chrome enterprise

Mitigate data breaches and enterprise identity theft with Chrome Browser Password Alert

Introduction

How safe can your organization and your data be if a large percentage of your employees reuse their corporate password on other sites?

A 2019 Google/Harris Poll survey asked 3,000 adults if they reuse passwords and 65% of respondents indicated they either reuse passwords on multiple (but not all) accounts or reuse the exact same password *on all their accounts*.

Password reuse is still a common practice

52% Reuse the same password for multiple (but not all) accounts

35% Use a different password for all accounts

13% Reuse the same password for all their accounts

chrome enterprise

A hacker only needs to acquire *one employee's corporate password* to gain access to that individual's devices and your organization's network and data. Hackers have many ways to acquire passwords. The three most common methods used are brute force guessing, social engineering, and phishing.

What if Chrome Browser proactively prevented corporate password reuse from happening? That would be one more layer of protection for your organization and employees — and added peace of mind for you.

Chrome Browser Password Alert Policy

Chrome Browser Password Alert is a policy that helps enterprises avoid identity theft and employee and organizational data breaches by detecting when an employee enters their corporate credentials into any other website.

The Chrome Browser Password Alert policy extends these capabilities and provides extra security for enterprise accounts and data by protecting Google *and* non-Google credentials. It enables IT to manage Password Alert policies on all major OSes, including Chrome OS, Windows[1], Mac[2], and Linux.

Protecting your privacy

Google takes user privacy seriously. We only store a non-reversible fingerprint of the password on the disk. No one can see your user's credentials. **Credential data never leaves the local machine. It is never sent to Google or shared with other 3rd parties.** So rest assured, turning on Password Alert does not compromise your user privacy or security.

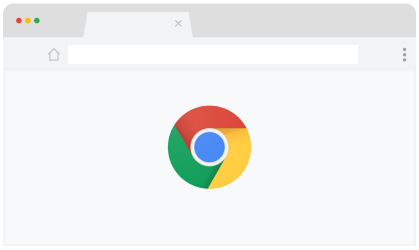
[1] Microsoft ®, Windows ®, and Internet Explorer ® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

[2] Mac and macOS are trademarks of Apple Inc., registered in the U.S. and other countries.

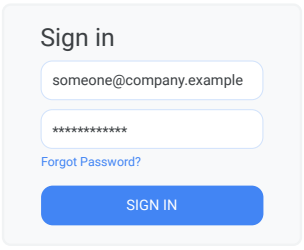
chrome enterprise

How Password Alert works

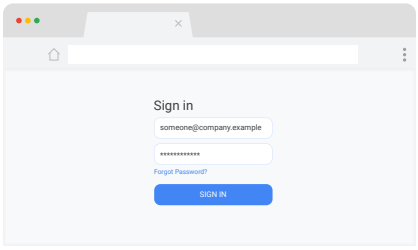
First, let's look at Password Alert from the end user's perspective.
Once IT has enabled Password Alert, the user's experience is seamless.



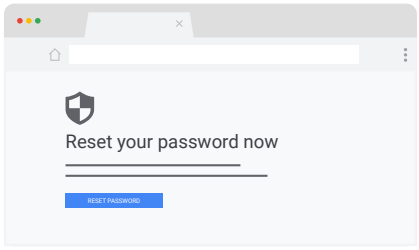
1. User opens Chrome Browser . . .



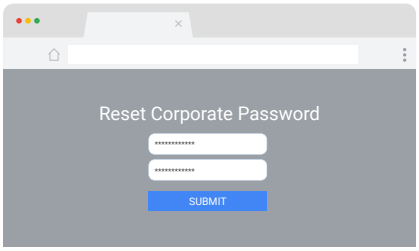
2. . . . signs in to enterprise network via your standard corporate login . . .



3. . . . navigates to a site and uses the same password (even with a different username).



4. Password Alert notifies the user they're using the same password. User can elect to . . .



5. . . . route to password reset page.

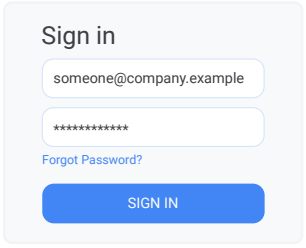
When a user reuses their corporate credentials on a non-corporate website, they are shown a warning and directed to the password change page where they have the option to change their password.

Here's what's happening on the backend, when Password Alert is enabled:

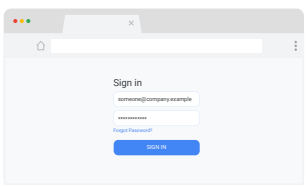
1. User signs in to enterprise network via your standard corporate login.

2. (Hidden to user) Without prompting the user, Password Alert captures and stores the password as a hash on the local machine.

3. User continues to work as usual.



1



3

You can configure Password Alert to operate in two modes.

Passive Monitoring Mode logs password reuse events onto the local filesystem or Windows Event Logger without showing warnings to the end user. This helps you gain insight into existing password reuse behavior inside your enterprise.

Active Detection Mode displays a warning to the user when they reuse their corporate credentials on non-corporate or phishing websites. These events can also be logged in the local filesystem or Windows Event Logger.

chrome enterprise

How to enable Password Alert

The Password Alert policy is included in Google's Enterprise templates. Across all operating systems, you can enable Password Alert in the Chrome Browser Cloud Management console. Additionally, you can also enable Password Alert via Group Policy in Microsoft environments.

Getting started with Chrome Browser Password Alert

Setting up Password Alert is straightforward for G Suite customers, G Suite customers with SSO and non G Suite customers. Password Alert policy can be enabled on any Chrome Enterprise browsers that are managed by GPO or cloud. Learn more about managing your Chrome Enterprise Browser in the cloud or via Group Policy. Visit the Chrome Browser Password Alert technical whitepaper to learn the in-depth steps for each configuration option.

Conclusion

Chrome Browser Password Alert adds yet another layer of security to protect your enterprise by warning users when they attempt to reuse their corporate password on phishing websites or non-approved sites. In today's hyper-connected world, where phishing and other types of attacks have become both commonplace and devastating, Password Alert is a must-have tool in your enterprise security toolkit.

Finally, to deepen your understanding of Chrome Browser Password Alerts, **consider the following resources:**

Watch the Password Alert Policy video

Read more on Chrome Browser Password Alert

If you have G Suite, read the G Suite admin help Phishing Prevention with Password Alert FAQ

Learn more about how you can prevent phishing attacks on your users

Chrome Browser downloads for your enterprise

Learn more about Chrome Browser Enterprise Support

Explore the Chrome Browser Policy List

Read the latest Chrome Browser Enterprise Release Notes

Stay up to date on the latest Chrome Browser release updates via the Chrome Releases Blog

Explore Google's official Safety & Security blog

Visit the Chrome Browser Enterprise Help Center and Chrome Browser Help Forum

Review the Chrome Browser Public Bug Tracker