powered by BOXX INSURANCE

BOXX CYBER PROTECT

GUIA DE USUARIO DE LA APP

VERSIÓN 1.0

Contenidos

BOXX INSURANCE

Capítulo 1

Introducción a BOXX Cyber Protect

BOXX Cyber Protect es una aplicación fácil de usar para todas sus necesidades de seguridad y protección de la privacidad.

BOXX Cyber Protect es un paquete todo en uno que incluye todo lo necesario para proteger su privacidad y sus dispositivos de las amenazas en línea. Se basa en la galardonada tecnología de protección antivirus. El producto le ofrece la siguiente cobertura completa:

- **Protege tus dispositivos de contenidos nocivos**

La aplicación te protege contra virus, troyanos, ransomware y otras aplicaciones dañinas que pueden recopilar, robar o bloquear datos personales, números de tarjetas de crédito, credenciales bancarias y otra información valiosa.

- **Protege su navegación, sus operaciones bancarias en línea y sus compras**

La aplicación puede proteger sus operaciones bancarias y sus compras en línea impidiendo que programas o sitios dañinos recopilen y envíen los datos personales que introduzca, como números de tarjetas de crédito, información de cuentas de usuario y contraseñas. Bloquea los sitios web que intentan estafarte con tu dinero o información personal con la protección de navegación. Te mantiene automáticamente alejado de malware y sitios de phishing protegiendo tu seguridad y privacidad.

En los dispositivos móviles, la protección bancaria está activada en Navegador Seguro.

- **Asegura tu conexión a Internet con un VPN de privacidad**

La aplicación protege tu privacidad y cifra tu conexión a Internet con una VPN rápida e ilimitada para evitar que hackers, rastreadores y empresas intrusivas espíen tus actividades en línea, incluso en redes WiFi públicas no seguras de hoteles, restaurantes y aeropuertos.

Esta tecnología VPN integrada añade otra capa de seguridad y privacidad durante la navegación.

- **Evita el robo de identidad en línea**

La aplicación ayuda a responder a las amenazas de apropiación de cuentas y usurpación de identidad.

Protege tu identidad en línea almacenando tus contraseñas de forma segura y permitiéndote acceder a ellas fácilmente desde cualquier dispositivo con El Gestor de contraseñas, un práctico gestor de contraseñas. El Gestor de contraseñas te facilita la creación de contraseñas seguras y únicas, y puedes sincronizarlas en todos tus dispositivos. Su función de análisis de contraseñas te permite saber si estás utilizando contraseñas comunes, débiles o incluso reutilizadas.

Con La Supervisión de ID, recibirá alertas en tiempo real cuando un servicio en línea que utilice sea pirateado y su información personal esté en peligro. Gracias a una combinación de inteligencia humana y vigilancia de la red oscura, recuperamos los datos vulnerados antes de que acaben en la red oscura una media de cuatro a seis meses antes que el resto del mercado.

- Te permite proteger a toda tu familia y amigos.

La aplicación ha sido diseñada para proteger a toda su familia, desde niños pequeños hasta adultos, ajustándose a las necesidades de protección personal con una sola aplicación.

Con la aplicación, puede gestionar fácilmente su suscripción, licencias y usuarios protegidos con su suscripción. La vista Personas y dispositivos le ofrece una visión general de las personas y sus dispositivos que usted, como propietario de la suscripción, ha protegido con su suscripción. Los usuarios que invites a tu grupo tendrán una cuenta de usuario propia.

Todos los perfiles de los niños se gestionan a través de tu cuenta. La aplicación permite a los padres establecer límites saludables para el uso de los dispositivos por parte de los niños sin olvidar la seguridad y la privacidad en línea. La aplicación garantiza que los niños puedan explorar Internet, instalar aplicaciones y comunicarse con amigos y familiares de forma segura.

También puede utilizar el portal de gestión en línea para proteger los dispositivos de su grupo.

Capítulo 2

Instalación de BOXX Cyber Protect

Puede descargar e instalar BOXX Cyber Protect desde el correo electrónico de invitación que se le ha enviado.

También puede utilizar el portal para enviar un enlace de instalación a un dispositivo por correo electrónico o SMS, lo que facilita la entrega de BOXX Cyber Protect a un dispositivo que desee proteger.

2.1 Instalación de BOXX Cyber Protect en su dispositivo móvil

1. Este tema proporciona instrucciones para instalar BOXX Cyber Protect en su smartphone o tableta.
2. Haga clic en "Instalar Cyber BOXX Protect" en el correo electrónico de bienvenida que se le ha enviado.
3. Instala Cyber BOXX Protect desde tu tienda de aplicaciones utilizando el enlace del correo electrónico de bienvenida.
4. Una vez instalada la aplicación en su dispositivo, ejecútela y complete el paso de configuración.
5. Introduzca los datos de acceso que se le enviaron en el correo electrónico de bienvenida (su dirección de correo electrónico y la contraseña de un solo uso facilitada en el correo electrónico de invitación).
6. Configurar las notificaciones

2.2 Comprobar que la aplicación funciona

La aplicación está funcionando y protegiéndote a ti y a tu dispositivo cuando veas una marca verde y el texto "Tu dispositivo está protegido" en la vista principal de la aplicación.

Si la protección está desactivada, aparece un signo de exclamación rojo en el centro del escudo con el texto "Tu dispositivo no está protegido". En la vista principal de la aplicación, una notificación te pide que actives la protección contra virus y amenazas. Seleccione Activar para activar la protección.

Si ha pasado algún tiempo desde la última vez que se analizó el dispositivo, puede activar manualmente un análisis de virus:

1. En la vista principal de la aplicación, seleccione Virus y amenazas. Se abrirá la vista Protección frente a virus y amenazas.
2. Pulse sobre Escanear para activar un escaneo de virus.

Una vez finalizada la exploración, podrá ver los resultados de la misma en la página.

Capítulo 3

Proteger su identidad en Internet

Con la Supervisión de ID, puede añadir sus direcciones de correo electrónico y otra información personal para su supervisión y recibir orientación sobre qué hacer si su información se filtra en una filtración de datos.

