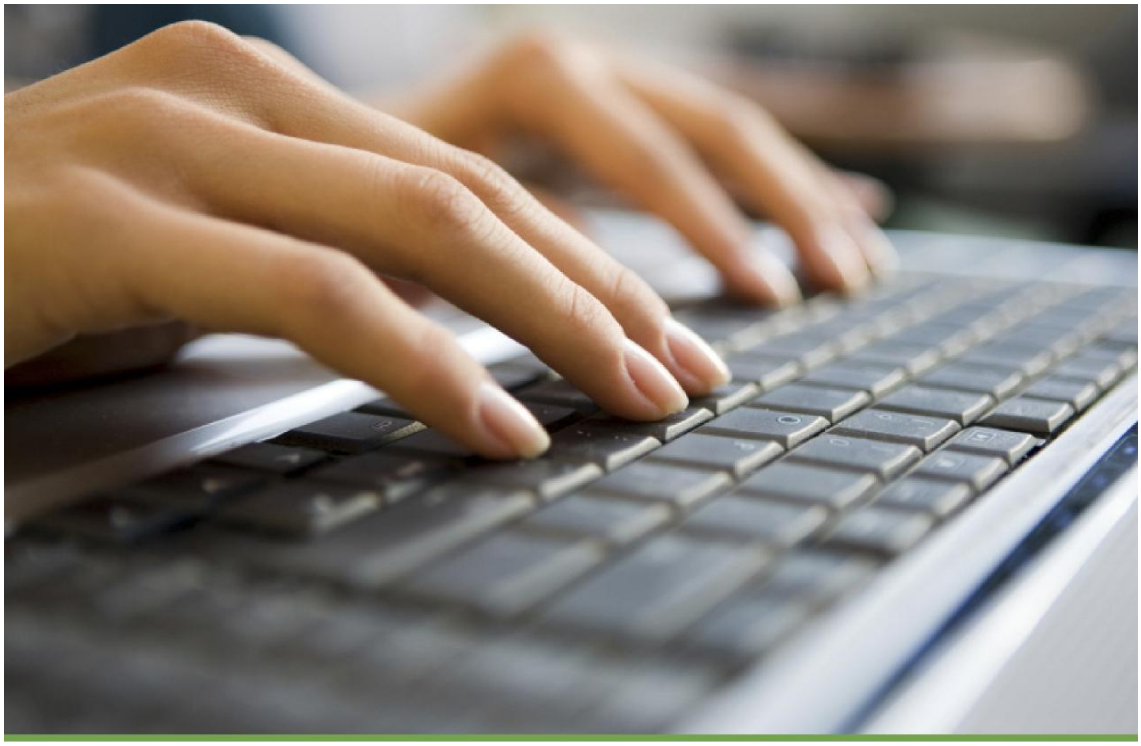


Sé dueño de tu espacio

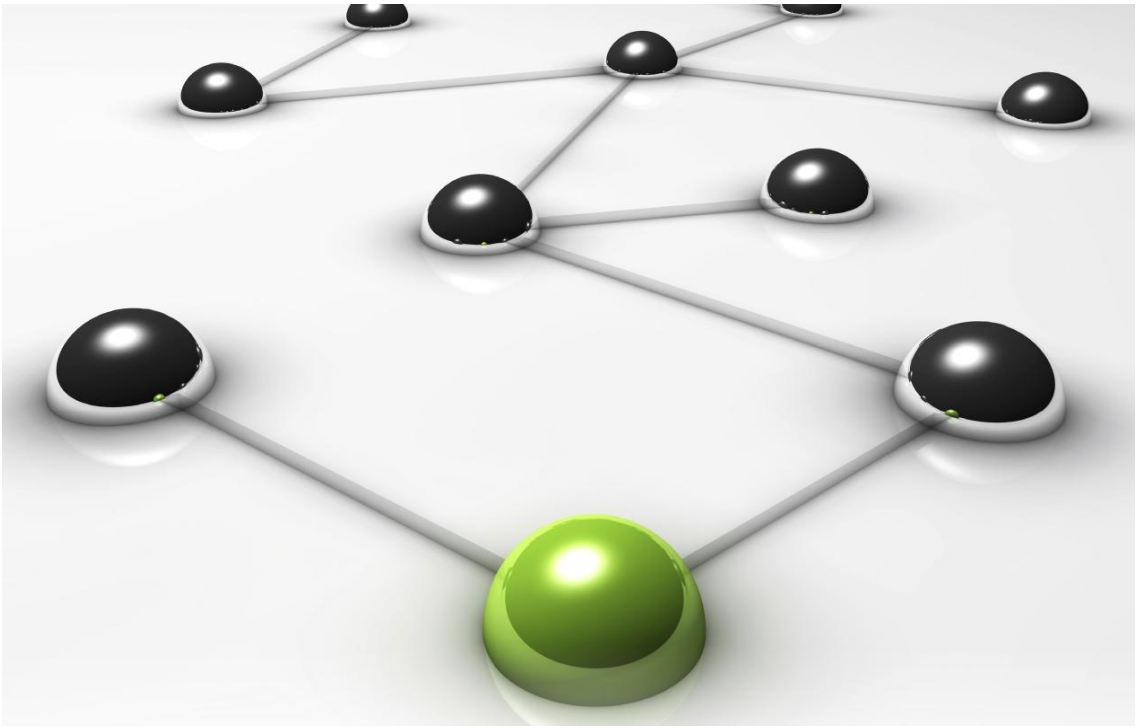
Guía de seguridad en Facebook

Para adolescentes, padres y educadores

Linda McCarthy, Keith Watson y Denise Weldon-Siviy

Esta guía online explica cómo puede:

- Proteger su cuenta en Facebook
- Evitar a los timadores
- Usar la configuración avanzada de seguridad
- Recuperar una cuenta de Facebook hackeada
- Poner coto a los impostores



Si hubo alguna duda respecto al increíble poder de las redes sociales, considere que cada día 500 millones de personas comparten más de mil millones de elementos de contenidos. Facebook conecta aproximadamente a unos 500 millones de personas en más de 210 países; realmente su población mundial excede el tamaño de la mayoría de los países europeos, y cuenta entre sus miembros a ciudadanos de todos los continentes.

