chrome enterprise

Gegevenslekken en zakelijke identiteitsdiefstal voorkomen met Password Alert voor de Chrome-browser

Inleiding

Hoe veilig zijn je organisatie en gegevens als een groot deel van je werknemers hun bedrijfswachtwoord hergebruikt op andere sites?

In een onderzoek van Google/Harris Poll uit 2019 werden 3000 volwassenen gevraagd of ze hun wachtwoord hergebruiken. 65% van de respondenten gaf aan dat ze hun wachtwoord hergebruiken voor meerdere (maar niet alle) accounts of hetzelfde wachtwoord gebruiken *voor al hun accounts*.

Wachtwoorden worden nog steeds vaak hergebruikt

52% Hergebruikt hetzelfde wachtwoord voor meerdere (maar niet alle) accounts

35% Gebruikt een ander wachtwoord voor elk account

13% Hergebruikt hetzelfde wachtwoord voor alle accounts

chrome enterprise

Een hacker hoeft maar *het bedrijfswachtwoord van één werknemer* te achterhalen om toegang te krijgen tot de apparaten van die werknemer en het netwerk en de gegevens van je organisatie. Hackers kunnen wachtwoorden op veel manieren achterhalen. De 3 meest voorkomende methoden zijn wachtwoorden raden met speciale programma's (brute force guessing), social engineering en phishing.

Wat als de Chrome-browser ervoor zou zorgen dat gebruikers hun bedrijfswachtwoord niet hergebruiken?
Dan zou je nog een beveiligingslaag kunnen toevoegen voor je organisatie en werknemers en hoef jij je minder zorgen te maken.

Het Password Alert-beleid voor de Chrome-browser

Password Alert voor de Chrome-browser is een beleidsregel waarmee bedrijven identiteitsdiefstal en lekken van werknemers- en organisatiegegevens kunnen voorkomen door het te detecteren als werknemers hun zakelijke inloggegevens invoeren op een andere website.

Met het Password Alert-beleid voor de Chrome-browser krijg je niet alleen deze functie, maar nog meer beveiliging voor werkaccounts en -gegevens doordat inloggegevens van Google *en* inloggegevens die niet van Google zijn worden beschermd. Met dit beleid kan het IT-team Password Alert-beleid beheren in alle grote besturingssystemen, zoals ChromeOS, Windows[1], Mac[2] en Linux.

Je privacy beschermen

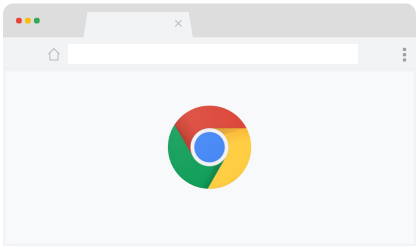
Google neemt de privacy van gebruikers erg serieus. We slaan alleen een onomkeerbare vingerafdruk van het wachtwoord op de schijf op. Niemand kan de inloggegevens van je gebruikers zien. **Inloggegevens verlaten het lokale apparaat nooit. Ze worden nooit naar Google gestuurd of gedeeld met andere externe partijen.** Als je Password Alert dus aanzet, heeft dit geen negatieve gevolgen voor de privacy of beveiliging van je gebruikers.

[1]Microsoft®, Windows® en Internet Explorer® zijn gedeponeerde handelsmerken van de Microsoft Corporation in de Verenigde Staten en/of andere landen.
[2]Mac en macOS zijn handelsmerken van Apple Inc., geregistreerd in de VS en andere landen.

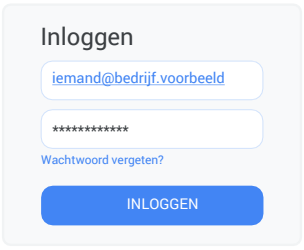
chrome enterprise

Hoe Password Alert werkt

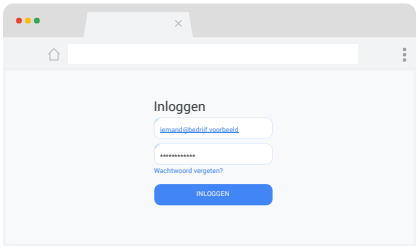
Laten we eerst eens kijken hoe Password Alert werkt vanuit het eindgebruikersperspectief. Nadat het IT-team Password Alert heeft aangezet, kunnen gebruikers gewoon efficiënt blijven werken.



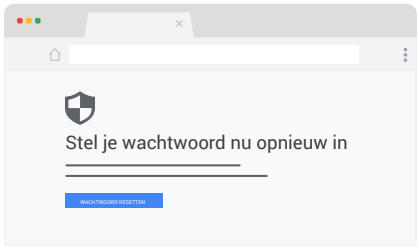
1. De gebruiker opent de Chrome-browser . . .



