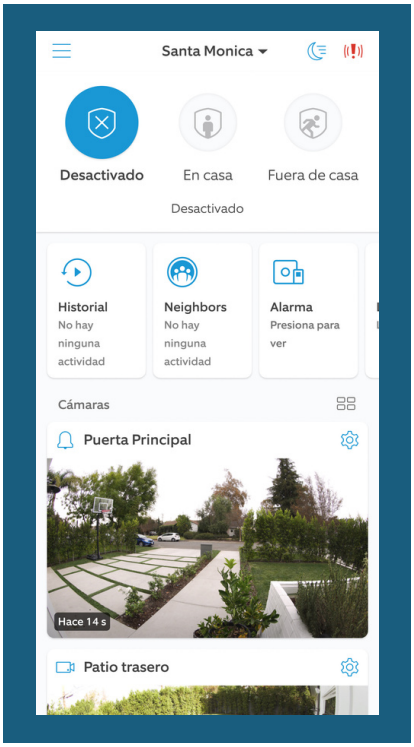
tcfv
TEXAS COUNCIL ON FAMILY VIOLENCE

LOS DISPOSITIVOS DE SEGURIDAD RING

Guía de seguridad para sobrevivientes

RESUMEN DE LA GUÍA

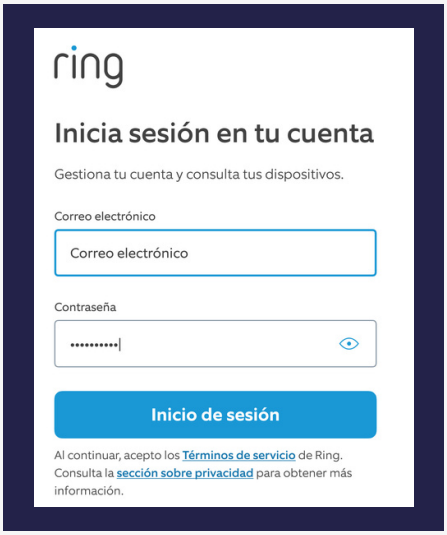
Los Dispositivos de Seguridad ring están a su disposición como complemento de su plan de seguridad si así lo desea. Esta guía, en asociación con una discusión con un defensor, está destinada a proporcionar información sobre los riesgos, los beneficios y los pasos que puede tomar para maximizar su seguridad. Esta guía destacará estos pasos, explicará las mejores prácticas y capacitará a cualquier persona para tomar decisiones para utilizar su dispositivo Ring de la forma más segura posible.



ACERCA DE LOS DISPOSITIVOS RING

Los dispositivos Ring, como los timbres con vídeo y las cámaras de vigilancia, se conectan a la aplicación Ring (en la imagen de la izquierda) en su teléfono, tableta u ordenador y le permiten ver una transmisión de vídeo en alta definición de una persona en su puerta (u otro lugar) y hablar con ella mediante una comunicación de audio bidireccional. Estos dispositivos se conectan a su red wifi doméstica y pueden enviar alertas cuando se detecta movimiento o cuando alguien pulsa el botón del timbre. Para obtener más información, visite Ring.com.

1 CONFIGURACIÓN Y SEGURIDAD DE LA CONTRASEÑA



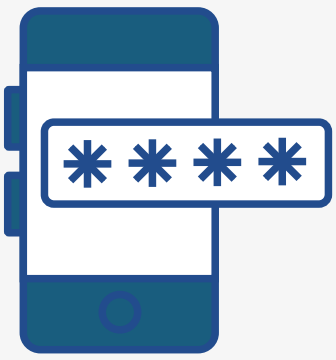
Su contraseña es la clave para acceder a su cuenta Ring desde cualquier dispositivo. Le sugerimos que utilice una contraseña nueva y única que nadie más conozca o pueda adivinar.

EN VEZ DE reutilizar una contraseña o usar algo personal como su fecha de nacimiento o la de un ser querido, el número de seguro social, el número de teléfono, el equipo deportivo favorito, etc.

