
***Issued 8/9/17***

## 306 Million Passwords You Should Never Use

More than 1 billion compromised usernames and passwords are floating around on lists on the internet. That's bad news for anyone running an online service. Sooner or later, a hacker will use details on the lists to attempt to take over accounts. Unfortunately, a lack of user-friendly alternatives to usernames and passwords for authentication means nothing is going to change much soon.

Although two- factor authentication can block the recycling of known credentials, its use is still far from widespread. But Troy Hunt, a security expert who runs the Have I Been Pwned data breach notification service, has an idea to help organizations prevent people continuing to use their own compromised passwords or selecting ones that have been leaked. His effort is aimed at companies battling what's known as "credential stuffing. That's when hackers cycle through the lists trying to find combinations of credentials that unlock someone's account. Credential stuffing has been fueled over the last few years by large breaches at LinkedIn, MySpace, Dropbox and many more (see 'Historical Mega Breaches' Continue: Tumblr Hacked). Companies contact him nearly every other day saying they are getting "hammered" by use of the password lists, Hunt says.

While there are defensive actions services can take, there's ultimately no good defense against a hacker who has valid user credentials. "Credential stuffing is just becoming enormously destructive at the moment," Hunt says. "It is a very, very hard problem." Hunt has a

gigantic trove of usernames and passwords from dozens of data breaches. Have I Been Pwned allows someone to see if their email address has appeared in a breach, and if so, details which breach. But Hunt doesn't let people see the password that was used for the particular compromised service. He also doesn't allow people to see passwords or hashes of passwords en masse, for security reasons.