CONSEJOS DE SEGURIDAD PARA PERIODISTAS

Agradecemos a estos socios el haber revisado estas normas de seguridad

CPJ

ConnectSafely

European Journalism Centre

JAMES W. FOLEY LEGACY FOUNDATION

facebook Journalism Project

10 CONSEJOS PARA MANTENER TU SEGURIDAD

Los periodistas están usando Facebook de maneras innovadoras para hacer su trabajo, relatar sus historias y conectarse directamente con la gente.

Queremos verificar que tu información y tus cuentas estén seguras para que puedas mantener tu seguridad en línea y protejas tus fuentes y contactos. Estos son 10 pasos a seguir:

1 PROTEGE TU CONTRASEÑA

Tu contraseña de Facebook debe ser única, segura y nunca se debe revelar a alguien ni en ningún lugar. Se debe evitar incluir en ella información clave, cualquier cosa que te pueda identificar personalmente, como tu nombre, tu número telefónico, tu fecha de nacimiento y tu dirección postal. Un consejo consiste en usar un administrador de contraseñas, el cual mantendrá tus contraseñas seguras y protegidas, y podrá generar contraseñas seguras para todas tus cuentas.

2 RECIBE AVISOS DE ALERTA DE DISPOSITIVOS NO RECONOCIDOS

Usa las alertas de inicio de sesión para recibir notificaciones cada vez que alguien intente entrar a tu cuenta con un dispositivo nuevo o no reconocido.

Activa las alertas de inicios de sesión no reconocidos en la sección de Seguridad e inicio de sesión que está en Configuración. Cuando las alertas están activadas, recibirás un correo electrónico o una notificación cada vez que alguien inicie una sesión en tu cuenta con un dispositivo o navegador no reconocido.

3 ACTIVA LA AUTENTICACIÓN EN DOS PASOS

La autenticación en dos pasos es una capa adicional de seguridad para tu cuenta. Esta se encuentra en la sección de Seguridad e inicio de sesión que está en Configuración. Al activar la autenticación en dos pasos, se te pedirá que escribas un código de seguridad especial cada vez que intentes entrar a tu cuenta de Facebook con una nueva computadora o un nuevo teléfono o navegador.

Estas son unas opciones para recuperar tu código de seguridad especial:

- Si tienes la aplicación de Facebook en tu smartphone o tablet, usa el generador de códigos.
- Si estás utilizando la última versión de Chrome u Opera, registra un dispositivo de seguridad físico en tu cuenta para que solo tengas que usar un pequeño dispositivo que se conecta a la unidad USB de tu computadora. Los dispositivos de seguridad se pueden adquirir en compañías como Yubico y funcionan con el estándar Universal 2nd Factor (U2F) abierto de FIDO Alliance.
- Si ninguno de estos métodos funciona para ti, Facebook también te puede enviar un mensaje de texto (SMS, que puede tener un costo) con un código de inicio de sesión cada vez que lo necesites
- También puedes obtener 10 códigos de recuperación para imprimirlos o escribirlos. Guárdalos en un lugar seguro para cuando los necesites, o compártelos con un amigo o colega en quien confíes mucho para respaldarlos.

4 USA LAS HERRAMIENTAS DE COMPROBACIÓN RÁPIDA DE FACEBOOK

Usa la comprobación rápida de seguridad para revisar y administrar la configuración de seguridad de tu perfil. Tú puedes:

- Ver los navegadores y las aplicaciones que has utilizado antes para iniciar una sesión en Facebook, pero que no has usado en más de un mes. eliminar rápidamente el acceso en los que ya no necesitas.
- Administrar alertas para cuando se haya iniciado una sesión con un dispositivo o navegador no reconocido.
- Ver consejos sobre cómo mejorar tu contraseña y con qué frecuencia cambiarla.

Usa la comprobación rápida de privacidad para que solo las personas de confianza puedan ver tu información y tus publicaciones, ya que quizás quieras compartir unas veces cosas públicamente y otras veces solo con tus amigos. Puedes revisar quién puede ver tus publicaciones y la información de tu perfil, como tu número telefónico y tu dirección de correo electrónico. También muestra la configuración de las aplicaciones con las que has iniciado una sesión en Facebook. Puedes utilizar la comprobación rápida de privacidad para revisar y hacer ajustes a tu configuración de privacidad y verificar que estés compartiendo tus historias con las personas que quieres que las vean.

5 ADMINISTRA TU PRESENCIA EN PERFILES Y PÁGINAS

Tu presencia puede ser tan pública o tan privada como quieras con tu audiencia en Facebook. Estos son algunos consejos para administrar lo que publicas.

