this crucial advice.

viii. Exercise caution when logging onto free wifi networks from public areas. These kinds of unsecured networks are used by online thieves to acquire user passwords and steal private information. Users can use a private browsing session to reduce exposure.

ix. Avoid clicking on dubious links! Social media is one of the most popular ways to transmit harmful links over the Internet because it is utilized to spread and share various types of content. In our example, that would be our Facebook profile.

x. Close your Facebook session. When utilizing a shared computer, such as one at work or in public, this piece of advice is helpful.

3.2 Ten Steps to Safeguard Your Twitter Account

One of the widely utilized social media platforms is Twitter, which is used by big companies and notable figures in the IT sector in addition to private users [42–45].

It has been associated with journalism because of its concise writing style, and it has even been utilized as a preferred method of news dissemination for uprisings and revolutions all over the world.

The additional precautions listed below should be followed to keep a Twitter account secure so that it is protected against malicious attacks that target social media accounts and so that internet criminals are prevented from obtaining users' private information:

3.2.1. Establish and use a solid password

Multiple online accounts can all have the same password, which is simple to remember. Possibly

using a well-known term like your name or your birthday. However, internet criminals also rely on this.

It's crucial to design a strong password that is over 12 characters long, including upper- and lowercase letters, digits, and symbols, and ensures that the account is secure from internet intrusions. Cybercriminals won't be able to access Twitter accounts easily this way.

Additionally, users should avoid using the same password across many online accounts. The explanation is simple: if one of your internet accounts is compromised, the others will inevitably follow. You lessen the possible loss in the event that your Twitter account is accessed by using different passwords. This will shield against brute-force assaults.

3.2.2. Employ login confirmation

Using the security feature of login verification, you may defend your Twitter account from brute force attacks.

You will be required to enter both an email address and a phone number in order to connect to your online account. This is a kind of two-factor authentication.

You have the following three choices for the second check that this login verification adds:

• key in a verification code received in the Twitter app on your phone.

Enter a backup code that was saved on your phone when you originally enrolled in login verification, or take a photo of it. Enter a text message that was delivered to your phone number.

The actions shown in Figure 10 should be taken in order to activate Login verification:

i. Log in to Twitter.

ii. Click the user image in the top right corner.

iii. From the drop-down menu, pick Settings.

iv. Select Security and privacy from the menu on the left.

v. Choose the relevant choice.

Figure 10 login verification

3.2.3. Avoid posting personal details and hiding your location.

Users shouldn't provide internet thieves access to their location or activities. Twitter is a public network by default, meaning that anybody may view user tweets and follow them.

Users should make the necessary changes in the Security and privacy section and click Protect my Tweets under the Privacy section if they want to manage other people's follow requests or wish to share tweets just with their followers.

Additionally, users should take care to avoid providing vital information to cybercriminals, like location data. When a hacker has to establish a persona for a user in order to carry out identity theft attacks or gain access to the user's private files, this kind of information becomes crucial. This will stop attempts at identity theft.

Here are the procedures to secure tweets and turn off tweet location, as shown in Figure 11:

i. Log in to Twitter.
ii. Click the user image in the top right corner.
iii. From the drop-down menu, pick Settings.
iv. Select Security and privacy from the menu on the left.
v. Pick the relevant choices.

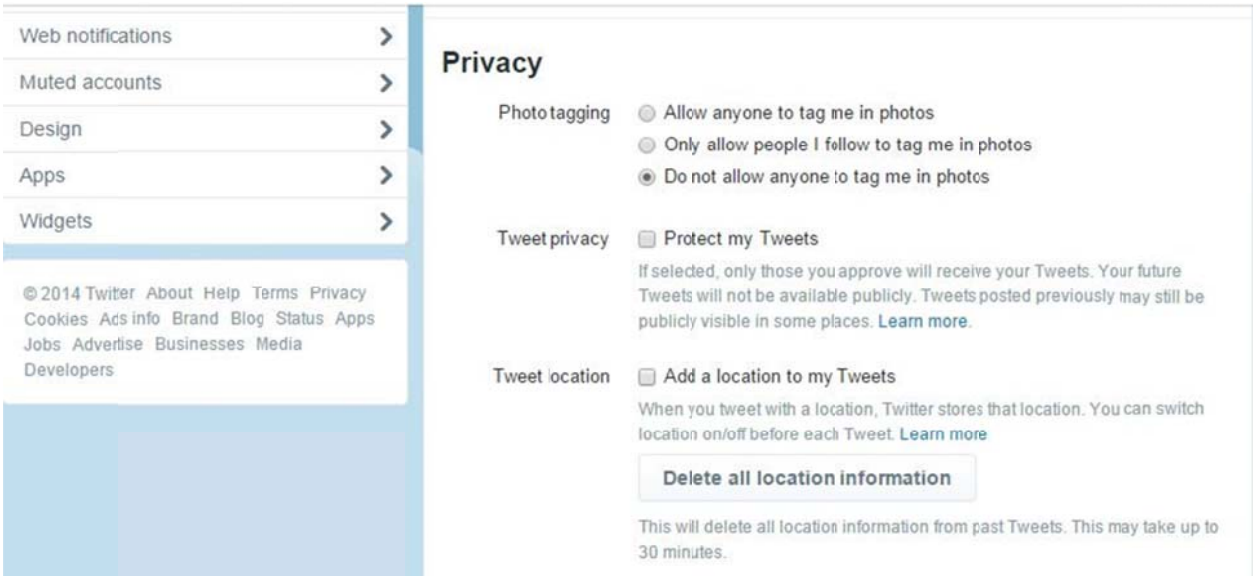


Figure 11 Privacy settings

3.2.4. Avoid falling victim to phishing scams

A typical Twitter phishing effort begins with a direct message from an unknown account asking for the victim's Twitter credentials in order to spam them. They are attempting to deceive you into disclosing private information or personal information by using a standard phishing assault.

