VenCERT

PROTEGEMOS LA CIBERSEGURIDAD DE LA NACIÓN

Recomendaciones de Seguridad en Correos Electrónicos Gmail

Lista de Verificación de Seguridad de Gmail

Con los consejos y las herramientas de esta lista de verificación, puedes evitar que personas no autorizadas accedan a tu Gmail y aumentar la seguridad de tu cuenta si hace poco se ha visto vulnerada.

- **Elige contraseñas seguras:** La contraseña es la primera línea de defensa contra los piratas informáticos. Si tu cuenta ha sido vulnerada recientemente, deberías cambiar tu contraseña ya.

1. Invéntate una contraseña muy segura
2. Utiliza contraseñas distintas y difíciles de adivinar para tus cuentas, sobre todo si son cuentas importantes (la de correo electrónico o la de banca por Internet, por ej.). Si eliges una sola contraseña para todas tus cuentas online es como si tuvieras una llave que abriera tu casa, tu coche y tu oficina: si un delincuente consigue tu contraseña, ya tiene acceso a todas tus cuentas.
3. Utiliza una contraseña larga. Cuanto más larga sea tu contraseña, más difícil será averiguarla.
4. Utiliza una contraseña que combine letras, números y símbolos.
5. Prueba a utilizar una frase que solo conozcas tú. Por ejemplo: si es para tu correo electrónico, podrías empezar por “Mis amigos Tomás y Julieta me envían un mensaje divertido al día" y luego utilizar las iniciales y números para resumirla. “MaT&Jme1mdad” es una contraseña con muchas variaciones.

- **Consejos para proteger tu contraseña**

1. No envíes tu contraseña por correo electrónico. Los sitios y servicios legítimos nunca te piden que les mandes tus contraseñas por correo electrónico.
2. Guarda tus recordatorios de contraseña en un lugar secreto y poco visible. No dejes notas con tus contraseñas a la vista, en tu ordenador ni en tu escritorio.

Actualiza las opciones de recuperación de tu cuenta

Las opciones de recuperación te ayudan a proteger tu cuenta de los ataques de piratas informáticos y te permiten acceder a tu cuenta si se te ha olvidado tu contraseña.

- **Teléfono móvil:** Una de las formas más rápidas y sencillas de proteger tu cuenta es un número de móvil. Es más seguro que una dirección de correo electrónico de recuperación porque sueles llevar el teléfono contigo. El que des un número de teléfono de recuperación a Google no implica que te apuntes a compañías de marketing ni que empieces a recibir montones de llamadas de telemarketing.
- **Correo:** Si tienes bloqueado el acceso a tu cuenta, tu dirección de recuperación nos permite enviarte un mensaje de correo electrónico para que vuelvas a configurar tu contraseña. Además, le complica mucho la vida a los piratas informáticos que intenten acceder a tu cuenta.

Busca en tu cuenta alguna actividad extraña

- Revisa tu cuenta con regularidad para detectar acciones raras o sospechosas.
- En tu página Actividad reciente se muestran las acciones relacionadas con la seguridad que tú has realizado: iniciar sesión en tu cuenta de Google, cambiar tu contraseña o añadir una dirección de correo electrónico o un número de teléfono de recuperación.
- Te recomendamos que repases esas acciones y te apuntes dónde y cuándo se realizaron. Si encuentras algo sospechoso (un inicio de sesión con un navegador que tú no usas nunca o desde un sitio que no conoces), deberías cambiar tu contraseña para aumentar la seguridad de tu cuenta.
- **Busca mensajes sospechosos o perdidos**
- Si han desaparecido muchos mensajes de tu cuenta, es posible que haya sido interceptada. También es probable que hayan interceptado tu cuenta si recibes mensajes de recuperación de contraseña que no has solicitado o si desde tu cuenta se envían mensajes que no te suenan de nada.
- **Comprueba que no haya ningún error en tus contactos**
- Inicia sesión en Gmail.
- En la esquina superior izquierda de tu página de Gmail, haz clic en Gmail y elige Contactos.