PRUEBE USAR una frase u oración más larga (una línea de una película, un libro, una canción, un chiste, etc.) o utilice una aplicación de gestión de contraseñas que le ayude a crear y recordar diferentes contraseñas para varias cuentas. Obtenga más información sobre gestores de contraseñas y sugerencias aquí. Ring también tiene requisitos y sugerencias específicas para las contraseñas que puedes leer aquí.

¿PUEDE ALGUIEN ENTRAR EN MI CUENTA SI CONOCE MI CONTRASEÑA?

Durante el proceso de configuración de la cuenta, es obligatorio que todos los usuarios de Ring tengan activada la **"verificación en dos pasos"**, lo que puede ayudar a impedir el acceso desde el inicio de sesión en su cuenta en su cuenta incluso si alguien conoce su nombre de usuario y contraseña. Con cada inicio de sesión en su cuenta Ring, recibirás un código único de seis dígitos por correo electrónico o mensaje de texto para verificar su intento de inicio de sesión. Una persona debe introducir ese código antes de que se le permita acceder a su cuenta Ring. Obtenga más información aquí.



Cuando se utiliza la verificación en dos pasos, sólo es segura si nadie más tiene acceso a su cuenta de correo electrónico o a los dispositivos donde se reciben los mensajes de texto. Puede ser útil actualizar su contraseña de correo electrónico y añadir un PIN o código de acceso a su cuenta de operador de telefonía móvil para ayudar a evitar cambios no autorizados. Cada compañía es diferente, así que acceda a la cuenta de su compañía de telefonía móvil o llama a su compañía de telefonía móvil para que le ayuden.

APLICACIONES DE AUTENTICACIÓN

Si prefiere que el código de seis dígitos no se envíe por correo electrónico o mensaje de texto, puede utilizar una "aplicación de autenticación" que genere el código por usted. Aunque alguien tenga acceso a su cuenta de correo electrónico o pueda ver sus mensajes de texto, no podrá obtener el código. Este proceso se explica aquí.

¿QUÉ PASA SI ALGUIEN LOGRA INICIAR SESIÓN CON ÉXITO SIN MI CONSENTIMIENTO?

Ring te enviará un correo electrónico cada vez que un nuevo dispositivo se conecte con éxito a su cuenta Ring. Si cree que alguien conoce su contraseña o ha iniciado sesión sin su consentimiento, debes abrir la aplicación Ring y:

Paso Uno ➡

Haga clic en las 3 líneas horizontales en la esquina superior izquierda > haga clic en el centro de control > haga clic en 'dispositivos autorizados por los clientes' para vea todos los dispositivos que actualmente han iniciado sesión > tome una captura de pantalla (por si la necesita como prueba más adelante) y > elimine cualquier dispositivo no autorizado tocando el icono del bote de basura rojo junto al dispositivo (las instrucciones están aquí).

Segundo Paso ➡

Actualice su contraseña (las instrucciones están aquí).

2 SU DIRECCIÓN DE CORREO ELECTRÓNICO

Ring utiliza su dirección de correo electrónico para enviar alertas de seguridad, enlaces para restablecer la contraseña y otra información importante. Si alguien tiene acceso a su cuenta de correo electrónico o dispositivo móvil, puede restablecer las contraseñas y eliminar las notificaciones importantes enviadas por Ring.

EN VEZ DE utilizar una dirección de correo electrónico que otras personas puedan conocer (o que tengan o hayan tenido acceso a ella).

INTENTA CREAR y utilizar una nueva dirección de correo electrónico (con una nueva contraseña única) para configurar su cuenta de Ring.

3 PROTECCIÓN DE SU(S) DISPOSITIVO(S)

¿Qué puede hacer alguien -como una pareja actual o anterior que ejerce la violencia- si consigue acceder físicamente a su smartphone, tableta u ordenador y abre la aplicación Ring?

Pueden:

1) Agregarse como usuario compartido (se explica en la siguiente sección).