La gente tiene en Facebook muchas posibilidades, pueden hacer Amigos, chatear, compartir actualizaciones de Estado, postear Comentarios, compartir Links, etiquetar Fotos, postear Videos, unirse a Grupos, crear Páginas, diseñar Polls (encuestas), y jugar juntos usando Aplicaciones. Usan Facebook para promover causas, intereses, e incluso así mimos. Facebook permite al mundo ser más abierto y estar conectado dando a sus usuarios las herramientas para interactuar y compartir de todas las formas imaginables. Parafraseando al superhéroe con un gran poder implica una gran responsabilidad. Tal y como una ciudad marca sus aceras, y los peatones miran ambos lados de la calle antes de cruzar, la seguridad en Facebook es una responsabilidad compartida entre Facebook y las personas que utilizan su plataforma.

Esta guía aspira sobre todo a facilitarte ser dueño de tu propio espacio, comprender lo que está haciendo Facebook para que el sitio sea más seguro y acometer las acciones que sean precisas en este nuevo mundo digital para protegerte a ti y tu cuenta. Pese a que la protagonista de esta guía es Facebook, las lecciones que aquí mostramos pueden aplicarse a cualquier página web que visites en la red. A lo largo de esta guía, haremos hincapié en las herramientas exclusivas que Facebook proporciona, de modo que puedas sacar provecho de su poder protegiendo tu cuenta, utilizando la configuración avanzada de seguridad, recuperando cuentas de Facebook hackeadas, y poner coto a los impostores.

Además de todo esto, queremos que adopte el lema: Párate. Piensa. Conéctate. Facebook tiene mucho que ofrecer a la gente, y con un poco de sentido común podrá sentirse seguro y a salvo. Esperamos que esta guía te sea útil. Por favor, únase a la conversación visitando la Página de Seguridad de Facebook en www.facebook.com/security.

Protege tu cuenta de Facebook

Eres la primera línea de defensa a la hora de proteger tu cuenta. Puedes tomar el control de tu protección utilizando una contraseña segura, sacando partido a la configuración avanzada de seguridad que proporciona autenticación, así como comunicaciones seguras, y asegurándote de que cierras la sesión cuando te desconectas.

Uso de las contraseñas adecuadas

Utilizar la contraseña adecuada es algo que deberías hacer cada vez que visites Internet, no sólo Facebook. Crear la contraseña adecuada es realmente sencillo. Tendrás que ser suficientemente compleja para que no pueda adivinarse, pero con suficiente sentido como para recordarla realmente.

¿Tienes una contraseña segura?

- No la uses para TODAS tus cuentas.
- No la compartas con amigos.
- Cámbiala periódicamente.
- Considera su almacenaje en una herramienta de contraseñas.

Una contraseña adecuada tiene al menos ocho caracteres, uno o más números, y al menos un carácter especial. No utilice palabras pero asóciela a una. Imagine que el nombre de su mascota es Buddy, usted vive en la calle State, tiene quince años, y le encanta mirar las estrellas por la noche. Una contraseña segura podría ser **budstatl5*.** O busqué algo gracioso que pueda recordar. Una mujer eligió como contraseña en el trabajo una que la recordaba porqué iba a trabajar **4da$cash**

¿No puedes recordar tantos detalles? usa una herramienta de contraseñas. Muchos navegadores integran actualmente cajas fuertes para contraseñas. Si el tuyo no la tiene considera utilizar una herramienta gratuita como "KeePass Password Safe" (http://keepass.info/). Y, si se da el caso de que aún así la olvides, asegurate de añadir una pregunta de seguridad y tu número de móvil en **CONFIGURACIÓN** DE CUENTA de tu cuenta en Facebook.

Cerrar la sesión de Facebook

Cerrar la sesión en Facebook cuando no se use es una forma sencilla y eficaz de proteger tu cuenta. Mucha gente cree que si cierra la página web o sale del navegador también cierra la sesión en Facebook. No es así. La siguiente persona que vaya a Facebook.com en tu ordenador se sorprenderá ya conectado a tu cuenta. Cerrar la sesión es esencial cuando accedas a Facebook fuera de casa.
Pero, también es importante si en casa compartes el ordenador. Pregúnteselo a Nathan, un chico de 16 años que dejo su cuenta de Facebook conectada en el ordenador familiar. Durante un entrenamiento de futbol, su hermana dejó plantada a su novia como si fuera él cambiando el estado de su relación en Facebook a SOLTERO. Desde entonces, siempre tiene cuidado de desconectarse de Facebook cuando sale de casa. Y recuerda, que si olvidas cerrar la sesión activa, siempre puedes cerrar la sesión de modo remoto

desde la sección **SEGURIDAD DE LA CUENTA** de la página de **CONFIGURACIÓN DE CUENTA**.

Pon coto a los timadores

Es humano evitar el peligro. Si ves que un piano te cae encima, automáticamente te quitas de debajo. Si ves un correo de un timador, vas a borrarlo e informar de que es spam. En Facebook, identificar a los timadores es más complicado dado que los mensajes parecen provenir de una persona que conoces y en la que confías. Luego, ¿cómo descubrir una impostura en Facebook? Permítenos empezar con una breve introducción.

Los timadores en Internet tienden a cambiar de objetivos. Al principio, los objetivos obvios de los timadores eran los adjuntos de correos de personas desconocidas. Entonces vinieron las alertas de seguridad de bancos o emisores de tarjetas. Hoy, puede ser también una actualización de Estado de un Amigo que te pide que veas un nuevo video o visitar una página web estupenda.

Timadores convencionales

Los timadores atacan a Facebook por la misma razón que al resto de la Red, quieren acceder a ta información, a tu ordenador o a tu dinero. Y algunas veces desean engañarte haciéndote descargar en tu ordenador programas maliciosos. Lo difícil es reconocer a los phishers, ladrones de cuentas y traficantes de programas maliciosos.

