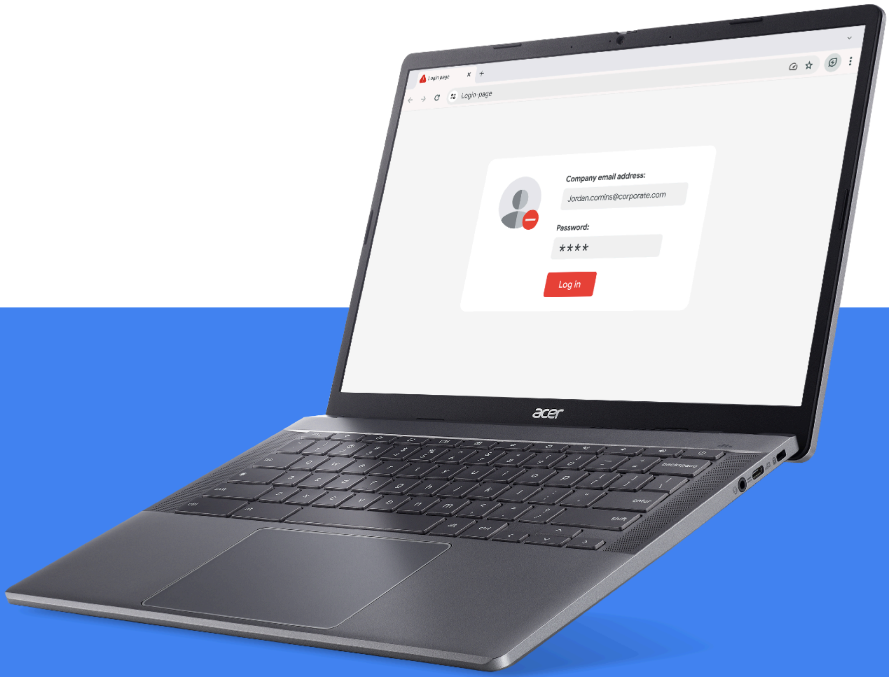
chrome enterprise

Mitigate Data Breaches and Enterprise Identity Theft with 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 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 are brute force guessing, social engineering, and phishing.

Chrome browser proactively prevents corporate password reuse, adding a layer of protection for your organization and employees.

Password Alert

Password Alert is a Chrome browser 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.

Password Alert protects both Google and non-Google credentials, and can be configured on all major operating systems, including ChromeOS, Windows, Mac, and Linux.

Protecting Your Privacy

Google takes user privacy seriously. Only a non-reversible fingerprint of the password is stored on the disk, and no one can see your credentials. Credential data never leaves the local machines and is never shared with Google or third parties. Rest assured, turning on Password Alert does not compromise your privacy or security.

How Password Alert Works

Once IT has enabled Password Alert, the user experience is seamless.

1. The user opens Chrome browser
2. The user signs into an enterprise network using a standard corporate login
3. Password Alert captures and stores the password as a hash on the local machine without prompting or alerting the user
4. The user navigates to a different login site and uses the same password with the same or a different username
5. Password Alert notifies the user they're using the same password and redirects them to the password reset page
6. The user changes their password, ensuring their corporate password remains unique

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 provides insight into existing password reuse behavior inside your enterprise.

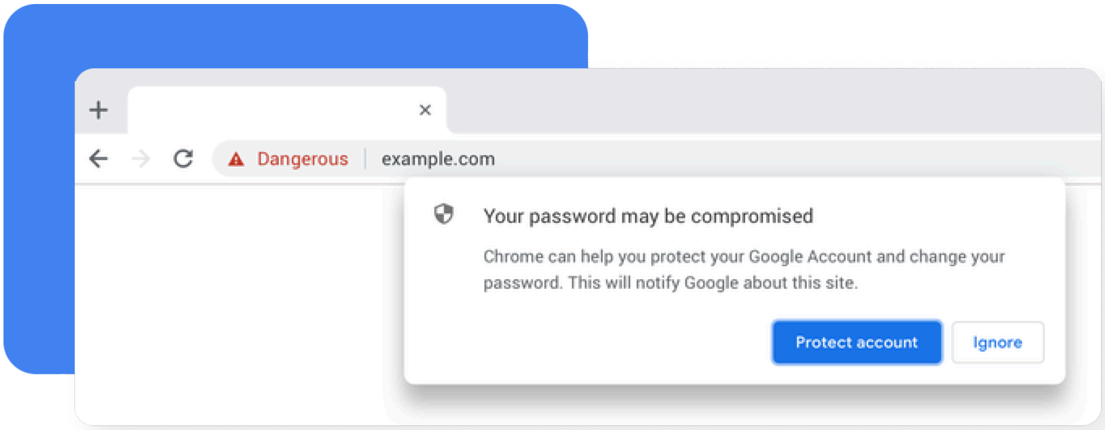
Active Detection Mode displays a warning to the user when they reuse their corporate credentials on non-corporate or phishing websites. These actions create events that can be reported via the Chrome Enterprise Connectors Framework to SIEM tools such as Chronicle, Splunk, and more to provide further insight into potential browser security events. To learn more, read this Chrome Enterprise and Education Help Center article.

How to Enable Password Alert

Password Alert is included in Google's Enterprise templates. You can enable Password Alert in Chrome's cloud management tool for all operating systems or via Group Policy for Microsoft environments. You can find the policies for Password Protection here.

Getting Started with Password Alert

Setting up Password Alert is straightforward for Google Workspace customers with and without SSO, as well as organizations that don't use Google Workspace. You can also enable Password Alert on any Chrome browsers that are managed using Chrome's cloud management tool or Group Policy.



Your password may be compromised

Chrome can help you protect your Google Account and change your password. This will notify Google about this site.

Conclusion

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.

To learn more about Password Alert, **consider the following resources:**

Watch the Password Alert video

Read more about monitoring and preventing password reuse

If you have Google Workspace, read the Phishing prevention with Password Alert FAQ

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

Download Chrome for your enterprise

Learn more about Chrome Enterprise support

Explore the Chrome Enterprise policy list

Read the latest Chrome Enterprise and Education release notes

Stay up to date on the latest Chrome Releases

Explore Google's official Safety & Security blog

Visit the Chrome Enterprise and Education Help Center and Google Chrome Help Community

Review the Chromium public bug tracker