PERFIL

- Usa la herramienta de selector de público para determinar quién puede ver tus publicaciones. Puedes elegir entre compartir con todo el mundo, solo con tus amigos o hasta con una audiencia personalizada. Al crear una audiencia personalizada, puedes compartir de manera selectiva con personas específicas.
- Para controlar quién ve lo que publicas, actualiza la configuración en la pestaña de Biografía y etiquetado. Puedes aprobar o quitar etiquetas que tus amigos agreguen a tus publicaciones. Una vez que apruebes una etiqueta, la persona etiquetada y sus amigos podrán ver tu publicación. La revisión de etiquetas se encuentra en la sección de "Biografía y etiquetado" que se encuentra en Configuración.
- Con la revisión de la biografía, puedes decidir si las publicaciones en las que te etiquetan aparecen en tu biografía o no. Si alguien que no es amigo tuyo te etiqueta en una publicación, esto irá automáticamente a la revisión de la biografía. Si también deseas revisar etiquetas por amigos, puedes activar la revisión de la biografía para ver las etiquetas de cualquier persona. La revisión de la biografía está en la sección de "Biografía y etiquetado" que se encuentra en Configuración.
- Administra la manera en que tu perfil se muestra a otras personas con la herramienta "Ver como". Solo ve a tu perfil, haz clic en "Ver como" y mira cómo ve tu perfil el público o una persona específica.

PÁGINA

Si eres un editor de medios sociales, un periodista que usa una página para llegar a sus lectores o audiencia, o un moderador de una página, hay varias opciones para mantener tu página segura. Al seleccionar y asignar las funciones administrativas correctas, podrás administrar tu página sin poner en riesgo las contraseñas. Cada persona iniciará una sesión en su cuenta personal y desde ahí trabajará en la página. Es importante asignar los roles correspondientes en la página porque no todos necesitan tener un control administrativo total de una página; algunas personas solo necesitan responsabilidades editoriales o de anunciantes.

- Verifica que los administradores de las páginas utilicen cuentas reales para que no pierdan el acceso a sus cuentas. En Facebook eliminamos cuentas falsas y de suplantación de identidad cuando las detectamos.
- Utiliza las herramientas de filtro y moderación de la página que están en la sección de configuración de la página, para moderar proactivamente los comentarios y las publicaciones de los visitantes. Estas herramientas también bloquearán palabras y activarán el filtro de groserías de tu página. No olvides filtrar las distintas variaciones de las palabras prohibidas. Puedes agregar puntos o espacios entre ellas y hashtags. Por ejemplo, para filtrar la palabra "arma", también incluye "a.r.m.a.", "#arma" y "a r m a". Si bien no puedes inhabilitar comentarios en las publicaciones de tu página, sí

puedes ocultar o eliminar comentarios individuales. Si ocultas un comentario, la persona que lo publicó no sabrá que está oculto.

- Puedes prohibir a las personas que publican continuamente spam en tu página. Puedes eliminar esta prohibición en cualquier momento. Al prohibir a alguien el acceso a tu página, esa persona podrá seguir compartiendo contenido de tu página con otros lugares de Facebook, pero ya no podrá publicar en tu página, hacer clic en "me gusta" o comentar las publicaciones de tu página, enviar mensajes a tu página ni marcar "me gusta" de la página.
- Si deseas que alguien en un lugar distinto transmita en vivo desde su página de Facebook, puedes darle el rol de "Colaborador en vivo". Esto le permitirá transmitir en vivo, pero le limitará el acceso a otras funciones de tu página.
- Facebook también te permite eliminar cualquier comentario que desees eliminar de tu perfil o página, independientemente de que contravengan nuestros estándares de la comunidad o no.

6 CONTROLA TU UBICACIÓN EN LAS PUBLICACIONES

Facebook te da la opción de incluir una ubicación en tus publicaciones. Facebook no comparte la ubicación de manera predeterminada, pero siempre es una buena idea actualizar o desactivar los servicios de ubicación de tu teléfono antes de publicar algo desde áreas que puedan comprometerte. Puedes actualizar la configuración de tu ubicación en tu dispositivo Android o iOS.

7 PROTEGE TU COMUNICACIÓN

Utiliza servicios de mensajes como WhatsApp y Facebook Messenger para comunicarte de manera privada con tus fuentes.

- WhatsApp hace un cifrado de extremo a extremo de manera predeterminada de cada mensaje que envíes o cada llamada de hagas. Cuando se hace un cifrado de extremo a extremo, tus llamadas y mensajes están protegidos de manera que solo tú y la persona con la que te comunicas pueden tener acceso a ellos y nadie más, ni siquiera WhatsApp. Para mayor protección, cada mensaje que envíes tiene su propia clave y su propio bloqueo, los cuales son especiales para cada mensaje. Todo esto sucede automáticamente: no hay necesidad de activar una configuración ni de configurar chats secretos especiales para proteger tus mensajes. También puedes mostrar notificaciones de seguridad para recibir notificaciones cuando el código de seguridad de algún contacto haya cambiado.
- Puedes enviar mensajes con cifrado de extremo a extremo en Messenger con tu dispositivo iOS o Android. Estas "conversaciones secretas" están pensadas para que solo las tengan tú y la otra persona, y nadie más, incluyéndonos a nosotros. En Messenger, inicia una nueva conversación y toca el ícono de candado en Android o la palabra 'Secreto' en tu iPhone para iniciar una conversación secreta con alguien. Recuerda que tendrás que seguir estos pasos para cada persona con la que converses.