2) Ver su información de seguridad.

3) Ver su dirección en la esquina superior izquierda.

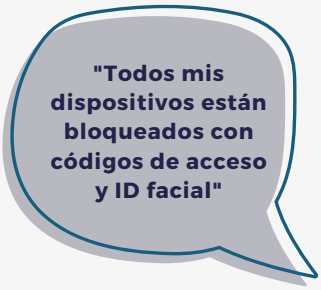
4) Cambiar la configuración de seguridad.

No Pueden:

1) Conocer o cambiar su contraseña.

2) Cambiar su dirección de correo electrónico sin introducir su contraseña.

3) Cambiar su número de teléfono sin introducir su contraseña.



MEDIDAS QUE PUEDE TOMAR PARA EVITAR EL ACCESO

1) Tener contraseñas fuertes y activar la huella dactilar o el ID facial.

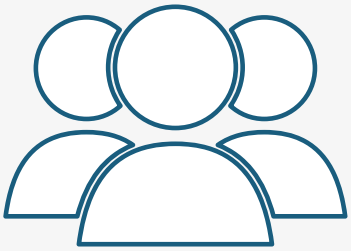
2) No permita que nadie acceda físicamente a su dispositivo a menos que sea absolutamente necesario. Si le da a alguien su dispositivo, esté presente cuando lo use.

3) Omprueba periódicamente la configuración de las cuentas para asegurarse de que todo es correcto:

- Usuarios compartidos.
- Dispositivos de clientes autorizados.
- Número de teléfono.

4

USUARIOS COMPARTIDOS



¿Qué es un usuario compartido?

Un usuario compartido es una persona que tiene permiso para ver su transmisión de vídeo en directo, ver las grabaciones de vídeo y recibir notificaciones o alertas de un dispositivo Ring de su propiedad. Tienen su propia cuenta separada y ven una pantalla similar a la del titular de la cuenta. Puede dar a un usuario compartido la capacidad de ver uno o más de los dispositivos de su cuenta Ring. **Los usuarios compartidos no pueden activar o desactivar la configuración de la alarma.** La adición de usuarios compartidos puede ser una adición positiva para la seguridad de sus hijos o miembros de la casa y a continuación se presentan algunos riesgos para tener en cuenta:

Escenario #1:
Si alguien tiene acceso físico a su smartphone, tableta u ordenador, puede añadirse a sí mismo como usuario compartido y el propietario no será notificado

Recomendaciones de Seguridad:
1) Configure un código de acceso y un ID facial/huella digital en su dispositivo para evitar el acceso no autorizado.

2) Compruebe si se han añadido "usuarios compartidos": haga clic en las 3 líneas horizontales en la esquina superior derecha > haga clic en configuración > haga clic en "acceso compartido" > pulse cualquier usuario desconocido y luego pulse "eliminar usuario".

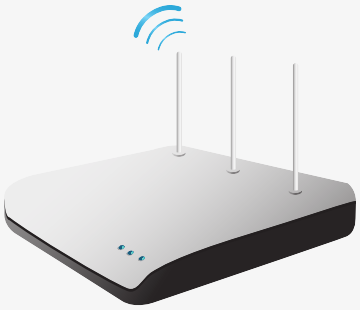
Escenario #2:
Alguien que ha añadido como usuario compartido tiene acceso a su cuenta por la persona que utiliza la violencia.

Ejemplo: Un hijo que está añadido como usuario compartido está visitando al otro padre y éste obtiene su nombre de usuario y contraseña. Ese padre ahora puede iniciar sesión en su propio dispositivo utilizando el nombre de usuario del niño cuando quiera, ver la información y las grabaciones de la cámara Ring y usted no será notificado.

Recomendaciones de Seguridad:
1) Sólo agregue usuarios compartidos que sean absolutamente necesarios, ya que puede ser un riesgo de seguridad importante.

