

Boletín Especial de Seguridad

Boletín N° 8
Enero 2012

PROTEGEMOS LA CIBERSEGURIDAD DE LA NACIÓN



Recomendaciones de Seguridad Correos Electrónicos - Gmail



Lista de Verificación de Seguridad de Gmail

- **Comprueba la existencia de virus y de software malicioso.**
Aunque ningún explorador de virus puede detectar el 100% de las infecciones, es importante ejecutar un Antivirus de confianza en el equipo (o instalar un programa que se ejecute en segundo plano y que realice exploraciones constantemente). Si el antivirus detecta aplicaciones o programas sospechosos, elimínalos inmediatamente. Estos software maliciosos pueden sustraer información de su equipo como archivos, imágenes y todo lo que se teclee en ese momento obteniendo así contraseñas, conversaciones, etc..
- **Asegúrate de que el navegador esté actualizado.**
Mediante las actualizaciones se garantiza que los navegadores hayan corregido fallos de seguridad. Para comprobar si hay actualizaciones en Firefox, solo tienes que hacer clic en la pestaña Ayuda y seleccionar la opción Buscar actualizaciones. Google Chrome se actualiza automáticamente cuando hay una nueva versión disponible, en Internet Explorer, selecciona la pestaña Herramientas y haz clic en Windows Update.
- **Comprueba la existencia de complementos, extensiones y programas/herramientas de terceros en el navegador que requieran acceso a las credenciales de tu cuenta de Google.**
Los complementos y las extensiones son programas de ordenador descargables que funcionan junto con el navegador para desempeñar tareas específicas. Por ejemplo, puedes haber descargado un complemento o extensión que compruebe si entran nuevos mensajes en la carpeta "Recibidos" de Gmail. No obstante, Google no puede garantizar la seguridad de estos servicios de terceros. En caso de que tales servicios se vean comprometidos, **también lo estará la contraseña de Gmail.**
- **Cambia la contraseña.**
Si la cuenta se ha visto comprometida recientemente, se debe actualizar la contraseña cuanto antes. Por lo general, se sugiere que se cambie periódicamente y que, para ello se tomen en cuenta las siguientes indicaciones:
 - Elige una contraseña exclusiva que no hayas utilizado antes en Gmail ni en ningún otro sitio. Si solo cambias un carácter o número, se considera que sigues usando la misma contraseña.
 - No utilices palabras del diccionario ni palabras comunes que se puedan adivinar con facilidad. Utiliza una combinación de números, caracteres especiales y letras en mayúscula y minúscula.
- **Actualiza las opciones de recuperación de tu cuenta.**
Todos podemos olvidar nuestras contraseñas en algún momento, así que recomendamos encarecidamente que actualices las opciones disponibles para la recuperación de la cuenta. Para ello, accede a tu cuenta de Google a través de la página <https://www.google.com/accounts> y, a continuación, haz clic en Cambiar opciones de recuperación de contraseña.
 - **Dirección de correo electrónico alternativa:** la cuenta de correo electrónica alternativa se puede usar para que gmail se comunique con la persona en caso que la misma pierda el acceso a la cuenta de correo o sea víctima de algún ataque.
 - **SMS:** Gmail se encargara de enviarte un código de recuperación a tu dispositivo móvil, que puedes utilizar para restablecer tu contraseña.
 - **Pregunta de seguridad:** esta opción solo se encuentra disponible si no puedes utilizar las opciones de recuperación anteriores y solo en el caso de que no hayas intentado acceder a la cuenta durante las últimas 24 horas. Una respuesta ideal a la pregunta de

seguridad es aquella que te resulte fácil de recordar y que, al mismo tiempo, sea difícil de adivinar para los demás.

- **Activar la verificación en dos pasos.**

La verificación en dos pasos añade una capa adicional de seguridad a tu cuenta, ya que requiere que accedas con algo que conoces (tu contraseña) y algo que tienes (un código enviado a tu teléfono). Para activar la verificación en dos pasos, sigue las instrucciones que mas adelante desarrollaremos.

