

[Google Launches Password Checkup Extension to spy on all of your passwords](#)

[Google has announced](#) a new extension for Google Chrome called [Password Checkup](#) that will monitor the passwords that you type into websites to see if they have been compromised in a third-party data breach. Google says it has access to over 4 billion credentials that have been compromised and Password Checkup will issue a warning if it detects you using a credential that is known to be unsafe. Google worked with cryptography experts at Stanford University to incorporate protections that ensure your privacy is maintained by encrypting your credentials and making sure that they are never revealed to Google. The tool also has safeguards built-in to keep hackers from abusing it to reveal unsafe usernames and passwords. The Password Checkup extension will be improved over the coming months with better site compatibility and password field detection.

 [News Image](#)

At a high level, Password Checkup needs to query Google about the breach status of a username and password without revealing the information queried. At the same time, we need to ensure that no information about other unsafe usernames or passwords leaks in the process, and that brute force guessing is not an option. Password Checkup addresses all of these requirements by using multiple rounds of hashing, k-anonymity, private information retrieval, and a technique called blinding.