BIZCOMMUNITY

5 Common mistakes we all make on social media

Facebook, Twitter, and Instagram are among the top 10 of the world's most visited websites. Although billions of people spend thousands of hours every day on these social media platforms, not many of them think of this activity as risky. The risk stems from the careless actions we all sometimes take online when we forget about our privacy.

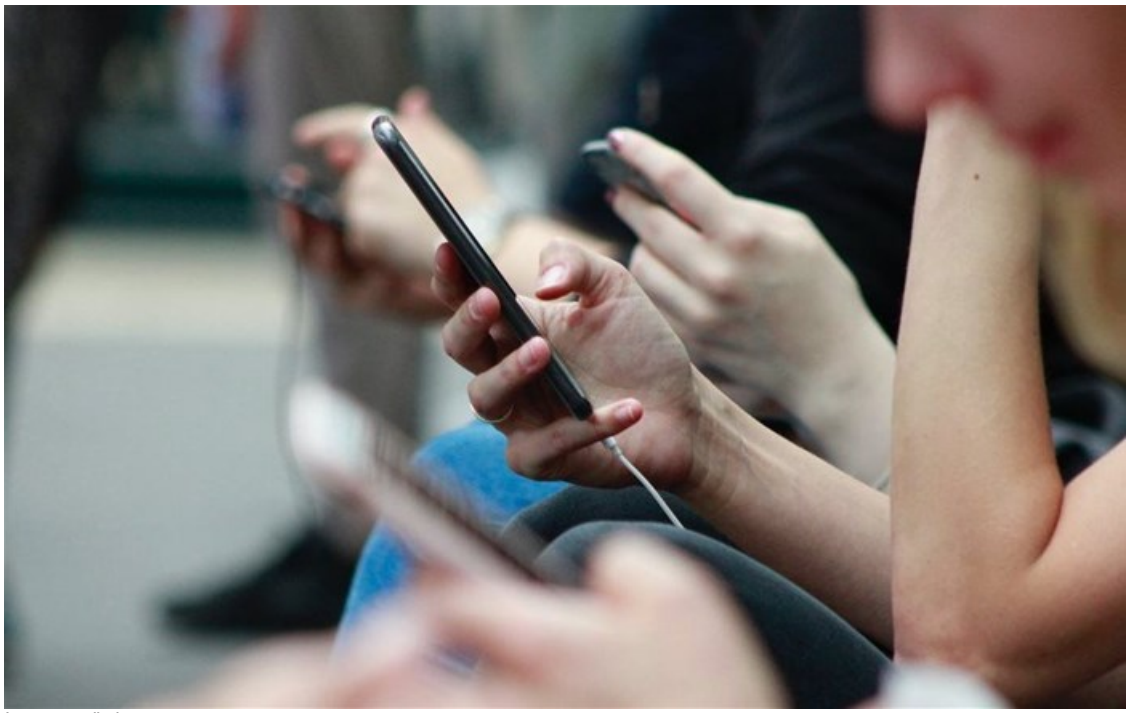

Image supplied

Daniel Markuson, a digital privacy expert at NordVPN, says that the privacy of your social network account is as important as the content you post. Though the privacy of social networking services as a personal choice might be debatable, the expert picked the most common mistakes all users make and explained how to avoid them:

Oversharing

It’s dangerous to reveal too much or too sensitive information, such as locations, plane ticket or passport photos with ID numbers, countdowns until you leave your home for a vacation, new expensive purchases, etc.

Criminals lurking online can use that information to steal your identity, break into your house, or simply blackmail you. Moreover, hackers often look for emotionally vulnerable people to attack, so your burst of emotions on social media might be turned against you.

Don’t share your personal details, such as home address and telephone number, on your social media profiles as they can be easily accessible to anyone.

Don't share everything on social media

4 Sep 2019

Markuson says it’s better to hold off with posting things online while being away, especially ones that include your location in real-time. The expert also argues against posting pictures of any documents that contain sensitive information or scannable codes, such as QR and barcodes. And remember not to share your private feelings or participate in heated online discussions that could catch the eyes of scammers.

Using the same password for all accounts on social media

Imagine your Twitter password gets leaked, and you use the same one for your Facebook and Instagram. A hacker now can block you from your social media accounts, access all your private information, including your photos, and use it in malicious ways.

Are your passwords being stored securely?

24 Jul 2019

To avoid possible identity theft, you should use different passwords on different social platforms. It is also a good practice to change your passwords frequently and use strong ones.

Markuson recommends using a password manager. It remembers your complicated passwords or generates them for you as well as lets you store, organize, and access your passwords from anywhere.

Forgetting about the privacy settings of your account

Social media users sometimes forget about cybersecurity as they share sensitive information and add people they don’t know to their friends’ list. However, some of these strangers might be cyber troublemakers who may feed you harmful fake news or send virus links over messages. These people also get access to the pictures and other information you share with your friends.

So don’t become friends on social media with people you don’t know. You can always go through the mutual friends' list or things in common before adding a person to your Facebook.

Secure your personal information with app permissions

23 Aug 2019

Even if you don’t befriend strangers, but your profile is public, anyone can scrape your data and use it for their own sneaky needs. Daniel Markuson reminds to check who you’re sharing your information with before posting anything online. Make sure your posts are visible to your friends only instead of everyone on the internet.

Doing quizzes

What will you look like in 50 years? Which Game of Thrones character are you? With malware plugins, scammers use these tests to get your personal information. This March, Facebook sued two Ukrainian quiz-makers who had been using such games to access and steal private data from Facebook users. The scammers served Facebook users their own ads instead of officially approved ones.

Facebook quizzes could get your identity stolen

16 Apr 2019

Although Facebook quizzes seem completely harmless, don't fall for them. Their algorithms are too simple to tell you the truth, so stay sceptical and just don't do them. According to Markuson, if you still can't resist that tempting test, check what information it requests from your profile and decide whether you really want to share it.

Using social media on unsecure public Wi-Fi

The latest survey shows that 79% of public Wi-Fi users take considerable risks when choosing a network. They select a hotspot for its Wi-Fi strength, go for a name that sounds appropriate, or simply pick any free option. However, hackers use unsecured public connections to spy on people's devices and steal their private data, including social media passwords.

Stay extra cautious when connecting to free Wi-Fi at coffee shops, hotels, and other public places, as they may be insufficiently protected. Don't log in to your social accounts or visit sensitive websites when on public Wi-Fi. One of the best ways to safely use a free hotspot is by installing a VPN. It will make sure your internet connection is private and no sensitive data can be stolen.