The link in this kind of mail directs the user to a fraudulent login page. Responding to this kind of email or clicking the linked link is not advised. However, a lot of Twitter users have pals that occasionally send an odd direct message to their whole following. In this instance, that specific account has been compromised, so no user should respond or follow any links it may contain.

3.2.5. To protect against spyware dangers, use a specialist security program

Users may need to be aware of spam campaigns, phishing attempts, and other security dangers by employing a specific security solution. Security programs like Malwarebytes, Spybot Search and Destroy, Lavasoft's Ad-Aware, etc. can help remove spyware from computers.

3.2.6. Verify which applications have access to your Twitter account.

Being cautious when granting access to third-party apps is another crucial step in keeping a Twitter account safe because these services have the ability to take complete control of an account. Users shouldn't grant access to unreliable third-party apps in order to ensure that their Twitter accounts are secure. When users grant account credentials to an app, they retain full control and are able to conduct actions that could result in the account being suspended.

It's crucial to pay close attention to apps that make money-making or follower-promising claims. If you're unsure, just type the name of the program into a search engine. Users can prevent identity theft, data breaches, malware, spyware, affiliate fraud, and phishing assaults if this option is configured appropriately. Users can view the permissions that apps have on a Twitter account, as shown in Figure 12. The actions listed below can help:

i. Log in to Twitter.
ii. Click the user image in the top right corner.
iii. From the drop-down menu, pick Settings.
iv. In the left menu, select Apps.
v. Take the required actions to grant or deny access.

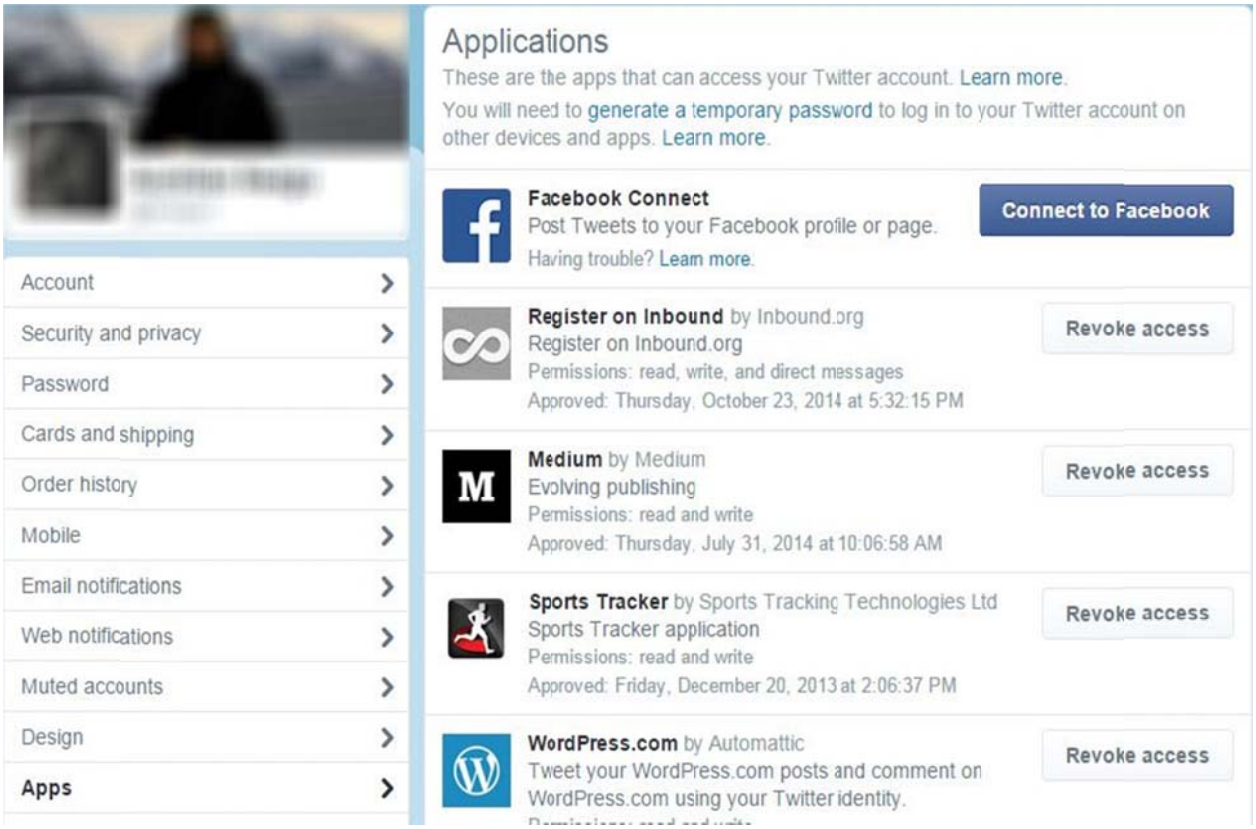


Figure 12 Twitter Apps permission dashboard

3.2.7. Ensure that you regularly update any susceptible apps

In recent months, significant security blogs and industry-related IT outlets have all published security news on software vulnerabilities.These dangers cannot be disregarded. To steal private information and utilize it in identity theft attempts, cybercriminals take use of software flaws in mobile phone apps and operating systems.

