LastPass •••|

De psychologie van het wachtwoord

Slechte wachtwoordgewoontes van medewerkers die een risico vormen voor uw bedrijf

Verbeter de beveiliging en compliance, zonder extra complexiteit in uw processen

Privé en werk lopen meer door elkaar heen dan ooit. Daardoor is het voor de veiligheid van uw bedrijf (en misschien zelfs voor het voortbestaan) belangrijker dan ooit dat uw medewerkers goed omgaan met hun wachtwoorden. IT-teams moeten zich aanpassen om ervoor te zorgen dat de aanmeldingsgegevens van medewerkers veilig blijven – ook als ze thuiswerken (of vanuit een café met twijfelachtige wifi).

Dit rapport over de Psychologie van het Wachtwoord bekijkt het wachtwoordgedrag van 3750 professionals van over de hele wereld. De inzichten kunnen ook uw bedrijf helpen op verschillende punten:

- **Verhoog het veiligheidsbewustzijn** en verbeter de zorgvuldige omgang met wachtwoorden.
- **Ontdek de best practices om** hergebruik van wachtwoorden te voorkomen en wachtwoorden veilig op te slaan**.**
- **Bepaal doelen** voor volledig inzicht in de veiligheid, ook bij het werken op afstand.

LastPass Business neemt frustratie weg voor gebruikers en IT-teams, waardoor iedereen gewoon zijn werk kan doen. **Bespaar tijd door het wachtwoordbeheer voor medewerkers te vereenvoudigen en beheerders een werkbaar overzicht te bieden**, van geavanceerde rapportages tot meer dan 100 aanpasbare beleidsregels.

Ga voor meer informatie naar
LastPass.com/business

Wachtwoordbeveiliging in 2021: menselijke zwakheden overwinnen

Door de pandemie stonden overal ter wereld miljoenen werkplekken en werkroutines op hun kop. Kantoren gingen dicht. Waar mogelijk werkten mensen vanuit huis. En omdat ze nergens heen konden, schoot hun schermtijd omhoog: nog meer tijd online.

Hiermee schoten ook de risico's omhoog. Want ook cybercriminelen pasten zich razendsnel aan:
voor hen zette het massale thuiswerken deuren open, met meer kansen om menselijke zwakheden uit te buiten. Ze zetten andere soorten aanvallen in om misbruik te maken van een nieuwe digitale realiteit.

Volgens het toonaangevende Data Breach Investigations Report (DBIR) van 2021 hebben cybercriminelen het steeds meer gemunt op particulieren en hun apparaten.

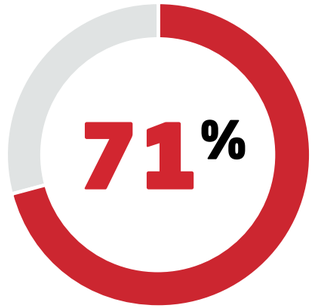
85%

De overgrote meerderheid van de gegevenslekken – niet minder dan 85% – is te herleiden tot menselijke factoren: phishing, gestolen aanmeldingsgegevens en menselijke fouten.

36%

36% van de lekken van vorig jaar kwam door phishing – een stijging van 11 procentpunt ten opzichte van vorig jaar.

Enkele statistieken uit de pandemie:



werkte geheel of gedeeltelijk op afstand.

besteedde meer tijd online voor entertainment en werk.

Overzicht van het onderzoek

In ons rapport over de Psychologie van het Wachtwoord gaan we in op de omgang met wachtwoorden van 3750 professionals verspreid over zeven landen. Hiervoor hebben we respondenten ondervraagd over hun doen & denken op het gebied van online veiligheid.

De landen in ons onderzoek:

- Verenigde Staten
- Verenigd Koninkrijk
- Duitsland
- Frankrijk
- Australië
- Singapore
- India

Veel bewustzijn, maar te weinig actie

Wat mensen zeggen.

79%
Vindt wachtwoordlekken een bron van zorg...

92%
geeft aan dat ze weten dat het een risico is om hetzelfde wachtwoord of varianten ervan te recyclen...

Wat mensen doen.

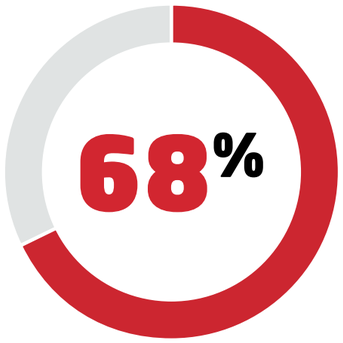
51%
... vertrouwt op hun geheugen om wachtwoorden te onthouden.

