

Programas que roban tus contraseñas: cómo evitarlos

Cómo llegan los programas dañinos, cómo leer el nombre real de un archivo, por qué un ladrón de contraseñas no se nota y qué hacer si ya abriste algo.



Un programa dañino es algo hecho para afectar tu teléfono o tu computador. No necesitas aprenderte sus nombres: casi todos entran por los mismos caminos, y casi todos necesitan que tú los abras deprisa.

Por dónde entran

- Un **adjunto que no esperabas**: «tu paquete no pudo entregarse», cuando no compraste nada.
- Una **ventana alarmante** que te pide instalar una «actualización» o un «limpiador».
- Una **app o programa fuera de la tienda oficial**, sobre todo los de pago ofrecidos «gratis».
- Una **memoria USB** que no sabes de dónde salió.
- Un **enlace con un premio** que hay que reclamar ya.

La regla que cubre casi todo: **inesperado + urgente = pausa**. No lo abras, confírmalo por un canal que ya conoces y pide ayuda si dudas.

El nombre real de un archivo

Lo que decide qué es un archivo es su **última terminación**. Un archivo llamado vacaciones_playa.jpg.exe no es una foto: es un programa que se hace pasar por una. Las fotos terminan en .jpg o .png y los documentos en .pdf o .docx; terminaciones como .exe, .scr, .bat o .js son programas.

En Windows conviene activar que se vean las extensiones: en el Explorador de archivos, menú **Vista** → **Mostrar** → **Extensiones de nombre de archivo**. Así ves el nombre completo y no solo el principio.

El ladrón que no hace ruido

Antes, un equipo infectado se notaba: iba lento o salían ventanas. Los **ladrones de credenciales** (en inglés, infostealers) están hechos para lo contrario. Se ejecutan, copian en segundos las contraseñas y las sesiones abiertas que encuentran, las envían a quien los creó y se quedan quietos o se borran.

Después de abrirlo no pasa nada visible. La señal llega días más tarde y en otro sitio: un amigo te pregunta por qué le pediste dinero, o tu correo aparece con mensajes que no escribiste.

Por qué el navegador es su primer objetivo

Guardar contraseñas en el navegador es cómodo, pero un programa que tú mismo ejecutas trabaja con tus mismos permisos y en muchos casos puede sacarlas de ahí. Peor todavía: también se lleva las **sesiones abiertas**. Con una sesión copiada se entra a tu correo o a tu tienda **sin contraseña y sin segundo paso**, porque esa sesión ya los había pasado.

Dos defensas ayudan mucho:

- Un **gestor de contraseñas aparte del navegador**, que guarda las claves en una bóveda cifrada con una clave maestra que solo está en tu cabeza y que se bloquea sola a los pocos minutos sin uso.
- **Pocas extensiones en el navegador**. Muchas piden «leer y cambiar datos en todos los sitios web»: con ese permiso ven lo que escribes en tu banco. Deja solo las imprescindibles, de autores conocidos.

Hábitos que te cubren

- Activa las **actualizaciones automáticas**: corrigen fallos que estos programas aprovechan.
- Instala solo desde la **tienda oficial** o la web del fabricante.
- Ten una **copia de seguridad** de tus fotos y documentos en otro lugar.

Si ya lo abriste

No te escondas ni te culpes: lo que cuenta es reaccionar pronto y en orden.

1. **Desconecta ese equipo de internet** y deja de usarlo para cosas importantes.

2. **Desde otro aparato que sea de confianza**, cambia las contraseñas, empezando por tu correo y lo que mueve dinero. Cambiarlas desde el equipo infectado podría regalarle también las nuevas.
3. En cada cuenta importante, **cierra todas las sesiones abiertas**: cambiar la contraseña no siempre expulsa a quien entró con una sesión robada.
4. **Pide ayuda** a una persona de confianza o a un servicio técnico, y explícale con claridad qué abriste y cuándo.

Tu lista para hoy

1. Activé las actualizaciones automáticas en mi teléfono y mi computador.
2. Hice visibles las extensiones de los archivos en mi computador.
3. Borré del navegador las extensiones que no uso.
4. Instalé un gestor de contraseñas desde su web o tienda oficial.
5. Sé el orden de los pasos si algún día abro algo que no debía.

Prácticalo · Módulo 6 de Tu primer escudo: Archivos y programas dañinos

En el módulo revisas una carpeta de descargas con cuatro archivos que llegaron la misma mañana y ordenas los pasos de alguien que instaló un juego «gratis» y días después descubrió que le habían robado sus cuentas. Puedes leer las salas sin cuenta; responder los casos y guardar tu avance pide iniciar sesión.

Empieza aquí: pro.whoami-labs.com/rutas/tu-primer-escudo/archivos-y-programas-daninos

Esta guía en la web: pro.whoami-labs.com/guias/programas-que-roban-contrasenas