As a result, it's crucial to keep popular programs like Java, Adobe Flash, Adobe Shockwave,

Adobe Acrobat Reader, and QuickTime up to date. It's also critical to pay attention to mobile phone apps and make sure the most recent upgrades are installed. Threats from software vulnerabilities will be avoided.

3.2.8. Hide your IP address by using a virtual private network

Wireless sniffers are one of the go-to techniques used by cybercriminals to extract data transferred across unprotected networks and steal credentials.Social media users can utilize a Virtual Private Network (VPN) to protect their social media accounts and online activities.

By using a VPN, a user can view multiple websites in a private setting while hiding their IP addresses and encrypting their connections. With this technique, sensitive data is protected from phishing scams, identity theft, data breaches, and other online crimes. CyberGhost is an illustration of a well-known VPN.

3.2.9. Protect your online behavior

Care should be taken while selecting a web browser, and any necessary adjustments should be made to increase security and privacy. Web browser flaws act as open doors for hackers who try to access social media accounts and systems to steal sensitive data.These recommendations can be followed to safeguard internet privacy and stop virus attacks:

i. Protect web browsers from attacks by cyber thieves by updating your browser to the most recent version and doing so.
ii. Users should select a private browsing session to hide their browser history if they visit their social media accounts from an insecure place.

3.2.10. Remember to log out of your Twitter account after you finish.

The user should adhere to this security precaution whenever they connect to their account on a shared computer. Users should remember to log out of their accounts when finished with online sessions to prevent various attacks, even though some users are accustomed to closing the web browser as soon as they are finished with their activity.

If this is not done, especially in a public place, the profile of the prior online user will be directly accessed by the subsequent user when they open their Twitter account, for example. Additionally, if users prefer to stop cookies or their authentication credentials from being retained, private browsing sessions are advised.

3.3 Ten steps to secure your LinkedIn account

Social media isn't just for having fun or inciting upheaval. The most recent news can be found on Twitter, and one can use Facebook to keep up with friends' changing interests. However, individuals must remain serious and professional when using their LinkedIn accounts. Even more so than on the other less "serious" channels, this is crucial.

Since more private information is posted openly on LinkedIn than on other well-known social media sites, it can become vulnerable to internet thieves. Users merely reveal and expose more personal information about themselves than on a Facebook profile. Users should therefore adhere to these 10 actions to increase security when using their LinkedIn online account:

3.3.1. Verify your LinkedIn connections to date

The user can view which devices are linked to their LinkedIn account and which sessions are still active by using this option, which is depicted

in Figure 13. If a user linked to their LinkedIn account from a computer that was shared with the public or from a computer at their old location, this LinkedIn function may be of assistance.

The user should select the option to sign out as quickly as possible from that device if they are linked to an online account from an unidentified device. Cybercriminals may be attempting to obtain private information from users' accounts in order to use it against the person in a later attempt at identity theft.

