



La ciberdelincuencia crece exponencialmente en todo el mundo y a las empresas les está costando muy caro.

Aquí explicamos cómo afecta esta preocupante tendencia a las empresas y por qué son tan importantes las llaves de acceso en la lucha contra los ciberdelitos.

¿Qué son los ciberdelitos?

Un ciberdelito es cualquier actividad delictiva que se lleva a cabo usando un ordenador, un dispositivo de red o una red.

El **95%** de los delitos tienen un objetivo económico.¹

Los ataques con ingeniería social, ransomware y por fuerza bruta se cuentan entre los tipos de ciberdelitos más habituales.



¿Por qué crece tanto la ciberdelincuencia?

El **62%** de los usuarios siempre o casi siempre usan la misma contraseña o una variante.²

Si un ciberdelincuente consigue descifrar una contraseña, puede servirle para acceder a otras cuentas profesionales.

El **74%** de los robos de datos tienen un componente humano, como credenciales expuestas.³



El coste de un ciberdelito

El coste medio de un robo de datos se situó en 2023 en **4,45 millones de USD**, un récord absoluto.⁴

Por desgracia, muchas empresas no tienen ni idea de qué ocurre cuándo se están produciendo estos ataques.

El **67%** de los ataques fueron revelados por un tercero con buenas intenciones o por los propios delincuentes.⁴



Llaves de acceso: Una forma más segura de iniciar sesión

Una llave de acceso está formada por un par de claves criptográficas:

- Una clave pública (compartida con el sitio web de la parte de confianza)
- Una clave privada (guardada directamente en el dispositivo del usuario)

Las dos claves son imprescindibles para que un usuario pueda autenticarse e iniciar sesión en una cuenta protegida con una llave de acceso.



A diferencia de una contraseña, la llave de acceso es única para cada sitio o aplicación, por lo que es muy difícil para un ciberdelincuente conseguir una llave de acceso o conectarse a la cuenta de un empleado.

Las llaves de acceso pueden proteger su empresa de los ciberdelitos.

Las llaves de acceso refuerzan la seguridad online y simplifican todo el proceso de inicio de sesión (no se necesita contraseña).



Con las llaves de acceso, las empresas pueden cerrar la puerta a los atacantes oportunistas, porque les resulta mucho más complicado meterse donde no les corresponde.

Para las empresas, todo son ventajas.

Fuentes:

1. 2023 Verizon Data Breach Investigations Report
2. Informe de psicología de las contraseñas 2022
3. 2023 Verizon Data Breach Investigations Report
4. Informe sobre el coste de un robo de datos, 2023



Más información

LastPass ayuda a las empresas a mejorar la seguridad de sus contraseñas, en todas partes.