Los phishers roban la información personal, a menudo los datos necesarios para cometer estafas o suplantar la identidad. El **Phishing** es un intento de engañar a los usuarios para que revelen información personal o datos financieros. Ya has visto timos en tu correo electrónico. En Facebook, los phishers pueden intentar timarte desde múltiples lugares en post de Estado de tu perfil, en mensajes de Facebook, y en el chat de Facebook. Incluso pueden remitir correos periódicamente fingiendo ser Facebook o un popular App como *Farmville* o *Mafia Wars*.

Los ladrones de cuentas intentan engañarte para que te conectes a una página falsa de Facebook para sustraerte tu nombre de usuario y contraseña. Por este motivo siempre debes comprobar la barra de direcciones de tu navegador para asegurarte de que estás en Facebook y no en alguna otra página no relacionada.

¿Para qué querría alguien tu cuenta en Facebook? Esperan acceder a otras cuentas usando tu contraseña. Podrían querer vender tu información, o timar a tus Amigos. La gente es más propensa a caer en un timo cuando viene de alguien en quien confía, como un Amigo.

Los traficantes de programas maliciosos buscan instalar programas informáticos perjudiciales en tu ordenador. Dichos programas maliciosos, llamados **malware**, están diseñados para dañar tu ordenador o robar información de carácter personal. Dicho malware puede hacer muchas cosas desagradables. Puede instalar programas espías (spyware) para registrar que teclas pulsas y recopilar tus números y contraseñas de cuentas financieras. O incluso bloquear tu ordenador y pedir un rescate. ¿Cómo seleccionan los traficantes de malware a los usuarios de Facebook? Se te ofrecerá descargar e instalar nuevos programas en tu ordenador. Puede ser un nuevo juego, un organizador de fotografías digitales, un reproductor musical digital, o cualquier otro programa informático de utilidad. Antes de descargar ningún programa "gratuito", pregúntate siempre quien lo ha hecho y porqué puede ser gratuito. Ante la duda, no lo descargues. Eres la primera línea de defensa contra el malware. ¡Piensa antes de hacer clic!

Phishing es un intento de engañar a los usuarios para que revelen información personal o datos financieros

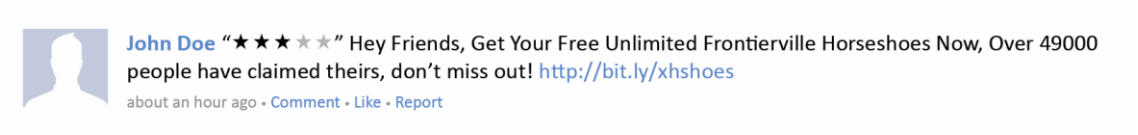
Malware son programas maliciosos que pretenden dañar su ordenador o sustraer información personal

Timadores que eligen Facebook

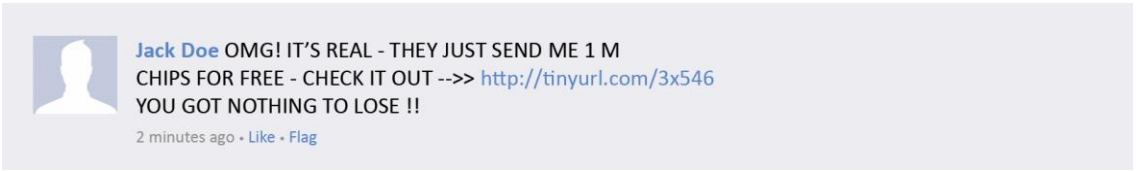
Además de los timadores vulgares y corrientes que se encuentran por doquier en Internet, hay diversos timos que eligen las redes sociales y a los usuarios de Facebook. Estos incluyen timos mediante aplicaciones de Juegos, timos que explotan la vanidad personal, robos de cuentas de Facebook, timos con scripts maliciosos, y Clickjackers (ladrones de clics).

Burlar los timos de juego

Cuando hablamos de timos mediante aplicaciones de Juegos, no queremos decir que las compañías de aplicaciones (Apps) le timen. Son realmente más una víctima, como los usuarios de Facebook que caen en la trampa. Si juegas en la red, ya sabes que tienes que tener cuidado para no caer en los timos de juego. Ya has visto ofertas engañosas y piratas. Muchas de ellas que prometen convertirte en un gran jugador están diseñadas en realidad para robar tu información personal.



Muchos timos de phishing fingen proceder de populares páginas web de juegos. El peligro no está en utilizar aplicaciones conocidas de terceros como *Frontierville*, sino dejarse engañar por phishers que supuestamente ofrecen puntos o claves para juegos. Los timos más comunes ofrecen premios como objetos virtuales gratis. Otros cebos te comunican que tu cuenta ha sido anulada y proporcionan un link para solucionar el problema. Alguno de estos timos llegaran a tu Muro, pero muchos llegarán directamente a tu correo electrónico. ¿Por qué? Números. *Farmville* cuenta con unos 16 millones de jugadores. Cualquier spammer que ataque a una extensa lista de correos electrónicos con un cebo para phising está destinado a atrapar un buen número de jugadores de *Farmville* sencillamente porqué hay muchos jugadores de *Farmville*.



También puedes ver post como el anterior en el Muro. Si haces clic en el enlace te dirigirán a una página web falsa de acceso a Facebook . Al intentar acceder a Facebook a través de la página falsa, estás proporcionando directamente tu contraseña al timador.

¿Cómo puedes saber que es un timo mediante phishing? Facebook nunca te dirigirá a la página principal una vez que hayas iniciado tu sesión.

Facebook nunca te dirige a la página principal si ya has iniciado la sesión.

Este timador también utiliza en el anterior ataque un servicio de vínculos abreviados. Pese a que los servicios de vínculos abreviados son de gran utilidad dado que simplifican las URL muy largas, lo malo es que desconoces a donde te llevan hasta que haces clic. Sé muy cuidadoso a la hora de hacer clic sobre esta clase de vínculos abreviados.

Evitar a los ladrones de cuentas de Facebook

Cuando se roba una cuenta de Facebook, suele ser debido a que la víctima ha picado el anzuelo y ha utilizado una página falsa de acceso a Facebook .

