LinkedIn confirms 2012 hack exposed 117M user passwords

May 18 2016

LinkedIn said Wednesday that a 2012 breach resulted in more than 100 million of its users' passwords being compromised—vastly more than previously thought.

The business social network said that it believes to be true a purported hacker's claim that 117 million user emails and passwords were stolen in the breach, up from the 6.5 million user credentials that the company originally said were compromised. Those 6.5 million passwords were reset in 2012 and the company advised the rest of its users to change their passwords too.

The hacker, who goes by the name "Peace," was trying to sell the passwords on the dark web for 5 bitcoin, or about $2,200, according to a Forbes report.

Mountain View, California-based LinkedIn Corp., which touts 400 million members in 200 countries and territories around the world, emphasized that there's no indication of a new data breach.

The company said it's working to determine just how many of the passwords in question are still being used and is in the process of resetting them and notifying the users in question.

Cybersecurity experts say news like this should serve as a reminder that passwords should be changed frequently, ideally every few months. That way when compromised information surfaces months or years down the

road, such as in this case, users have little to worry about.

It's also a good idea to pick long and unique passwords that are harder to guess and to avoid using the same password for different online accounts. That way, a password stolen in the LinkedIn hack, for example, couldn't be used to compromise online banking, or other critical accounts.