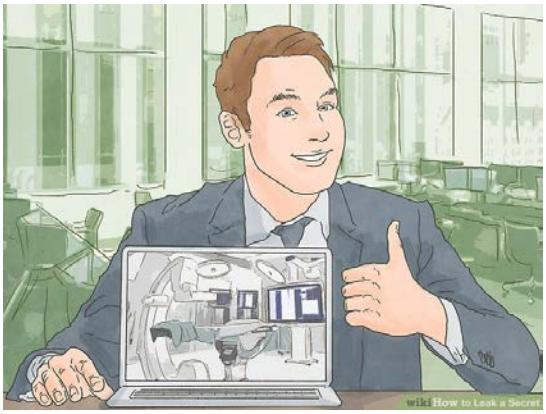
Cómo filtrar información de forma segura y totalmente anónima

En la sociedad actual, puedes filtrar un secreto si sientes que es importante para que otras personas lo sepan. Tienes algunas opciones para filtrar cuidadosamente un secreto que incluye el uso de un ordenador, correo electrónico, correo postal o un teléfono. Lo más importante es filtrar los secretos de una manera que excluya la información personal, aunque la organización, normalmente, elabora complejos procedimientos para lograrlo por si tú no ha podido o no supiste como hacerlo.

Método 1

Enmascarar su identidad en línea

1



Compre un ordenador portátil barato que sólo lo utilice para filtraciones. Su ordendor personal casi seguramente tendrá información personal almacenada, lo que hace que sea fácil de encontrar. No utilice nunca un ordenador del trabajo o una personal con el que entra en las redes sociales y demás. Utilice dinero en efectivo para comprar un ordenador portátil barato y utilizarlo para filtraciones. Manténgalo apagado en todo momento, excepto cuando lo está utilizando para gestionar secretos. Si la alimentación está encendida, la localización del ordenador portátil puede ser rastreada. Nunca utilice este ordenador portátil para nada, excepto para filtrar información, y nunca lo utilice para ingresar información personal. No acceda a las redes sociales ni a las cuentas financieras.

Compre también un pendrive, una tarjeta de memoria o cualquier dispositivo de almacenamiento y no lo utilice para nada que no sea filtraciones. Antes de utilizarlo, encríptalo y pon una contraseña para cifrar los datos:

1. Conecta tu pendrive o memoria USB al ordenador, portátil, etc.
2. Abre Mi Pc.
3. Sobre el pendrive clic botón derecho del ratón.
4. Pulsa sobre la opción Activar BitLocker.
5. Espera a que termine de procesar. Tiene que llegar al 100%.
6. Listo. Ya está. Desconecta tu pendrive y vuelve a conectarlo para que solicite contraseña.

2

Cree una dirección de correo electrónico designada para gestionar filtraciones. Es posible que ya tenga varias cuentas de correo electrónico, pero todas tienen al menos su nombre adjunto. Utilice Gmail u otro servicio para establecer una cuenta de correo electrónico para las filtraciones. No ingrese ninguna información personal, especialmente su nombre o número de teléfono, sino que tiene que utilizar información ficticia y falsa, invéntatela. Haga que el nombre sea genérico y que no represente ningún vínculo contigo. Los ejemplos son: misfiltraciones@gmail.com, solosecretos2773379@yahoo.com, o cosascorreo97654@gmail.com.

3

Acceso wifi desde un lugar público. Cada punto de acceso wifi tiene información adjunta que lo identifica específicamente.
Las fugas o filtraciones de datos bajo una fuente de wifi personal o de un lugar de trabajo son fáciles de rastrear. Su actividad en línea se etiquetará con la dirección de IP. Es recomendable ir a algún lugar público como una cafetería para estar en una capa de anonimato.