2)Desactive el acceso del niño cuando esté con el otro padre o fuera de casa de la siguiente manera: haga clic en las 3 líneas horizontales en la esquina superior derecha > haga clic en configuración > haga clic en "acceso compartido" > haga clic en el nombre del usuario compartido y desactive su acceso.

5 WIFI EN EL HOGAR



Los dispositivos Ring requieren wifi para funcionar. Si alguien (como una expareja que utiliza la violencia) tiene o tuvo acceso a la cuenta de servicio de internet o configuró el wifi doméstico que se utiliza para el dispositivo Ring, entonces usted debe[LLB1] tomar algunas medidas adicionales para asegurar la red wifi de su hogar.

Recomendaciones de Seguridad:
Cuenta del proveedor de servicios de internet: Acceda a su cuenta en el sitio web del proveedor de servicios de internet y confirme que nadie más tiene acceso. Este proceso variará en función de su proveedor. Si existe la posibilidad de que otra persona conozca su contraseña, puede cambiarla.

Actualizar contraseñas: Actualizar la contraseña del wifi no siempre es sencillo. Si su proveedor de servicios de internet proporciona una aplicación para utilizar con su cuenta, es probable que pueda actualizar la contraseña de esta manera.También puede llamarles y preguntarles cómo actualizar la contraseña. O puede intentar actualizar la contraseña usted mismo siguiendo las instrucciones que encontrará aquí.

También considere cambiar el nombre de usuario y la contraseña de su enrutador de la configuración predeterminada. Aprende más aquí.

6 GRABACIÓN EN VIDEO

Si su dispositivo incluye un plan Ring Protect, puede guardar, revisar y compartir las grabaciones de los vídeos de sus dispositivos Ring en su cuenta Ring. Su dispositivo Ring puede grabar un incidente que podría ser relevante para un asunto de derecho de familia, una orden de protección o una investigación criminal. No tiene la obligación de compartir las grabaciones de vídeo a menos que decida hacerlo.

Las grabaciones se guardan durante 60 días. Este período de tiempo se puede acortar dentro del centro de control de cuentas. Asegúrese de almacenar los videos guardados en un lugar seguro. Una opción para almacenar las pruebas de forma segura es DocuSafe, creado por la Red Nacional para Acabar con la Violencia Doméstica. Lea sobre ella aquí y haz clic aquí para saber más sobre cómo compartir y descargar vídeos.

Para obtener ayuda sobre lo que puede ser útil para documentar y cómo hacerlo de forma segura, póngase en contacto con su centro local de violencia familiar.

7 CONSIDERACIONES DE PLANIFICACIÓN DE SEGURIDAD

Planificación de la Seguridad

Un dispositivo Ring no es un sustituto de su plan de seguridad, pero puede ser un paso que elija tomar como parte de su plan de seguridad. Todavía se recomienda practicar hábitos de seguridad fuertes como: mantenga las puertas y ventanas cerradas, mantenga el control sobre las llaves de su hogar, mantenga su teléfono cargado, etc. Si tiene preguntas sobre la planificación de la seguridad, comuníquese con su organización local de violencia familiar o con la Línea Directa Nacional de Violencia Doméstica para obtener apoyo. No importa qué pasos elija tomar, la violencia nunca es su culpa.

Pasos Durante un Incidente:

IEn el caso de que le avisen a través de la aplicación Ring de la presencia de una persona insegura en la puerta de su casa o a la vista de la cámara de vigilancia, puede planificar de antemano qué acción tomar. A continuación, se indican algunas opciones a tener en cuenta:

Opciones si está en casa:

1) Utilize el altavoz bidireccional del dispositivo para comunicarse en lugar de abrir la puerta.

2) Utilize el altavoz bidireccional del dispositivo para crear la percepción de que estás en la casa mientras sale de ella con seguridad.

Opciones si no está en casa:

1) Asegúrese de que las alertas de movimiento están activadas cuando están fuera de casa. La aplicación Ring permite varios ajustes personalizables para las alertas de movimiento. Por ejemplo, puede recibir una alerta (estando en casa o fuera de ella) cada vez que una persona pase por delante de un timbre de vídeo o una cámara de vigilancia. Esto es útil para evaluar la seguridad antes de volver a casa o para proporcionar tranquilidad mientras se está en ella.