¿Cómo te hacen picar los timadores? Los timadores intentan pillarte con la guardia baja y te golpean con una página falsa de acceso de Facebook cuando realmente YA estás utilizando Facebook. El timador puede postear una actualización de Estado en tu Muro que incluya un vínculo a algo tentador. Lo pueden hacer mediante una cuenta que hayan robado de uno de tus Amigos para ganarse tu confianza. El mensaje será algo que llamará tu atención. Pueden ser fotos escandalosas, una primicia de una próxima película picante o un video raro. Cuando haces clic en el vínculo, te piden que inicies de nuevo la sesión en Facebook, salvo que ya no estás en Facebook. El vínculo te remite realmente a una página web diferente, de forma que cuando vuelves a acceder a Facebook con tu usuario y contraseña se los estás dando a un timador.

Además de otros timos cuyos correos electrónicos que son realmente horrorosos y escritos en un pésimo inglés, la mayoría de las páginas de acceso falsas de Facebook son bastante creíbles.

La anterior página falsa de acceso se reconoce porqué falta una e de Facebook (se ve Facbook) en la barra de direcciones. Este es un timo muy cuidado dado que la gente, al leer, introduce sin darse cuenta las vocales que faltan en una palabra.

¿Cómo evito engaños tan sutiles como éste? Recuerda que Facebook nunca contactará enviándote un mensaje de Facebook o posteando un mensaje de Estado en tu Muro y, comprueba SIEMPRE cuidadosamente el vínculo en la barra de direcciones y los vínculos sobre los que hace clic. Ante la duda NO HAGAS CLIC. Si Facebook contacta contigo, será a través del correo electrónico ordinario que proporcionaste cuando abriste tu cuenta de Facebook.

Comprueba siempre el vínculo y NO HAGAS CLIC si parece sospechoso.

Además, recuerda que Facebook sólo necesita que te registres para acceder una vez en cada sesión. Si te lo piden de nuevo NO es Facebook.

Evitar los timos mediante scripts maliciosos

Los timos con scripts maliciosos son uno de los ataques furtivos más empleados contra los usuarios de Facebook. Uno de los métodos de ataque más comunes consiste en hacerte creer que puedes ver quien está mirando tu perfil. Este tentador timo intenta engañarte y hacer que pegues un texto en la barra de direcciones de tu navegador.

El "código único" que se muestra arriba es el script malicioso. Mientras que esperas pacientemente según las instrucciones, el script está configurando tu perfil para mandar spam a todos sus Amigos.

Como respuesta para detectar estos ataques, Facebook añadió comprobaciones para ayudar a detectar scripts que se pegan en la barra de direcciones. Así, si se pega un script en la barra de direcciones, Facebook te pedirá que confirmes que realmente deseas pegar dicho script, e incluso te informará de que es una mala idea. Presta atención a dichos avisos.

No pegues un script en la barra de direcciones salvo que sepas exactamente que hace y cómo.

¿Cómo evitar timos mediante scripts maliciosos? No pegues un script en la barra de direcciones salvo que sepas *exactamente qué* hace y *cómo* lo hace. Avisa también a tus Amigos si empiezas a recibir spam de ellos. Tus Amigos pueden desconocer completamente que sus cuentas de Facebook han sido hackeadas. Comunícaselo para que cambien sus contraseñas y recuperaren sus cuentas hackeadas si lo precisan. (Lee más adelante cómo recuperar una cuenta hackeada.)

Evita el clickjacking (secuestro de clics)

El clickjacking es una técnica utilizada por los atacantes para engañar a los usuarios para que hagan clic en sus enlaces o botones ocultos a la vista. El clickjacking es posible debido a un fallo de seguridad en los navegadores que permiten a las páginas web ocultarse por capas y no ser vistas. Crees que estás haciendo clic en un botón

normal, cómo el botón **PLAY** de un video raro, pero en realidad estás haciendo clic en un vínculo oculto. Dado que no puedes ver el vínculo oculto del clickjacker, no tienes ni idea de lo que realmente hace. Puedes estar descargando malware o haciendo que toda tu información en Facebook se vuelva pública sin percatarte de ello.

Una forma de clickjacking es esconder un botón **LIKE (me gusta)** bajo un botón aparentemente inocente. Es lo que se denomina un Likejacking. Un timador puede engañarte haciéndote decir que te gusta un producto del que nunca has oído hablar en un solapado intento de crear un aviso de marketing viral. A primera vista, likejacking parece más molesto que peligroso, pero no siempre es cierto. Si te engañan para decir que te gusta Justin Bieber, no se va a acabar el mundo, pero puedes estar colaborando a propagar spam o enviando a tus Amigos a algún sitio que posiblemente contiene malware.

¿Cómo puedes evitar que te pinchen? Tecnológicamente, puedes minimizar los riesgos manteniendo al día las actualizaciones de tu navegador. Los navegadores añaden continuamente actualizaciones para cerrar vulnerabilidades que permiten operar a los clickjackers y otros timadores. Si utilizas Firefox, considera instalar también el complemento NoScript. Además, presta atención a lo que coges y de quien. ¿Compartiría realmente un profesor de facultad un post para ver videos de cámara oculta? Si un post de uno de tus Amigos te parece sospechoso, ¡no hagas clic en él!

Un post sospechoso puede ser síntoma de que la cuenta de Facebook de tu Amigo ha sido secuestrada o que a tu Amigo le han clickjackeado a **LIKE (me gusta)** o **SHARE (compartir)** sin saberlo. Si conoces a tus Amigos, sabes lo que realmente marcarían como **LIKE** o **SHARE**. Por eso tu mejor protección contra los timos es no confirmar peticiones de Amigos de gente a la que realmente no conoces.

Otra gran herramienta para ayudarte a evitar el clickjacking es Web of Trust (WOT) [Página web de confianza]. WOT es una herramienta gratuita para el navegador que mantiene una base de datos de reconocidos sitios web seguros, así como de webs consideradas maliciosas por la comunidad WOT. Si intentas visitar una web que se sabe es maliciosa WOT te avisará de antemano. La descarga de WOT es fácil de instalar, sólo tienes que visitar www.mywot.com.