2. . . . logt in bij het bedrijfsnetwerk via je standaard bedrijfslogin . . .



3. . . . gaat naar een andere site en gebruikt hetzelfde wachtwoord (zelfs met een andere gebruikersnaam).



4. Password Alert laat gebruikers weten dat ze hetzelfde wachtwoord gebruiken. Gebruikers kunnen ervoor kiezen om . . .

5. . . . naar de pagina te gaan om hun wachtwoord te resetten.

Als gebruikers hun zakelijke inloggegevens hergebruiken op een website die niet van het bedrijf is, zien ze een waarschuwing en worden ze naar een pagina gestuurd waarop ze hun wachtwoord kunnen wijzigen.

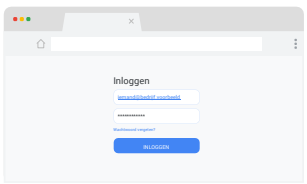
Dit gebeurt er in de backend als Password Alert aanstaat:

1. De gebruiker logt in bij het bedrijfsnetwerk via je standaard bedrijfslogin.

2. (Verborgen voor gebruiker) Zonder de gebruiker iets te laten zien, slaat Password Alert het wachtwoord op als hash op het lokale apparaat.

3. De gebruiker blijft werken zoals normaal.

1



3

Je kunt Password Alert instellen in 2 modussen.

Als in de **passieve controlemodus** een wachtwoord wordt hergebruikt, wordt deze gebeurtenis opgeslagen in het lokale bestandssysteem of in het Windows-gebeurtenislogboek zonder dat de eindgebruiker een waarschuwing te zien krijgt. Zo krijg je inzicht in bestaande instanties van wachtwoordhergebruik in je bedrijf.

Als een gebruiker in de **actieve detectiemodus** het bedrijfswachtwoord hergebruikt op een website die niet van het bedrijf is of een phishingwebsite, ziet deze een waarschuwing. Deze gebeurtenissen kunnen ook worden opgeslagen in het lokale bestandssysteem of het Windows-gebeurtenislogboek.

chrome enterprise

Password Alert aanzetten

Je vindt het Password Alert-beleid in de zakelijke templates van Google. In alle besturingssystemen kun je Password Alert aanzetten via de console voor Cloudbeheer voor de Chrome-browser. Je kunt Password Alert ook aanzetten via groepsbeleid in Microsoft-omgevingen.

Aan de slag met Password Alert voor de Chrome-browser

Google Workspace-klanten, Google Workspace-klanten met SSO en niet-Google Workspace-klanten kunnen Password Alert heel makkelijk instellen. Je kunt Password Alert-beleid aanzetten voor elke Chrome Enterprise-browser die je beheert via GPO of in de cloud. Bekijk hoe je de Chrome Enterprise-browser beheert in de cloud of via groepsbeleid. Bekijk de technische whitepaper over Password Alert in de Chrome-browser voor uitgebreide stappen voor elke configuratieoptie.

Conclusie

Met Password Alert voor de Chrome-browser wordt er nog een beveiligingslaag toegevoegd voor je bedrijf, doordat gebruikers een waarschuwing zien als ze proberen hun bedrijfswachtwoord te hergebruiken op phishingwebsites of sites die niet zijn goedgekeurd. De wereld is hyperverbonden. Phishing- en andere soorten aanvallen komen steeds vaker voor en richten veel schade aan. Daarom is Password Alert een must-have in je zakelijke beveiligingstoolkit.

Bekijk de volgende bronnen om nog beter te begrijpen hoe Password Alert voor de Chrome-browser werkt:

Bekijk de video over Password Alert-beleid

Lees meer over Password Alert voor de Chrome-browser

Als je Google Workspace gebruikt, lees je de beheerdershulp voor Google Workspace: Veelgestelde vragen over phishing voorkomen met Password Alert

Bekijk hoe je phishingaanvallen op je gebruikers voorkomt

Download de Chrome-browser voor je bedrijf

Bekijk meer informatie over Enterprise Support voor de Chrome-browser

Bekijk de lijst met beleid voor de Chrome-browser

Lees de nieuwste release-opmerkingen voor de zakelijke Chrome-browser

Blijf op de hoogte van de nieuwste release-updates van de Chrome-browser via de Chrome Releases-blog

Bekijk de officiële Safety & Security-blog van Google

Ga naar het Helpcentrum voor de zakelijke Chrome-browser en het Helpforum voor de Chrome-browser

Bekijk de openbare bugtracker voor de Chrome-browser