Should you worry about 32 million hacked Twitter passwords?

June 9 2016, by David Hamilton

Yet another security outfit is reporting that millions of stolen passwords—this time, for Twitter accounts—are floating around the dark side of the internet. Should you be worried?

In truth, it's hard to say. And that's rapidly emerging as the latest dilemma of digital life.

The website LeakedSource said it received a cache of Twitter data that contains 32 million records, including passwords. Twitter said that its

systems haven't been breached. LeakedSource said the passwords were most likely collected over time by malware-infected browsers that sent saved passwords to hackers.

Twitter said it's taking the disclosure seriously. "We've been working to help keep accounts protected by checking our data against what's been shared from recent other password leaks," the company said in a statement.

So while 32 million is a big number, it's not itself a reason to panic. This particular data set contains a large number of credentials associated with Russian email addresses, suggesting that the malware may have been most prevalent there. In addition, many of these passwords are old and possibly no longer current. The LeakedSource website will let you check to see if your logic credentials were included.

Even old passwords can create problems, particularly for accounts you may have set up and used only a few times. Just ask Facebook founder Mark Zuckerberg, who found his largely dormant, seven-year-old Twitter account hijacked earlier this week .

The best way to protect yourself is to make sure you're not re-using passwords across accounts. That way, a breach of, say, your Twitter password won't also put your bank account at risk. It's also a good idea to change passwords regularly, which of course is much more difficult if you're using unique passwords for every account.

Password managers can help. These programs will generate random passwords for your accounts, store them in a central, encryption-protected vault and auto-fill them on websites and even mobile apps. Popular options include 1Password, LastPass and Dashlane. But these programs still aren't completely intuitive for many people.

As if things weren't murky enough, the provenance of such hacked passwords is almost always unclear. LeakedSource, which describes itself as a newcomer on the leaked-data security scene, said it obtained the data from an anonymous user.

The site itself is also something of an unknown. It doesn't describe itself in any detail or offer contact information beyond an email form. In addition to the free checks of your own data, it sells more in-depth subscription access for roughly a dollar a day.

Over a week ago, LeakedSource reported that more than 360 million records from Myspace were obtained from a hacking incident in 2013. The website has also reported that data from 167 million LinkedIn accounts were also affected from a prior hacking incident.

More information: LeakedSource blog: www.leakedsource.com/blog/twitter