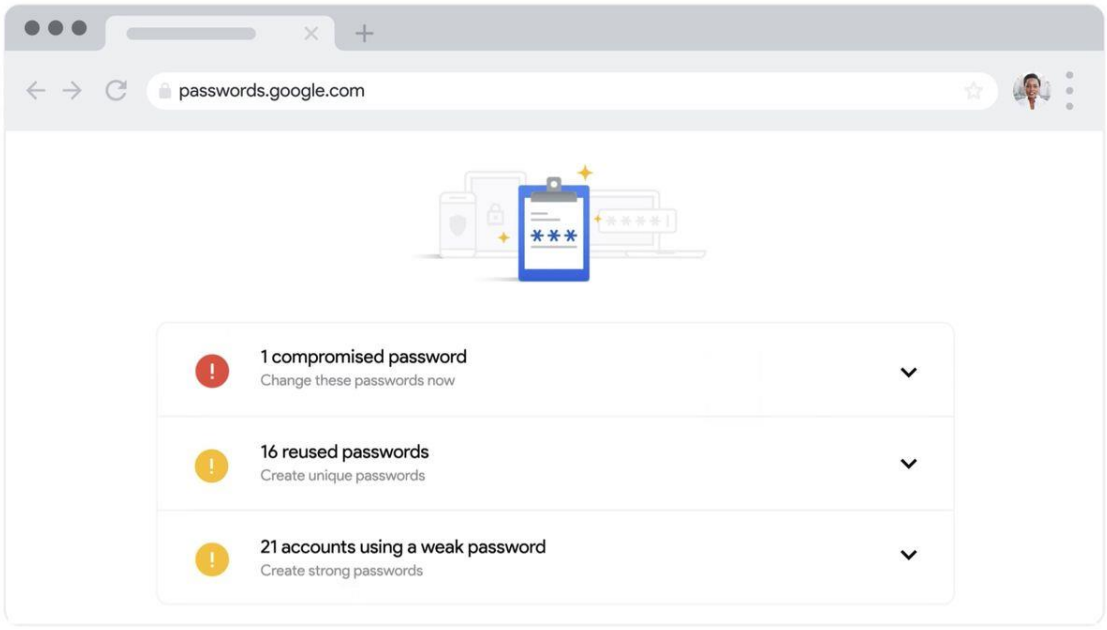
Google Password Checkup

Google has added Password Checkup, a feature that analyzes your logins to ensure they haven't been part of a security breach. Password checkup was already available as an extension, but now Google is building it right into Google account controls. Your login credentials are compared against millions of known compromised accounts that've been part of major breaches.



If your password has been included in a breach, Google will encourage you to change the affected password. Same goes if Google sees that you're reusing passwords, everything should have a unique login. Google will also notify you of accounts using weak passwords that are easy to guess.

Since Password Checkup relies on sending your confidential information to Google, the company is emphasizing that it is encrypted, and that it has no way of seeing your data. Passwords in the database are stored in a hashed and encrypted form, and any warning that's generated about your details is entirely local to your machine.

Password habits of people in the US revealed that too many are still including items that are easy to find out like a birthday or pet's name in their passwords. Password reuse is one of the things Google is trying to discourage, because using the same password for multiple services could put you in a terrible situation should one of them is compromised.

For security settings and recommendations to help keep your account secure, go to your Google Account and click on the Security tab. If you notice unfamiliar activity on your Google account, someone else might be using it without your permission. To help spot suspicious activity and make it more secure go to https://support.google.com/accounts/answer/6294825.

If you suspect your password has been compromised, report it to the IT Department at 925 606-3258 or email it-security@lvjusd.org and change your password immediately.