RECOMENDACIONES PARA PROTEGER CONTRASEÑAS EN RR.SS.

Los cibercriminales están aprovechando la necesidad de información por la emergencia del covid-19 para multiplicar sus ataques. Hoy más que nunca, debemos ser cuidadosos, necesitamos comunicaciones autenticas y verdaderas en RRSS, para no confundir a la ciudadanía. Especial atención deben tener hoy las autoridades de gobierno y las personas de interés público en la privacidad de sus cuentas. CSIRT comparte algunos consejos.

CONSEJOS PARA PROTEGER EL ACCESO A TUS CUENTAS DE REDES SOCIALES

Las diferentes redes sociales disponen de políticas de seguridad que obligan a los usuarios a contar con una contraseña relativamente segura, pero no todos tienen el mismo estándar. Nosotros aconsejamos seguir ciertas normas para proteger el acceso a las cuentas, ya sea de redes sociales, correos y/o servicios disponibles en la red.

RECOMENDAMOS

- Que tu clave tenga una extensión de, al menos, 9 caracteres.
- Utilizar mayúsculas, minúsculas, números y caracteres especiales (puntos y símbolos).
- Utiliza frases de canción, poema, cita, película o pasaje de un libro.
- Utiliza secuencia de palabras inconexas (con reglas de mayuscula/minúscula incluida).
- Utiliza tres palabras bajo la secuencia "persona", "acción" y "objeto" (con reglas de mayuscula/minúscula incluida).

AL CREAR UNA CLAVE NUNCA

- NUNCA Utilizar el nombre, o el nombre de algún familiar.
- NUNCA Utilizar el nombre de alguna mascota.
- NUNCA Utilizar fechas de cumpleaños
- NUNCA Usar direcciones del trabajo o domicilio particular
- NUNCA Usar el RUT personal o de algún familiar
- NUNCA Usar el número de teléfono

UN EJEMPLO DE CONTRASEÑA SEGURA ES LA UTILIZACIÓN DE UNA FRASE QUE SEA FÁCIL DE RECORDAR

Ejemplo:

creando mi clave segura

1 Una vez tengamos nuestra frase la modificamos para hacerla más robusta y la reemplazamos los espacios por símbolos:

creando_mi_clave_segura

2 Luego podemos agregar mayúsculas:

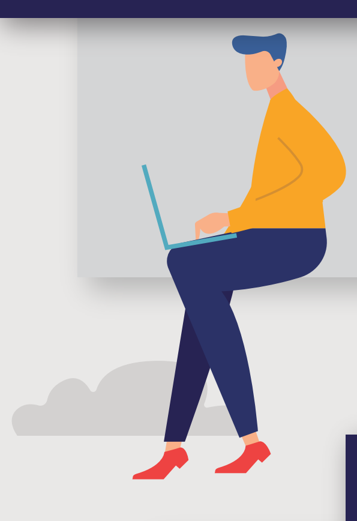
Creando_Mi_Clave_Segura

3 También podemos reemplazar vocales por números:

Cr34nd0_M1_Cl4v3_S3gur4

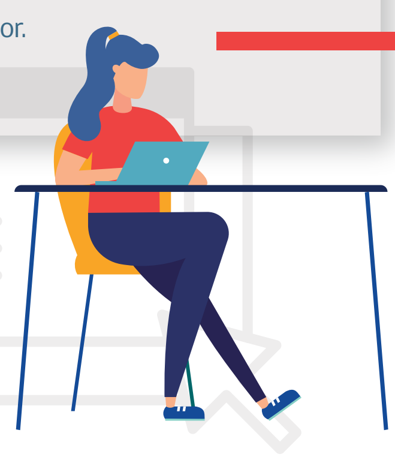
UNA VEZ CREADA LA CONTRASEÑA, UNA CONSIDERACIÓN IMPORTANTE ES PROTEGER NUESTRAS CLAVES ANTE POSIBLES "ROBOS" O FILTRACIONES. PARA ESTO, ALGUNAS RECOMENDACIONES SON:

- Verificar que la URL o APP que esté utilizando sea la genuina.
- Evitar el uso de redes públicas para el acceso a sus cuentas.
- Cambiar constantemente las contraseñas.
- No comparta su contraseña.
- No anote su contraseña en un papel.