65%
...gebruikt altijd of meestal (variaties van) hetzelfde wachtwoord.

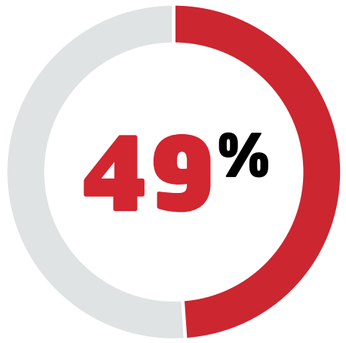
45% HEEFT HUN WACHTWOORDEN NIET GEWIJZIGD

45% van de respondenten heeft hun wachtwoorden niet gewijzigd in het afgelopen jaar, zelfs niet na een beveiligingslek.

Mensen zijn selectief met hun wachtwoordbeveiliging, maar ze zouden sterkere wachtwoorden aanmaken voor:

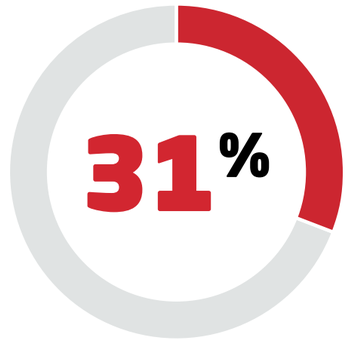


Financiële accounts



E-mailaccounts

Werkgerelateerde accounts



Medische dossiers

8%

Voor slechts 8% mag een sterk wachtwoord niet gebaseerd zijn op persoonlijke gegevens.

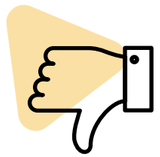
Dat betekent dat de overgrote meerderheid wachtwoorden aanmaakt die gebruik maken van persoonlijke gegevens als verjaardagen of adressen, die mogelijk openbaar beschikbaar zijn.

ONZE TIP:

Dwing het gebruik van onzinnige zinnetjes af, met veel cijfers en symbolen in plaats van afzonderlijke, samenhangende woorden. Zo worden wachtwoorden langer en sterker om hackers tegen te gaan, maar kunne medewerkers ze nog steeds onthouden.

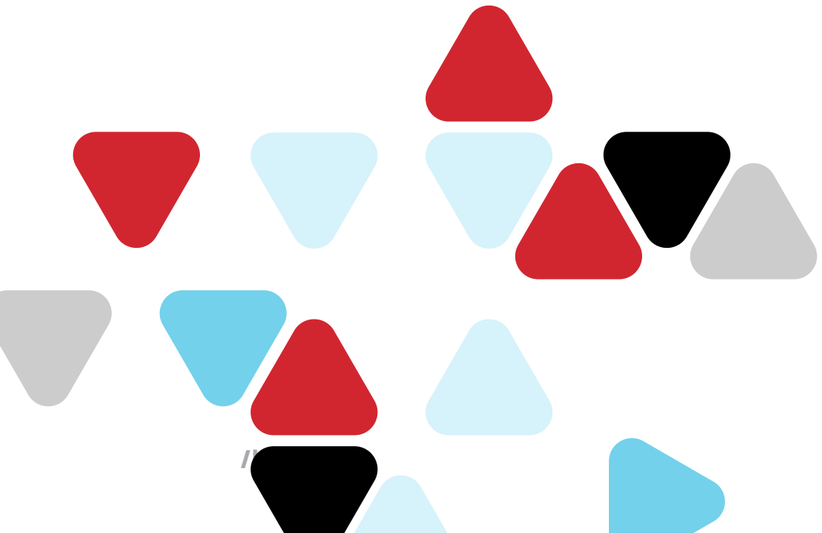
Blinde vlekken en redenen tot optimisme

Cognitieve dissonantie viert hoogtij. Mensen zijn kieskeurig en doen alleen moeite voor de beveiliging van accounts die ze belangrijk genoeg achten. Het gevolg: ze gaan bewust riskant om met wachtwoorden, zelfs nu ze ongeëvenaard veel tijd online zijn voor werk en entertainment.



83% zou niet weten of hun gegevens beschikbaar zijn op het dark web.

76% zegt gebruik te maken van meervoudige verificatie voor persoonlijke en professionele accounts, een stijging van 10% ten opzichte van vorig jaar.



ONZE TIP:

Beschouw alle accounts en aanmeldingsgegevens als belangrijk en kwetsbaar. Misschien denken uw medewerkers dat het account van hun lokale fitnessstudio niet de moeite waard is voor hackers. Maar als hun wachtwoord hiervoor lijkt op de wachtwoorden die ze gebruiken voor professionele accounts, kan een gegevenslek bij de fitnessstudio ook uw gevoelige financiële gegevens in gevaar brengen.