- **Comprueba la lista de sitios web que tienen autorización para acceder a los datos de tu cuenta de Google.**

Asegúrate de que la lista de sitios web autorizados sea precisa y de que hayas sido tú quien los haya elegido. En caso de que tu cuenta de Google se haya visto comprometida recientemente, es posible que estas personas malintencionadas hayan autorizado a sus propios sitios web para que accedan a los datos de tu cuenta. Esto les puede permitir acceder a tu cuenta de Google incluso después de que hayas cambiado la contraseña.

Para editar la lista de sitios web autorizados:

1. Accede a la página principal de Cuentas de Google.
2. Haz clic en el enlace **Mi cuenta** que aparece en la parte superior derecha de la página.
3. Haz clic en **Cambiar sitios web autorizados**. En esta página aparecerán todos los sitios de terceros a los que hayas concedido acceso.
4. Haz clic en el enlace **Revocar acceso** para inhabilitar el acceso de un sitio en concreto.

- **Utiliza una conexión segura para acceder.**

En la configuración de Gmail, selecciona "Usar siempre https". Esta configuración protegerá tu información y evitará que otras personas puedan disponer de ella cuando accedas a Gmail a través de una red inalámbrica pública como, por ejemplo, en una cafetería o en un hotel.

- **Comprueba si recientemente se ha producido alguna actividad extraña en tu cuenta.**

Haz clic en el enlace **Información detallada** situado junto a la entrada **Última actividad** de la cuenta que se encuentra en la parte inferior de tu cuenta para ver la hora, fecha, dirección IP y la ubicación asociada del acceso reciente a tu cuenta.

Motivos por los que debes utilizar la verificación en dos pasos

Además de tu nombre de usuario y de tu contraseña, deberás introducir un código que Google te enviará a través de un mensaje de texto o de voz una vez que hayas iniciado sesión.

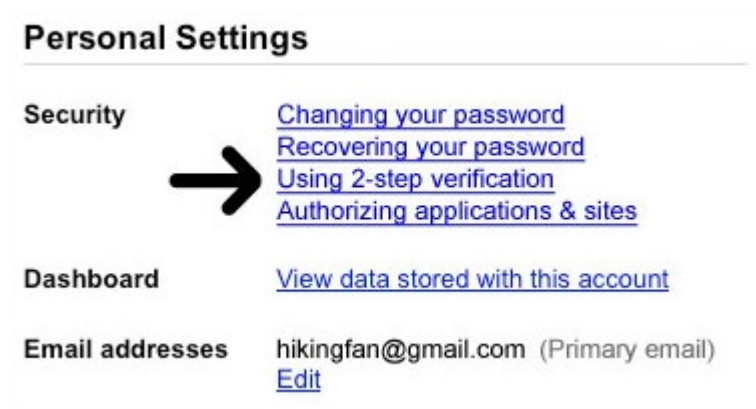
La verificación en dos pasos reduce drásticamente las posibilidades de que otra persona robe la información personal de tu cuenta de Google. ¿Por qué? Porque los piratas informáticos no solo tendrían que obtener tu contraseña y tu nombre de usuario, sino que también tendrían que robar tu teléfono.

Configuración de la verificación en dos pasos

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

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

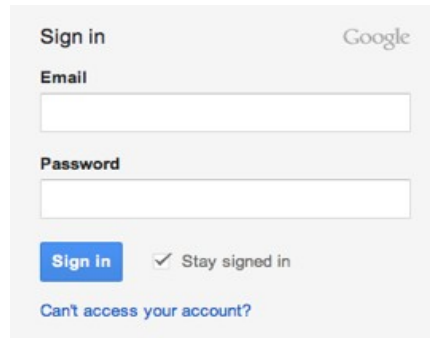
1. Inicia sesión en tu cuenta de Google y accede a la [página de configuración de la verificación en dos pasos](#).