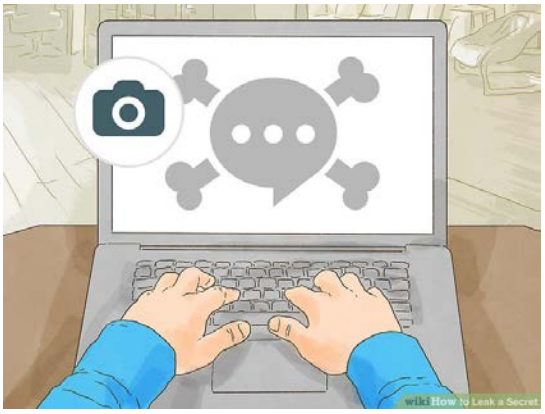
4

Descargue y utilice el Navegador Tor**.** Este navegador utiliza un sistema de redes de retransmisión que oculta tu información cuando se conecta a Internet a través de ellas. Al usar Tor, ocultas tu ubicación y dirección IP, así como la información personal adjunta a su ordenador. Para descargar el navegador y obtener más información sobre cómo funciona, visite el sitio web de Tor Browser. Para los que conocen Linux, hay una forma diferente de navegar en anonimato utilizando Tails, el sistema operativo que se puede iniciar en casi cualquier ordenador o portátil desde un dispositivo USB o cualquier tarjeta de memoria.

Método 2

Envío de documentos filtrados por correo electrónico

1



Envía una captura de pantalla o una foto de la información secreta. Si no puedes descargar los archivos y tan solo tienes permisos de lectura, haz fotos con el móvil, que tendrías según las explicaciones de esta guía en el método 4.
Si tiene documentos imposibles de obtener en un equipo, tome las fotos que puedas de la pantalla y conviértelas en un documento aparte. Envíe este documento según las instrucciones siguientes.

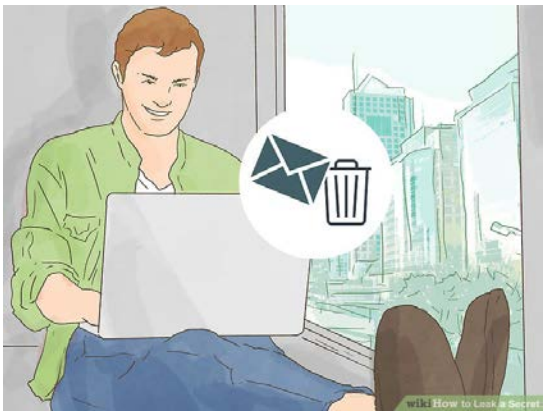
2

Elija una web de alojamiento de archivos en la nube. Si envía un correo electrónico a la cuenta de una organización, será fácil de localizar la filtración por el enlace a descargar. Archiva siempre en formato rar o zip, antes de enviar, los documentos, audios, imágenes o videos con el programa 7 Zip y pon una contraseña. Utiliza siempre nombres alfanuméricos para los archivos a guardar y las contraseñas superiores a 8 caracteres con mayúsculas, minúsculas, letras y signos especiales. Que nada guarde relación con alguna información personal en cuanto a fechas de nacimiento, nombres y demás.

Para textos o multitud de textos, lo mejor es AES Crypt, un software de cifrado de archivos disponible en varios sistemas operativos que utiliza el estándar avanzado de cifrado (AES) estándar de la industria para cifrar archivos de forma fácil y segura.
Es mejor que tengas tus secretos archivados o encriptados y envía la contraseña del archivo en cuestión junto con el enlace a descargar.

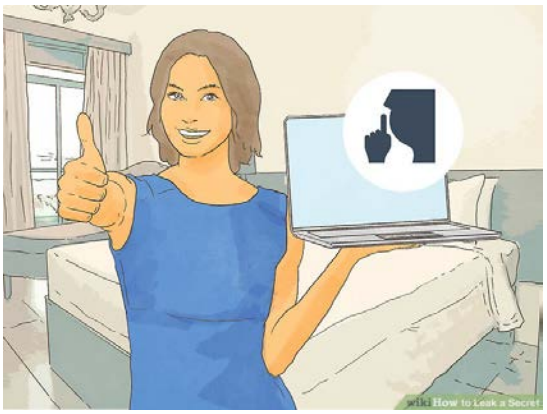
Mega, y Mediafire son plataformas alternativas mucho mejores que Google Drive, DropBox o Onedrive, en cuanto a anonimato, privacidad y rapidez de crear la cuenta y utilizarla.

3



Borra las cookies y apaga el wifi. Después de haber filtrado los documentos secretos a través de una fuente segura, cierre las ventanas que haya utilizado. En caso de que no utilizas Tor. Abre la configuración en tu navegador. Elimine las cookies y cualquier otro dato que su navegador esté configurado para guardar. A continuación, apague el wifi.

4



Apague el portátil antes de salir. Si su ordenador portátil está encendido, puede ser rastreado.

Ya que has filtrado el secreto desde un lugar público, apague el ordenador portátil mientras todavía estés allí. Asegúrate de esperar y comprobar que está completamente apagado antes de salir.