Uitbreiding van het digitale leven

Meer accounts dan ooit.

91% van de respondenten heeft het afgelopen jaar minstens één nieuw account aangemaakt.

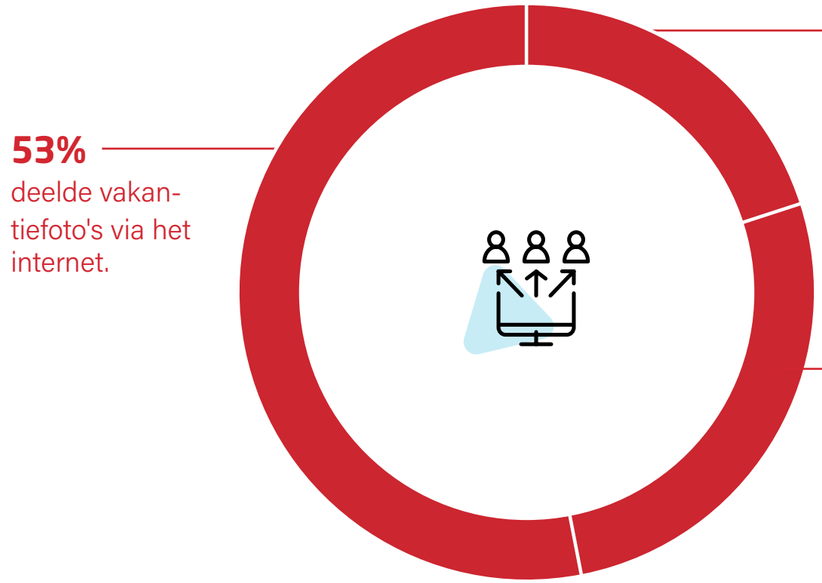
90% van de respondenten geeft aan dat ze tot 50 online of app-accounts hebben.

50% Respondenten hebben in 2021 ongeveer 50% meer accounts dan in 2020.

Nu we steeds meer online doen, hebben medewerkers en bedrijven betere bescherming nodig.

Door de pandemie zijn onze digitale levens sterk gegroeid. De afstand in het dagelijks leven zorgde voor meer verlangen naar verbinding online. Het aantal online accounts explodeerde dan ook – waardoor ook steeds meer persoonlijke informatie online gedeeld werd.

De hoeveelheid persoonlijke gegevens online neemt toe:



53%
deelde vakantiefoto's via het internet.

20%
deelde foto's van huisdieren – met namen, die ze ook verwerken in hun wachtwoorden. **Dit is een stijging van 5% ten opzichte van 2020.**

27%
deelde foto's van hun huis of buurt, **7% meer dan in 2020.**

ONZE TIP:

Cybercriminelen analyseren profielen en gebruiken ogenschijnlijk onschuldige gegevens om accounts buiten uw social media te hacken. Moedig medewerkers aan om hun persoonlijke updates en social media privé te houden.

Werken op afstand: perspectieven van werkgevers en werknemers

Gewoontes van medewerkers bij het werken op afstand:

47% heeft gewoontes voor online veiligheid niet veranderd sinds de overstap naar werken op afstand.

46% gebruikt geen sterkere wachtwoorden voor het werken op afstand.

44% heeft gevoelige gegevens en wachtwoorden voor zakelijke accounts gedeeld tijdens het werken op afstand.

Gewoontes van werkgevers bij het werken op afstand:

39% heeft ervoor gezorgd dat medewerkers bij het werken op afstand een veilig netwerk gebruiken voor hun aanmelding bij het bedrijfsnetwerk.

35% heeft afgedwongen dat medewerkers hun wachtwoorden vaker wijzigen.

35% heeft verificatiemethoden uitgebreid.

Er wordt veel gevraagd van IT-beheerders. Het feit dat er risico's zijn, betekent niet dat mensen automatisch gemotiveerd zijn om veiliger te werken. Bijna de helft van de medewerkers gaat niet goed om met wachtwoorden bij het werken op afstand.

Medewerkers werken anders - en dat vraagt om nieuwe beveiligingsstrategieën van IT-beheerders.

ONZE TIP:

Investeer in een goede **zakelijke wachtwoordbeheerder** om de wachtwoordgewoontes te verbeteren en de beveiliging te versterken. Werk met **SSO** en **MFA** om alle toegangspunten te beveiligen. Organiseert trainingen om het bewustzijn bij medewerkers te verhogen.

