4 Ways to Protect Your Privacy on Social Media

*4 Ways to Protect Your Privacy on Social Media ~ Toranvichara

The article is based upon facts and can be trusted. The references are provided below

Article Author:-Toran Jung Bam

Added In:-09 Feb 2025 Sun

"*The more personal details you disclose on social*

media, the greater the risk of your personal information being compromised."

This Article uses AI only for paraphrasing.

Introduction

Social media has become an integral part of our daily lives, with platforms like Facebook, Instagram, Twitter, and TikTok serving as vital tools for communication and connection. Recent studies indicate that the average person spends approximately 2.5 hours per day on social media, which translates to over 17 hours a week. This extensive usage allows us to stay in touch with

friends and family, seek support from communities, learn new skills, explore diverse interests, and uncover various opportunities, both personal and professional.

However, this convenience comes at a cost. Social media companies have access to vast amounts of data, often collecting information that users may not even realize they are sharing. According to a report by the Pew Research Center, 79% of Americans are concerned about how their data is being used by social media companies. Furthermore, a staggering 64% of users have experienced some form of privacy violation, whether through data breaches or unwanted exposure of personal information.

As we use this digital landscape, it is important to be aware of the potential risks associated with sharing personal information online. In this article we will discuss about effective strategies to protect your privacy on social media, ensuring that you can enjoy the benefits of these platforms while minimizing the risks to your personal data.

Avoid Sharing Your Live Location or Daily Routines:

Of course! Social media is designed for sharing our stories, experiences, and activities with friends, family, and even a broader audience with good intentions. It serves as a platform to connect us and share our lives with our loved ones. Posting pictures from your travels or showcasing the places you've visited can be enjoyable and fulfilling.

But it's essential to consider the potential risks associated with sharing this information. What if someone were to exploit this data to cause you harm?

INTERVIEWS

Social media and burglary risk

Teenagers posting details about their whereabouts on social media networks can risk burglaries.

New research by security firm ADT suggested that nine out of ten young people aged 16 to 21 years-old share information which could put their family home at risk on social networking sites.

Over half of young people (56pc) post their location or movements on social media at least once a week, 81 per cent upload photos of themselves and friends when out and about, 48 per cent share pictures of things they have just bought and 29 per cent highlight locations and places to meet.

Meanwhile, a survey of ex-burglars found that over three quarters believed most crooks use social media to find easy properties to target and three quarters said they knew Google Street View was being used to stake out homes before breaking in*.

Senior officers have said risky status updates include 'checking in', posting photos when on a family holiday, or sharing photos of expensive gadgets and other purchases.

Assistant Chief Constable Gareth Morgan, spokesman on burglary for the Association of Chief Police Officers, said: "Social networking has become a part of everyday life. Unfortunately there are some individuals who use it as a means of gathering information to commit crime.

Home › News › Industry › Social Media Burglary and its Impact

Social Media Burglary and its Impact

Written by Garima Negi

3 Comments

With the changing digital transformation, social media has gathered a lot of traction in recent years. Social media platforms allow you to connect with people and share life events and memories with your social circles. From holiday check-ins on Facebook to a brand new car post on Instagram, we see people sharing their personal information online.

Professional burglars are smart and are using social media as a potential tool to find soft targets. Nowadays, with the help of social media, burglars can track people online. Most of us are naive and do not think before putting anything in public. Information like this could benefit the burglars who find their potential targets on such platforms and pose a threat to us.

According to Swinton insurance survey, 88% of the Twitter profiles are public. In fact, 66% of Twitter users have their location in their bios. It is a huge number of people who can be tracked via their social profiles. Burglars can easily monitor locations of these people from their Twitter profiles that are apparently public.

The most common types of posts that catch burglars' attention are:

There's a genuine possibility that your home could be targeted for a burglary, or if you are a public figure, you might face threats while visiting certain locations. The true intentions of those who view your posts can be unpredictable, and even if you restrict your audience only to your friends, the risk remains.