El correo electrónico de notificación incluye información sobre qué información de identificación personal (IIP) se ha asociado a la violación; en qué consistió la violación; qué empresa o entidad fue violada; cuándo tuvo lugar la violación; y qué otras piezas de IIP se han asociado a la dirección de correo electrónico vigilada, como contraseñas, números de tarjetas de crédito, dirección postal, etc.

Nota: Al crear su cuenta, su dirección de correo electrónico se añade automáticamente para su supervisión. Recibirá un correo electrónico de confirmación a la dirección en cuestión, y deberá confirmar la dirección de correo electrónico antes de poder acceder a la información detallada sobre las infracciones y los datos filtrados, en su caso, asociados a esta dirección de correo electrónico.

Proteger su identidad en Internet

Con Supervisión de ID, puede añadir sus direcciones de correo electrónico y otra información personal para su supervisión y recibir orientación sobre qué hacer si su información se filtra en una filtración de datos.

El correo electrónico de notificación incluye información sobre qué información de identificación personal (IIP) se ha asociado a la violación; en qué consistió la violación; qué empresa o entidad fue violada; cuándo tuvo lugar la violación; y qué otras piezas de IIP se han asociado a la dirección de correo electrónico vigilada, como contraseñas, números de tarjetas de crédito, dirección postal, etc.

Nota: Al crear su cuenta, su dirección de correo electrónico se añade automáticamente para su supervisión. Recibirá un correo electrónico de confirmación a la dirección en cuestión, y deberá confirmar la dirección de correo electrónico antes de poder acceder a la información detallada sobre las infracciones y los datos filtrados, en su caso, asociados a esta dirección de correo electrónico.

Para añadir más elementos para la supervisión:

1. Abre la aplicación y selecciona Supervisión de ID.
2. En la vista Supervisión de ID, seleccione Elementos supervisados. Se abre la vista Elementos supervisados.
3. Selecciona + Añadir elemento.

Se abrirá el cuadro de diálogo Añadir nuevo, con una lista de todos los tipos de elementos disponibles para elegir. Tenga en cuenta que si aún necesita añadir una dirección de correo electrónico para la supervisión, el producto le pedirá que añada primero una dirección de correo electrónico para la supervisión. Sólo después podrá añadir otros tipos de elementos para la supervisión.

4. Seleccione el tipo de elemento que desea añadir para su supervisión. Se abre la vista Nuevo elemento supervisado.
5. Introduzca la información solicitada y seleccione Añadir.

La monitorización busca inmediatamente filtraciones con tus datos y te muestra el resultado de la búsqueda. Ten en cuenta que para ver información más detallada sobre tus datos filtrados, si los hay, y las acciones recomendadas, asegúrate de haber confirmado tu dirección de correo electrónico.

Si aún necesita confirmar su dirección de correo electrónico, abra el mensaje de confirmación y seleccione el enlace para verificar que se trata de su dirección de correo electrónico.

7. Para ver los detalles de su información personal expuesta y lo que debe hacer, pulse sobre la infracción específica que aparece en la vista Supervisión de ID.

Importante: Si su información se ha visto expuesta a una violación de datos, le instamos a que ejecute las acciones recomendadas lo antes posible para eliminar el riesgo de que su información sea utilizada indebidamente.

3.2 Editar y eliminar elementos supervisados

Este tema describe cómo editar un elemento supervisado y cómo eliminar un elemento de la supervisión.

No puede editar directamente un artículo añadido para su supervisión. Si necesita editar un artículo supervisado existente, elimine el artículo y añádalo de nuevo para su supervisión.

Para eliminar un elemento supervisado:

1. Abra la aplicación y seleccione Supervisión de ID.
2. En la vista Monitorización, seleccione Elementos monitorizados.

Se abre la vista Elementos supervisados, con una lista de todos los elementos supervisados actualmente.

3. Para eliminar un artículo de la lista, seleccione los tres puntos situados junto al artículo y, a continuación, seleccione Eliminar. Se abre el cuadro de diálogo ¿Eliminar artículo supervisado? .

4. Para confirmar que desea dejar de supervisar el elemento, seleccione Eliminar. El elemento desaparece de los elementos supervisados.

Nota: Para editar la dirección de correo electrónico de contacto o eliminarla de la supervisión, debe eliminar todos los demás elementos supervisados, si los hay, antes de poder editar o eliminar la dirección de correo electrónico de contacto.

Capítulo 4

Almacenamiento y protección de contraseñas

Gestor de contraseñas almacena y protege su información personal, como contraseñas, números de tarjetas de crédito y códigos PIN.

Gestor de contraseñas le ofrece una forma sencilla de garantizar que las credenciales de su cuenta de servicios en línea, los datos de su tarjeta de crédito y otra información importante permanezcan seguros y cómodamente accesibles.

Las principales ventajas de la función Gestor de contraseñas son:

- **Almacenamiento de contraseñas:** Almacena de forma segura todas tus contraseñas, datos de acceso, códigos PIN, datos de tarjetas de crédito y credenciales de banca online.
- **Cree contraseñas:** Genera contraseñas más seguras y únicas para todos tus servicios y cuentas.
- **Autorrellenar contraseñas:** Consigue que tus contraseñas se introduzcan automáticamente en las páginas de inicio de sesión de tu navegador web para que acceder a tu cuenta sea más fácil y rápido.
- **Conexión de dispositivos:** Puedes conectar tus dispositivos para sincronizar tus contraseñas de forma segura en todos ellos.

Con Gestor de contraseñas, todos los datos están encriptados, y la única forma de acceder a ellos es con su contraseña principal. Nadie puede acceder a sus datos. Además, el servicio es anónimo, lo que significa que nadie puede relacionarle con sus datos. No hay acceso a tus datos a través de un navegador web, por lo que nadie puede acceder a ellos sin robar tu dispositivo.

Gestor de contraseñas almacena sus datos, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, en el ordenador o dispositivo móvil que utiliza para ejecutar la aplicación.

Tus contraseñas se almacenan en un formato cifrado, y nadie puede acceder a ellas a menos que conozca tu contraseña principal y acceda a tu dispositivo.