Mantén limpio tu dispositivo

- **Si tu ordenador está infectado de software malintencionado, quita ese software cuanto antes,** una forma de limpiar tu ordenador es analizarlo con un producto antivirus de alta calidad como mínimo (lo ideal es utilizar varios antivirus). No podemos responder de la eficacia de estos programas, pero te recomendamos que pruebes sus últimas versiones. Si tu cuenta ha sido vulnerada hace poco tiempo, cambia tu contraseña otra vez después de borrar el software malintencionado de tu ordenador.
- **Mantén actualizado tu sistema operativo, L**os sistemas operativos publican parches para reparar los puntos débiles de su seguridad. Tanto si tu sistema operativo es Windows como si es Mac OS, te recomendamos que protejas tu ordenador habilitando las actualizaciones automáticas y que lo actualices en cuanto recibas una notificación para hacerlo.
- **No ignores las actualizaciones regulares de software, a**unque actualizaciones de software no vengan incluidas en las del sistema operativo, son igual de importantes. Los productos de software tales como Adobe Flash, Adobe Reader o Java sacan frecuentes actualizaciones que pueden incluir la reparación de puntos débiles de seguridad.

Actualiza tu navegador

- Es importante que siempre tengas instalada la versión más reciente de tu navegador, pues así cuentas con las últimas actualizaciones de seguridad.

Activa la verificación en dos pasos

- La mayoría de los usuarios solo protege sus cuentas con una contraseña. Con la verificación en dos pasos, en cambio, proteges tu cuenta con tu contraseña *y t*u teléfono. Si algún delincuente consigue robarte o adivinar tu contraseña, también necesita tu teléfono para entrar en tu cuenta.
- El inicio de sesión con la verificación en dos pasos es algo distinto. Primero escribes tu contraseña, como siempre, y luego el código de verificación que te llegue a tu móvil. Puedes simplificar este procedimiento para los ordenadores o dispositivos que utilices con más frecuencia.

Defiéndete contra la suplantación de identidad y las estafas

- **Si en una web o en un mensaje sospechoso te piden tus datos personales o financieros no respondas,** desconfía siempre de los mensajes y sitios web que te pidan datos personales, así como de los mensajes que te remitan a una página web que no conozcas donde te pidan nombres de usuario, contraseñas, números de la Seguridad Social, DNI, NIF, números de cuentas bancarias, PIN, números completos de tarjetas de crédito, el apellido de soltera de tu madre o la fecha de tu cumpleaños.
- No respondas ni rellenes ningún formulario ni pantalla que pueda estar vinculada a dichos mensajes.
- **Denúncialos como mensajes de suplantación de identidad, si** recibes un mensaje de correo electrónico en el que te piden datos personales (para la suplantación de identidad o "phishing"), puedes denunciarlo a Google.

1. Inicia sesión en Gmail.
2. Abre el mensaje que desees denunciar.
3. En la esquina superior derecha del mensaje, haz clic en la flecha hacia abajo que hay al lado de Responder  .
4. Selecciona **Denunciar suplantación de identidad. Sé prudente al responder a mensajes extraños de tus contactos ,** Si te llega un mensaje de un conocido pero que no suena como él, es posible que un pirata haya interceptado su cuenta y esté intentando sacarte dinero o información. ¡Cuidado con lo que contestas!, Entre las tácticas habituales está el pedirte que envíes dinero urgentemente porque se encuentra en otro país y no puede regresar y no te ha llamado porque le han robado el teléfono. En ese mensaje también pueden pedirte que hagas clic en un enlace para ver una foto, un artículo o un vídeo, pero ese enlace en realidad de conduce a un sitio donde pueden robar tus datos. ¡Piénsatelo bien antes de hacer clic!

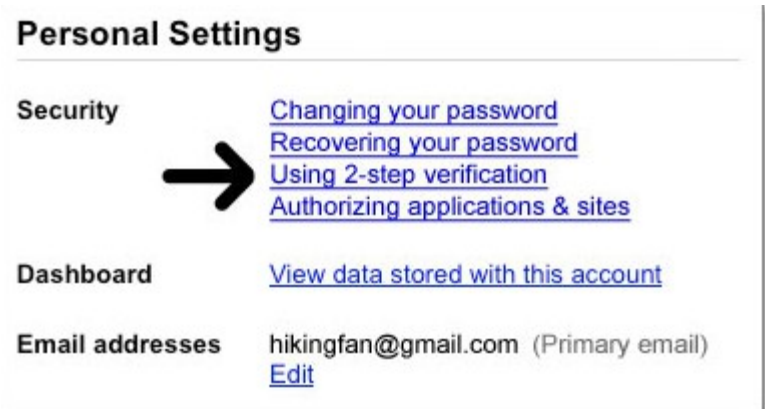
- **Ignora los mensajes que supuestamente ha enviado Google** por desgracia, mucha gente sin escrúpulos utiliza la marca Google para estafar a otras personas.
- **Ante la duda, no te arriesgues,** si un anuncio o una oferta te parecen sospechosos, ¡confía en tu instinto! Haz clic únicamente en los anuncios o productos en venta de los sitios seguros, conocidos y fiables.