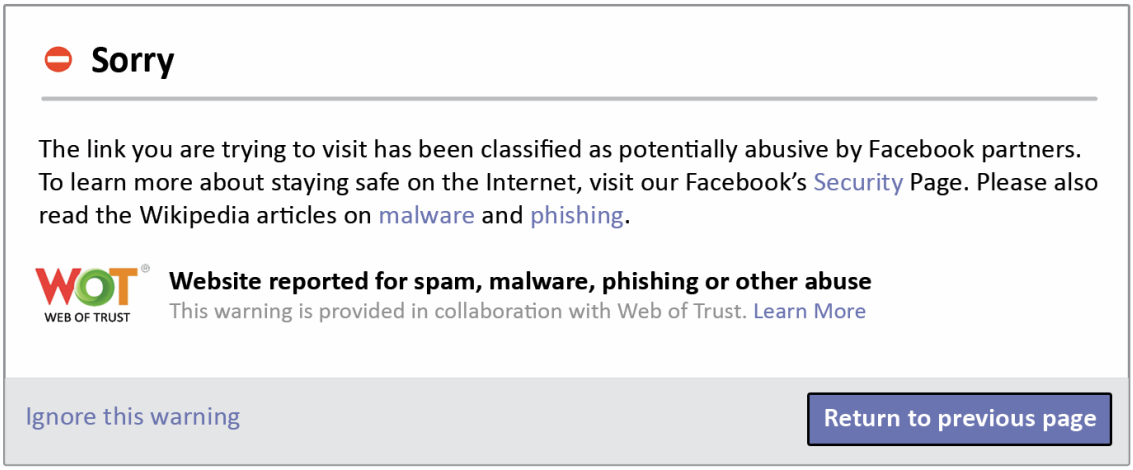
Consejos de seguridad

• Mantén tus programas actualizados.

• No hagas clic en vínculos sospechosos.

• Usa las herramientas de seguridad disponibles.

Facebook también efectúa comprobaciones para detectar páginas web maliciosas o que envían spam. Si añades WOT a las comprobaciones que efectúa Facebook consigues una herramienta más para tu arsenal contra los hackers. Ambas comprobaciones trabajan juntas proporcionando un sistema de alerta conjunto si intentas visitar una web de la que se ha informado contiene malware, phishing, o spam:



Clickjacking es una técnica utilizada por los atacantes para engañar a los usuarios para que hagan clic en vínculos o en botones ocultos a la vista.

Uso de la Configuración de Seguridad avanzada

Facebook adopta ciertas de medidas entre bastidores para mantener la seguridad del sitio web. Facebook también proporciona herramienta que la gente puede usar para proteger sus cuentas y reputación en la web. Dichas herramientas incluyen opciones de navegación segura, contraseñas de un solo uso, inicio único de sesión, posibilidad de supervisar las actividades de la cuenta, aprobación de contraseñas, la posibilidad de dar por finalizada la sesión de la cuenta de modo remoto, y autenticación social.

Uso de la navegación segura

La navegación segura te permite usar Facebook con seguridad en puntos de conexión públicos. Cuando compras en Internet, tu navegador utiliza una encriptación muy sólida para transmitir los datos. La encriptación es una técnica que se usa para cifrar la información y que nadie más pueda verla.

El **protocolo** SSL encripta la transmisión de los datos y se le denomina *https* o *navegación segura*.

La navegación segura es una configuración avanzada en Facebook que puedes personalizar. Al usar https para conectarte a Facebook suceden varias cosas importantes. Primero, en una red inalámbrica abierta, impide que los atacantes roben tu conexión de red a Facebook o husmeen en tu comunicación. También hace uso de un certificado de verificación para garantizar que si tu navegador dice que está conectado a Facebook, estés realmente conectado a Facebook y no una pagina impostora que finge ser Facebook.

Para activar https, vaya a la sección **SEGURIDAD DE LA CUENTA** de la **CONFIGURACIÓN DE CUENTA** de tu Facebook y selecciona: **NAVEGA EN**

FACEBOOK SIEMPRE QUE SEA POSIBLE MEDIANTE UNA CONEXIÓN SEGURA (HTTPS).

¿Cómo puedes saber que el protocolo https está en uso? Cuando SSL está en uso, sabrás que ta comunicación entre páginas web es segura porque verás un "https" al comienzo de la URL. También veras un candado. Busca el icono del candado en tu navegador, y si lo ves, entonces tu configuración de navegación segura está activada.

Utilización de contraseñas de un solo uso

Siempre hay un pequeño riesgo cuando accedes a tu cuenta de Facebook desde un ordenador que no es de tu propiedad. Nunca sabrás realmente donde habrá estado ese ordenador. Puede estar infectado con un programa de registro de pulsaciones de teclado que puede registrar todos tus movimientos, incluida la contraseña de tu cuenta en Facebook. No puedes impedirlo, pero puedes asegurarte de que la contraseña robada no va ha funcionar al usar contraseñas de un solo uso.

Para usar una contraseña de un solo uso, primero necesitas estar registrado y verificar tu teléfono móvil con Facebook. Una vez hecho esto, puedes conseguir una contraseña de un solo uso mandando el mensaje "otp" (por "***o**ne-**t**ime **p**assword*" que significa "contraseña de un solo uso") al 32665 (FBOOK). Facebook te enviará un mensaje de texto con una contraseña temporal que puedes usar para acceder a tu cuenta de Facebook en vez de usar tu contraseña habitual. Si consiguen esa contraseña, no importa porque sólo funciona una vez, mejor dicho sólo durante 20 minutos. Es una buena idea utilizar una contraseña de un solo uso si utilizas el ordenador de otra persona.

Uso del inicio único de sesión

Uno de los pasos más importantes para proteger tu información es tener una contraseña diferente para cada cuenta que tengas. Por supuesto, recordar todas las contraseñas es difícil. Facebook ha abierto su sistema de cuentas de usuario a otras páginas web para su uso. Eso quiere decir que puedes utilizar tu cuenta de Facebook para acceder a otras páginas web que admitan acceso a través de Facebook. La primera vez que uses tu acceso a Facebook desde una nueva página web, Facebook te pedirá permiso para compartir tu información con esa página web. Si lo permites, la página web puede cargarse automáticamente al reconocer que ya has accedido a Facebook, lo cual es una gran ventaja. Cuantas más páginas web permitas que reconozcan tu acceso registrado a Facebook menos nombres de usuarios y contraseñas tendrás que recordar.

