

# How to Check if Your Password/Username Has Been Stolen

Many websites have leaked passwords. Attackers can download databases of usernames and passwords and use them to “hack” your accounts. This is why you shouldn’t reuse passwords for important websites, because a leak by one site can give attackers everything they need to sign into other accounts.

## Why You Should Worry Whenever a Service’s Password Database Is Leaked

Troy Hunt’s *Have I Been Pwned* website maintains a database of username and password combinations from public leaks. These are taken from publicly available breaches that can be found via various sites on the web. This database just makes it easier to check them yourself without visiting the sketchier parts of the web.

To use this tool, head to the main **[Have I Been Pwned?](#)** page (this is a hyperlink) and search for a username or email address. The results tell you whether your username or email address has ever appeared in a leaked database. Repeat this process to check multiple email addresses or usernames. You’ll see which leaked password dumps your email address or username appears in, which in turn gives you information about passwords that might have been compromised.

If you want to get an email notification should your email address or username appear in a future leak, click the “Notify me when I get pwned” link.