Configuración de la verificación en dos pasos

1. Debes configurar tu número de teléfono para recibir códigos a través de mensajes de texto SMS o de llamadas de voz. Si tienes un smartphone, puedes descargarte una aplicación que te permite generar códigos sin mensajes de texto e, incluso, sin cobertura.

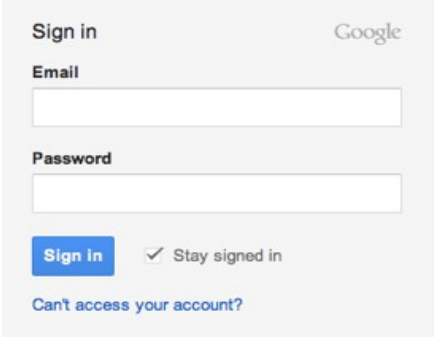
Sigue los pasos que se indican a continuación para configurar la verificación en dos pasos:

a) Inicia sesión en tu cuenta de Google y accede a la página de configuración de la verificación en dos pasos.



b) En el menú desplegable, selecciona el país en el que esté registrado el teléfono e introduce tu número de teléfono en el cuadro.
c) Selecciona si prefieres recibir los códigos a través de un mensaje de texto o de una llamada de voz. Puedes cambiar esta preferencia en cualquier momento.
d) Introduce tu número de teléfono y, a continuación, haz clic en **Enviar código de verificación** para recibir un código en tu teléfono. Te recomendamos que utilices un número de teléfono móvil en lugar de un número de teléfono fijo o de un número de Google Voice.
e) Introduce el código del mensaje de voz o de texto en el cuadro y haz clic en **Verificar.**
f) A continuación, deberás confirmar si quieres recordar el ordenador que estás utilizando. Si seleccionas la casilla de verificación, no tendrás que introducir un código para iniciar sesión en este ordenador en los próximos 30 días. No selecciones la casilla de verificación si estás utilizando un ordenador público o un dispositivo que no utilices habitualmente para iniciar sesión.

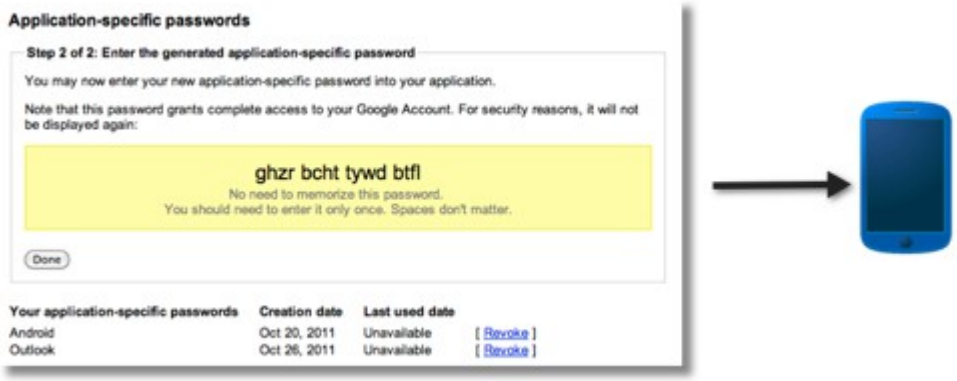
g) Haz clic en **Activar verificación en dos pasos** para completar el proceso. Accederás automáticamente a la página de configuración de tu cuenta.
h) Accede a la página de inicio de sesión e introduce tu nombre de usuario y tu contraseña como harías normalmente.



2. A continuación, deberás introducir un código de seis dígitos que recibirás en el teléfono. Si quieres, cuando introduzcas el código, puedes seleccionar que el ordenador lo recuerde durante 30 días. En este caso, no tendrás que volver a introducir un código al iniciar sesión en este ordenador durante 30 días. No obstante, si inicias sesión en otro ordenador, deberás introducir un código.

• Cuando actives la verificación en dos pasos, las aplicaciones y los dispositivos sin navegador que utilicen tu cuenta de Google (por ejemplo, Outlook o Gmail para móviles) no podrán conectarse a tu cuenta. Sin embargo, en pocos pasos puedes generar una contraseña especial, denominada

contraseña específica de aplicaciones, para permitir que la aplicación se conecte a tu cuenta. Además, solo tendrás que repetir el proceso una vez para cada dispositivo o aplicación, por lo que no tienes que preocuparte por nada.



Mas Informacion en Soporte Gmail:
https://support.google.com/accounts/answer/46526?hl=es