PARA CADA RED SOCIAL UTILIZA SIEMPRE UNA CLAVE DISTINTA, CON ESTO EVITARÁS QUE SI SE LLEGA A FILTRAR UNA CLAVE NO TODAS LAS RR.SS. SE VERÁN COMPROMETIDAS.

Algunas redes nos ofrecen la opción de una autenticación de doble factor. Esto significa que, además de utilizar la clave que hemos creado, se deberá ingresar una segunda clave dinámica la que, dependiendo del servicio, nos podrá llegar vía correo al celular mediante un SMS, o bien, utilizando una aplicación de celulares como Google Authenticator.



EN LAS REDES SE ENCUENTRAN DIFERENTES PÁGINAS QUE NOS PUEDEN AYUDAR A VERIFICAR EL ESTADO DE NUESTRAS CUENTAS Y CONTRASEÑAS, ALGUNAS DE ELLAS SON:

- https://haveibeenpwned.com/
  En este sitio web se puede verificar si alguna de sus cuentas ha sido parte de alguna filtración.
- https://password.kaspersky.com/es/
  Con este servicio podemos verificar que tan robusta es nuestra contraseña.

¿QUÉ HACER CUANDO LAS CUENTAS HAN SIDO HACKEADAS?

Tres de las redes sociales más populares utilizadas entre personas, empresas e instituciones son Twitter, Facebook y LinkedIn. En todos los casos, las empresas ofrecen diferentes herramientas para brindar seguridad extra en las cuentas, las que están disponibles en sus respectivos centros de ayuda o seguridad. Pero, ¿qué sucede cuando perdemos el control de las cuentas?.

TWITTER

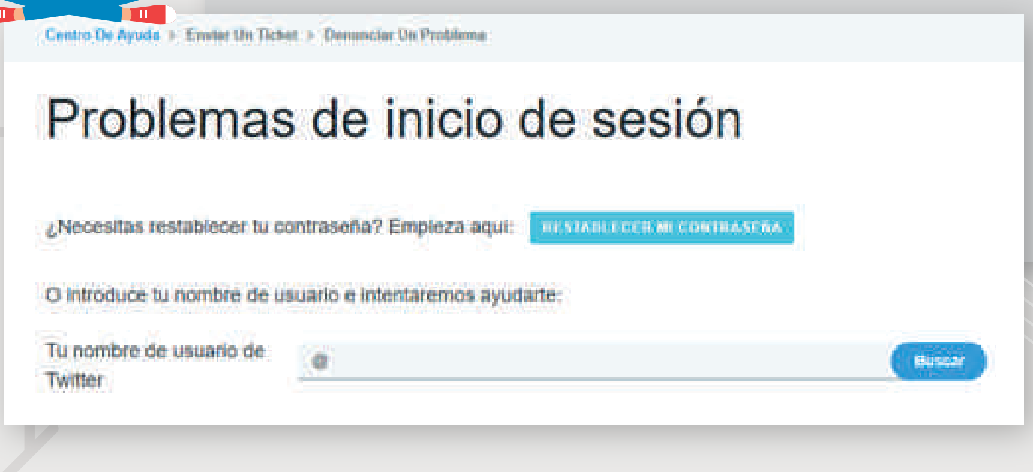
El Centro de Ayuda de Twitter ofrece a los usuarios recuperar su cuenta en el enlace **https://help.twitter.com/es/safety-and-security/twitter-account-hacked** en la que hay dos opciones. La primera el solicitar un restablecimiento de la contraseña. Para ello twitter va a solicitar un correo electrónico, un número de teléfono o un nombre de usuario asociado a la cuenta en cuestión.

Restablecimiento de contraseña

Encuentra tu cuenta de Twitter

Ingresa tu correo electrónico, número de teléfono o nombre de usuario.

