

El peligro de repetir contraseñas en internet

El uso repetido de contraseñas es uno de los mayores riesgos de seguridad en línea, según advierte la compañía **ESET**.

Este hábito facilita los ataques de «**credential stuffing**», donde ciberdelincuentes aprovechan una contraseña filtrada en una plataforma para acceder a otras cuentas del mismo usuario, como redes sociales, bancos o servicios de streaming.

Estos ataques se aprovechan de que los usuarios reutilizan sus credenciales en múltiples servicios. Si una contraseña se filtra, los atacantes usan bots automatizados para probarla en miles de sitios, logrando acceder a cuentas de forma sigilosa sin ser detectados por intentos de acceso fallidos.

Casos que demuestran la magnitud del problema

El impacto del *credential stuffing* es masivo. ESET cita casos recientes que demuestran el alcance de esta amenaza:

- **PayPal:** En 2022, un ataque comprometió miles de cuentas, exponiendo datos personales como nombres, direcciones y números de identificación.
- **Snowflake:** En 2024, más de 165 organizaciones se vieron afectadas cuando atacantes usaron credenciales robadas para acceder a cuentas de clientes, aprovechando la falta de **autenticación multifactor**.

«Repetir contraseñas es como usar la misma llave para abrir la casa, el auto y la caja fuerte», explica **Camilo Gutiérrez Amaya**, jefe del Laboratorio de Investigación de ESET Latinoamérica. «Hábitos simples pueden marcar la diferencia».

¿Cómo protegerte de este tipo de ataques?

Para evitar ser víctima del *credential stuffing*, los expertos de ESET recomiendan:

- **No reutilices contraseñas:** Usa una contraseña única y robusta para cada cuenta.
- **Usa un gestor de contraseñas:** Esta herramienta almacena tus claves de forma segura y puede generar contraseñas complejas automáticamente.
- **Activa la autenticación de dos factores (2FA):** Este paso

de seguridad adicional es crucial, ya que incluso si tu contraseña es robada, el atacante no podrá acceder a tu cuenta sin el segundo factor de autenticación.

- **Verifica tus credenciales filtradas:** Utiliza sitios web de confianza para comprobar si tus contraseñas ya han sido expuestas en alguna filtración y cámbialas de inmediato.

Con información de ***Banca y negocios***