Puedes sincronizar tus contraseñas en todos tus dispositivos. Por motivos de seguridad, no proporcionamos acceso a las contraseñas a través de nuestros servidores. Te recomendamos que sincronices tus contraseñas con otro dispositivo que ejecute la aplicación si pierdes o rompes tu dispositivo. No importa lo que le ocurra a uno de tus dispositivos, la sincronización te asegura que siempre tendrás acceso a tus contraseñas en los otros dispositivos.

4.1 Introducción al Gestor de contraseñas

Este tema describe cómo poner en funcionamiento Gestor de contraseñas en el dispositivo que esté utilizando en ese momento.

Cuando empiece a utilizar Gestor de contraseñas, lo primero que debe hacer es crear una contraseña principal. La contraseña principal es la única que debe recordar una vez que haya configurado Gestor de contraseñas.

Para configurar Gestor de contraseñas:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Seleccione Soy un nuevo usuario.

Nota: Si ya utilizas la aplicación en otro dispositivo, puedes conectar los dispositivos para sincronizar tus contraseñas seleccionando Soy un usuario existente.

3. Cree una contraseña principal segura y seleccione Continuar.
4. Repita la contraseña principal y seleccione Confirmar.
5. Cree un código QR de recuperación seleccionando Guardar. El código se guarda como una imagen en tus Fotos.

Importante: Le recomendamos encarecidamente que cree inmediatamente un código QR de recuperación para la contraseña principal. Es la única forma de recuperar tu contraseña principal si la olvidas.

6. Si desea utilizar la autenticación biométrica, por ejemplo, Touch ID, para acceder más rápidamente a su Bóveda de Contraseñas, asegúrese de que la opción Utilizar Touch ID para desbloquear esté activada y seleccione Guardar. Tenga en cuenta que si no desea utilizar la autenticación biométrica ahora, puede hacerlo más adelante desde la configuración del almacén de contraseñas.

Recuerde: No olvide su contraseña principal. De vez en cuando, tendrá que introducir su contraseña principal para desbloquear Gestor de contraseñas.

4.1.1 Acerca de la contraseña principal

La contraseña principal es fundamental, ya que le da acceso a sus datos de Gestor de contraseñas.

Cuando configure Gestor de contraseñas, lo primero que debe hacer es crear una contraseña principal. La contraseña principal es la única contraseña que deberá recordar una vez que haya puesto en funcionamiento Gestor de contraseñas.

Elija una contraseña principal o frase de contraseña difícil de adivinar que pueda recordar, ya que Gestor de contraseñas no podrá restablecer su contraseña principal si la olvida. El hecho de que no haya forma de restablecer una contraseña principal olvidada ha sido una decisión consciente para aumentar su seguridad y privacidad y proteger sus datos.

Se le pedirá que cree un código QR de recuperación al final de la configuración de Gestor de contraseñas. Le recomendamos encarecidamente que cree el código, ya que es la única manera de recuperar el acceso a sus datos de Gestor de contraseñas en caso de que olvide su contraseña principal.

Cambiar la contraseña principal

This topic describes how you can change your master password for El Gestor de contraseñas on any device.
Este tema describe cómo puede cambiar su contraseña principal para Gestor de contraseñas en cualquier dispositivo.

Para cambiar tu contraseña principal:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Seleccione el icono de configuración en la esquina superior derecha de la pantalla. Se abrirá la vista de configuración de Gestor de contraseñas.
3. Seleccione Cambiar contraseña principal.
4. Introduzca su antigua contraseña principal y seleccione Continuar.
5. Introduzca una nueva contraseña principal segura.
6. Repita la nueva contraseña principal y seleccione Confirmar.

Nota: Si utiliza autenticación biométrica, proporcione la autenticación solicitada.

7. Como ha cambiado su contraseña principal, debe crear un nuevo código QR de recuperación. Selecciona Crear ahora y, a continuación, Guardar como imagen.

El código se guarda en la ubicación predeterminada de tu dispositivo.

Su contraseña principal ha sido modificada. Una vez que hayas cambiado la contraseña principal en un dispositivo, deberás utilizar la nueva contraseña en todos los dispositivos conectados.

Nota: Si cambias la contraseña principal por cualquier motivo, deberás crear un nuevo código QR de recuperación. Cualquier código antiguo dejará de ser válido. Por lo tanto, asegúrate de que el código QR de recuperación esté siempre actualizado y sea válido para tu contraseña principal actual.

4.1.2 Acerca del código QR de recuperación de la contraseña principal

El código QR de recuperación de la contraseña principal es un código único y personal que constituye la única forma de recuperar el acceso a los datos de Gestor de contraseñas en caso de que olvide su contraseña principal.

Importante: Recomendamos encarecidamente que, como paso final al utilizar Gestor de contraseñas, cree un código QR de recuperación para su contraseña principal.

Por razones de seguridad, no podemos restablecer ninguna contraseña principal, ya que esto significaría acceder a tu contraseña principal, lo que podría considerarse un riesgo para la seguridad.

El código QR de recuperación está fuertemente encriptado y sólo puede desencriptarse en uno de los dispositivos conectados. Esto significa que no se puede descifrar en ningún otro dispositivo de usuario.

Hay que tener en cuenta algunas cosas importantes sobre el código QR de recuperación:

- Cada vez que cambies tu contraseña principal, deberás crear un nuevo código QR de recuperación.

- Siempre necesitará el último código QR de recuperación para volver a acceder a sus datos de Gestor de contraseñas.

- Si conectas nuevos dispositivos, la aplicación puede pedirte que crees un nuevo código QR de recuperación. Si este es el caso, asegúrate de crear un nuevo código QR de recuperación, ya que el código antiguo dejará de funcionar.

- Recomendamos guardar el código QR de recuperación como una imagen e imprimir una copia para guardarla. La impresión del código QR de recuperación no debe guardarse en la ubicación exacta de tu dispositivo.

Nota: Si cambias la contraseña principal por cualquier motivo, deberás crear un nuevo código QR de recuperación. Cualquier código antiguo dejará de ser válido. Por lo tanto, asegúrate de que el código QR de recuperación esté siempre actualizado y sea válido para tu contraseña principal actual.

Crear un código QR de recuperación para la contraseña principal

Este tema explica cómo crear un código QR de recuperación para la contraseña principal de Gestor de contraseñas.