Nowadays, the trend of sharing personal routines and daily activities on social media has surged in recent years. Various social media trends encourage users to disclose daily routines about their lives, which can significantly compromise their security. Sharing your live location, daily habits, food

preferences, or even minor details about your life can provide stalkers and hackers with valuable information that could be used against you. It's crucial to be mindful of what you share to protect your safety and privacy.

Precautions:

- Hold Off on Posting Travel Photos Until You Return
  Although if you have an urge to share your photos on your trip. Forbid from sharing images on social media while you are still on your trip and wait until you're back home.

- Limit Sharing Personal Details
  Avoid disclosing sensitive information such as your workplace, upcoming events, travel plans, or daily activities. Always be cautious and discreet when posting personal information online.

- Verify Friend Requests
  If you receive a friend request from someone who appears to be a friend already in your

network, take the time to verify their identity before accepting. There's a strong possibility that it could be a fake profile created with harmful intentions.

Don't Share Your Identification Numbers:

We often have to share our identification numbers in various contexts, such as passports, citizenship documents, or licenses, for online transactions, joining social media platforms, and participating in online communities. However, sharing these identity documents online poses significant risks, as they can be exploited by others to impersonate us.

Criminals may use the acquired information to open bank accounts or apply for credit in the victim's name, which can adversely affect their financial history, access to government services, and online reputation.

Even when sharing documents with good intentions, such as verifying identity on an online platform, doing so without engaging with trustworthy providers can result in a loss of control over your information. There is a possibility that your data may be stored, shared, or even sold to criminal organizations or companies that employ invasive techniques to target users.

Precautions:

- Utilize Temporary or Disposable Information
  Whenever possible, opt for a temporary email address or phone number when signing up for services. This approach helps safeguard your primary contact information.

- Restrict Shared Information
  Only provide identification numbers that are essential. Refrain from sharing any additional personal details unless absolutely necessary.

- Create Strong, Unique Passwords
  Develop robust passwords for your accounts and avoid reusing the same password across different websites.

- Examine App Permissions
  Before signing up for any service, review the permissions that the app or website is requesting. Only grant access to the informations that is truly necessary.

Limit Information Shared in Your About Section:

Social media platforms offer us the opportunity to share details about ourselves, but it's crucial to be cautious when doing so. Even seemingly minor details, such as your maiden name or hometown, can assist hackers in answering security questions. While these platforms may provide options to share personal information, there is no obligation to disclose everything.

We should be particularly mindful of, or even avoid sharing, the following information online:

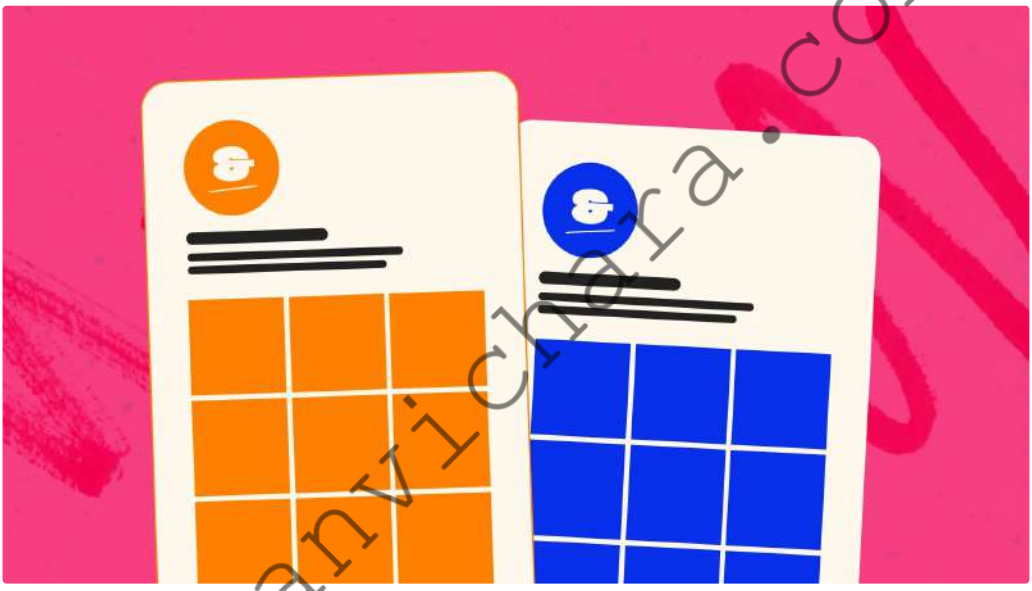
- Full name
- Home address

- Phone number
- Email address
- School or workplace details
- Travel plans
- Political or religious beliefs
- Any sensitive information regarding family or friends

Only Accept Connection Requests from People You Know:

Social media serves as an excellent platform for connecting with new individuals and making friends online. It provides us the opportunity to establish a

personal brand, grow our audience, and express our opinions. However, it's crucial to only accept friend requests and followers from people you genuinely know. If you're looking to cultivate a public persona, consider setting up a separate account for that purpose.



When we can share everything online, what counts as oversharing?

What's considered 'excessive' is open to interpretation. Influencers, for example, share a lot because
Getty Images/fStop

A study suggests communicating too much about yourself can be a bad thing – but we need to share to make connections, too

Sign up to Reclaim your brain: our free email to help you spend less time on your phone

I recently made a new friend, and we became Instagram mutuals right away. From her posts, I'm getting a sense of what she does on the weekends and what she likes to cook. It's helping me to get to know her even though we don't see each other very often.

As I learned about her hobbies and how many brothers she has, I also noticed how much the act of sharing personal details has evolved. The photos or

What Are the Risks of Oversharing on Social Media?

Oversharing can make it easier for cyber criminals to learn important details that can give them access to your online accounts. A lot of users create passwords using personal information to make them easier to remember. This allows cyber criminals to crack passwords more easily as they can learn that information about you on social media. The following are some of the risks that come from oversharing on social media.

Identity theft

Identity theft is when someone steals a victim's Personally Identifiable Information (PII) without permission and uses it to impersonate the victim and commit fraud. PII is the data that can identify a person such as their address, email, phone number or Social Security number. Cyber criminals can steal this information through cyber attacks, data breaches or a person's social media profile.

A person's social media profile can share personal details which can help cyber criminals steal their identity. Once a cyber criminal steals a victim's identity, they can impersonate the victim to commit crimes such as credit card fraud.

Social engineering

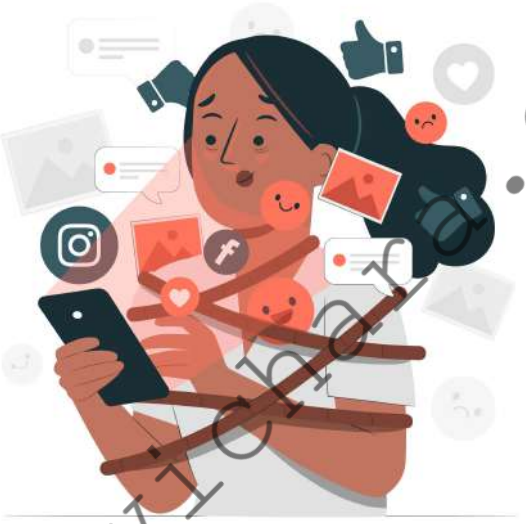
Social engineering is the psychological manipulation used to get others to do things or reveal private information. Social engineering starts by gathering information about a target. Cyber criminals can learn a lot about their victims by looking at their social media to find out their interests and online behavior. Once the information has been collected, cyber criminals can tailor their social engineering attacks to their victims with the information found on social media.

These social engineering attacks have the goal of either installing malware on your device or tricking you into revealing personal information such as your login credentials through methods like phishing attacks.

Even if you are cautious about your own posts, your friends can still view what others share about you. With a bit of investigation, they can easily discover your date of birth and sift through your friends list for additional information. Furthermore,

individuals behind fake accounts may use them for scams, defraud your friends, or even engage in blackmail activities.