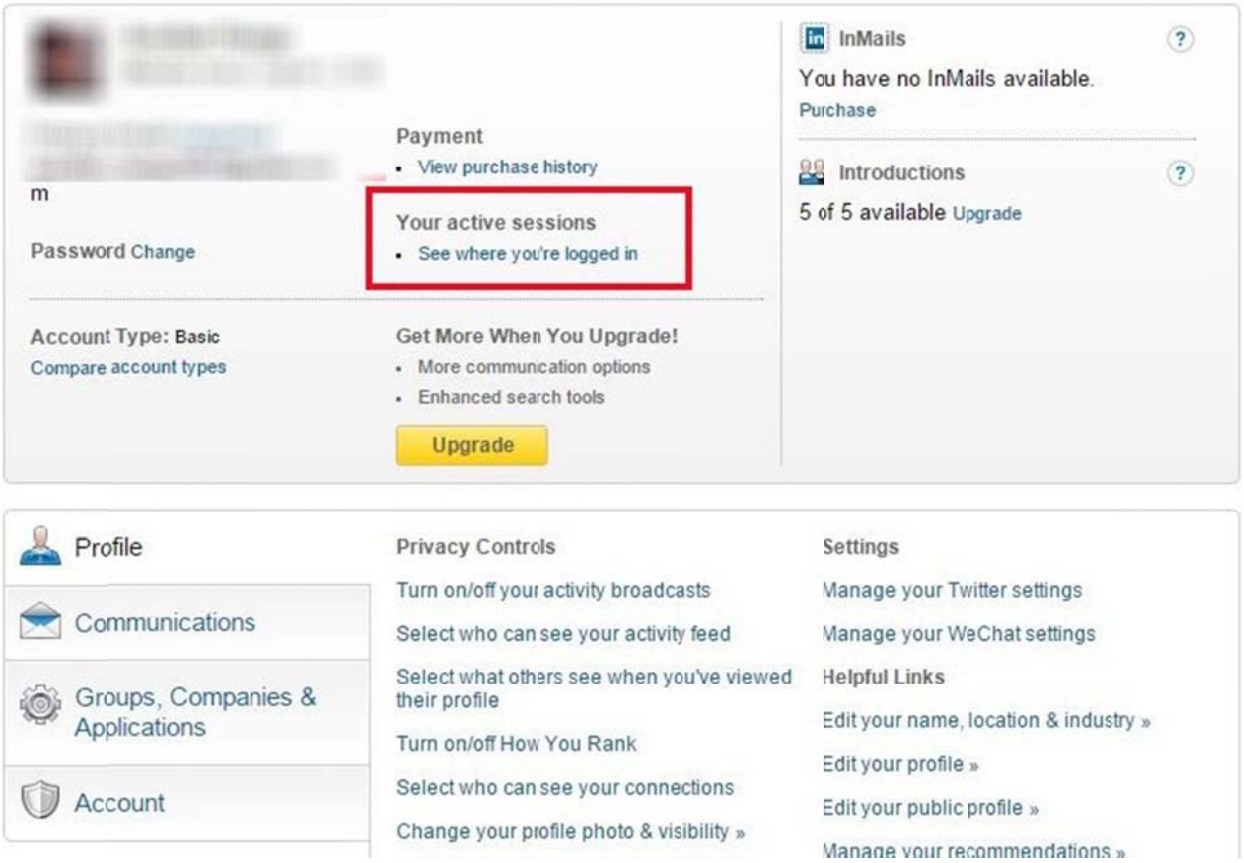


Figure 13: Current connections to LinkedIn

3.3.2. Request a copy of your data's archive.

Users can ask LinkedIn to provide them an archive of their account data by using this option, which is depicted in Figure 14. Allowing the user to see not only what information they made publicly available online for others, but also IP records of their previous login connections, recent searches, and other details to prevent data breach assault is a crucial step for online privacy.

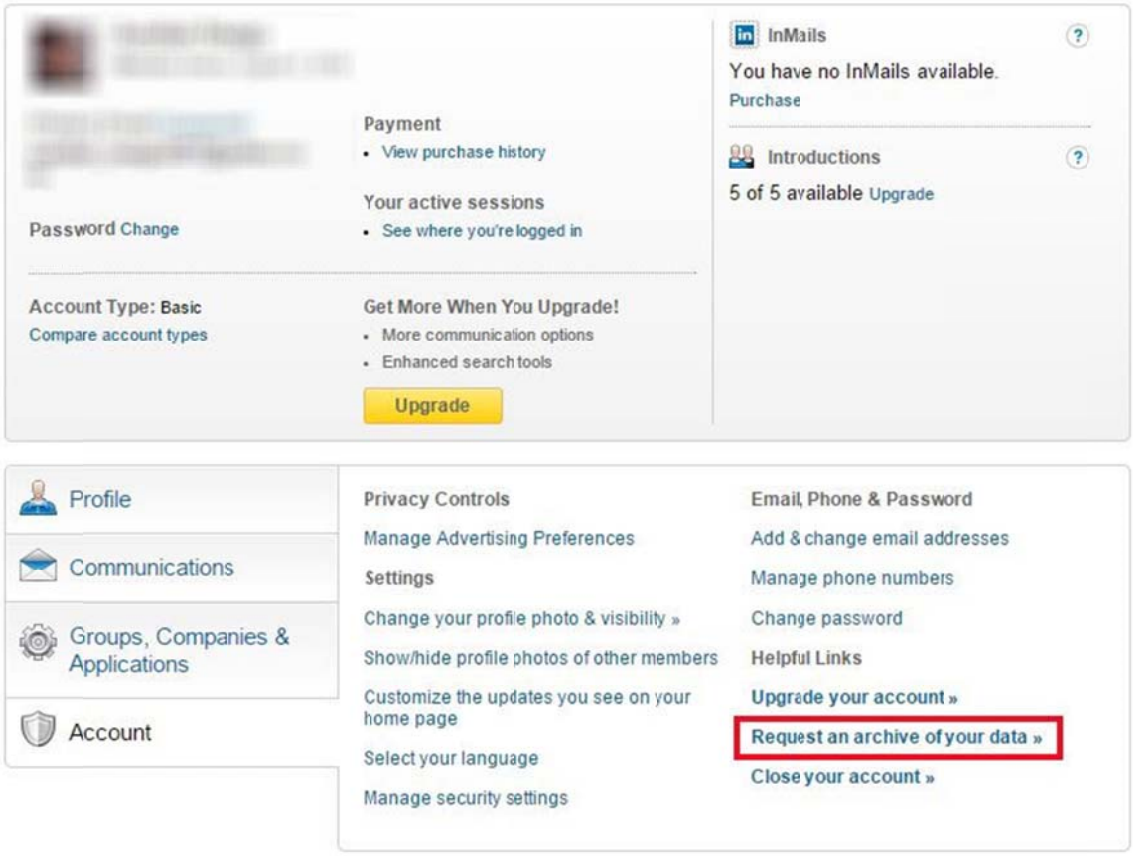


Figure: 3.14: How to request an archive of your data

3.3.3. With whom do you interact?

Only persons they know and trust should be connected by users. The likelihood of adding internet criminals who are simply interested in using your personal information increases when they add unknown or barely acquainted people to their list of contacts. This is being done to stop identity theft.

Cybercriminals try to put all this information together before conducting an identity theft operation by using this professional data, which can be linked with personal data from social media sites, such as Facebook.

These thieves have been known to steal money from users' internet banking accounts without their knowledge in some instances.

3.3.4. Let's keep it secret: guard your confidential data

Online privacy and security are related. In the event that cybercriminals acquire access to private information, they may use it against a genuine user. In order to prevent identity theft attempts, social media users must be careful about the information they share with others, especially with those to whom they have granted access to their LinkedIn profile. Users can increase their online privacy by using the following options, which are depicted in Figure 15:

- Turn on/off activity broadcasts: Users can uncheck this box to keep their connections from learning about changes they make to their profiles, who they follow, or when they make suggestions.
- Choose who can view your activity feed: Users can choose from the drop-down menus for Everyone, Your network, Your connections, or Only you to hide their LinkedIn activity or to limit who can see their activity to certain relationships.
- If users don't want their connections to know that they have accessed their LinkedIn profile, they can control who

else can see that. This option allows you to remain anonymous.