Protocolo. Protocolo es un conjunto de reglas que utilizan los ordenador es para comunicarse entre si.

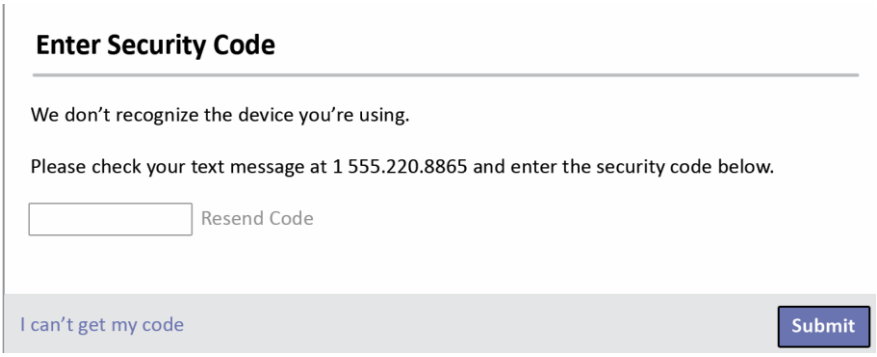
Supervisar la actividad de la cuenta

Cuando accedes a tu cuenta, Facebook reconoce tu ordenador o teléfono móvil. Si quieres, Facebook puede decirte cuando ha accedido alguien a tu cuenta desde otro sitio.

En la sección **SEGURIDAD DE LA CUENTA** de tu **CONFIGURACIÓN DE CUENTA** puedes usar la **NOTIFICACIONES DE ACCESO** para pedir a Facebook que te envíe un correo electrónico si un ordenador o dispositivo móvil distinto accede a tu cuenta. Si el nuevo acceso no es tuyo, sigue el vínculo del correo electrónico para expulsar al intruso. Si lo prefieres, puedes hacer que Facebook te envie un SMS en vez de un correo electrónico.

Puedes incluso expulsar al intruso tu mismo. En la sección **SEGURIDAD DE LA CUENTA** de tu **CONFIGURACIÓN DE CUENTA** encontraras la lista de ordenadores asociados a tu cuenta y con la actividad de la misma. Si en la lista hay ordenadores que ya no utilizas o que no has utilizado nunca, puedes borrarlos. En la sección **ACTIVIDAD DE LA CUENTA,** puedes encontrar la actividad más reciente y otras sesiones activas. Si alguna de ellas pareciese sospechosa, haz clic en **FINALIZAR ACTIVIDAD,** cerrando así la sesión inmediatamente.

Otra estupenda característica de seguridad es la **APROBACIÓN DE ACCESOS**. Si tienes un teléfono móvil, Facebook puede enviarte un mensaje de texto con un código único para usarlo cuando accedas a Facebook desde un ordenador diferente. Si lo tienes activado, se te pedirá que introduzcas un código que recibirás a través de un mensaje de texto cuando intentes acceder. Es una característica estupenda que aporta otro nivel de seguridad para aquellos que acceden a Facebook desde localizaciones remotas. Asegúrate de tener tu móvil y ve a la sección **SEGURIDAD DE LA CUENTA** de tu **CONFIGURACIÓN DE CUENTA** para personalizarla. Una vez introducidas dichas configuraciones, la siguiente vez que accedas desde un ordenador distinto te enviarán a tu móvil un mensaje de texto con el código de aprobación. A continuación puedes ver la pantalla de Facebook que te pide que introduzcas dicho código.



Uso de la autenticación social

Cuando una página web desea impedir a un programa automático que registre una serie de cuentas falsas, le pide que haga algo que sólo puede hacer un ser humano. Suelen ser a menudo un test que implica la resolución de un sencillo problema matemático, responder a una pregunta fácil, o teclear una serie de letras y números de una imagen. Esas imagenes con palabras raras son un CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart)* o Prueba de Turing pública y automática para diferenciar máquinas y humanos. Estas sencillas imágenes impiden que los atacantes utilicen software para crear muchas cuentas que envien spam o señuelos de phishing a gran escala.

Facebook utiliza una prueba similar denominada Autenticación Social cuando Facebook detecta que tu cuenta está en uso pero cree que el usuario puedes no ser tu. Por ejemplo,

si vives en Indiana y se accede a tu cuenta desde la India, Facebook empieza a sospechar.

¿Por qué Autenticación Social? Para empezar, Facebook ES una red social, Y lo que es más importante, Facebook buscaba una forma sencilla para identificarte que no se viese comprometida si la cuenta si lo estuviese. Obviamente, si alguien más está usando tu cuenta realmente, bien puede haber adivinado o robado tu contraseña de forma que preguntar directamente por ello no ayudaría en modo alguno.

¿Conoces a todos tus Amigos?

Facebook supone que sí. Si accedes desde un lugar extraño, como cuando estás de vacaciones en Europa, Facebook comprueba tu identidad haciéndote identificar a tus Amigos en las fotografías etiquetadas.
Aquí es donde entran tus Amigos. Si Facebook sospecha que alguien más está intentando utilizar tu cuenta, te pedirán que identifiques a tus Amigos. Literalmente. Facebook crea una serie de imágenes a partir de tu lista de Amigos y las coloca como un examen con respuestas múltiples . Cada foto tiene una lista de nombres, tienes que seleccionar el nombre que coincide con el nombre del Amigo etiquetado en dicha foto. Dado que es poco probable que un timador pueda reconocer a simple vista a tus Amigos, ésta es una buena prueba.

