

Cómo saber si alguien ha entrado en nuestro Gmail

¿Tienes la duda de que alguien durante tu ausencia, haya usado tu computadora y leído tu correo? En esta pequeña guía te enseñamos **cómo saber si alguien ha entrado en nuestro Gmail**, de forma rápida y sencilla.

Normalmente, abres tu cuenta desde diferentes dispositivos, no solo está en tu computadora y dispositivo móvil, sino que también revisas tu correo electrónico en el trabajo. Gmail es seguro y te advierte si tu cuenta se ha abierto desde un dispositivo nuevo.

Sin embargo, es natural preocuparse por la seguridad de tu cuenta, porque espiar tu Gmail representa un riesgo significativo para tu privacidad. Pueden leer tus correos electrónicos, ver tus facturas íntimas, y también obtienen tus mensajes comerciales con datos financieros.



Cómo saber si alguien ha entrado en nuestro Gmail y a otros servicios de Google
Si hay un intento de acceso que Google reconoce como "sospechoso", se te enviará un correo con una alerta pidiéndote que verifiques que realmente fuiste tú quien intentó ingresar. En caso contrario te aconsejo cambiar la contraseña lo antes posible.

Es importante conocer que Gmail tiene muchas características interesantes, una de ellas es la capacidad de ver todos los inicios de sesión realizados en tu cuenta. **Simplemente ve al buzón de correo e inicia sesión normalmente.**

Conoce cómo validar [emails como prueba en un juicio](#)

Cómo saber si alguien ha entrado en nuestro Gmail, a través de la revisión de la cuenta

Para conocer **cómo saber si alguien ha entrado a nuestro Gmail**, debemos tener en cuenta que **una vez iniciemos sesión, la pantalla se abrirá con la lista completa de los correos electrónicos entrantes.**

Justo en la parte inferior de la página, encontrará las palabras "última actividad de la cuenta" y la hora o los minutos en que se vio tu cuenta por última vez al realizar el acceso.

Ya a partir de esta información es posible entender si alguien ha interferido con tu cuenta. Puedes verificar si el último acceso se realizó en un momento en el que no utilizaste el correo electrónico, entonces se deduce que lo hizo otra persona.

Sin embargo, es posible hacer aún más: simplemente haz clic en la palabra "detalles" y se abrirá una ventana con todos los detalles relacionados con el acceso a tu cuenta. Junto al tipo de acceso y la posición encontrarás la indicación de la fecha y hora.

Compruébalos y fíjate si en ese período de tiempo utilizaste la PC y específicamente te has conectado a tu Gmail. En caso de que el intento fuera fraudulento, una vez que hayas cambiado tus credenciales, investiga.

Para hacer esto, simplemente ve a la parte inferior de la página en la pantalla "bandeja de entrada" y haz clic en la palabra "detalles" en la parte inferior derecha. Se abrirá una pequeña ventana emergente con un informe que contiene una lista de los últimos 10 accesos a la cuenta.



Informe de revisión

El informe proporciona los datos de país y estado, tipo de acceso: navegador, teléfono móvil, fecha, hora y la dirección IP. **Con esto ya es posible identificar accesos no autorizados a tu cuenta y por eso, siempre recomiendo dejar habilitada la opción de alertas por actividades inusuales.**

Porque, si hay algún acceso desconocido en la cuenta, se mostrará en este informe. Para ello, accede a preferencias de alerta, y en Cambiar, marca la opción "Mostrar una alerta para actividades inusuales". **De forma predeterminada, esta opción ya está marcada.**

Según el informe, es posible concluir si hubo o no acceso no autorizado a tu cuenta a través de la [dirección IP](#) y la ciudad / país que se muestran. En caso de ser afirmativo, el ingreso fraudulento es necesario cambiar tus credenciales.

Descubre: 10 Consejos prácticos para [mejorar la seguridad informática](#)

Mayor privacidad

Para aumentar el control sobre el acceso y cómo saber si alguien ha entrado a nuestro Gmail, podemos asegurarnos de que se notifique cuando ocurra una situación de este tipo. La operación a realizar en este caso es sumamente sencilla.

Selecciona la frase "mostrar un aviso en caso de actividad anómala" y recibirás un mensaje si hay accesos simultáneos o de áreas que normalmente no se utilizan para tus inicios de sesión. Al hacerlo, puedes proteger aún más tu privacidad.



Seguridad por contraseña

Cambia tu contraseña para mantener alejadas a otras personas de tu cuenta ingresando en Gmail, ve a "Cuentas e importación" y haz clic en "Cambiar contraseña". Elige una contraseña o frase de contraseña segura que incluya números y caracteres en mayúscula.

Se requiere al menos ocho caracteres, pero pueden ser 12, 16 o incluso más, y cuanto más, mejor. No será aleatorio, a menos que uses un administrador de contraseñas, pero evita apellidos, nombres de mascotas, cumpleaños, equipos deportivos y otros elementos obvios.

