Quora Gets Hacked: 5 Tips on What Users Should Do Now

Hackers have gained access to the personal data of 100 million Quora users. NordVPN offers expert advice and tips on what users should do after the breach.

PANAMA, PANAMA, December 6, 2018 /EINPresswire.com/ -- Quora, the world's most popular question-and-answer social media site, was hacked. This Monday, Quora confirmed that unknown hackers had gained access to the account information of about 100 million of its users.

“This year has once again proved that even giant companies are not doing enough to secure sensitive user data. In September, the personal details of about 50 million Facebook users were exposed. Marriott, world’s biggest hotel chain, has just confirmed that the data of half a billion guests had been stolen,” says Ruby Gonzalez, Head of Communications at NordVPN. “We urge all Internet users to share as little as possible online and to use a VPN to encrypt their online activities.”

> We urge all Internet users to share as little as possible online and to use a VPN to encrypt their online activities”
>
> *Ruby Gonzalez, Head of Communications at NordVPN*

The personal user data compromised in the Quora breach includes the following:
• account information (names, emails, hashed passwords, and data imported from linked social networks like Twitter and Facebook);
• public actions (questions, answers, comments, and upvotes);
• non-public content (answer requests, downvotes, and direct messages).

What to do if your account gets compromised

If your account has been hacked or compromised in a data breach, you should act quickly, before hackers can get their hands on other important information. NordVPN shares 5 most essential steps to keep yourself safer.

1. Get back into your account

The first important step for you to do is to log into your account and change password immediately. It shouldn’t be ‘password’ or ‘imthekingoftheworld.’ Your password needs to be strong. Try this trick: think of a statement, for example, “I love to go for a walk every evening." Then, turn it into 1l2g4awEVe (replacing I with 1, to with 2, for with 4, and every with EV).

If possible, use two-step authentication and get a password manager like LastPass or 1Password. Most importantly, never reuse the same password for all of your accounts.

2. Take care of your other accounts

If you used the same or similar password for more than one account, change it on all other key platforms and accounts immediately. That includes your email, Facebook, Amazon, Twitter, LinkedIn, and other. Even though hackers, most probably, got hold of your hashed password, there's still a chance they can decrypt it and get the real password.

Check haveibeenpwned.com to see if you have an account that has been compromised in a data breach before.

3. Update your settings and available data

Go through the privacy settings and data you provide both on the breached platform and all the other important platforms you use. Make sure you share only the required information and remove what's not necessary, for example, your phone number and favorite locations. This way, even if your account gets hacked, it will be of less value for hackers.

Common advice is to share as little as possible online. If you are not intent on getting worldwide attention, change your account settings from 'Public' to 'Private.'

4. Revoke access to third-party apps

In Quora case, for the user convenience, there was a possibility to import some data from linked social networks like Twitter and Facebook. And it seems that hackers got hold of this information as well. Check, whether you permitted access to view one of those accounts.

We recommend reviewing which of your accounts are linked and rethink if you really need that. Revoke access to applications that are no longer in use, as well as suspicious ones.

5. Beware of phishing scams

Since hackers may have detailed profile information of 100 million users on Quora, we are likely to see more personalized and sophisticated phishing scams in the near future. Phishing scams are very effective, as criminals usually use a piece of real private information.

You should be careful if you get seemingly legitimate, personalized messages from banks or any other familiar organizations. That is especially valid if they ask for more personal details, fund transfers or to click on any link. For additional safety, use a VPN, like NordVPN. Using a VPN when browsing can help to protect you against malicious websites and phishing sites.

ABOUT NORDVPN

NordVPN is the world's most advanced VPN service provider that is more security oriented than most VPN services. It offers double VPN encryption, ad blocking & Onion Over VPN. The product is very user-friendly, offers one of the best prices on the market, has over 5,000 servers worldwide and is P2P-friendly. One of the key features of NordVPN is zero log policy. For more information: nordvpn.com.

Laura Tyrell
NordVPN
+44 2071935407
email us here