LastPass •••|

Psicología de las contraseñas

Las malas prácticas de los empleados que ponen en riesgo su negocio

Aumente la seguridad y el cumplimiento sin añadir trabas

Las vidas profesionales y personales se están fundiendo a una velocidad sin precedentes, por lo que resulta fundamental seguir buenas prácticas con las contraseñas para garantizar el éxito y la seguridad de su empresa. Los equipos de TI deben adaptarse para asegurarse de que las credenciales de los empleados sigan protegidas con independencia del lugar donde trabajen.

El informe "Psicología de las contraseñas" analiza las conductas con respecto a las contraseñas de 3750 profesionales de todo el mundo para ayudar a su negocio a:

- **Tener más presente la seguridad** y mejorar la protección de las contraseñas.
- **Adoptar buenas prácticas** para acabar con la reutilización de contraseñas y guardarlas de forma segura.
- **Establecer objetivos** para tener mayor cuidado con las contraseñas en el contexto del teletrabajo.

LastPass Business ayuda a los empleados porque elimina los problemas para los usuarios y los equipos de TI. **Ahorre tiempo simplificando la gestión de contraseñas de los empleados mientras proporciona una visualización práctica para los administradores** que incluye informes avanzados y más de cien políticas de seguridad personalizables.

Consulte más información en
lastpass.com/business

Seguridad de las contraseñas en 2021: cómo superar las vulnerabilidades humanas

La pandemia por COVID-19 ha afectado a millones de lugares de trabajo en todo el mundo. Muchas oficinas han echado el cierre. Multitud de personas ahora teletrabajan. Y al no poder salir, pasan más tiempo en internet.

Las personas y las empresas están más en peligro que nunca.
Los hackers están aprovechando las vulnerabilidades humanas. El tipo de ataques ha cambiado debido al gran número de personas que teletrabajan y pasan más tiempo en internet.

Según el informe Data Breach Investigations Report (DBIR), las personas y sus dispositivos están cada vez más en el punto de mira de los ciberdelincuentes.

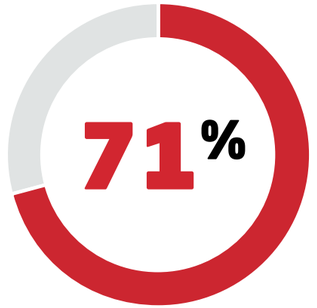
85%

Detrás de la mayoría de filtraciones de datos (un abrumador 85%) está el factor humano (phising, credenciales robadas o errores humanos).

36%

En el último año, el phishing estuvo presente en el 36% de las vulnerabilidades, lo que representa un aumento del 11%.

Durante la pandemia:



trabajó a distancia siempre o casi siempre.

dedicó más tiempo al ocio personal y al trabajo en internet.

Resumen de la encuesta

Este informe ha analizado el comportamiento en cuanto a las contraseñas de 3.750 profesionales en siete países. Los encuestados han compartido sus opiniones y su actitud con respecto a la seguridad online.

Países de la encuesta:

- Estados Unidos
- Reino Unido
- Alemania
- Francia
- Australia
- Singapur
- India

Hay conciencia, pero falta iniciativa

Qué dicen

79%
Coinciden en que la filtración de contraseñas les preocupa...

92%
Saben que usar la misma contraseña o una variante supone un riesgo...

Qué hacen

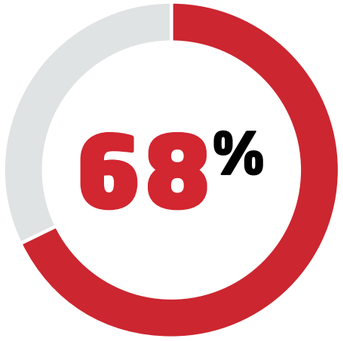
51%
... Confían en su capacidad de memoria para recordar las contraseñas.

65%
... Siempre o casi siempre usan la misma contraseña o una variante.

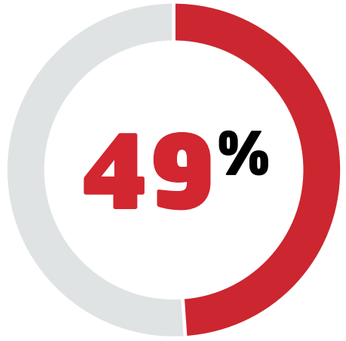
EL 45% NO HA CAMBIADO SUS CONTRASEÑAS

El 45% de los encuestados no ha cambiado sus contraseñas en el último año, ni siquiera después de una vulnerabilidad.

