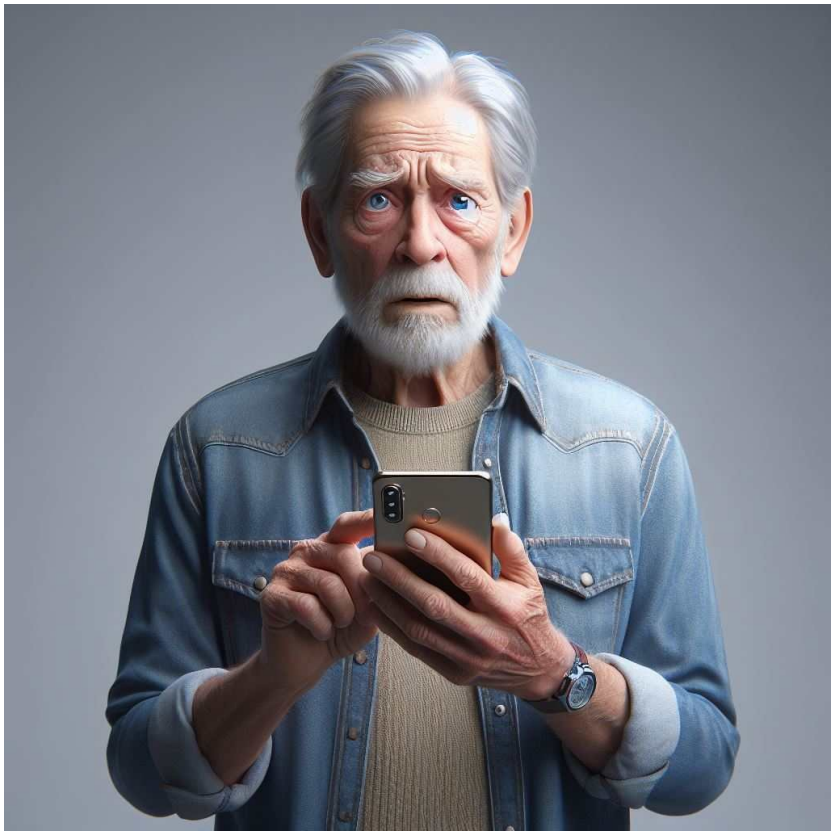
Millones de cuentas al desnudo: el reality show sin consentimiento de tus contraseñas

En la era en que una selfie vale más que mil palabras y una contraseña mal elegida puede arruinar una vida entera, mayo de 2025 nos trajo un recordatorio brutal: la privacidad es una especie en extinción. Un hallazgo reciente destapó una base de datos sin protección con más de **184 millones de credenciales** robadas de servicios como Facebook, Instagram, Gmail, Microsoft, Snapchat y hasta Roblox. Sí, incluso los universos digitales de tus hijos no están a salvo.

ALCANCE GEOGRÁFICO	MUNDIAL
N.º DE REGISTROS /CANTIDAD DE DATOS	184.162.718 / 47,42 GB
TIPO DE DATOS EXPUESTOS	CORREOS ELECTRÓNICOS, NOMBRES DE CUENTA, CONTRASEÑAS Y URLS DE AUTORIZACIÓN
RIESGOS POTENCIALES	ATAQUES DE PHISHING DIRIGIDO PARA OBTENER INFORMACIÓN ADICIONAL QUE PODRÍA UTILIZA-SE PARA ROBO DE IDENTIDAD O FRAUDE FINANCIERO. SECUESTRO DE CUENTAS E IN-GENIERÍA SOCIAL CON LA CUENTA DE LA VÍC-TIMA.

Cybersecurity Researcher, Jeremiah Fowler

Los responsables de esta filtración masiva no fueron hackers de película con acento ruso y mirada intensa, sino algo aún más inquietante: programas invisibles llamados **«infostealers»** —ladrones de información que se infiltran como polvo en los rincones de tu computadora y roban todo sin que te des cuenta. Como un carterista elegante en una ópera: ni lo ves venir, pero cuando salís, te falta todo.



Así se siente ser vulnerado. Pero podés prevenirte!

