How to keep your social media safe from hackers

AHMAD TOUSIF JAMI

Concerns over security on social media are growing on both personal and commercial levels. Hackers often try to take over social media accounts for unethical purposes. Regardless of the platform, there are a few steps that may be taken to secure your social media in preventing the possibility of hackers from taking over. Some of these steps are discussed below.

Use multi-factor authentication (MFA)
Using MFA on your social accounts helps you add an additional layer of security to the authentication process of logging in and other sensitive processes such as changing your password, phone number or email address. This means that even if a hacker can somehow break through to know your password, they still cannot access your account.

The MFA can be set up with authenticator apps such as Google Authenticator or Microsoft Authenticator. They help you generate a new code every sixty seconds that only the device on which you remotely have that application set up. This is a recommended step for additional security and peace of mind.

Make your password stronger
Your password is the most elementary key to accessing your account. If your password is easy to guess or is too common - the possibility of your account getting compromised is high. For instance, a password that is your name or a string of numbers or keys of a keyboard is some of the easily guessable passwords that can be cracked through a hacking attack type known as brute force, where the attacker tries on a variety of combinations of passwords repeatedly.

You may use unique information or text that is not common to have a strong password. It is recommended to use a combination of texts and numbers and special symbols when possible. Also, the password should be at least 12-16 characters long. If needed, there's no loss in using passwords of 30 characters in length either. A common technique is using sentences/phrases in a password instead of a single word. Usage of both upper case and lower case alphabets are also recommended.

Although this does not make your password impossible to hack, it should make it much harder to crack. To analogise, it's like putting a lock on the bicycle. A thief with enough resources will still be able to crack open the lock, but putting two or three locks will make it undesirable for the thief to steal the bike in the first place.

Responsibly click on links
There are various phishing links and scam third-party apps on the internet. Sometimes, they are directly given to your inbox in the disguise of an award or a gift that the hacker would claim you have "achieved". It could also come in other forms, such as a request for emergency help, and may take you to a phishing website, which is essentially a cheap copy of the actual sites that look like the site you are trying to browse. They might have very similar addresses and very similar landing pages as well.

In these situations, please do not click on any link that does not look genuine. A general rule of thumb is never to click on any link you do not trust 100%, even if it came from a friend. Moreover, it is highly recommended that you not give your account password in any portals because the hacker could access your provided password from that link. The same applies to scam third-party apps, which may come in disguise as games or something else. Remember, your social media password would never be needed on any website other than the social media itself while logging in or changing sensitive information such as your password.

They are not always secure if it is about downloading any games, software, or operating systems from unofficial sites. So, if you find yourself downloading them, only go ahead if you trust the website you are downloading from. Also, always check for community feedback on the content you are downloading/ browsing from such websites.

Keep your system up-to-date
Beyond specific recommendations you can follow to keep your account secure, a properly updated device would take a long way. If you have the latest Windows Defender or similar antivirus activated, it can help prevent you from going to scam websites and prevent phishing links from opening.

You can choose to use any reputed antivirus software from the internet. Based on your need, you may choose either the free version or, for specific requirements, use the premium version. Doing this can also ensure that any sensitive information, which may or may not be stored on your social media account. However, this will ensure security for your remote device. Active antivirus software can prevent system hijacking from potential malware as well.

Know signs of a potential compromise
Often, a hacker might access your account without you even realising it. To avoid such cases, you can keep your eye out for a few things. For instance, keep an eye out for the email you have set up to set notifications for your social handles. If you receive an email of a logging-in that is not you, that may also mean someone is attempting to access your account.

Moreover, if you see advertisements that are unusual for a prolonged period, such as foreign products, or if you have trouble logging in to your account with prompts similar to "too many attempts, try again", your account may be under attack. This could also be situations such as you see you are suddenly following accounts you never followed or even your friends asking you if you sent them a link you cannot see from your end. In short, any unwarranted or unusual activity is worth inspecting to confirm your account stays secure.