Importante: Le recomendamos encarecidamente que cree inmediatamente un código QR de recuperación para la contraseña principal. Es la única forma de recuperar tu contraseña principal si la olvidas.

Para crear un código QR de recuperación para tu contraseña principal:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Seleccione el icono de configuración en la esquina superior derecha de la pantalla. Se abrirá la vista de configuración de Gestor de contraseñas.
3. Seleccione Crear código de recuperación y realice una de las siguientes acciones:

- Si utiliza la autenticación biométrica, proporcione la autenticación solicitada. Como alternativa, seleccione Usar la contraseña e introduzca su contraseña principal.

- Introduce tu contraseña principal y selecciona Confirmar para crear un código QR de recuperación.

La imagen del código de recuperación se crea automáticamente.

4. Seleccione Guardar.

El código se guarda en la ubicación predeterminada de tu dispositivo. Suele ser la carpeta Fotos.

5. Vaya a la carpeta, seleccione la imagen y envíela a un servicio desde el que pueda imprimirla.

Nota: Le recomendamos que guarde el código como una imagen y que imprima el archivo para conservarlo en lugar de almacenarlo en un servicio de almacenamiento en la nube.

Utilizar el código QR de recuperación para recuperar una contraseña principal olvidada

Este tema explica cómo recuperar tu contraseña principal utilizando el código QR de recuperación.

Importante: Sólo podrás recuperar tu contraseña principal si previamente has creado un código QR de recuperación para tu contraseña principal.

Para recuperar tu contraseña principal con el código QR de recuperación:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. En la pantalla de inicio de sesión, seleccione ¿Ha olvidado la contraseña principal?
3. Realiza una de las siguientes acciones:

- Seleccione Importar imagen y, a continuación, seleccione la imagen de código de la carpeta en la que la guardó.

- Seleccione Escanear código de recuperación y escanee la impresión del código.

Su contraseña principal aparece en la pantalla.

4. Copie la contraseña principal en el portapapeles y péguela en el campo Contraseña principal de la página de inicio de sesión.

5. Selecciona Desbloquear.

4.1.3 Uso de la autenticación biométrica para desbloquear el Gestor de contraseñas

Si su dispositivo móvil es compatible con la autenticación biométrica, puede utilizar, por ejemplo, su huella dactilar para desbloquear Gestor de contraseñas.

Nota: Antes de utilizar la autenticación biométrica para desbloquear Gestor de contraseñas, debe registrar su huella dactilar.

Consulte el manual de usuario de su dispositivo para saber cómo utilizar la autenticación biométrica en su dispositivo.

En Gestor de contraseñas, puede utilizar la autenticación biométrica cuando cree su contraseña principal o más tarde seleccionando la autenticación biométrica para desbloquear en la vista de inicio de sesión de Gestor de contraseñas.

Recuerde: No olvide su contraseña principal. De vez en cuando, tendrá que introducir su contraseña principal para desbloquear Gestor de contraseñas.

4.2 Utilizar Gestor de contraseñas

Con Gestor de contraseñas, puedes crear y editar contraseñas de contraseñas y tarjetas de pago, dejar que la aplicación genere contraseñas seguras para tus servicios en línea y acceder a tu historial de contraseñas.

4.2.1 Cómo debe ser una buena contraseña

La recomendación general para una buena contraseña es que sea única y contenga una combinación de letras, números y caracteres especiales. Que sea fácil de recordar para ti, pero difícil de adivinar para los demás.

Además de estas directrices generales, existen otros enfoques que mejoran la seguridad de sus cuentas de servicios en línea:

Utilice contraseñas generadas. Cuando utiliza una contraseña generada por Gestor de contraseñas, no se puede utilizar ningún sistema de memorización u otras pistas para descifrar la contraseña.

- Cambie su contraseña. Es una buena idea cambiar tus contraseñas de vez en cuando, pero si nada lo impide, cambia tu contraseña inmediatamente para cualquier servicio que te notifique de una posible violación de datos.

- Siempre que sea factible, utilice diferentes direcciones de correo electrónico para distintos servicios en línea. De este modo, si piratean tu cuenta de correo electrónico, no pondrán en peligro todas tus cuentas online.

- Evita utilizar tu dirección de correo electrónico como nombre de usuario siempre que sea posible. Muchos servicios crean automáticamente tu cuenta con tu dirección de correo electrónico como nombre de usuario.

¿Por qué es necesario utilizar contraseñas diferentes para cada servicio y cuenta?

Por lo general, los expertos en seguridad recomiendan utilizar contraseñas fuertes y únicas para cada uno de sus servicios y cuentas en línea.

En algunos servicios en línea es obligatorio utilizar contraseñas seguras que contengan varios caracteres: la contraseña que introduzca al registrarse sólo se aceptará si es lo suficientemente larga o compleja.

Sin embargo, incluso si se le ocurre una contraseña muy compleja que sea prácticamente imposible de adivinar para cualquier otra persona, la seguridad de su cuenta de servicios en línea está en peligro si utiliza esa misma contraseña para cada cuenta. Por ejemplo, si los piratas informáticos consiguen acceder a los datos de inicio de sesión de uno de sus servicios, podrán utilizar esa información para acceder a cualquiera de sus otras cuentas en línea en las que haya utilizado la misma contraseña. Utilizar una contraseña única para cada cuenta significa que sus gastos adicionales no corren peligro, ni siquiera en caso de violación de los datos de uno de los servicios que utiliza.

4.2.2 Almacenamiento de contraseñas

Instrucciones paso a paso sobre cómo crear contraseñas en la aplicación y cómo dejar que la aplicación genere contraseñas seguras para tus servicios en línea.

Guardar una nueva contraseña en un dispositivo móvil

Puedes almacenar nuevas contraseñas en la aplicación de tu dispositivo móvil.

Para guardar una nueva contraseña:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Selecciona + Añadir.
3. Seleccione Contraseña.
4. En el campo Título, dé un nombre descriptivo a su contraseña.
5. Para personalizar el icono de contraseña de la izquierda, pulse sobre él y seleccione un color de fondo y un símbolo para la contraseña. Una vez hecho esto, confirme su selección seleccionando Hecho.
6. En el campo Nombre de usuario, introduzca su nombre de usuario para la aplicación o el servicio en línea.
7. En el campo Contraseña, cree una contraseña o frase de contraseña segura.