- If users don't want to share their list of connections with others in the list, they can choose who can see their connections. They can then alter it to Only you by using this option.
- Edit your public profile: Here, individuals can change any information they want to have publicly available, such as their current or previous employment details, talents, or educational background.

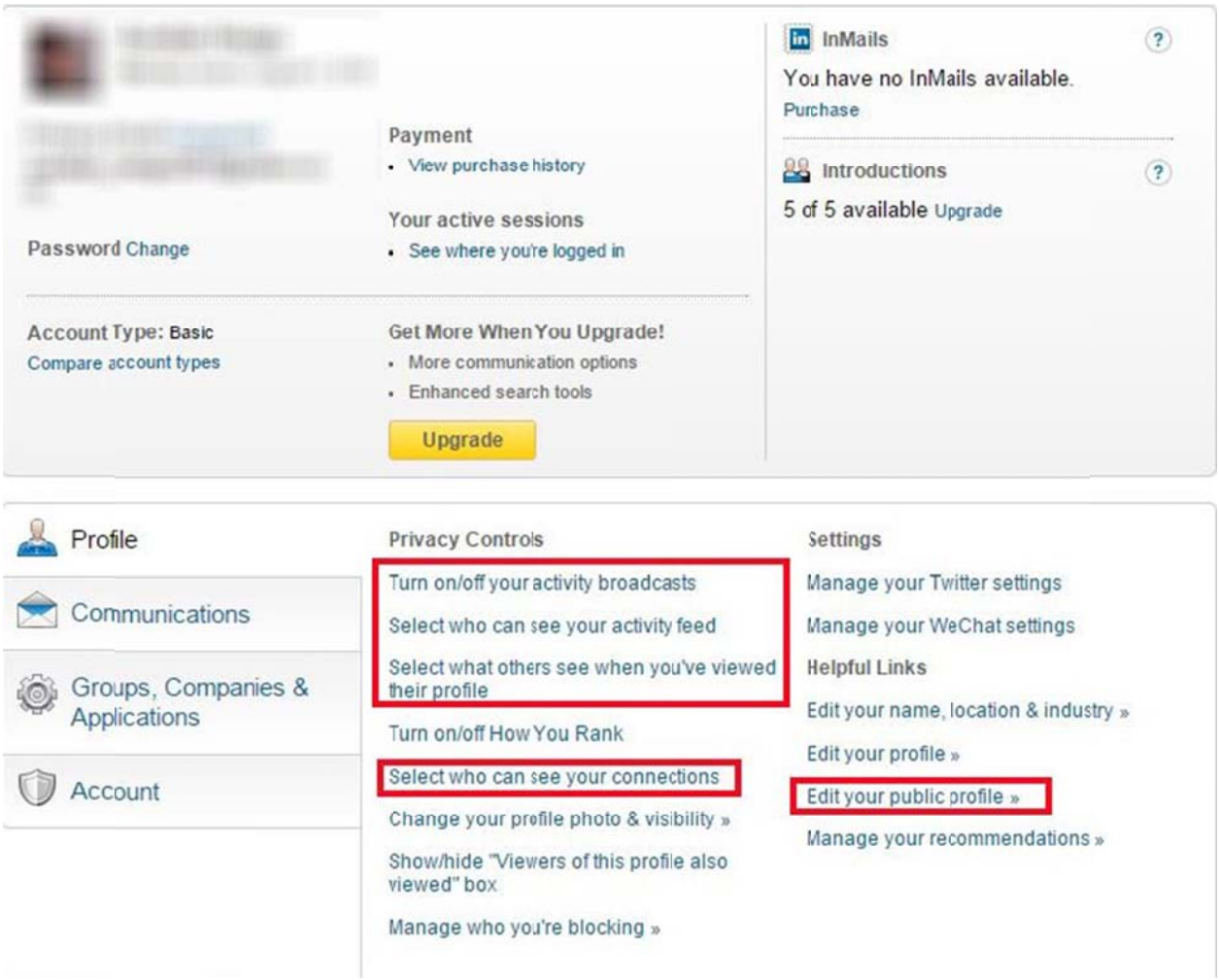


Figure 15 Privacy control

3.3.5. To prevent cybercriminals from accessing your online account, use two-step verification

To avoid brute force attacks, identity theft, and unauthorized access to LinkedIn online accounts, the security precaution depicted in Figure 16 should be activated and used for any online account where this option is offered. Some of the most well-known online accounts, including Google, Facebook, Yahoo Mail, and Dropbox, to mention a few, permit activating this protection measure.

When two-step verification is enabled, you must provide a security code that is texted to your phone each time you connect from an unidentified device. Using this protection feature is highly advised because the majority of cybercriminal threats and identity theft attempts come from unidentified devices.