Para mayor comodidad, tu navegador o programa de correo electrónico puede recordar tu contraseña. Si lo permites, tu correo electrónico será tan seguro como tu PC, cualquiera que pueda acceder a tu PC puede acceder a tu correo electrónico.



Pirateo de correos

Hoy en día, por supuesto, la forma más sencilla de piratear el correo electrónico de alguien es mediante un ataque de phishing. En este caso, una persona te envía un enlace en un correo electrónico que pretende provenir de Google.

Al hacer clic en el enlace, se abre una pestaña del navegador donde "Google" te pide que inicies sesión con tu dirección de correo y contraseña, y el atacante obtiene los resultados. Si tu dispositivo cae en un ataque de phishing, no importa qué tan fuerte sea tu contraseña.

Todo lo que debes saber sobre la [Suplantación de identidad](#)

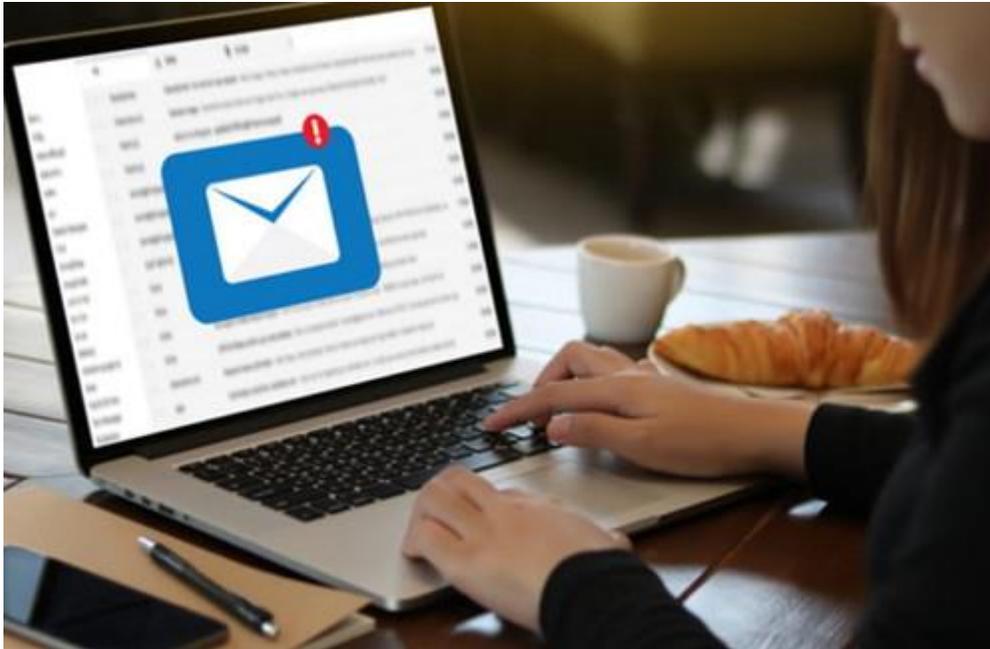
Verificación en dos pasos

Si alguien puede acceder a tu cuenta de Gmail, puede cambiar tu contraseña y bloquearlo, esto lo evitas mediante la "verificación en dos pasos". Esta validación significa que Google enviará un código de texto a tu teléfono móvil, esto está bien hasta que pierdas tu teléfono.

Por lo tanto, Gmail solicita un número de teléfono de respaldo, los teléfonos fijos funcionan (recibe un mensaje de voz). También te permite imprimir un pequeño conjunto de números de verificación que puedes usar cuando viajas.

Notificación de dos pasos de Google

Google ofrece una alternativa a los SMS en forma de Google Authenticator, una aplicación gratuita para dispositivos Android de Google, iPhones y iPads de Apple. También logras simplificar la verificación mediante el uso de "contraseñas específicas de la aplicación".



Para utilizar estas funciones desde Gmail, ingresa en Cuentas e importación, entra en "Otras configuraciones de la cuenta de Google" y en "Inicio de sesión y seguridad". Esto proporciona acceso a cambios de contraseña, verificación en dos pasos y recuperación de cuenta.

Espero te haya servido esta pequeña guía de revisión para verificar el acceso a tus servicios de Google. Sin embargo, si requieres mayor información sobre pirateo de tus cuentas, te ofrezco los servicios periciales de mi equipo de profesionales ingresando a www.peritinformatic.com

Puedes comunicarte conmigo a través del correo electrónico lluis@peritinformatic, si requieres además, de otros servicios de peritos especializados en diversas áreas. Te atenderemos con mucho gusto para solventar alguna situación en la que te encuentres y necesites ayuda pericial.

Perito: José Luis Martir Millán