Consejo: Seleccione el icono del dado para abrir la vista Generar contraseña, donde puede dejar que la aplicación genere una contraseña fuerte y aleatoria para usted. Toque el icono del dado hasta que esté satisfecho con la contraseña generada. Para guardar la contraseña, seleccione Hecho.

8. En el campo Dirección web, introduzca la dirección web (URL) de la página de inicio de sesión del servicio en línea.
9. En el campo Notas, introduzca cualquier información adicional.
10. Para guardar la contraseña, seleccione Hecho.

Importante: Si cambia o genera una contraseña en Gestor de contraseñas, recuerde cambiar también su contraseña en el servicio en línea o aplicación en cuestión.

Almacenamiento de datos de tarjetas de pago en un dispositivo móvil

Puedes almacenar de forma segura los datos de tus tarjetas de pago, como las de crédito y débito, en la aplicación de tu dispositivo móvil.

Para almacenar los datos de su tarjeta de pago:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Selecciona + Añadir.
3. Seleccione una tarjeta de crédito.
4. Para personalizar el icono de contraseña de la izquierda, pulse sobre él, elija uno de los símbolos de tarjeta de pago disponibles y seleccione Hecho.
5. En el campo Título, introduzca el nombre de la tarjeta de pago.

6. En el campo Nombre del titular, introduzca su nombre tal y como figura en la tarjeta de pago.
7. En el campo Número de tarjeta de crédito, introduzca el número de su tarjeta.
8. En el campo PIN, introduzca el número de identificación personal asociado a la tarjeta
9. En el campo Fecha de caducidad, introduzca la fecha de caducidad de la tarjeta en el formato MM/AA.
10. Introduzca el código de verificación de su tarjeta (CVV) en el campo Código de verificación.
11. En el campo Dirección web, introduzca la dirección web (URL) del servicio.
12. En el campo Notas, introduzca cualquier información adicional.
13. Para guardar la nueva contraseña, seleccione Hecho.

4.2.3 Edición de contraseñas

Instrucciones paso a paso para editar contraseñas en la aplicación.

Editar una contraseña existente

Es posible que tenga que editar una contraseña de Gestor de contraseñas en algún momento.

Para editar una contraseña:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Seleccione la contraseña que desea editar.
3. Seleccione el icono del lápiz para abrir la vista Editar.
4. Realice los cambios necesarios.
5. Para guardar los cambios, seleccione Hecho.

Generar una contraseña con Gestor de contraseñas

Gestor de contraseñas puede generar una contraseña segura para usted cuando necesite cambiar una contraseña.

Para cambiar una contraseña:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Vaya a la contraseña cuya contraseña desea cambiar y seleccione el icono del lápiz.
3. En el campo Contraseña, seleccione el icono del dado.
4. En la vista Generar contraseña, puede hacer lo siguiente:

    - Arrastre el control deslizante de un lado a otro para seleccionar el número de caracteres que desea en su contraseña.
    - Seleccione el tipo de caracteres (letras minúsculas y mayúsculas, números y caracteres especiales) que desea en su contraseña.
    - Toque el icono del dado situado debajo de la contraseña generada si no está satisfecho con la contraseña.

5. Para utilizar la contraseña generada, seleccione Hecho.
6. Para guardar la contraseña, seleccione Hecho.

Importante: Si cambia o genera una contraseña en Gestor de contraseñas, recuerde cambiarla también en el servicio web o aplicación en cuestión.

Puedes almacenar nuevas contraseñas en la aplicación de tu dispositivo móvil.

Eliminar una contraseña

Puede eliminar las contraseñas de Gestor de contraseñas que ya no necesite.

Para borrar una contraseña:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Seleccione la contraseña que desea eliminar.
3. Seleccione el icono del lápiz para abrir la vista Editar.
4. Para eliminar la contraseña, seleccione el icono de la papelera.
5. Para confirmar el borrado, seleccione Borrar.

4.2.4 Acceder a tus antiguas contraseñas

El registro del historial de contraseñas contiene sus contraseñas anteriores, si las hubiera, para el servicio en línea en cuestión.

Después de cambiar una contraseña en Gestor de contraseñas, es posible que aún tenga que iniciar sesión en el servicio en línea con la contraseña antigua. Además, muy a menudo, antes de poder cambiar la contraseña de un servicio, es necesario introducir la contraseña antigua.

Para acceder a las contraseñas anteriores:

1. Abre la aplicación y selecciona Gestor de contraseñas.
2. Abra la contraseña cuyas contraseñas anteriores desea ver.
3. Seleccione Historial de contraseñas.

Nota: Si no puede ver el Historial de contraseñas en la contraseña, no hay contraseñas anteriores disponibles para ese servicio en línea en particular.

4. Seleccione el icono del ojo abierto en la esquina superior derecha para ver las contraseñas ocultas.

Nota: Si lo desea, puede eliminar el historial de contraseñas seleccionando primero el icono de la papelera situado en la esquina superior derecha y, a continuación, Borrar en el cuadro de diálogo Borrar historial de contraseñas.

5. Para cerrar la vista del historial de contraseñas, seleccione el icono x en la esquina superior izquierda.

4.3 Utilizar Autorrellenar Contraseñas

Con Gestor de contraseñas, no tienes que introducir nombres de usuario y contraseñas manualmente.

Debe tener el nombre de usuario, la contraseña y la dirección web del servicio guardados en Gestor de contraseñas para que Autocompletar funcione. Cuando inicie sesión en una aplicación o sitio web con credenciales guardadas en Gestor de contraseñas, puede hacer que la aplicación introduzca su nombre de usuario y contraseña automáticamente.

4.3.1 Autocompletar y gestionar contraseñas integrados en el navegador

En este tema se explican los gestores de contraseñas integrados en el navegador y cómo pueden afectar a la función Autorrellenar contraseñas de Gestor de contraseñas.

Como la mayoría de los navegadores tienen un gestor de contraseñas incorporado, las contraseñas pueden guardarse automáticamente en el navegador.
Para mantener tus contraseñas seguras, la mejor práctica es evitar guardarlas en tu navegador.