2) Si se recibe una alerta de movimiento, las opciones posibles son:

- Llamar a las autoridades.
- Hablar con la persona a distancia a través de la aplicación, en lugar de responder a la puerta.

8 OTRAS CONSIDERACIONES DE SEGURIDAD

Cifrado de Extremo a Extremo (E2EE)

Esta función ofrece una opción de cifrado adicional y avanzado para que los usuarios tengan aún más control sobre quién puede ver sus videos. Con E2EE, sólo su dispositivo móvil registrado tiene la clave especial necesaria para desbloquear estos videos, diseñada para que nadie más pueda verlos, ni siquiera Ring o Amazon. Obtenga más información sobre esta función aquí.

Cuando se activa, los usuarios pierden ciertas funciones, pero pueden ganar en seguridad. Por ejemplo, los usuarios compartidos perderán el acceso a los dispositivos inscritos. Los pasos para activar esta característica se pueden encontrar aquí.

Vecinos

En la aplicación Ring hay una fuente de noticias llamado 'Vecinos' que proporciona actualizaciones en tiempo real sobre la delincuencia y la seguridad en su zona. Otros usuarios de Ring pueden publicar grabaciones de sus dispositivos y otras notas sobre lo que ocurre en el barrio. Esto también está disponible como una aplicación independiente y una persona no debe tener un dispositivo Ring para descargar la aplicación de vecinos. Ring tiene directrices comunitarias sobre lo que se puede publicar y usted puede marcar el contenido para solicitar que se retire. Le puede resultar útil controlar la aplicación de vecinos para asegurar su privacidad.

Solicitud de Asistencia

La fuente de noticias de vecinos incluye las características de 'Solicitudes de asistencia', permiten a las agencias de seguridad pública pedir ayuda al pueblo con una investigación activa. Los usuarios no tienen ninguna obligación de participar o responder a las solicitudes de asistencia. Puede encontrar más información, incluso sobre cómo desactivar esta función, aquí.

9 EXPECTATIVAS DE SEGURIDAD

Riesgos

Como ocurre con todas las plataformas tecnológicas y las cuentas en línea, existe el riesgo de que se produzca una filtración de datos que esté fuera de su control y que pueda exponer la información del usuario y/o proporcionar acceso no autorizado a las cuentas. En el caso de los dispositivos de seguridad para el hogar como Ring, esto puede significar el acceso no autorizado a su transmission de video de vídeo y grabaciones. Si desea obtener más información sobre algunos problemas de seguridad pasados de Ring, y cómo Ring los abordó, con el fin de tomar una decisión informada sobre la instalación y el uso de sus productos, puede leer artículos como éste y realizar su propia investigación en línea sobre Ring.

Contacto con Ring

En el caso de que tenga un problema que requiera asistencia (bloqueo de su cuenta, problemas de seguridad, etc.), puede comunicarse con Ring directamente aquí para obtener asistencia a través del chat o el teléfono. Si se trata de una emergencia, llame al 911.

Enlaces de Recursos:

- Red Nacional para el Fin de la Violencia Doméstica
- Consejo de Violencia Familiar de Texas
- EndTAB
- Línea telefónica Nacional contra la Violencia Doméstica

Descargo de responsabilidad: La información proporcionada en esta guía no constituye, ni pretende constituir, un asesoramiento jurídico; por el contrario, toda la información y el contenido de la misma tienen únicamente fines informativos generales. Los lectores de esta guía deben ponerse en contacto con un abogado para obtener asesoramiento con respecto a cualquier asunto legal concreto. La información contenida en esta guía puede no constituir la información más actualizada y esta guía contiene enlaces a otros sitios web de terceros, que son sólo para la comodidad del lector. TCFV no recomienda ni respalda el contenido de los sitios de terceros.