

Seguridad en Correo electrónico

Gmail y Outlook: la llave maestra de todas tus cuentas

Tu correo es la llave de todo lo demás: con él se recuperan las contraseñas de tus redes, tu banco y tus apps. Si alguien entra en tu correo, puede entrar en todo. Por eso es la primera cuenta que hay que blindar. Las rutas son para Gmail (cuenta de Google) y Outlook/Hotmail (cuenta de Microsoft).

¿Dónde están los ajustes? Gmail: myaccount.google.com · Outlook: account.microsoft.com. Los nombres pueden variar un poco según la versión de la app o del móvil.

9 medidas, paso a paso

1 Haz la Revisión de seguridad de Google

Ruta: Gmail: entra en myaccount.google.com → Seguridad → Revisión de seguridad → Empezar.

Te dice en un minuto qué está mal: dispositivos raros, apps con acceso, datos de recuperación desactualizados.

2 Activa la verificación en dos pasos

Ruta: Gmail: myaccount.google.com → Seguridad → Verificación en dos pasos. Outlook: account.microsoft.com → Seguridad → Opciones de seguridad avanzadas → Verificación en dos pasos.

Usa la app del móvil (Google Authenticator o Microsoft Authenticator) mejor que el SMS.

3 Crea una llave de acceso (passkey)

Ruta: Gmail: myaccount.google.com → Seguridad → Llaves de acceso. Outlook: Opciones de seguridad avanzadas → Agregar una nueva forma de iniciar sesión.

Entrarás con tu huella o tu cara. Es mucho más difícil de robar que una contraseña.

4 Actualiza tu teléfono y correo de recuperación

Ruta: Gmail: Seguridad → Formas de verificar que eres tú. Outlook: Seguridad → Información de seguridad.

Si tu expareja o alguien de quien te has alejado tenía acceso a esos datos, cámbialos hoy.

5 Revisa los dispositivos con sesión abierta

Ruta: Gmail: Seguridad → Tus dispositivos. Outlook: account.microsoft.com → Dispositivos.

Cierra sesión en cualquiera que no reconozcas.

6 Comprueba que nadie reenvía tus correos

Ruta: Gmail (en ordenador): rueda dentada → Ver todos los ajustes → Reenvío y correo POP/IMAP, y también la pestaña Filtros. Outlook: rueda dentada → Correo → Reenvío y Reglas.

Es una forma muy usada de espiar: una regla oculta que envía copia de todo a otra dirección. Borra lo que no hayas creado tú.

7 Revisa quién tiene acceso delegado

Ruta: Gmail: rueda dentada → Ver todos los ajustes → Cuentas e importación → Conceder acceso a tu cuenta.

Si aparece alguien, quítalo.

8 Quita el acceso a apps que ya no usas

Ruta: Gmail: Seguridad → Tus conexiones con aplicaciones y servicios de terceros. Outlook: account.microsoft.com → Privacidad → Aplicaciones y servicios.

Cada app conectada es una puerta más.

9 Aprende a reconocer el phishing

Ruta: Desconfía de correos urgentes («tu cuenta se cerrará», «pago pendiente», «paquete retenido») con enlaces o adjuntos.

Comprueba la dirección real del remitente. Ante la duda, no pulses: entra tú directamente en la web oficial.

Señales de alarma

- Tus contactos reciben correos tuyos que no has enviado.
- Desaparecen correos o dejas de recibir avisos de tus redes sociales: puede haber un filtro o reenvío oculto.
- Google o Microsoft te avisa de un inicio de sesión desde un sitio desconocido: pulsa «No he sido yo» y cambia la contraseña.

¿Te está pasando algo de esto?

No estás solo y no es culpa tuya. En la Asociación Rainbow E Safe acompañamos a personas LGTBIQ+ que sufren violencia digital: te ayudamos a recoger pruebas, a recuperar tus cuentas y a valorar si denunciar.

presidente@rainbowesafe.com · rainbowesafe.com · @rainbowesafe

Si estás en peligro, llama al **112**. Si la violencia viene de tu pareja o expareja: **016** (gratuito, 24 h, no deja rastro en la factura). Antes de borrar nada, haz capturas: son tu prueba.