La segunda opción es solicitar ayuda al soporte de Twitter. En ese caso, serás redirigido a un sitio de ayuda en que se pueden seleccionar diferentes alternativas dependiendo del problema: Inicio de sesión y cuenta; Funciones y configuración; Denunciar una infracción.
En la sección de "inicio de sesión y cuenta" aparece como tercera alternativa, "cuenta Hackeada", que permite al usuario reestablecer la contraseña con el nombre de usuario de Twitter.

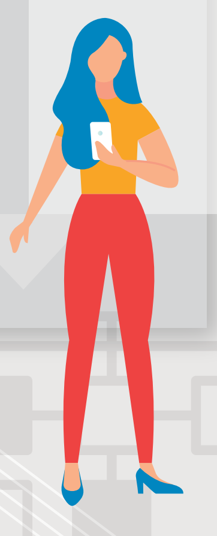


Problemas de inicio de sesión

¿Necesitas restablecer tu contraseña? Empieza aquí:

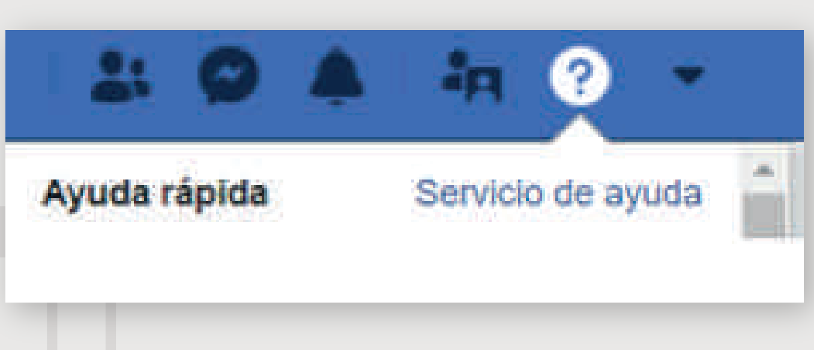
O introduce tu nombre de usuario e intentaremos ayudarte:

Tu nombre de usuario de Twitter: @

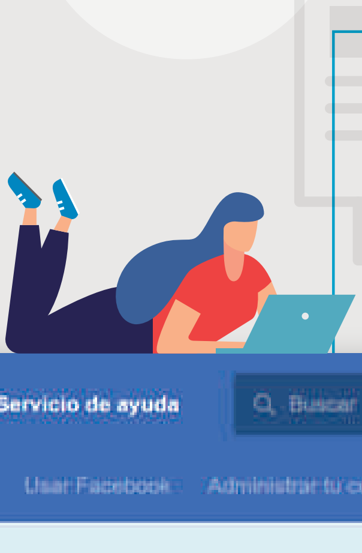


FACEBOOK

En el caso de Facebook, para acceder al asistente que guía la recuperación de recuperar la contraseña en caso de ser hackeada, es necesario ir al símbolo con el signo de interrogación en el banner superior del sitio y seleccionar el enlace "servicio de ayuda".



El enlace deriva a los usuarios a una página que ofrece diferentes servicios. Para la asistencia en este caso, se debe escoger en "Privacidad y seguridad" la opción "Cuentas falsas y robadas".



Preguntas más frecuentes

¿Qué nombres están permitidos en Fa

¿Cómo puedo elegir las notificaciones Facebook?

¿Dónde está mi configuración de Facebook?

¿Cómo cambio o restablezco mi contraseña de Facebook?

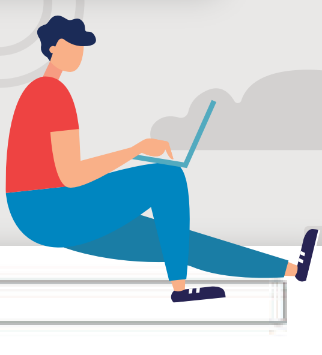
¿Por qué veo un mensaje de error en el que se indica que no puedo responder a una conversación en Facebook?

