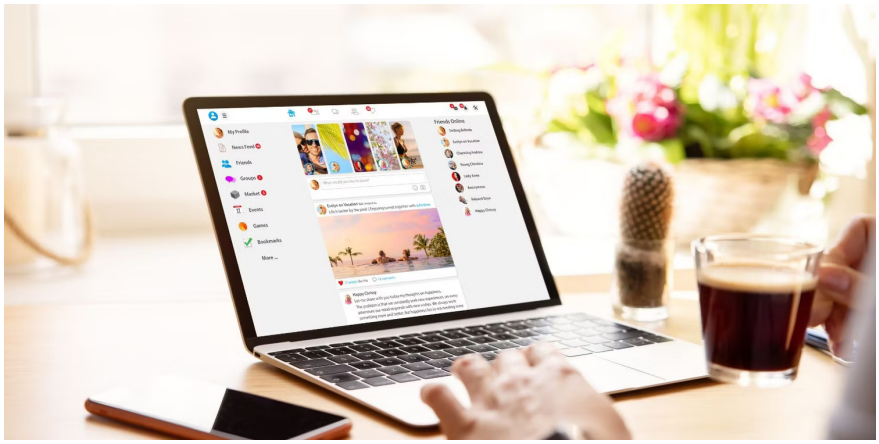
7 mistakes on social networks to avoid if you want to protect your privacy

If you want to maintain a private online presence and avoid a data breach, avoid these common social media mistakes.

With the prevalence of identity theft and harassment on social media, it is more important than ever to prioritize protecting privacy. Paying attention to how you navigate online is key to avoiding data mining.

1. Give the app access to social media accounts



First, you should avoid using third-party apps or extensions to improve your social media experience or unlock premium features not available in the free version. These apps often request access to your account, and if you check their terms and conditions, you'll see they may have permission to view your photos, chats, profile details, etc.

Likewise, the option to use social logins for other apps has become popular. While logging into a game or other app with social media credentials may seem harmless, it gives those apps access not only to account information but also the ability to Enter the login details you used.

Therefore, it is recommended to avoid sharing this sensitive data with third-party applications and do not use social network accounts to log in on social networks.

2. Leave your profile in public mode

When a social network profile is public, everyone can see it. Anyone can see your photos, personal information, and everything you post on your feed or timeline. Fraudsters can exploit this publicly available information.

They can create a fake profile with your identity to impersonate you.

Not only does this damage your reputation, but it also puts your friends and family in danger. Imposters may use your identity to demand money or try to get personal information from your contacts. To prevent these risks, you should lock your social network profile, restricting access to only being visible to friends.

Most social media platforms offer this security feature. If your profile is currently public, you should make it private.

3. Revealing too much personal information

Even if you set your profile to private, you should still be cautious when sharing personal information. Avoid sharing your date of birth, phone number or home address as these details can easily be used for identity theft. Also, avoid taking selfies with sensitive documents such as ID cards, passports or credit/debit cards.

Also, don't share too much about your health, relationships or financial status. Likewise, don't discuss workplace-related issues to avoid compromising company privacy.

4. Ignore privacy settings

Ignoring basic security measures can also leave your account and privacy vulnerable. This includes using weak, easy-to-guess passwords or using the same password across multiple social media platforms. Likewise, not enabling two-factor authentication makes it easier for hackers to break into accounts and compromise privacy.

To minimize these risks, always use strong, hard-to-guess passwords and use unique passwords for each social media account. Also, avoid storing login information online. If you haven't turned on two-factor authentication, set it up to increase account security.

It's also a good idea to review your social media profile's privacy settings to check if you're sharing data you don't want to share.

5. Share travel plans

Travel plans are one of the important things that should not be shared on social networks. If you announce your vacation plans, it could alert thieves monitoring your activities that your home is unoccupied, increasing the risk of burglary. Similarly, real-time check-in during your trip provides scammers with information about your whereabouts that they can exploit.

To protect your privacy, avoid posting your travel plans on social media, don't check in, and remove location details from photos to avoid revealing your location.

Tip : If you are an influencer traveling alone and have to interact with your audience during your trip, develop the habit of checking in from your previous location after moving to your new location.

6. Interact with unknown people

We all have some people on our friends list who are just acquaintances on social networks. We may have connected with them through a public group or post, despite never meeting them in person or having any video communication. Even though they are strangers, they still have a place in our friends list.

Even if you've taken steps to make your account more private, these unknown people can still pose a serious privacy risk because you never really know them. Who is. They may have connected just to monitor your activities and exploit information later. If you have people you don't know on your list, consider unfriending them.

If that feels too drastic and you want to stay connected, at least adjust your privacy settings to limit what they can see of your activity. Also, from now on, avoid adding strangers.

7. Using social media accounts in public places or on public computers

Finally, using social media accounts on public computers can also endanger privacy. Fraudsters can install keyloggers on these devices to get login information, hackers can intercept data, and if you forget to log out when leaving the device, anyone can access your account. you later.

Using a social media account while at work or in other public places can allow strangers to glance over your shoulder and see your personal information. To avoid this risk, limit your use of social media on public computers or in shared spaces.

Similarly, you should avoid connecting your phone or computer to public Wi-Fi networks because these networks are often insecure and hackers can intercept information shared through them. When in public, it's safer to use phone data instead of connecting to random free networks.

Here are some mistakes you should avoid to protect your privacy when using social media platforms. Make it a habit to regularly check the devices logged into your account. If an unfamiliar device is detected, it could be a sign that your account has been compromised.

Taking quick action to remove an unknown device can help protect your account and privacy in a timely manner.