

# How to check if your password has been compromised.

Privacy violations and password leaks are no longer uncommon issues for internet users today. So, how can you ensure your safety online and know if your password has been compromised? Let's find out in this article from TipsMake!

Privacy violations and password leaks have recently become hot topics on the internet. **LinkedIn** , **Yahoo** , and many other websites have been compromised. There are also numerous tools available to check if your passwords have been compromised. You can also protect yourself by setting unique passwords for each account.



Tips to check if your password has been compromised.

Leaked passwords can cause unforeseen dangers, especially since many people often use the same password for multiple accounts. If you register an account on a website using your email address and use the same password as your email, this email-password combination will be saved to a list of leaked email-passwords.

Hackers can then use this information to gain access to your email account. Even if you use a different password for your email, they can still use that username and password combination to access your other accounts.

For example, hackers recently compromised over 11,000 Guild Wars 2 accounts. They didn't use keyloggers , nor did they hack into the game's servers. They simply attempted to log in using email addresses and passwords they obtained from leaked password lists. When players reused the leaked passwords, their accounts were compromised. The same thing can happen on other websites.

To protect your passwords from being leaked, make sure you use a different password for each website – and that these passwords are long and strong enough. Otherwise, if one account is hacked, it's easy for attackers to

gain access to others. While websites will send you notifications whenever your password is leaked and ask you to change it immediately, this is useless if you use the same password for multiple accounts.

However, remembering all the passwords for multiple accounts is not easy, and this is where password managers like LastPass or KeePass come in handy .

### ***How to check if your password has been compromised.***

Using the **PwnedList** tool is one of the best ways currently available to check if your password has been compromised. LastPass now uses PwnedList to manage whether the email addresses used to register for their service have been leaked. For example, if your LastPass registration email address is **[email protected]** , you will receive a notification whenever [email protected] appears in a list of leaked email addresses and passwords. However, this feature only applies to the single email address you used to register your LastPass account.

If you want to check manually, you can visit the PwnedList website. Simply enter your email address, and PwnedList will tell you if it appears in any leaked lists. If your email address does appear somewhere, don't worry too much; it just means you shouldn't continue using the same password for multiple accounts and need to change it immediately.

LastPass also has several tools to help you check if a password is strong enough. You can enter the password to see if anyone is using it. The results will indicate the security of the password you are trying to set. For example, when you enter " **password123** ", you will see that at least one person is using it as their LinkedIn password.

Email accounts are the most important element of privacy when working online, and many websites only allow password changes by clicking a confirmation link sent to your email. If someone accesses your email account, then other accounts will certainly be compromised as well. Therefore, you should regularly change your email password to strong characters. If you use Gmail, you can refer to how to change your Gmail password here.

You finished reading the article "**How to check if your password has been compromised.**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.