Las contraseñas guardadas en el navegador también pueden causar problemas con Autocompletar en Gestor de contraseñas, ya que la aplicación no puede identificar las contraseñas correctamente para el servicio en el que se está iniciando sesión.

Por lo tanto, antes de empezar a utilizar la función Autocompletar en Gestor de contraseñas, le recomendamos lo siguiente:

- Desactive el gestor de contraseñas integrado en el navegador que utilice.
- Asegúrese de que todas las contraseñas del gestor de contraseñas incorporado están almacenadas en Gestor de contraseñas. Mueva sus contraseñas a Gestor de contraseñas si aún no lo ha hecho.

4.3.2 Activar Autorrellenar Contraseñas

Con Autorrellenar contraseñas, puedes iniciar sesión en aplicaciones y sitios web sin tener que introducir manualmente nombres de usuario y contraseñas.

Debe tener el nombre de usuario, la contraseña y la dirección web del servicio guardados en Gestor de contraseñas para que Autocompletar funcione. Cuando inicie sesión en una aplicación o sitio web con credenciales guardadas en Gestor de contraseñas, puede hacer que la aplicación introduzca su nombre de usuario y contraseña automáticamente.

Para activar Autocompletar en tu iPhone o iPad:

1. Ve a Ajustes de tu dispositivo > Contraseñas y cuentas.
2. En Contraseñas y cuentas, seleccione Autorrellenar contraseñas.
3. En Autorrellenar contraseñas de contraseñas, active Autorrellenar contraseñas de contraseñas si está desactivado.
4. En Permitir rellenar desde, seleccione Bóveda de Contraseñas.

Iniciar sesión en una aplicación o sitio web

For El Gestor de contraseñas to be able to show the correct entry for an app or website, make sure that you have entered its URL in the relevant access.

Para iniciar sesión en una aplicación o sitio web en tu iPhone o iPad:
1.
2. Abre la aplicación o la página web de inicio de sesión y toca el campo de nombre de usuario. Las contraseñas aparecerán en la parte superior del teclado de tu dispositivo.
3. Seleccione Contraseñas.
4. Seleccione Bóveda de Contraseñas.
5. Desbloquea la Bóveda de Contraseñas.
6. Seleccione Iniciar sesión.
7. Selecciona la contraseña que necesites.

Ya has iniciado sesión en la aplicación o el servicio web.

4.4 Conexión de dispositivos

Puede conectar sus dispositivos para sincronizar sus datos de Gestor de contraseñas.

Para sincronizar los datos de Gestor de contraseñas en todos sus dispositivos, debe conectar los dispositivos con la aplicación instalada.

Si tiene la aplicación en un solo dispositivo, sus datos de Gestor de contraseñas se almacenarán únicamente en ese dispositivo. La aplicación ha sido diseñada para que la conexión de sus dispositivos le permita tener sus datos disponibles y siempre actualizados en sus otros dispositivos. Cuando tiene sus datos también en otro dispositivo, no hay necesidad de preocuparse si un dispositivo se pierde, es robado o dañado; sus datos seguirán intactos en uno de sus otros dispositivos.

Advertencia: Si solo tiene la aplicación en un dispositivo móvil y lleva a cabo un restablecimiento de fábrica, el restablecimiento también borra todos sus datos de Gestor de contraseñas del dispositivo. Después de esto, no hay forma de recuperar los datos.

4.4.1 Conectar los dispositivos para sincronizar los datos de Gestor de contraseñas en ambos dispositivos

Si ya utiliza Gestor de contraseñas en otro dispositivo o aplicación, puede conectar los dispositivos y sincronizar sus datos para tenerlos disponibles y siempre actualizados en su otro dispositivo.

Asegúrate de que tienes ambos dispositivos a mano y de que también tienes la aplicación instalada en el otro dispositivo.

Para conectar tus dispositivos y sincronizar tus datos de Vault en ambos dispositivos:

1. Abra la aplicación en el dispositivo que contiene sus datos de Gestor de contraseñas y seleccione Gestor de contraseñas.
2. Seleccione el icono de configuración en la esquina superior derecha de la pantalla. Se abrirá la vista de configuración de Gestor de contraseñas.
3. Seleccione Conectar dispositivos.

Se abre la vista Conectar dispositivos.

4. Seleccione Generar código de sincronización.

Un código de sincronización se genera automáticamente y es válido durante 60 segundos cada vez. Se genera un nuevo código inmediatamente después de que caduque el actual.

5. Abre la aplicación en el otro dispositivo que quieras conectar, sincroniza tus datos y selecciona Gestor de contraseñas.
6. Seleccione Soy un usuario existente.

Se abre la vista Conectar dispositivos.

7. Introduce el código de sincronización generado en el paso 4 en el campo Código de sincronización y selecciona Conectar.
8. Cuando se le solicite, introduzca la contraseña principal que utiliza en el dispositivo donde generó el código de sincronización y seleccione Confirmar.
9. Por último, seleccione Guardar si desea empezar a utilizar la autenticación biométrica para desbloquear Gestor de contraseñas.

Sus datos se han sincronizado entre estos dos dispositivos. Si tiene más dispositivos que conectar, repita los pasos anteriores con cada uno de ellos.

4.5 Desbloqueo y bloqueo del Inventario de Constraseñas

Cuando no utilices Gestor de contraseñas, te recomendamos que lo bloquees para añadir una capa extra de seguridad.

Para desbloquear y bloquear Gestor de contraseñas, haga lo siguiente:

- Para desbloquear, introduce tu contraseña principal y selecciona Desbloquear o toca el sensor de tu teléfono si utilizas autenticación biométrica.

- Para bloquear, seleccione el icono de configuración y, a continuación, Bloquear ahora en la configuración de Gestor de contraseñas.

Nota: Por defecto, Gestor de contraseñas se bloquea automáticamente transcurridos quince minutos. En la configuración de Gestor de contraseñas, puede establecer el tiempo tras el cual Gestor de contraseñas se bloquea automáticamente.

Capítulo 5

Protección de personas y dispositivos

Esta sección proporciona información sobre cómo utilizar el producto para proteger sus propios dispositivos, así como los de sus familiares y amigos.