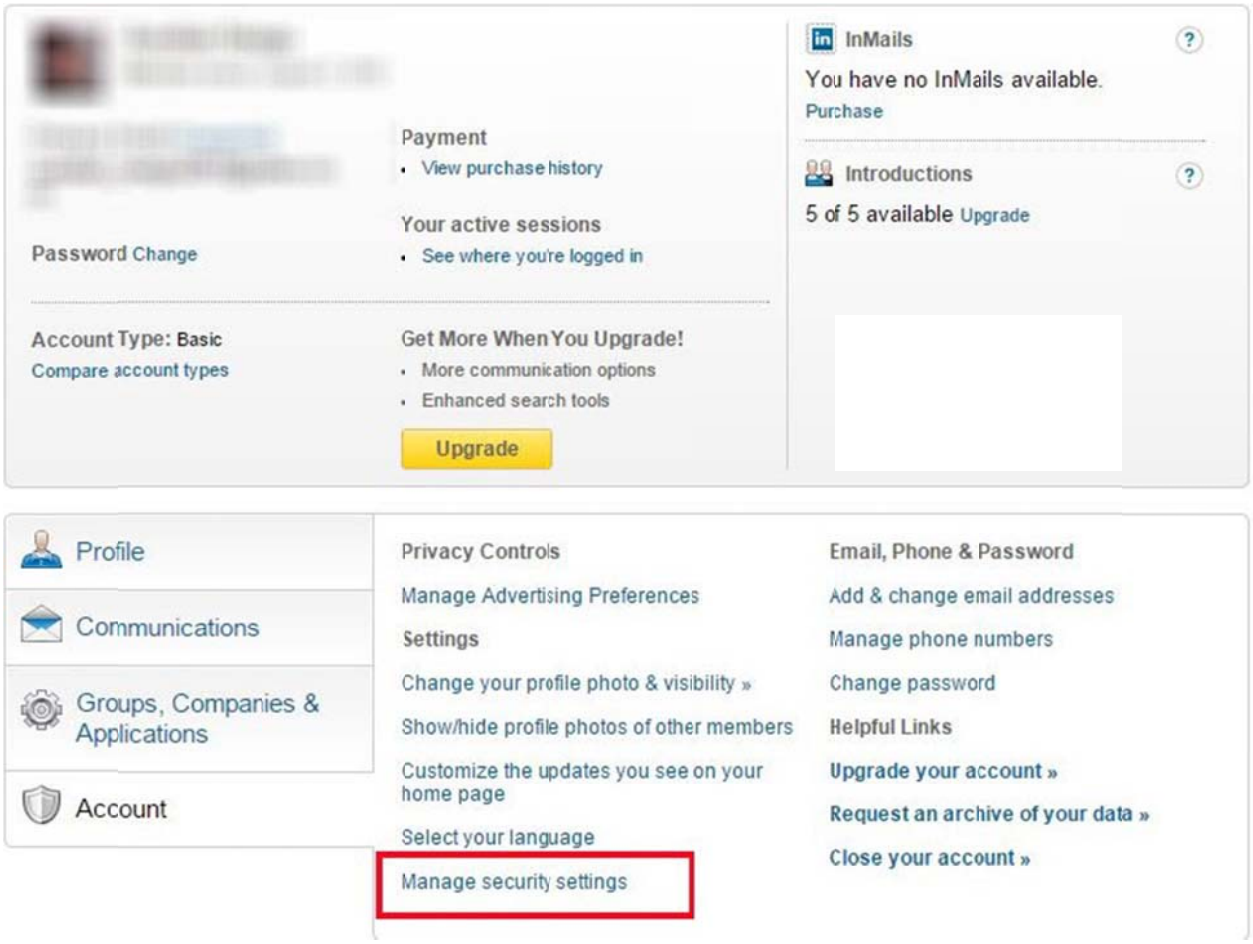


Figure 16 Two Step verification

3.3.6. Use the HTTPS option to secure your connection

There is an option to enable secure browsing mode in the same place in the LinkedIn security settings where users can enable two-step verification, as shown in Figure 16. This security feature should be used as an additional layer of defense against malware-enabled unauthorized access to browser sessions and to confirm that users are genuinely signed into their legitimate LinkedIn accounts.

If users frequently browse LinkedIn from risky or open locations, such as Wi-Fi networks in cafés, airports, or hotels, it is advised that they activate and use this secure browsing option. Online fraudsters frequently utilize these locations to access and retrieve user login information for banking websites and other online accounts.

3.3.7. Remember to close your internet account before leaving it

Users frequently mistakenly believe that simply closing the web browser after finishing their online activities on a public computer or an unsecured Wi-Fi network is sufficient, but they should always remember to log out.

The user risks sending everyone who accesses the browser—especially in a public setting—directly to their online profile if they forget to do this.

The usage of a "private browsing" session, which prevents browsing session history and credentials from being retained, is advised if the user must use a computer from a public area but is unsure of its security settings. This will stop data breaches from happening.

3.3.8. Maintain software updates

Software flaws appear to be getting worse every day. They now rank among the most common techniques used by online thieves to exploit systems.

Users of social media and other systems enable cyber criminals to leverage these security flaws and acquire access to their programs and apps by failing to update their Windows operating system and our products. It is common knowledge that popular and extensively used susceptible software programs like Java, Adobe Flash, Adobe Shockwave, Adobe Acrobat Reader, and QuickTime are installed on most people's computers.

Few individuals truly realize, in response, that these solutions are at risk from cybercriminals and that they need use a specialized solution to maintain them current to guard against software vulnerability threats.

3.3.9. Create a Secure Password for Your LinkedIn Account

Users of social media are advised to create secure passwords for their online accounts in order to prevent brute force attacks.

Here are some easy steps to take:

i. Use separate passwords for various online accounts. At least the other online accounts won't be affected if an IT criminal gains access to one of the online accounts.
ii. The password needs to be longer than 12 characters.
iii. Symbols, capital letters, and numbers should all be used.
iv. LastPass or another password manager should be used.