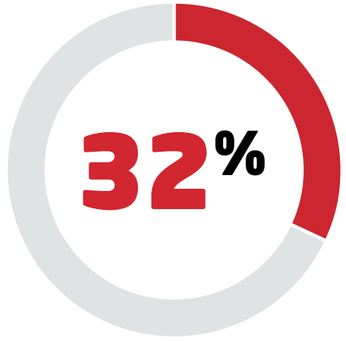
Los usuarios toman solo algunas medidas de seguridad, pero crean contraseñas seguras para:



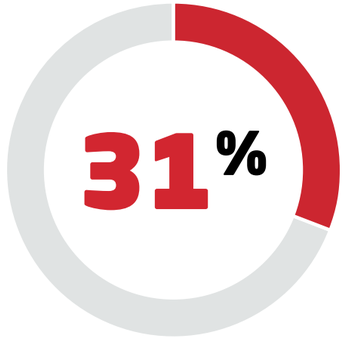
Cuentas financieras



Cuentas de e-mail



Cuentas relacionadas con el trabajo



Historiales médicos

8%

Solo el 8% cree que las contraseñas seguras deben estar desvinculadas de la información personal.

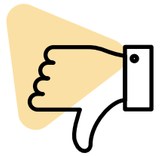
Esto significa que la mayoría de los usuarios crea contraseñas a partir de información personal que podría ser pública, como su fecha de nacimiento o su dirección.

NUESTRO CONSEJO

Obligue a usar frases sin sentido con distintos números y símbolos en lugar de palabras concretas. De esta forma, las contraseñas de sus empleados serán más largas, seguras y fáciles de recordar, al tiempo que resultan más difíciles de descifrar.

Puntos a favor y en contra

Prevalece la disonancia cognitiva. Los usuarios eligen la información que merece la pena proteger según su criterio. Por tanto, toman decisiones arriesgadas con respecto a sus contraseñas a sabiendas, incluso ahora que pasan más tiempo en internet con fines laborales y personales a raíz de la pandemia.



El **83%** no sabe si su información se ha hackeado.

El **76%** dice usar la autenticación multi-factor (MFA) en su vida personal y laboral, un 10% más que el año pasado.

NUESTRO CONSEJO

Trate todas sus credenciales con la misma precaución. Los empleados quizá piensen que sus credenciales del gimnasio no tienen ningún interés para los hackers, pero si son idénticas a las credenciales del trabajo y hay un incidente de seguridad en su gimnasio, su información financiera también quedará expuesta.

Vida digital en expansión

Existen más cuentas que nunca.

El **91% de los encuestados** ha creado al menos una cuenta nueva este año.

El **90% de los encuestados** dice que tiene hasta 50 cuentas en internet o aplicaciones.

50% Los encuestados tienen un 50% más de cuentas en 2021 que el año anterior.

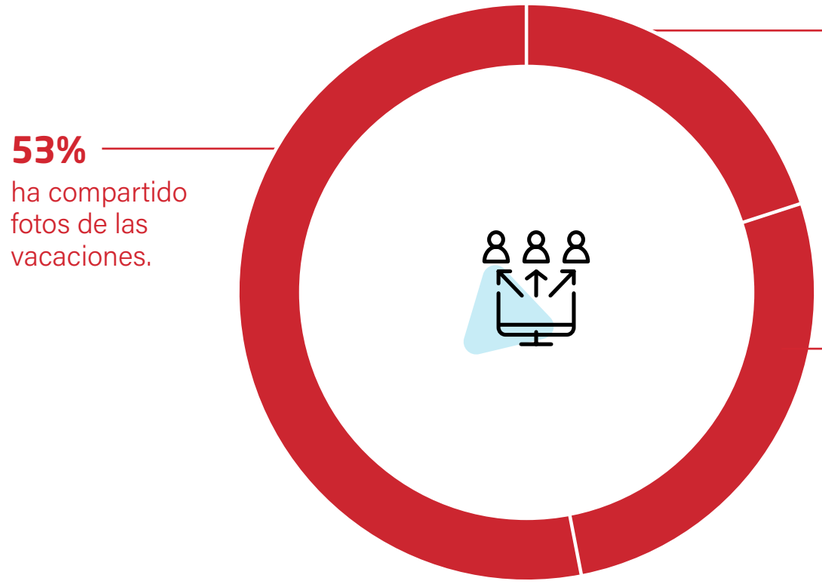
Tanto los empleados como las empresas deberán aumentar el nivel de protección a medida que aumente su presencia digital.

Nuestra vida digital ha aumentado considerablemente durante la pandemia por COVID-19. Perder nuestras rutinas nos ha llevado a conectarnos más que nunca. ¿El resultado? Hemos creado más cuentas y compartimos más información personal online.

NUESTRO CONSEJO

Los hackers pueden extraer datos de los perfiles públicos y usar información aparentemente inofensiva para acceder a otras cuentas más allá de sus redes sociales. Anime a los empleados a no compartir contenido digital ni novedades personales.

La cantidad de información personal online va en aumento:



53%
ha compartido fotos de las vacaciones.

20%
ha compartido fotos de sus mascotas junto a sus nombres y luego ha usado esos nombres en contraseñas **hasta un 5% más con respecto a 2020.**

27%
ha compartido fotos de su casa y su vecindario, **hasta un 7% con respecto a 2020.**

El teletrabajo desde el punto de vista del empleado y de la empresa

¿Cuáles son los hábitos de teletrabajo de los empleados?

47% No han cambiado sus hábitos de seguridad online desde que trabajan a distancia.

46% No han reforzado sus contraseñas desde que trabajan a distancia.