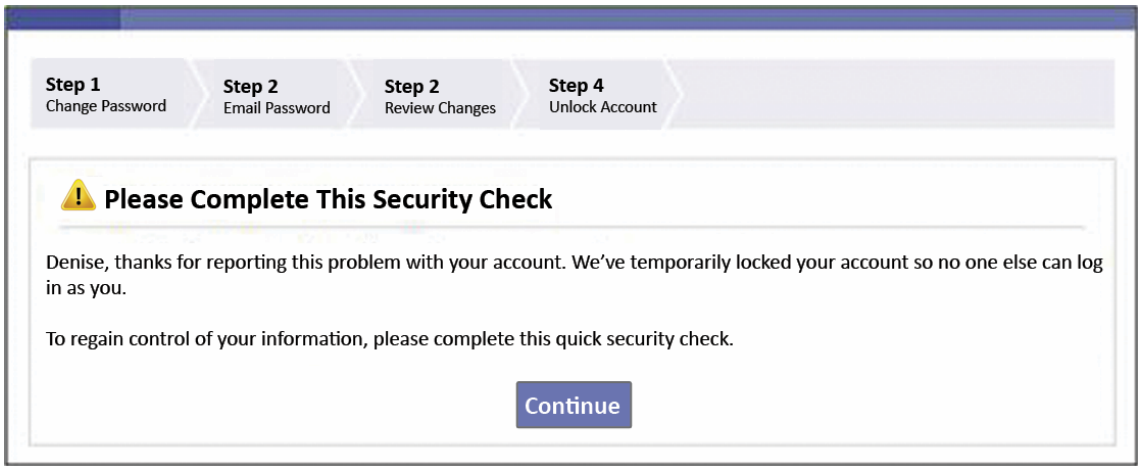
Recuperación de una cuenta de Facebook hackeada

Hay cierto número de síntomas que pueden indicar que tu cuenta de Facebook ha sido hackeada. Puedes notar actualizaciones de Estado que no has posteado o recibir contestaciones a mensajes de Facebook que no has enviado. Esto *podría* significar que tu cuenta ha sido hackeada. Cambia inmediatamente tu contraseña y asegúrate de que usas de las configuraciones de seguridad avanzadas.

Otro indicio de que tu cuenta ha sido hackeada es que no puedas acceder a ella. Esto sucede cuando el timador que ha hackeado la cuenta ha cambiado tu contraseña. No puedes volver a cambiarla porque ya no sabes cual es. Algunos timadores incluso cambian la información personal de modo que no puedes verificar quién eres.

El equipo de Facebook se dedica a ayudarte a proteger tu cuenta. Facebook ha construido sistemas que buscan y bloquean actividades sospechosas, posts y mensajes falsos. Facebook también cuenta con un proceso bien definido si te roban la cuenta para ayudarte a expulsar al timador y recuperarla.

Si tu cuenta se ha visto comprometida, ve a http://www.Facebook.com/hacked y selecciona **PROTEGE TU CUENTA**.



Tan pronto lo comuniques, Facebook bloqueará tu cuenta, tu no podrás utilizarla aún pero el timador tampoco. Facebook te pedirá entonces: **POR FAVOR, COMPLETE ESTA COMPROBACIÓN DE SEGURIDAD** para desbloquear tu cuenta.

Facebook te lo pone fácil, simplemente sigue el proceso de cuatro pasos para reclamar tu cuenta.

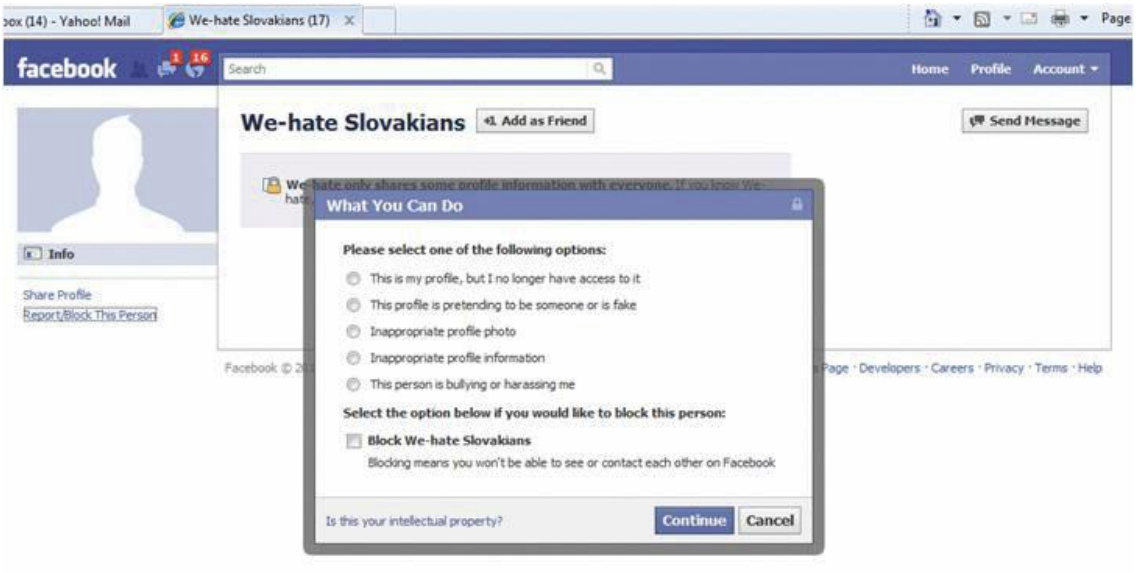
Una vez que hayas recuperado tu cuenta, asegúrate de configurar las Características de seguridad avanzadas para añadir una capa de seguridad adicional a tu cuenta. Concretamente, asegúrate de activar la navegación segura (https) y establecer las notificaciones de acceso; así Facebook te hará saber inmediatamente si se ha accedido a tu cuenta.