3.3.10. Be wary of phishing mails that ask for sensitive or personal information

Phishing is a time-honored method that IT criminals use when attempting to steal personal data and financial information from online consumers. Users should therefore pay attention to messages sent via LinkedIn accounts as well as email messages.

Before opening any attachments or clicking any links in the message, users should always carefully review the email they have just received. Users should search them up online for further information if they are unsure about the sender or sender's identity.

It's not a good indication that you can trust the message if you're prompted to download and install an application. Additionally, if there is a link to click, users should first see if it leads to a valid place by just hovering the mouse over the link. Users can use a trustworthy URL checker like VirusTotal to verify the suspicious links.

3.4 How to defend against brute force attacks

Users of the internet should practice good password hygiene. This might include choosing longer passphrases with a variety of characters, utilizing a reliable password manager to store their login information, and using a different password for each of their accounts. Multi-factor authentication (MFA) must be used as well. With MFA, hackers won't be able to access users' information right away by guessing their passwords.

In order to stop brute force attack tools from accessing their systems, organizations should also think about restricting invalid login attempts and/or implementing CAPTCHAs. Additionally, it is suggested to regularly change passphrases. Additionally, businesses should have a secure password policy and actively monitor platform activities to further improve the security of their workers and customers. Cybercriminals can't surprise users if users employ safe procedures and are vigilant [49].

3.5 Things to avoid while choosing a password

All of the "clever" methods that people use to build their passwords are known to cybercriminals and password breaker developers. Several typical password errors that ought to be prevented include [50]:

i. **Using a word from the dictionary:** Dictionary attacks are made to quickly test every word in the dictionary as well as popular variations.
ii. **Using private information:** Dictionary words include the names of pets, family members, places of birth, favorite sports teams, and so on. Even if they weren't, there are ways to take this data from social media and use it to create a wordlist for an attack.
iii. **Using patterns**: Some of the most widely used passwords are 1111111, 12345678, qwerty, and asdfgh. They are also on every wordlist used by password crackers.
iv. **Using character substitutions**: Well-known character substitutions are $ for S and 4 for A. Dictionary attacks automatically check for these substitutions.
v. **Only using required numbers and special characters at the end**: The majority of people only use the necessary numbers and special characters at the end of the password. Password crackers are equipped with these patterns.
vi. **Using widely-used passwords:** Organizations like Splashdata [51] release lists of the most used passwords each year. They compile these lists by deciphering compromised passwords in the same manner that an attacker would. Never use any of the passwords or similar ones that are on these lists.
vii. **Choosing a password that isn't random**: Passwords should be lengthy, unpredictable, and distinct. To securely create and save passwords for online accounts, use a password manager.

REFERENCES

[1] William Stallings, “Network Security Essentials – Applications & Standards,” in Book of Pearson Education Publication. Inc. 5th Edition, Upper Saddle River, NJ 07458, 2012.

[2] A. E. Omolara, A. Jantan, O. I. Abiodun, V. Dada, H. Arshad, and E. Emmanuel, “A Deception Model Robust to Eavesdropping over Communication for Social Network Systems,” no. Im, pp. 1–21, 2019

[3] S. Perera, H. Fernando, “Investigation of social media security: A Critical Review”, pp 1-5, 2021

[4] K. Musial and P. Kazienko, “Social networks on the Internet,” *World Wide Web*, pp. 31–72, 2012.

[5] A. Singhal and S. Jajodia, “Data warehousing and data mining techniques for intrusion detection systems,” *Distrib Parallel Databases*, vol. 20, pp. 149–166, 2006.

[6] O. Logvinov, “Standard for an Architectural Framework for the Internet of Things (IoT),” 2021.

[7] “Social Media Attacks,” 2020. Available at https://www.hhs.gov/sites/default/files/s

ocial-media-attacks.pdf, accessed July, 2023.

[8] P. Jucevi and G. Valinevičienė, "A Conceptual Model of Social Networking in Higher Education," Electron. Electr. Eng., vol. 6, no. (102, 2010.

[9] "Cyber crime Magazine', 2023. Available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021, accessed July, 2023.

[10] "Social Media threats you should be aware of", Available at ttps://www.pandasecurity.com/en/mediacenter/social-media/social-media-threats/, accessed July, 2023

[11] H. Gohel, A. Upadhyay, P. Sharma, "Analysis of Social Media Attacks and Classify Advances to preserve", International Research Journal of Engineering and Technology (IRJET) vol 02 issue 03, June 2015, pp 708-711

[12] Shantanu Ghosh,"Top Seven Social Media Threats" in article on http://searchsecurity .techtarget.in, 2011, (Accessed on April 2015)

[13] R. Alguliyev, R. Aliguliyev and F. F. Yusifov, "Role of Social Networks in E-government: Risks and Security Threats.," Online Journal of Communication and Media Technologies., 2018. [Online]. Available: https://www.researchgate.net/publication/328896849_Role_of_Social_Networks_in_E-government_Risks_and_Security_Threats. [Accessed 10 August 2020].

[14] P. Goud Kandikanti, Puneet Kumar Goud, "Investigation on Security Issues and Features in Social Media Sites (Face Book, Twitter, & Google+)" (2017). All Student Theses. 94. Available at http://opus.govst.edu/theses/94, accessed July 2023

[15] I. Ud Din, N. Islam, J. Rodrigues and M. Guizani, "Privacy and Security Issues in Online Social Networks," 2018. [Online]. Available: https://www.researchgate.net/publication/329118582_Privacy_and_Security_Issues_in_Online_Social_Networks/citation/download. [Accessed 15 August 2020]

[16] C. Timm, *Seven Deadliest Social Networks Attacks*. USA: Elsevier Inc., 2010.