44% Comparten contraseñas e información confidencial con cuentas profesionales.

¿Cuáles son los hábitos de teletrabajo de las empresas?

39% Se aseguran de que los empleados accedan a la red de la empresa de forma segura.

35% Obligan a los empleados a cambiar sus contraseñas con más frecuencia.

35% Han mejorado los métodos de autenticación.

Los administradores de TI deben prestar atención. Los riesgos por sí mismos no animan a las personas a reforzar la seguridad. La mitad de los empleados actúa de forma irresponsable con las contraseñas al trabajar a distancia.

Los administradores de TI deben replantearse sus estrategias de seguridad a medida que los empleados cambian su manera de trabajar.

NUESTRO CONSEJO

Invierta en una solución de **gestión de contraseñas** para mejorar la seguridad y los hábitos. Adopte el **inicio de sesión único (SSO)** y la **autenticación multifactor (MFA)** para proteger todos los puntos de acceso. Imparta formación de seguridad.

Panorámica regional:

Reino Unido

El **61%** sabe que las contraseñas únicas y complejas no deben incluir información personal.

También son los menos propensos a compartir información personal online **(41%).**

Alemania

Alemania lidera la clasificación en cuanto al conocimiento de la Dark Web **(79%).**

Solo el **14%** sabe si su información personal se ha hackeado.

Francia

Solo el **15%** de los encuestados franceses ha tele-trabajado durante la pandemia.

Solo el **43%** ha cambiado sus hábitos de seguridad online al trabajar a distancia.

Singapur

Singapur es el país que más se preocupa por las contraseñas en riesgo **(93%).**

También encabezan la lista en cuanto a saber si les han hackeado **(74%).**

India

En la India hay muchas más probabilidades de usar un gestor de contraseñas o un navegador para almacenar contraseñas que en otros países **(64%).**

Los encuestados indios están a la cabeza en lo que respecta a cambiar los hábitos de seguridad online al teletrabajar **(81%).**

Australia

El **71%** de los australianos usa siempre o casi siempre la misma contraseña.

Sin embargo, en general, los australianos han pasado menos tiempo en internet durante la pandemia **(61%).**

Estados Unidos

Los estadounidenses tienen más probabilidades de usar servicios de control de crédito si su cuenta ha estado en riesgo **(31%).**

Sin embargo, el **39%** cree que no hace falta cambiar sus hábitos de seguridad online al teletrabajar porque ya son adecuados.

Todo encaja

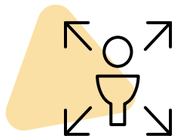
¿Por qué los usuarios tienen malas costumbres con las contraseñas si son conscientes de ello?

68% de los usuarios que reutilizan sus contraseñas temen no acordarse de ellas.

52% de los usuarios que reutilizan sus contraseñas quieren tenerlas bajo control.

36% de los usuarios no considera que sus cuentas tengan tanto valor para los hackers.

¿Por qué es tan arriesgado reutilizar contraseñas, sobre todo ahora que hacemos más vida digital?



Con solo hackear el nombre de usuario y la contraseña de una cuenta, los ciberdelincuentes tienen acceso a otras muchas.

Cuando un ciberdelincuente accede a un dispositivo que se utiliza para fines personales y laborales, tiene la llave a una red corporativa donde robar datos o dinero.

LAS PERSONAS TIENEN MALAS COSTUMBRES CON LAS CONTRASEÑAS

Vidas digitales en constante expansión, falta de asistencia en cuanto a ciberseguridad, una combinación de hábitos, emociones y falta de urgencia... Todos estos factores impiden que los usuarios cambien su comportamiento en internet.

Cómo corregir las malas costumbres

La pandemia por COVID-19 ha producido un cambio sin precedentes en nuestra forma de trabajar y relacionarnos. Pasamos más tiempo en internet. Compartimos más contenido. Ya sabemos por qué las personas tienen esta actitud frente a las contraseñas, pero ¿cómo podemos evitarla?

¿Cuáles son las mejores prácticas en cuanto a las contraseñas?

- Use contraseñas únicas para cada caso.
- Recurra a combinaciones de caracteres sin sentido.
- Active la autenticación multifactor.
- Cambie la contraseña si ha habido una vulnerabilidad.

Combata el miedo.

Use un **gestor de contraseñas** para administrar y proteger sus claves de acceso. Esta herramienta se encargará de crear, recordar y rellenar las contraseñas.

Combata la ansiedad.

Añada otro nivel de seguridad con la **autenticación multifactor (MFA)** para asegurarse de que solo sus empleados tengan acceso a la información.

Combata la apatía.

Tenga los datos bajo control y compruebe **si los han hackeado.**

LastPass

LastPass Business ayuda a minimizar las molestias para los empleados y, a la vez, mejorar el control y la visibilidad para los equipos de TI, de la mano de una solución de gestión de contraseñas fácil de administrar y todavía más fácil de usar.

LastPass Business permite a los empleados generar, proteger y compartir credenciales de forma sencilla y, a la vez, ofrece toda la protección de la infraestructura de seguridad de conocimiento cero de LastPass.

Más información