La Seguridad en Gmail.

Si deseas cerciorarte de que tu cuenta de correo sea segura, sigue estos consejos que hemos recopilado de la Web de ayuda del servidor Gmail.

1. Comprueba la existencia de virus y de software malicioso.

Aunque ningún explorador de virus puede detectar el 100% de las infecciones, es importante ejecutar una exploración en el equipo con un software antivirus de confianza (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. Aquí puedes encontrar exploradores antivirus.

2. Asegúrate de que el sistema operativo esté actualizado.

Los sistemas operativos publican parches destinados a reparar las vulnerabilidades de seguridad. Tanto si eres usuario de Windows como de Mac OS, te recomendamos que habilites la configuración de actualización automática y que actualices cuando recibas una notificación a fin de proteger tu equipo.

3. Asegúrate de llevar a cabo actualizaciones del software de forma regular.

Algunas actualizaciones del software no vienen incluidas en las actualizaciones del sistema operativo, pero son igual de importantes. Se suelen realizar actualizaciones periódicas de software como Adobe Flash, Adobe Reader y Java que pueden incluir reparaciones de las vulnerabilidades de seguridad.

4. Asegúrate de que el navegador esté actualizado.

Para comprobar si hay actualizaciones en Internet Explorer, selecciona la pestaña **Herramientas** y haz clic en **Windows Update**. 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.

5. **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 nos avisa de que no puede garantizar la seguridad de estos servicios de terceros. En caso de que tales servicios se vean comprometidos, también lo estará tu contraseña de Gmail.

6. **Cambia la contraseña.**

Si tu cuenta se ha visto **comprometida recientemente**, debes actualizar tu contraseña cuanto antes. Por lo general, te sugerimos que la cambies periódicamente y que, para ello, sigas estas indicaciones:

- Elige una contraseña exclusiva que no hayas utilizado antes en Gmail ni en ningún otro sitio. Si sólo 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 y letras en mayúscula y minúscula.

7. **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:

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

8. **Actualiza las opciones de recuperación de tu cuenta.**

Todos podemos olvidar nuestras contraseñas en algún momento, así que es recomendable actualizar las opciones que hay disponibles para la recuperación de la cuenta. Para ello, accede

a tu cuenta de Google a través de de este enlace y, a continuación, haz clic en **Cambiar opciones de recuperación de contraseña**.

- **Dirección de correo electrónico alternativa:** si dispones de otra cuenta de correo, Gmail podrá comunicarse contigo en el caso de que pierdas el acceso a tu cuenta.
- **SMS:** pueden enviarte un código de recuperación a tu móvil, que podrás utilizar para restablecer tu contraseña.
- **Pregunta de seguridad:** esta opción sólo se encuentra disponible si no puedes utilizar las opciones de recuperación anteriores y sólo 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.

9. 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.

10. 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.

11. Confirma la precisión de la configuración del correo para garantizar que tu correo se envíe donde desees y no salga de allí.

Accede a tu cuenta y haz clic en el enlace **Configuración** de la parte superior para comprobar las siguientes pestañas:

- **General**: comprueba las opciones **Firma** y **Respuesta automática** para comprobar que no hay spam.
- **Cuentas**: comprueba la configuración de **Enviar mensaje como**, que incluye la verificación de la configuración de la dirección de respuesta, y **Comprobar correo mediante POP3**.
- **Filtros**: comprueba que ningún filtro envíe tu correo a la **Papelera** o la carpeta **Spam**, y que no se reenvíe a alguna cuenta desconocida.
- **Reenvío y correo POP/IMAP**: asegúrate de que tu correo no se envía a ninguna cuenta ni cliente de correo desconocidos.

12. **Recela de los mensajes que te piden el nombre de usuario o la contraseña.** Gmail nunca solicita esta información.

13. **Nunca introduzcas tu contraseña después de seguir un enlace** que alguien te haya enviado en un mensaje, incluso aunque parezca tratarse de la página de acceso de Gmail. Accede a Gmail directamente escribiendo https://mail.google.com en la barra de direcciones del navegador

14. **No compartas tu contraseña con otros sitios web;** Google no puede garantizar la seguridad de otros sitios y, además, la contraseña de Gmail podría verse comprometida

15. **¡Hay secretos que deben guardarse!** No reveles a nadie tu contraseña ni tu pregunta y respuesta secretas, y si lo haces, modifica esta información lo antes posible.

16. Borra los **formularios**, las **contraseñas**, la **caché** y las **cookies** de tu navegador con regularidad, sobre todo, si se trata de un equipo público.

17. **Seleccionar "No cerrar sesión" puede ser peligroso,** hazlo únicamente si accedes al programa de correo desde un equipo personal.