Additional Tips:



- Review Privacy Settings
  Regularly check and update your privacy settings on your accounts to ensure your information is properly protected.

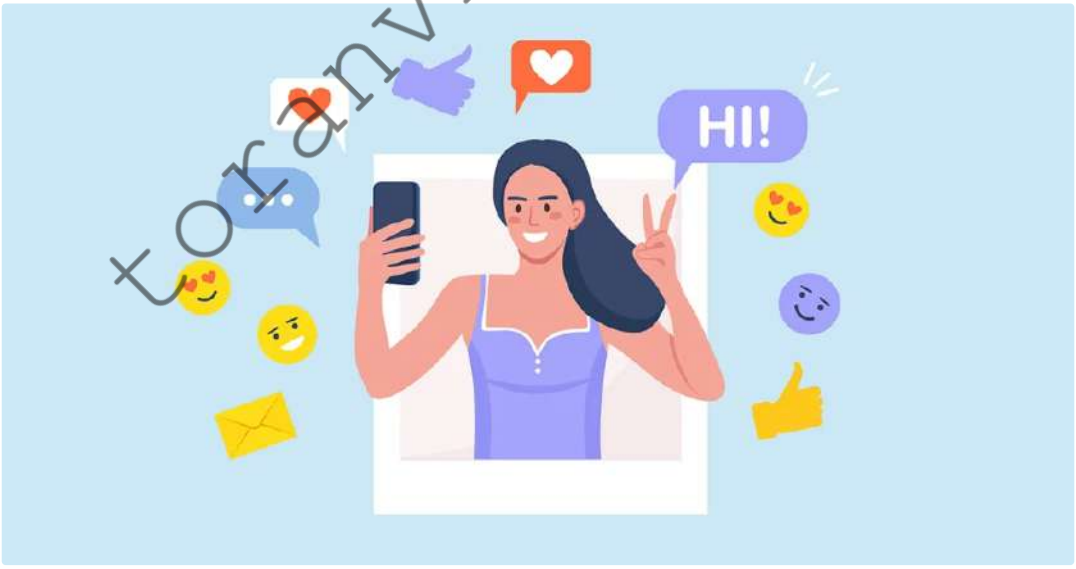
- Enable Two-Factor Authentication
  Activate two-factor authentication, a security measure that requires a one-time password (OTP) valid for only a few minutes, along with

your regular password and device verification.

- Conduct Privacy Checkups
  Perform regular privacy check ups provided by the social media to evaluate and enhance your security measures on social media.

- Limit Third-Party Access
  Be cautious about granting access to third-party applications and services that may compromise your privacy as Social media platforms are not responsible for data collected by third parties.

Conclusion:



Social media is no doubt a great tool for networking and being close to your loved one. But it also caters various threats to its users. Your privacy can be at risk if you are oversharing or if you aren't following security precautions. Following these suggestions can help you protecting your data and your privacy for keeping you safe in the digital platforms. Best Wishes!!

References:

- https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html
- https://www.linkedin.com/pulse/we-okay-social-media-websites-hampering-our-privacy-pooja-garg/
- https://www.aura.com/learn/how-to-protect-your-personal-information-on-social-media
- https://www.mcafee.com/blogs/privacy-identity-protection/how-to-protect-your-social-media-accounts/
- https://rainn.org/safe-media
- https://netchoice.org/tools-to-protect-your-privacy-

on-social-media/

- https://dataprivacymanager.net/how-to-protect-your-privacy-on-social-media/
- https://www.youtube.com/watch?v=se2pELXlMo8
- https://youtu.be/z68CHwqBhDU?si=KMneAXuBqUn3_nKE

Toran Jung Bam
Namaskar! This is the first article shared on the niche of technology on our platform. I have gone through various articles and information on the Internet to ensure quality. AI is used (only) for paraphrasing my words for optimal readability. Thank You For viewing my article. I love to share my thoughts and my perspective. Do see my other articles and keep reading!