[17] O. Simeon, A. J. Ekanem, G. N. Ezeh, " Smart phone security threats and risk Mitigation strategies" Journal of Multidisciplinary Engineering Science Studies, vol 8, issue 7, July, 2022, pp 4585-4597

[18]https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/. Accessed 12th march, 2022

[19] https://www.malwarebytes.com/keylogger. Accessed 14th April, 2022

[20] "Survey: How Brands Use Social Media Giveaways Today" available at https://www.easypromosapp.com/blog/en/survey-how-brands-use-social-media-giveaways-today/, accessed July, 2023

[21] Federal Trade Commission | Protecting America's Consumers (ftc.gov), accessed July

[22] "Clickjacking: Definition and Attack Prevention - Panda Security", available at https://www.pandasecurity.com/en/mediacenter/malware/clickjacking/, accessed July 2023

[23] https://digitalsecurityguide.eset.com/en-us/no-password-is-strong-enough-learn-about-brute-force-attacks, accessed July 2023

[24] 10 most popular password cracking tools [updated 2020] | Infosec Resources (infosecinstitute.com), available at https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/, accessed July 2023

[25] "MOBILedit" available at: http://www.mobiledit.com/sim-cloning/, accessed July, 2023

[26] "Magic SIM" available at: https://www.magic-sim.com/, accessed July, 2023

[27] "USB Cell Phone SIM Card Cloner" available at: https://www.amazon.com/VizGiz-Standard-Telephone-Directory-Transfer/dp/B09W5TQY81/, accessed July, 2023

[28] "SIM Explorer by Dekart" available at: https://www.dekart.com/products/card_management/sim_explorer/, accessed July, 2023

[29] "Mister SIM" available at: http://mister-sim.software.informer.com/, accessed July, 2023

[30] "Top 5 SIM Cloning Tools To Clone SIM Card Easily- Dr.Fone (wondershare.com)" available at https://drfone.wondershare.com/phone-clone/sim-card-clone-app.html, accessed July, 2023

[31] C. Noonan and A. Piatt, *Global Social Media Directory*, no. October. USA: U.S. Department of Energy, 2014.

[32] H. Wilcox and M. Bhattacharya, "A Human Dimension of Hacking : Social Engineering through Social Media," in *IOP Conference Series: Materials Science and Engineering*, 2020.

[33] C. Suggs, "Hacking Social Media." Available at https://www.scribd.com/document/554579077/Chanel-Suggs, accessed July 2023

[34] J. Patterson, "Hacking: Beginner to Expert Guide to Computer Hacking, Basic Security, and Penetration Testing (Computer Science Series)."

[35] E. S. Dandaura, U. M. Mbanaso, G. N. Ezeh, and U. C. Iwuchukwu, "The Use of Social Networking Service among Nigerian Youths between Ages 16 and 25 Years," 2015.

[36] J. Bagadiya, "367 Social Media Statistics You Must Know In 2021," *Social Pilot*, 2021. [Online]. Available: https://www.socialpilot.co/blog/social-media-statistics. [Accessed: 12-Oct-2001].

[37] S. Walsh "Biggest Social Media Sites" available at https://www.searchenginejournal.com/social-media/biggest-social-media-sites/#close, accessed July, 2023

[38] "Facebook help center" available at https://www.facebook.com/help, accessed July 22, 2023

[39] "Top 10 measures for facebook account" available at https://appslova.com/security-measures-facebook-account/, accessed July 2023

[40] "Introducing Facebook's cyber-security system" available at https://www.the-art-world.com/blog/2023/02/28/introducing-facebook-s-cyber-security-system/, accessed July, 2023

[41] "How can I stay safe on Facebook and what safety resources are available to me?" available at https://en-gb.facebook.com/help/122006714548814, accessed July, 2023

[42] B. Wong "Top Social Media Statistics And Trends Of 2023" available at

https://www.forbes.com/advisor/business/social-media-statistics/, accessed July 2023

[43] S. Dixon "Most popular social networks worldwide as of January 2023, ranked by number of monthly active users" available at https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/, accessed July 2023

[44] D. Anyaegbunam "The Top 20+ Social Media Platforms and Sites for 2023" available at https://mirasee.com/blog/social-media-platforms-2/, accessed July 2023

[45] M. Iskiev "The Fastest Growing Social Media "Platforms of 2023 [New Data] available at https://blog.hubspot.com/marketing/fastest-growing-social-media-platforms, accessed July 2023

[46] New MobileIron Report Details Most Common Mobile-reats and Blacklisted Apps, https://www.techrepublic.com/article/new-mobileironreport-details-most-common-mobile-threats-andblacklisted-apps/last,2020.

[47] A. Harkness, "Mobile malware threats," 2019, https://www.netmotionsoftware.com/blog/security/mobile malware-threats, accessed March, 2023

[48] "Common Software Vulnerabilities in 2022 and Ways to Prevent Them" available at" https://codesigningstore.com/common-software-vulnerabilities, accessed July 2023

[49] https://digitalsecurityguide.eset.com/en-us/no-password-is-strong-enough-learn-about-brute-force-attacks, accessed July 2023

[50] 10 most popular password cracking tools [updated 2020] | Infosec Resources (infosecinstitute.com), https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/

[51] SplashData - Powerful productivity tools, available at https://splashdata.com, accessed July, 2023