18. **Sal siempre de tu cuenta de correo con el botón o enlace SALIR,** cuando termines de leer los mensajes. Nunca lo hagas cerrando la ventana pues, si estuvieras en un equipo público, el siguiente usuario podría acceder a tu cuenta con toda facilidad.

Otros problemas relacionados con el uso del correo electrónico son el pishing, el spam y los hoax:

Suplantación de identidad (Pishing).

Se llama así a un tipo de delito que consiste en suplantar la identidad de una persona o entidad de confianza, por ejemplo un banco, con la intención de obtener información de nuestra cuenta o tarjeta bancaria o las contraseñas para luego estafarnos. Más información del tema y ejemplos en Wikipedia

Correo basura (Spam).

Según Wikipedia, se llama ***spam***, **correo basura** o **mensaje basura** a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina *spamming*. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Si recibes algún mensaje de este tipo es conveniente denunciarlo como spam. Gmail trasladará el mensaje a la carpeta Spam y ese remitente no podrá volver a enviarte ningún mensaje.

1. Selecciona los mensajes no deseados.
2. Haz clic en **Marcar como spam**.

Para eliminar spam definitivamente de tu correo:

1. Haz clic en la etiqueta **Spam,** situada en el lateral izquierdo de cualquier página de Gmail.
2. Selecciona los mensajes que deseas eliminar y haz clic en **Suprimir definitivamente**.
3. O elimina todo haciendo clic en **Suprimir todos los mensajes spam ahora**.

Gmail mejorará su sistema de detección de spam en la medida en que los usuarios marquen este tipo de correo. Si tanto los usuarios como Gmail nos equivocamos y marcamos un mensaje como spam, selecciónalo y haz clic en **No es spam,** en la parte superior del mensaje. Si lo has marcado como spam, puedes también hacer clic en **Deshacer** inmediatamente después para recuperar el mensaje.

Bulo informático (Hoax).

Es un mensaje de correo electrónico con contenido falso o engañoso y atrayente. Normalmente es distribuido en cadena por sus sucesivos receptores debido a su contenido impactante que parece provenir de una fuente seria y fiable o porque el mismo mensaje pide ser reenviado.

Las personas que crean un bulo suelen tener como objetivo captar direcciones de correo (para mandar correo masivo, virus, mensajes con suplantación de identidad o más bulo a gran escala); engañar al destinatario para que revele su contraseña o acepte un archivo malicioso (malware); o confundir o manipular a la opinión pública de la sociedad.

Básicamente, los bulos pueden ser alertas sobre virus incurables; falacias sobre personas, instituciones o empresas; mensajes de temática religiosa; cadenas de solidaridad; cadenas de la suerte; métodos para hacerse millonario; regalos de grandes compañías; leyendas urbanas; y otras cadenas.

- **Pautas para reconocer un bulo en Internet**

Algunas de las pautas para reconocer si cierta información es un bulo o no son:

1. Los bulos son anónimos, no citan fuentes (ya que carecen de las mismas) y no están firmados para evitar repercusiones legales.

2. Los bulos carecen de fecha de publicación y están redactados de la manera más atemporal posible para que pervivan el máximo tiempo circulando en la red.

3. Los bulos contienen un gancho para captar la atención del internauta. El éxito del bulo residirá en cuán morboso, monetario, generador de miedo sea su gancho y sobre todo en la manera que encaja con la coyuntura del entorno.

Ejemplo Hotmail: *Hotmail cerrará sus cuentas. Perdida de contactos y multa de una gran cantidad de dinero* — (Gancho de miedo basado en valor monetario)

Ejemplo Actimel: *Actimel es malo para la salud. Produces L. Casei y dejas de fabricar defensas* — (Gancho de miedo basado en la salud)

Ejemplo Redbull: *Redbull contiene veneno en su composición química* — (Gancho de miedo basado en el daño a la salud)

Ejemplo Teléfono móvil: *Recibes una llamada telefónica en dónde en lugar de un número de teléfono aparece la palabra "INVIABLE!!". Si aceptas o rechazas la llamada el extorsionador accede a la SIM de tu teléfono, la duplica y la usa para llamar desde la cárcel* — (Gancho de miedo basado en ser víctima de una estafa)

4. Los bulos están por general escritos en castellano neutro (en el caso de que este sea el idioma utilizado), para facilitar la difusión a nivel internacional.

5. Los bulos normalmente contienen una petición de reenvío: Se solicita el reenvío para alertar a otras personas, para evitar mala suerte, para evitar la muerte, o con cualquier otro motivo. El objetivo de esta petición de reenvío reside en captar direcciones IP, crear bases de datos, realizar posteriores campañas de Correo masivo o simplemente difundir la información falsa el máximo posible.

Más información de tema en Wikipedia y Rompecadenas