La vista Personas y dispositivos le ofrece una visión general de las personas y sus dispositivos que usted, como propietario de la suscripción, ha protegido con su suscripción. Para ver información detallada sobre un usuario, selecciónelo y se abrirá una vista específica del usuario, que le ofrecerá una visión general de la protección del usuario.

En la vista Personas y dispositivos, puede añadir más usuarios y dispositivos a su grupo enviando el enlace de instalación del producto al dispositivo del usuario por correo electrónico o SMS.

Los usuarios que invites a tu grupo tendrán una cuenta de usuario propia. Todos los perfiles de los niños se gestionan utilizando tu cuenta.

Nota: También puede utilizar el portal de gestión en línea para proteger los dispositivos de su grupo.

5.1 Proteger tu propio dispositivo

Este tema describe cómo empezar a proteger tu dispositivo.

Para configurar la protección de tu dispositivo:

1. Abra la aplicación y seleccione Personas y dispositivos. Se abrirá la vista Personas y dispositivos.
2. Selecciona + Añadir dispositivo.
3. Selecciona Mi dispositivo > Continuar.
4. Seleccione cómo desea enviar el enlace de instalación al dispositivo que desea proteger y, a continuación, seleccione Enviar enlace.
5. Abre el mensaje con tu dispositivo y sigue las instrucciones de instalación.
6. Seleccione Instalar desde la tienda de aplicaciones para ir a la tienda de aplicaciones y seleccione Obtener para iniciar la instalación.
7. Tras la instalación, seleccione Abrir para iniciar la aplicación. Se abre la página Bienvenido a BOXX Protect SAFE.
8. Si está de acuerdo con los Términos de Licencia de Usuario Final, seleccione Aceptar y continuar.
9. A medida que configure la protección para usted, seleccione Continuar para finalizar la seguridad del dispositivo.

Importante: Para proteger tu dispositivo y tus conexiones, la aplicación requiere que permitas el acceso a las fotos, medios y archivos de tu dispositivo.

Ya ha configurado la protección de su dispositivo. Para ver y gestionar la protección del dispositivo anterior, seleccione Personas y dispositivos, o inicie sesión en su cuenta para acceder al portal de gestión en línea.

5.2 Proteger el dispositivo de su hijo

Este tema describe cómo empezar a proteger los dispositivos de sus hijos.

Para establecer la protección de su hijo:

1. Abra la aplicación y seleccione Personas y dispositivos. Se abrirá la vista Personas y dispositivos.
2. Selecciona + Añadir dispositivo.
3. Seleccione Dispositivo de mi hijo > Continuar.
4. Seleccione cómo desea enviar el enlace de instalación al dispositivo que desea proteger y, a continuación, seleccione Enviar enlace.
5. Abre el mensaje con tu dispositivo y sigue las instrucciones de instalación.
6. Seleccione Instalar desde la tienda de aplicaciones para ir a la tienda de aplicaciones y seleccione Obtener para iniciar la instalación.
7. Tras la instalación, seleccione Abrir para iniciar la aplicación. Se abre la página Bienvenido a BOXX Protect SAFE.
8. Acepte los Términos de Licencia de Usuario Final seleccionando Aceptar y continuar.
9. Mientras configura la protección para su hijo, seleccione Instalar para un niño.
10. En el menú desplegable Configurar protección para, seleccione Nuevo perfil infantil y, a continuación, Continuar. Se abrirá la vista Crear nuevo perfil infantil.
11. Introduzca el nombre del niño, seleccione el grupo de edad al que pertenece y, a continuación, seleccione Siguiente. Se abre la vista de configuración de Reglas familiares.
12. Activa Hora de acostarse utilizando los controles deslizantes para limitar el uso nocturno de aplicaciones o dispositivos en las noches de colegio y las noches de fin de semana, y selecciona Siguiente.

Se abre la vista Filtrado de contenidos.

13. Active Filtrado de contenidos, seleccione las categorías de contenidos web que desea bloquear y seleccione Siguiente.

El dispositivo de tu hijo ya está protegido.

Para facilitar su uso, puede gestionar la actividad en línea de su hijo en su dispositivo. Esta es una forma versátil de hacer cambios y añadir o eliminar restricciones sobre la marcha sin tener el dispositivo de su hijo físicamente con usted.

5.2.1 Editar la configuración de las Reglas de Familia

Esta sección describe cómo realizar cambios en la configuración actual de las Reglas familiares.

Fijar la hora de acostarse

Si fijas una hora para irse a la cama, te asegurarás de que tu hijo se duerma cuando debe.

Con el ajuste de la hora de acostarse, puedes establecer una hora de acostarse diferente para las noches de colegio -de domingo a jueves por la noche- y las noches de fin de semana -de viernes a sábado por la noche-.

Para fijar la hora de acostarse, haga lo siguiente:

1. Abra la aplicación y seleccione Personas y dispositivos. Se abrirá la vista Personas y dispositivos.
2. Seleccione el dispositivo del niño en la lista.
3. En REGLAS FAMILIARES, si Hora de acostarse está Desactivada, seleccione Hora de acostarse.
4. En la vista Bedtime, impida el uso del dispositivo por la noche de la siguiente manera:

- Para Noches de colegio, active el panel de configuración Noches de colegio.
- Arrastre el control deslizante para fijar la hora de inicio y fin de la hora de acostarse.
- Para las noches de fin de semana, active el panel de configuración Noches de fin de semana.
- Arrastre el control deslizante para fijar la hora de inicio y fin de la hora de acostarse.
- Seleccione Guardar.

Los límites de la hora de acostarse ya están establecidos.

Nota: La realización de llamadas telefónicas y el envío de mensajes SMS están siempre permitidos.

Bloqueo de contenidos web

Con el filtrado de contenidos, puede asegurarse de que su hijo sólo vea contenidos apropiados en su dispositivo.

El filtrado de contenidos restringe los sitios web a los que puede acceder su hijo. Los tipos de sitios web a los que puede acceder su hijo se basan en el perfil configurado para él y en el grupo de edad seleccionado.

Por esta razón, el Filtrado de Contenidos sólo funciona si establece Navegador Seguro como navegador predeterminado o principal en el dispositivo de su hijo.

