PHYS.ORG

Facebook hack reveals the perils of using a single account to log in to other services

October 2 2018, by Mike Johnstone

Credit: Unsplash/CC0 Public Domain

Facebook announced on Friday that its engineering team had discovered a security issue affecting almost 50 million accounts. Due to a flaw in Facebook's code, hackers were able to take over an account and use it in the same way you would if you had logged into the account with a password.

The company says it has now fixed the problem in its code and reset access tokens for those accounts – along with 40 million other accounts that were vulnerable to the flaw. If you found yourself logged out of your Facebook account last week, it's likely you were affected.

Beyond that, little is known about the extent of the security breach. In its security update, Facebook said: "Since we've only just started our investigation, we have yet to determine whether these accounts were misused or any information accessed. We also don't know who's behind these attacks or where they're based. "

What it means

This is not the worst data breach to date. That accolade belongs to the credit bureau Equifax, which had personal data stolen from the accounts of 147 million people. But, unfortunately for Facebook, there are several flow-on effects from the recent hack.

First, the breach may run afoul of the European Union's General Data Protection Regulation (GDPR), which was introduced in May. Although the GDPR only applies to European citizens, the penalties for data breaches are severe – up to 4% of global turnover per breach.

Second, any accounts on other platforms that use Facebook verification are also at risk. That's because it's now a common practice to use one account as an automatic verification to connect to other platforms, for example by using a Facebook account to log in to another social media platform such as Twitter, Spotify or Instagram. This is known as single sign-on (SSO).

How single sign-on works

If you connect to any system, you need some form of authentication – usually a login credential such as a username and password pair. When you have many different systems that all require credentials before you can use them, suddenly you're faced with remembering ten different (ideally very long) passwords.

Some people can do this, but many can't. And we still want the systems to be secure. If we could connect to one system that was trusted by the others, and use the trusted system's password, then we wouldn't need ten passwords – just one. That's the principle behind SSO.

But this only works as long as the trusted system is secure. If it's not, a cybercriminal could use the hacked account on one platform (in this case, Facebook), to access any other connected platform.

What you should do

Authentication usually works because of one of three factors:

- something you know, such as a password
- something you have, such as an access card
- something you are, such as a fingerprint.

Clearly, using more than one factor increases security. In your Facebook account, you can choose to use two-factor authentication. That means that you would need to enter your password plus a code sent to you via an SMS message when you next log in.

The future of verification

There is always a tension between usability and security. People want systems to be secure so that their identities aren't stolen, and they also want the same systems to be easily accessible. SSO is an attempt to balance usability and security, but the Facebook hack reveals its limitations.

Many people don't like passwords, so they choose easily remembered, and therefore easily breakable, passwords. Cybercriminals have access to lists of millions of common passwords (hint: "Gandalf" isn't as unique as you might think).

Access tokens, such as cards or other physical devices (as used by some banks, for example) are a solution – as long as you don't lose it. It might be that using a unique physical attribute is the best way forward. After all, you always carry your fingerprint, iris or voice with you.

Provided by The Conversation

Citation: Facebook hack reveals the perils of using a single account to log in to other services (2018, October 2) retrieved 19 June 2024 from https://phys.org/news/2018-10-facebook-hack-reveals-perils-account.html