Los periodistas también pueden usar Facebook con el navegador Tor para ayudar a ocultar su dirección IP, con el fin de que Facebook, los anunciantes, las redes telefónicas locales y los ISPs no vean en dónde están iniciando una sesión. Así se protege aún más la seguridad de su ubicación y conexión con Facebook. Para tener acceso a Facebook con el navegador Tor, visita https://facebookcorewwwi.onion/. En Android, Facebook también funciona con Tor a través de la aplicación proxy Orbot, que puedes descargar de Google Play.

8 BLOQUEA LOS MENSAJES DE ACOSO

Cuando bloqueas a alguien, esa persona ya no podrá hacer cosas tales como etiquetarte ni ver las cosas que publicas en tu biografía. Si son amigos, el bloqueo también les eliminará de sus listas de amigos.

PARA BLOQUEAR A ALGUIEN EN UNA COMPUTADORA DE ESCRITORIO:

1. Haz clic en la parte superior derecha de cualquier página de Facebook.
2. Haz clic en **Accesos directos de privacidad**
3. Haga clic en ¿**Cómo evito que alguien me siga molestando?**
4. Escribe el nombre de la persona que deseas bloquear y haz clic en **Bloquear**.
5. En la lista que aparece, selecciona la persona específica que deseas bloquear y haz clic nuevamente en **Bloquear**.

PARA BLOQUEAR A ALGUIEN EN MESSENGER:

iPhone y iPad:

1. Abre una conversación con la persona que deseas bloquear
2. Toca su nombre en la parte superior de la conversación
3. Desplázate hacia abajo y toca **Bloquear**
4. Toca junto a **Bloquear mensajes**

Android:

1. Abre la conversación con la persona que deseas bloquear
2. Toca, desplázate hacia abajo y toca **Bloquear**
3. Toca **Bloquear todos los mensajes**

Las personas no recibirán una notificación cuando las bloquees.

Si no puedes encontrar la persona que deseas bloquear con este método, visita el perfil de la persona y selecciona **Bloquear** en el menú de su foto de portada.

9 REPORTA CONTENIDO ABUSIVO Y SUPLANTACIÓN DE IDENTIDAD

La mejor manera de reportar contenido abusivo, spam o suplantación de identidad en Facebook es mediante el vínculo "Reportar" que aparece cerca del contenido en sí. Nosotros revisaremos el reporte y tomaremos las medidas necesarias.

Estos son algunos ejemplos de cómo puedes reportar contenido:

- Para reportar un comentario en Facebook:
  - En la parte superior derecha, haz clic en la flecha que apunta hacia abajo
  - Selecciona "**Reportar publicación**"
- Para reportar un mensaje en Messenger en una computadora de escritorio:
  - Abre el mensaje que deseas reportar
  - Haz clic en el engranaje de Opciones que está en la parte superior derecha
  - Haz clic en **Reportar** o **Bloquear** y sigue las instrucciones que aparezcan en la pantalla
- Para reportar una suplantación de identidade:
  - Ve al perfil suplantado
  - Haz clic en el "..." que está junto a "Mensaje" en la foto de portada
  - Selecciona "Reportar"
- Para ver instrucciones para todos los tipos de contenido, ve a https://www.facebook.com/report

Si sientes alguna amenaza, ponte en contacto con las autoridades. Para denunciar un acoso ante las autoridades, haz capturas de pantallas y copia los enlaces URL de cualquier comunicación no deseada **antes** de bloquear al acosador. Después de bloquear a alguien, la relación que haya tenido contigo ya no será visible.

10 INFÓRMATE PARA SABER QUÉ HACER EN CASO DE HACKEO

Si crees que han hackeado o tomado el control de tu cuenta, debes protegerla lo antes posible. Para ayudar a evitar esta situación, puedes tener habilitada la autenticación en dos pasos.

Si puedes iniciar una sesión en tu cuenta, te recomendamos cambiar tu contraseña. Revisa los datos de contacto de tu cuenta para verificar que esté correcta y no la hayan alterado. Si no puedes iniciar una sesión en tu cuenta, podemos ayudarte a proteger tu cuenta al requerir que cambies tu contraseña y que revises la actividad de los inicios de sesión recientes. También puedes ir a facebook.com/hacked.

Agradecemos a estos socios el haber revisado estas normas de seguridad

COMMITTEE TO PROTECT JOURNALISTS

CONNECTSAFELY

EUROPEAN JOURNALISM CENTRE

INTER AMERICAN PRESS ASSOCIATION (IAPA)

JAMES FOLEY FOUNDATION

JON CAMFIELD, MEGAN DEBLOIS/INTERNEWS

facebook.com/journalists