Método 3

Envío de documentos a través de Correos, Seur, Express,..etc

1

Maneje el documento y el sobre con guantes en su casa o lugar privado. Dejas huellas dactilares en todo lo que tocas. Al imprimir y recoger los documentos, use guantes. También asegúrese de usar guantes cuando ponga los documentos en el sobre y en cualquier momento que maneje el sobre.

2

Imprima una etiqueta de dirección. Dado que su escritura tiene una marca distinta, en realidad se puede estudiar y ser rastreado por los profesionales en seguridad nacional.
Por esta razón, querrá evitar el direccionamiento del sobre a mano. La impresión de una etiqueta es una manera rápida de evitar que su escritura le delate en caso de que, alguien se entere de lo que hace y los servicios de seguridad encuentre el sobre antes que el destinatario.
Si no tiene acceso a una impresora, escriba la dirección con su mano no dominante o modifique su estilo de escritura típico tanto como sea posible.

3

Deje la dirección en blanco. Puede parecer obvio, pero no quiere que nadie sepa quién envió el documento secreto, así que no escriba su dirección en el sobre.
Tras conocer el lugar del destino, si lo entregas tú mismo, vaya a horas punta e intenta vigilar el lugar una media hora antes por si ves a alguien conocido. Disfrázate para que no te reconozcan por si te encuentras a alguien y contrata a alguien que te lo lleve si es de confianza.
En caso de que lo envíes por correo o alguna empresa de paquetería, mejor contrate el servicio de recogida a domicilio y hazlo desde uno que no sea el tuyo y que esté muy lejos de tu casa o alguna propiedad privada tuya.

4

Si no puedes hacerlo de las formas anteriores, es mejor que dejes caer el sobre en un buzón público que no está cerca de tu casa. Nunca envíes por correo documentos seguros desde tu propia casa. No debes dejar rastro de la procedencia del sobre o paquete ya que podría ser intervenida la acción de filtración.

Método 4

Secretos filtrados por teléfono o tablet

1

Compre un teléfono y una tarjeta prepago con dinero en efectivo. Sus teléfonos personales y laborales son fáciles de localizar, así que nunca los utilices para la filtración de secretos.
Vaya a una pequeña tienda que está fuera de su área habitual y compre un teléfono y una tarjeta prepago que podrá utilizarla durante 7 días sin dar los datos personales y titularizarla. Utilice el saldo que tenga o cárguela siempre con dinero en efectivo. Cuando se le bloquea para pedir los datos personales, tírala y compra otra para los próximos 7 días. Nunca utilices las tarjetas que le puedan delatar directamente.

2

Deje el teléfono apagado a menos que lo esté utilizando. Cuando se enciende la alimentación, la ubicación del teléfono es notada por las torres de antenas GSM, aunque tengas desactivada la ubicación o no tengas conexión a internet y, es mejor que lo hagas en lugares aleatorios y lejos de su casa. Nunca lo conectes dos veces en el mismo lugar y no utilice patrones fijos para elegir el próximo, hágalo al azar. Siempre deje el teléfono apagado y saque la batería cuando no lo necesites.

3

Vaya a un lugar público y sólo conecte la batería y encienda el teléfono cuando llegue. Vaya a algún lugar donde sabe que siempre estará aglomerado de personas, como una tienda de ropa, un supermercado grande o un parque céntrico. Inserte la batería y encienda el teléfono para que pueda realizar la llamada, enviar el mensaje SMS, el correo electrónico o enviar las filtraciones por internet.

4

Haga su llamada lo más rápido posible. Incluso con un teléfono encriptado, alguien, en algún lugar podría estar escuchando la llamada y no tardará mucho en darse cuenta adonde está y quién es exactamente.

Por eso, como protocolo de seguridad, sobre todo después del primer contacto con la organización destinataria de la filtración, es mejor que diga lo que necesita decir de una manera eficiente y directa. Cuelgue el teléfono tan rápido como pueda, desconecte la batería y aléjate del lugar entre la multitud. No dé su nombre ni ninguna otra información personal. Limitase a dar o recibir una dirección de correo, página web o lugar de encuentro. Nada más, ni contraseñas, ni datos, ni nada de nada.

¡Adelante con tu iniciativa y no dejes que los miedos acaben con ella!

SocialLeaks ha elaborado esta guía para la filtración de datos actualizando y complementando un artículo publicado en WikiHow