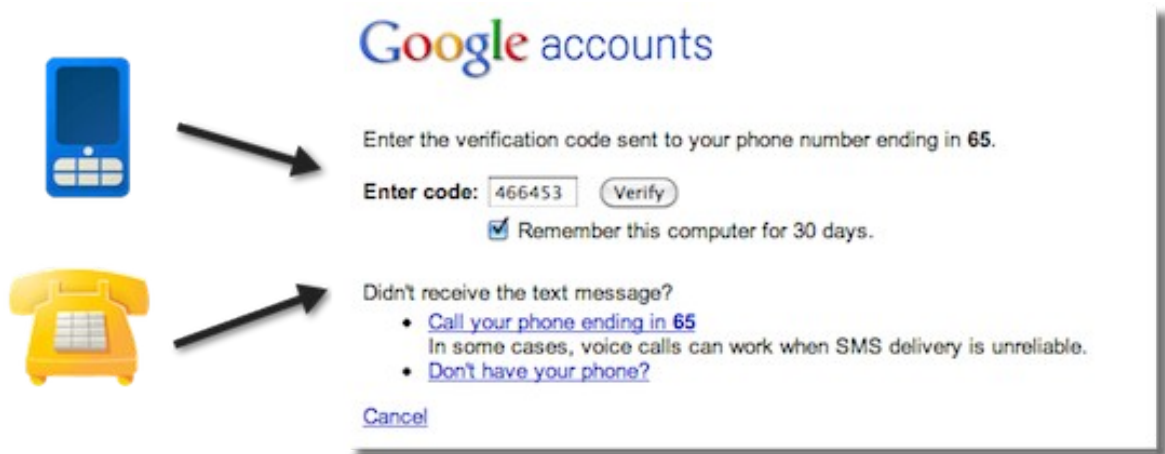
2. En el menú desplegable, selecciona el país en el que esté registrado el teléfono e introduce tu número de teléfono en el cuadro.
3. Selecciona si prefieres recibir los códigos a través de un mensaje de texto o de una llamada de voz. Puedes cambiar esta preferencia en cualquier momento.
4. Introduce 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.
5. Introduce el código del mensaje de voz o de texto en el cuadro y haz clic en **Verificar**.
6. 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.
7. Haz clic en **Activar verificación en dos pasos** para completar el proceso. Accederás automáticamente a la página de configuración de tu cuenta.

Cómo iniciar sesión en tu cuenta con la verificación en dos pasos

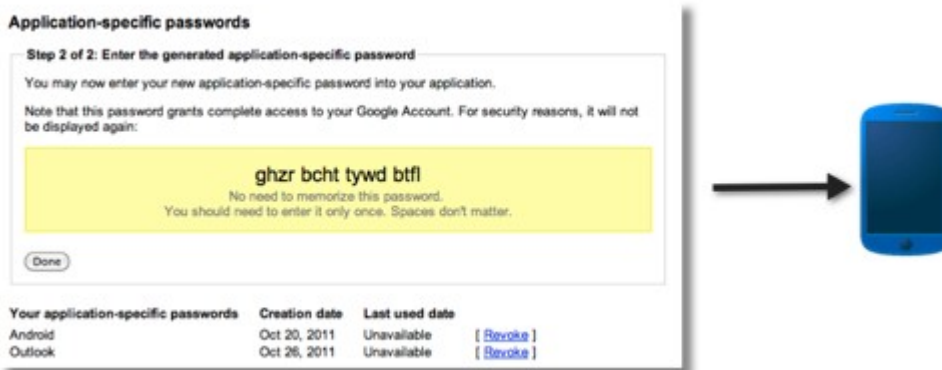
1. Accede a la página de inicio de sesión e introduce tu nombre de usuario y tu contraseña como harías normalmente.



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.



3. 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.



Para mayor información visitar:

Soporte Gmail: <https://support.google.com/accounts/?hl=es>