Regionale verschillen:

Verenigd Koninkrijk

61% weet dat een sterk en uniek wachtwoord niet op persoonlijke informatie gebaseerd mag zijn.

De Britten waren ook het minst geneigd om persoonlijke informatie online te plaatsen **(41%).**

Duitsland

In Duitsland is de kennis van het dark web het hoogste **(79%).**

Slechts **14%** zou echter weten of hun eigen persoonlijke gegevens op het dark web te vinden zijn.

Frankrijk

Slechts **15%** van de Franse respondenten werkte tijdens de pandemie op afstand.

En slechts **43%** veranderde hiervoor zijn veiligheidsgewoontes.

Singapore

In Singapore maken mensen zich het meeste zorgen over wachtwoordlekken **(93%).**

Ze weten ook beter dan anderen wat ze moeten doen als ze worden gehackt **(74%).**

India

Indiërs maken significant vaker dan anderen gebruik van een wachtwoordbeheerder of browser om wachtwoorden op te slaan **(64%).**

Respondenten uit India liepen ook voorop bij het aannemen van andere digitale veiligheidsgewoontes voor het werken op afstand **(81%).**

Australië

71% van de Australiërs gebruikt meestal of zelfs altijd hetzelfde wachtwoord of een variatie erop.

Over het geheel genomen besteedden Australiërs tijdens de pandemie echter minder tijd online **(61%).**

Verenigde Staten

Amerikanen waren meer geneigd om kredietmonitoring in te zetten als een account gehackt was **(31%).**

39% zag geen noodzaak om online veiligheidsgewoontes bij te stellen voor het werken op afstand – die waren al in orde.

Verbanden leggen

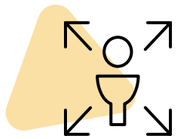
Waarom gaan mensen onveilig om met hun wachtwoorden, als ze duidelijk weten hoe het eigenlijk moet?

68% van de mensen die wachtwoorden hergebruikt, is bang om ze te vergeten.

52% van de hergebruikers willen de controle houden over al hun wachtwoorden.

36% beschouwt hun accounts niet als waardevol genoeg voor hackers.

Hergebruik van wachtwoorden brengt enorme risico's met zich mee, zeker nu we steeds meer online doen. Maar waarom eigenlijk?



Als mensen dezelfde aanmeldingsgegevens gebruiken voor verschillende accounts, komen hackers na één lek direct overal binnen.

Als cybercriminelen toegang krijgen tot een apparaat dat zowel zakelijk als privé gebruikt wordt, komen ze snel binnen op bedrijfsnetwerken om gegevens of geld te stelen.

MENSEN HANTEREN SLECHTE WACHTWOORDGEWOONTES

Meer en meer online. Te weinig hulp met cyberbeveiliging. Vastgeroeste gewoontes en emoties. En geen gevoel van dringende noodzaak. Het zijn allemaal factoren die mensen weerhouden van verbetering.

Tegengaan van slechte wachtwoordgewoontes

De manier waarop we werken en contact maken met anderen staat sinds de pandemie grondig op zijn kop. We doen meer online. We delen meer digitaal. Als we de oorzaak van onveilig gedrag kennen, hoe kunnen we het dan tegengaan?

Hoe ziet een veilige omgang met wachtwoorden eruit?

- Maak ieder wachtwoord uniek.
- Gebruik onzinnige combinaties van tekens.
- Schakel meervoudige verificatie in.
- Werk wachtwoorden bij na een lek.

Ga de angst te lijf.

Gebruik een **wachtwoordbeheerder** om wachtwoorden te beheren en te beveiligen. Laat veilige software wachtwoorden aanmaken, onthouden en invullen.

Ga zorgen te lijf.

Voeg een extra beveiligingslaag toe met **meervoudige verificatie (MFA)** om ervoor te zorgen dat alleen uw medewerkers toegang hebben tot zakelijke gegevens en toepassingen.

Kom in actie.

Monitor uw gegevens en zorg ervoor dat u gewaarschuwd wordt als er gegevens zijn stolen, met **monitoring van het dark web**.

LastPass •••|

LastPass Business helpt om frustraties rondom wachtwoordgebruik weg te nemen bij medewerkers. En voor uw IT-afdeling biedt het inzicht en controle, met eenvoudig beheer en moeiteloos gebruik.

Met LastPass Business kunnen medewerkers gemakkelijk wachtwoorden genereren, beveiligen en delen, robuust beveiligd door de LastPass-infrastructuur voor cyber-beveiliging op basis van het zero-knowledge principe.

Meer informatie