🔓 Infostealers: el virus que sonríe mientras te desvalija

Podríamos pensar en los infostealers como una especie de mosquitos digitales. No hacen ruido, no piden permiso y, cuando te pican, apenas lo notás… hasta que te das cuenta de que tu cuenta bancaria saluda desde Tailandia. Estos programas suelen entrar a través de correos falsos, sitios web camuflados de inocencia o software pirata que promete mucho y entrega desastre.

¿Te llegó un mensaje sospechoso? A mí también

Una vez adentro, hacen un recorrido turístico por tu dispositivo: desde el navegador donde guardás tus contraseñas, hasta tus apps de mensajería, pasando por tus billeteras digitales. Nada es demasiado privado, ni siquiera tus secretos más mal escritos.

🤔 ¿Y a mí qué?

Buena pregunta. Porque si alguna vez usaste algunos de estos servicios y seguro que lo hiciste, no te hagás el distraído y además, eres del club de los que repiten la misma contraseña como si fuera un mantra sagrado, estás en riesgo. **Riesgo real, de esos que no se arreglan con cerrar sesión**.

Con esas credenciales filtradas, un ciberdelincuente puede convertirse en vos. Puede entrar a tu cuenta, leer tus mensajes, hacerse pasar por vos o simplemente usar tu nombre para vender suplementos milagrosos en alguna red social. El robo de identidad ya no es un thriller, es una comedia negra protagonizada por gente común. Que te puede afectar a vos y a mí, sin distinción.

🛡️ ¿Cómo protegerse en este mundo tan expuesto?

No es necesario convertirse en experto en ciberseguridad ni mudarse a una cabaña sin WiFi. Basta con

tomar algunas decisiones tan simples como urgentes:

1. **Cambiá tus contraseñas.** Especialmente si las reutilizás en varios sitios. Que no te pase como a los que ponen “contraseña123” y después culpan al destino.
   ¿Contraseñas seguras? ¡Qué aburrido!, mejor vive al límite usando: 123456
2. **Activá la verificación en dos pasos.** Sí, es molesto. Pero también lo es que te vacíen la cuenta bancaria.
3. **No hagas clic en cualquier cosa.** Sos curioso, lo sabemos. Pero no todo lo que brilla es un email legítimo.
4. **Usá un administrador de contraseñas.** Es como un mayordomo digital: se acuerda de todo por vos y no te juzga.
   El mejor gestor de contraseñas
5. **Revisá si tus datos fueron filtrados.** Herramientas como «**Have I Been Pwned**» (*) te permiten saber si tu información ya está en la ruleta rusa de Internet.

(*) **Have I Been Pwned** es un servicio en línea (Ir al sitio web) que permite a los usuarios verificar si su dirección de correo electrónico ha sido expuesta en alguna violación de datos. El sitio recopila datos de diversas violaciones de seguridad y permite a los usuarios ingresar su dirección de correo electrónico o número de teléfono para comprobar si han sido comprometidos. Si se encuentra una coincidencia, el usuario recibe información sobre la violación y puede tomar medidas para proteger sus cuentas, como cambiar contraseñas o habilitar la autenticación de dos factores.

Privacidad o resignación

La paradoja es cruel: vivimos en una era donde compartir es la norma, pero protegerse debería ser la regla. La filtración de estas credenciales es solo un capítulo más de una historia más amplia: la lucha entre el deseo de conexión y la necesidad de protección.

Porque al final, nuestras contraseñas dicen más de nosotros que muchas de nuestras publicaciones. Son nuestros secretos compactados, nuestros hábitos, nuestras manías con formato alfanumérico. Tal vez ha llegado el momento de tomarlas más en serio. Y esto, para los más cercanos, se los vengo diciendo desde hace mucho tiempo.

O seguiremos repitiendo “123456” hasta que alguien nos lo recuerde… desde otra cuenta.

Tu identidad es tuya. Defendela. Pensá en tus claves como si fueran tus llaves, no como si fueran papelitos con tu nombre. Y hacelo tanto por vos como por tu familia.

Desde aquí podés acceder a la publicación original donde se reportó este grave incidente.

Yo soy Pablo, tu asistente tecnológico humano, como la IA, pero con «tracción a sangre».

Por favor, síguenos y danos «me gusta»:

Seguir
Compartir
Tuitear