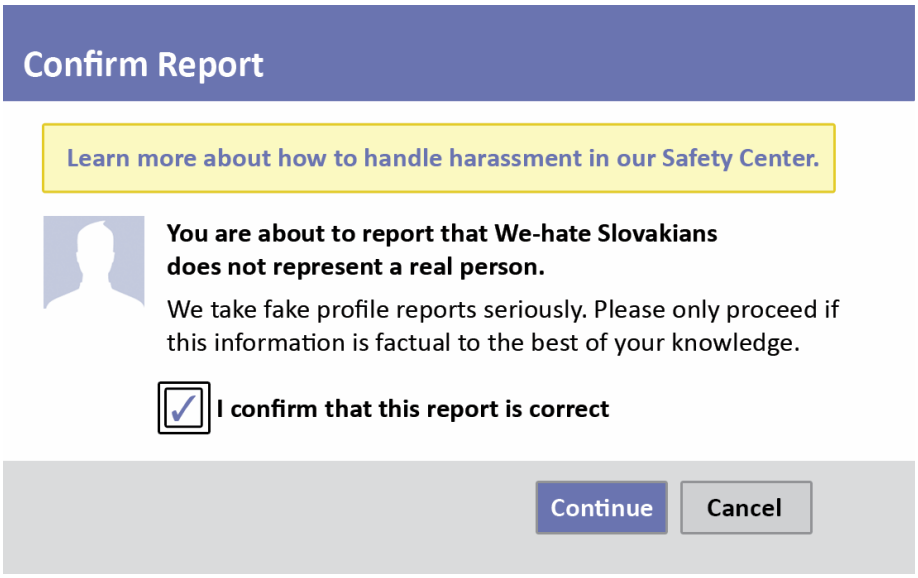
Pon coto a los impostores

Es muy triste que una buena cuenta funcione mal porque la han robado. Resulta desagradable cuando una cuenta se INICIA mal porque se creó para acosar, avergonzar o intimidar a alguien. Esto es lo que hace la cuenta de un impostor, cuando alguien finge SER tú creando una página en Facebook. Las páginas de los impostores se crean para acosar o intimidar a la persona por la que se hacen pasar. Si ves la página de un impostor, comunícalo inmediatamente Facebook.

El vínculo a **INFORMAR/ BLOQUEAR ESTA PERSONA** está disponible en la parte inferior izquierda de todos los perfiles de Facebook.

Puedes informar sobre gente que se está haciendo pasar por ti o un Amigo. Puedes también usar este vínculo para informar de personas falsas, negocios que pretenden ser personas y grupos de odio ocultos bajo la apariencia de personas.





Si informas sobre una persona falsa o información inapropiada, no necesitas hacer más. Facebook te agradecerá que informes del problema y luego investigará tu queja y cerrará la cuenta si procede.

Si informas sobre un impostor o un caso de ciberacoso, hay un paso más. Dado que una forma de acosar a la gente en Facebook ha sido acusarles falsamente de acoso, Facebook no hará nada hasta que proporciones un número de teléfono válido. Aparentemente, a los acosadores no les gusta dar sus números de teléfono. Una vez que hayas proporcionado un número de teléfono valido, Facebook enviará un código a tu teléfono que deberas introducir para confirmar tu queja antes de investigarla.

Un futuro más seguro

Los riesgos para la seguridad cambian constantemente. ¿Recuerdas las "stalker Apps" (aplicaciones acosadoras que prometen mostrarte quien está viendo tu perfil) que engañaron a todos el año pasado? ¿Y los vínculos que prometen fotos graciosas editadas tuyas o de imágenes en las que estás etiquetado de este año? Por supuesto que ninguna de estas fotos existió, pero el tentador vínculo se envió para intentar pillar al usuario con la guardia baja. Continuamente surgen nuevas amenazas.

El riesgo de hoy puede estar anticuado mañana. El truco es reconocer los riesgos futuros cuando se presenten. Los equipos de seguridad de Facebook trabajan duro para protegerte, pero tu tienes que participar en mantener a salvo tu cuenta. Para aprender más sobre seguridad y recibir posts sobre amenazas y nuevas características de seguridad de Facebook, comprueba las páginas de seguridad de Facebook (**FACEBOOK SECURITY** y **FACEBOOK SAFETY)**.

Los mejores trucos para mantenerte a salvo en Facebook

• Haz sólo Amigo a quien conozcas.

• Crea una buena contraseña y úsala sólo para Facebook.

• No compartas tu contraseña.

• Cambia periódicamente tu contraseña.

• Comparte tu información personal sólo con las personas y empresas que lo necesites.

• Accede a Facebook sólo UNA VEZ cada sesión. Si parece que Facebook te pide que inicies la sesión por segunda vez, haz caso omiso de los vínculos y teclea directamente www.facebook.com en la barra de direcciones de tu navegador.

• Cuando utilices el ordenador de otra persona usa una contraseña de un solo uso.

• Cierra la sesión de Facebook después de usar un ordenador que no sea tuyo.

• Haz uso de la navegación segura siempre que te sea posible.

• Descarga Apps sólo de páginas de confianza.

• Mantén actualizado tu antivirus.

• Mantén tu navegador y demás aplicaciones actualizadas.

• No pegues scripts (código) en la barra de direcciones de tu navegador.

• Usa complementos para tu navegador como "Web of Trust" y "NoScript" de Firefox para prevenir que tu cuenta sea secuestrada.

• Cuidado con los posts "goofy" de cualquiera, incluso Amigos. Si parece algo que tu Amigo no postearía, no hagas clic en ello.

• Los timadores pueden hackear las cuentas de tus Amigos y enviar vínculos desde sus cuentas. Cuidado con vínculos tentadores que provengan de tus Amigos.

¡Recuerda PÁRATE | PIENSA | CONÉCTATE!

Si quieres una mayor protección en la Red, por favor consulta la campaña *Párate, Piensa, Conéctate* tanto dentro como fuera de Facebook. Consulta la página de seguridad de Facebook y haz el test de Seguridad de forma que compruebes tus conocimientos y aprendas las prácticas recomendadas sobre seguridad en Internet.

Sobre el equipo

La Guía de seguridad en Facebook ha sido escrita conjuntamente por reputados autores del sector de la seguridad.

Linda McCarthy fue Directora principal de Seguridad en Internet de Symantec. Linda aporta 20 años de experiencia en áreas de formación en seguridad, auditoría, y desarrollo de productos.

Keith Watson es ingeniero en investigación de seguridad en la Universidad Purdue. Sus áreas de investigación han sido: arquitectura de la seguridad, biometría, ciencias forenses digitales, programación de seguridad y privacidad.

Denise Weldon-Siviy es profesora y editora con dos décadas de experiencia en edición y una casa llena de adolescentes usuarios de Facebook.

PÁRATE | PIENSA | CONÉCTATE