

Hackers selling 117 million LinkedIn passwords

Your video will play in 00:24

LinkedIn was hacked four years ago, and what initially seemed to be a theft of 6.5 million passwords has actually turned out to be a breach of 117 million passwords.

On Wednesday, the professional social network company [acknowledged](#) that a massive batch of login credentials is being sold on the black market by hackers.

The worst part about it is that, because people tend to reuse their passwords, hackers are more likely to gain access to 117 million people's email and bank accounts.

The advice for everyone who uses LinkedIn ([LNKD](#), [Tech30](#)) at this point is: Change your password and add something called two-factor authentication, which requires a text message every time you sign in from a new computer.



This episode drudges up some embarrassing history for LinkedIn.

Because of the company's old security policy, these passwords are easy for hackers to crack in a matter of days.

Companies typically protect customer passwords by encrypting them. But at the time of the [2012 data breach](#), LinkedIn hadn't added a pivotal layer of security that makes the jumbled text harder to decode.

Put on the defensive, LinkedIn is now scrambling to try to stop people from sharing the stolen goods online -- often an impractical task. The company is also invalidating all customer passwords that haven't been updated since they were stolen.

LinkedIn said it's reaching out to individual members affected by the breach. This particular hack affects a quarter of the company's 433 million members.

Now, computer security experts are wondering why it took so long for LinkedIn to figure out what happened to their own company computers -- or acknowledge it publicly.

"If LinkedIn is only now discovering the scale of data that was exfiltrated from their systems, what went wrong with the forensic analysis that should have discovered this?" said Brad Taylor, CEO of cybersecurity firm Proficio.

Hackers are selling the stolen LinkedIn database on a black market online called "The Real Deal," according to tech news site [Motherboard](#).

For its part, LinkedIn offered the same, go-to statement used by every company after a data breach.

"We take the safety and security of our members' accounts seriously," wrote Cory Scott, the company's chief information security officer.

CNNMoney (New York)

First published May 19, 2016: 9:23 AM ET

Paid Content

