

SEGURIDAD

Cómo proteger tus cuentas: contraseñas, verificación en dos pasos y phishing

Los hábitos que más protegen tu correo, tus redes y tu banco: contraseñas únicas, verificación en dos pasos y cómo reconocer un phishing.

3 min de lectura · Actualizada el 2 de octubre de 2026 · rossium.xyz/guias/proteger-cuentas-2fa

La mayoría de cuentas robadas no caen por un ataque sofisticado, sino por una contraseña repetida o un enlace falso. Con unos pocos hábitos te proteges de casi todo.

Una contraseña distinta para cada cuenta

Cuando un sitio sufre una filtración, los atacantes prueban esa misma contraseña en tu correo, tus redes y tu banco. Por eso cada cuenta necesita la suya.

- Usa frases largas, por ejemplo cuatro palabras al azar: son más fáciles de recordar y más difíciles de adivinar.
- Guárdalas en un gestor de contraseñas: Bitwarden, 1Password, o el de Google o Apple.
- Empieza por tu correo principal: quien controla tu correo puede recuperar casi todas tus cuentas.

Activa la verificación en dos pasos

Además de la contraseña, la cuenta pide un código o una aprobación desde tu celular. Aunque alguien tenga tu contraseña, no puede entrar.

- Mejor una app de autenticación (Google Authenticator o Microsoft Authenticator) que los códigos por SMS.
- Las llaves de acceso (passkeys) son todavía más seguras donde estén disponibles.
- Guarda los códigos de recuperación en papel o en tu gestor de contraseñas.

Cómo reconocer un phishing

- Urgencia: «tu cuenta será suspendida hoy» o «último aviso».
- Un remitente o una dirección web que imita a la real, con letras cambiadas o palabras de más.
- Te piden datos que la empresa ya tiene o los códigos que te llegan por SMS.
- Archivos adjuntos que no esperabas y premios que nunca pediste.

Consejo: Ningún banco, tienda ni plataforma sería te pide por mensaje tu contraseña o un código de verificación. En ROSSIUM tampoco: nunca te los vamos a pedir.

Antes de tocar un enlace

1. Mira la dirección completa; en el celular, mantén presionado el enlace para verla sin abrirlo.
2. Si dudas, entra escribiendo tú la dirección o desde la app oficial.
3. Nunca inicies sesión desde un enlace que te llegó por WhatsApp o SMS.

Revisa si tus datos se filtraron

En haveibeenpwned.com escribes tu correo y te dice en qué filtraciones conocidas apareció. Cambia la contraseña de esos servicios y de cualquier otro donde la hayas repetido.

Mantén tus equipos al día

- Actualiza el sistema operativo y el navegador: muchas actualizaciones cierran fallas de seguridad.
- Descarga apps solo de las tiendas oficiales.
- Para operaciones bancarias, usa tus datos móviles en lugar del Wi-Fi público.
- Protege el celular con PIN, huella o reconocimiento facial.

Si te roban una cuenta

1. Intenta recuperarla desde la página oficial, con la opción «¿Olvidaste tu contraseña?».
2. Cambia primero la contraseña de tu correo principal.
3. Cierra la sesión en todos los demás dispositivos.
4. Avisa a tus contactos para que no caigan en mensajes falsos enviados desde tu cuenta.
5. Si hay dinero de por medio, llama a tu banco de inmediato.

Aprende ciberseguridad desde cero

Nuestros kits y cursos de ciberseguridad te enseñan con ejemplos prácticos, en español y a tu ritmo.

rossium.xyz/market

Guía gratuita de ROSSIUM. Puedes compartirla tal cual con quien quieras. Información general: no reemplaza asesoría profesional para tu caso.