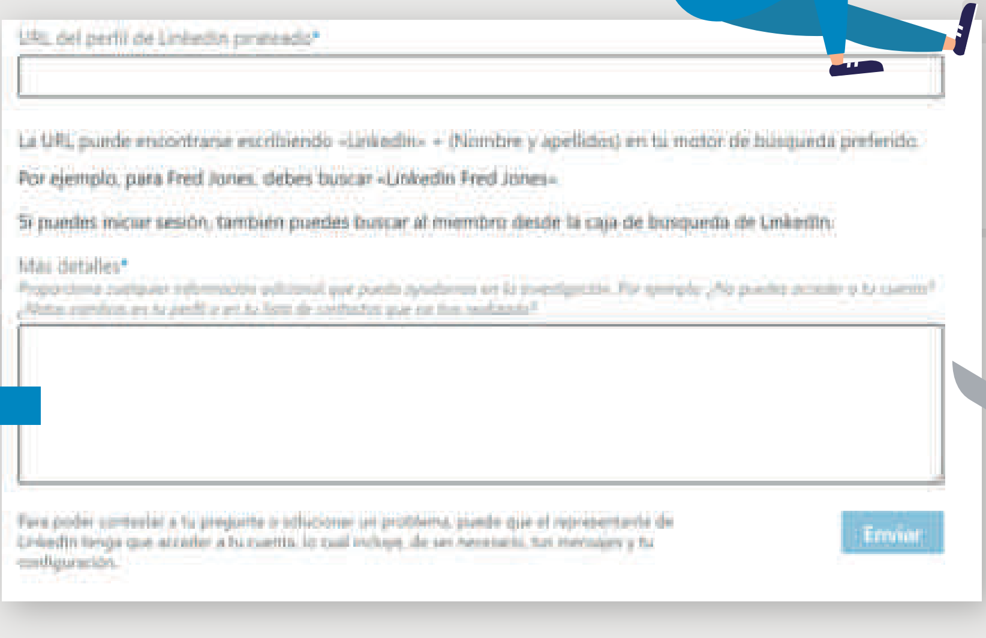
En la sección, a la que se puede acceder en este enlace **https://www.facebocom/hep/1216349518398524?helpref=hc_global_nav**, se ofrece orientación al usuario sobre qué hacer en caso de cuentas hackeadas, suplantación de identidad y cuentas falsas. La primera de estas tres opciones es la que recomendamos para obtener una mejor asistencia, específicamente el artículo "Creo que alguien hackeó mi cuenta de Facebook o la está usando sin mi permiso".

LINKEDIN

En el caso de LinkedIn, para buscar asistencia en debes acudir a la parte inferior del perfil de usuario, donde se encuentra la opción ¿tienes preguntas?. El enlace redirecciona al centro de ayuda del sitio. Una forma fácil de obtener ayuda es colocando en la búsqueda "Denunciar una cuenta pirateada". La búsqueda llevará de inmediata a un artículo en el que Linkedin ofrece ayuda sobre el tema. Aquí ofrecemos acceso directo a la página **https://www.linkedin.com/help/linkdin/answer/60005.**

Linkedin permite denunciar el pirateo de la cuenta llenando un formulario. Una vez que Linkedin recibe el formulario y verifican la cuenta, ayudan a los usuarios a recup.erar el acceso.





URL del perfil de LinkedIn pirateado*

La URL puede encontrarse escribiendo «LinkedIn» + (Nombre y apellidos) en tu motor de búsqueda preferido.

Por ejemplo, para Fred Jones, debes buscar «LinkedIn Fred Jones».

Si puedes iniciar sesión, también puedes buscar al miembro desde la caja de búsqueda de LinkedIn.

Más detalles*

Para poder contestar a tu pregunta o solucionar un problema, puede que el representante de LinkedIn tenga que acceder a tu cuenta, lo cual incluye, de ser necesario, tus mensajes y tu configuración.

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl

Síguenos en nuestras redes sociales
Infórmate sobre nuestras actividades y escríbenos directamente