Nota: También recomendamos desactivar Safari y otros navegadores en el dispositivo de los niños para evitar que accedan a sitios web desde otros navegadores. También es una buena idea establecer una contraseña para proteger la configuración de la aplicación. De este modo, podrá hacer todo lo posible para garantizar la seguridad de su hijo en Internet.

To select the types of web content to block on all browsers:

Para seleccionar los tipos de contenido web a bloquear en todos los navegadores:

1. Abra la aplicación y seleccione Personas y dispositivos. Se abre la vista Personas y dispositivos.
2. Seleccione el dispositivo del niño en la lista.
3. En REGLAS FAMILIARES, asegúrese de que Filtrado de contenidos está activado.

- Si Filtrado de contenidos está desactivado, seleccione Filtrado de contenidos y utilice el control deslizante para activarlo; a continuación, seleccione Guardar.

4. En CATEGORÍAS DE CONTENIDO BLOQUEADAS, compruebe que las categorías de contenido a las que no desea que accedan sus hijos están bloqueadas.

Nota: Toque una categoría de contenido para ver información más detallada sobre ella.

5. Cuando esté seguro de que ha seleccionado todas las categorías de contenido que desea bloquear, seleccione Guardar.

Si su hijo intenta acceder a un sitio web que contenga alguna de las categorías de contenido bloqueadas por el Filtrado de Contenidos, el navegador lo bloquea

5.3 Compartir la protección con algun familiar o amigo

Este tema describe cómo compartir la protección con un familiar o un amigo.

Cuando invitas a familiares o amigos a tu grupo, las personas invitadas obtienen una cuenta de usuario que les permite proteger sus dispositivos utilizando tus licencias.

Compartir la protección con otra persona:

1. Abra la aplicación y seleccione Personas y dispositivos. Se abrirá la vista Personas y dispositivos.
2. Selecciona + Añadir dispositivo.
3. Selecciona Dispositivo ajeno > Continuar.
4. Para invitar a un usuario a tu grupo:

- Introduzca el nombre del usuario.
- Introduzca el apellido del usuario.
- Introduzca la dirección de correo electrónico del usuario.
- Selecciona Enviar invitación.

Esta persona recibe el correo electrónico de invitación y ahora tiene una cuenta que le permite proteger sus dispositivos utilizando tus licencias. Los usuarios de tu grupo no verán los dispositivos ni otros detalles de otros usuarios o perfiles del grupo.

Tenga en cuenta que si la persona a la que desea invitar a su grupo ya ha sido añadida a su grupo o pertenece a otro grupo de My BOXX Cyber Protect, verá un mensaje en el cuadro de diálogo de invitación diciendo que la persona ya pertenece a dicho grupo o a otro grupo. Esto significa que la dirección de correo electrónico utilizada en la invitación ya ha sido activada para una cuenta BOXX Cyber Protect.

Puede solucionarlo utilizando otra dirección de correo electrónico, si existe, para invitar al usuario a su grupo, o puede pedir a este usuario que elimine la cuenta BOXX Cyber Protect existente, tras lo cual podrá utilizar la dirección de correo electrónico en la invitación.

5.3.1 ¿Recibió una invitación para proteger sus dispositivos?

Este tema describe cómo empezar a proteger tus dispositivos si has recibido una invitación de tu amigo.

Cuando tu amigo comparta la protección contigo, recibirás un correo electrónico invitándote a utilizar sus licencias para proteger gratis tu PC, Mac, smartphone y tableta. Ya hemos creado una cuenta para ti, y puedes encontrar los detalles de tu cuenta en el mensaje.

Para empezar a proteger tus dispositivos:

1. Abra el correo electrónico de invitación y léalo atentamente. Toma nota de los datos de tu cuenta.
2. Seleccione Iniciar ahora.

Se abre la página de acceso a tu cuenta.

3. Introduzca las credenciales de acceso a su cuenta que le fueron enviadas en el correo electrónico de invitación y seleccione iniciar sesión. Se abrirá la ventana Cambie su contraseña.
4. Cree una nueva contraseña segura para su cuenta, seleccione Cambiar y, a continuación, Continuar.

Se abrirá su portal de gestión en línea. Comience a proteger sus dispositivos seleccionando Añadir dispositivo para instalar el producto en uno de sus dispositivos.

Ahora puede gestionar sus dispositivos y su protección a través del portal de gestión en línea o de la vista Personas y dispositivos del producto. Como usuario invitado, puede gestionar su cuenta de las siguientes formas:

- Proteger más dispositivos propios si la suscripción lo permite.
- Puedes cambiar el nombre del dispositivo que se está protegiendo.
- Puedes liberar la licencia en uso. Ten en cuenta que el propietario de la suscripción, o la persona que te invitó a compartir la protección, puede retirar tus licencias en cualquier momento.
- Puedes abandonar el grupo en cualquier momento.
- Puede realizar cambios en la configuración de su cuenta, como cambiar la contraseña de la cuenta y poner en marcha la verificación en dos pasos.

Capítulo 6

Privacidad VPN

Crea una conexión segura y cifrada desde tu dispositivo a Internet. Protege tu conexión en una red WiFi haciendo que tus datos sean ilegibles para extraños. Incluso impide que alguien modifique tus datos o secuestre el tráfico de tu red.

Cuando navega por Internet, las empresas de recopilación de datos rastrean sus actividades en línea y venden sus datos a los anunciantes. VPN de privacidad bloquea estos intentos de rastreo del tráfico HTTP para que puedas navegar de forma anónima y sin ser molestado.

VPN de privacidad escanea en busca de malware, cookies de rastreo y otras amenazas online. Estarás protegido de sitios dañinos, rastreadores y aplicaciones que quieren enviar tus datos sin que lo sepas.

Cuando utiliza BOXX Cyber Protect, la aplicación le pide permiso para establecer una conexión VPN. Debe permitirlo para que VPN de privacidad pueda supervisar el tráfico de red. Más tarde, puedes activar y desactivar VPN de privacidad en la vista principal del producto.

6.1 Activar y desactivar la conexión VPN

Puedes activar y desactivar la conexión VPN en la página principal del producto.

Cuando instalas el producto en tu dispositivo móvil, la aplicación te pide permiso para establecer una conexión VPN. Si no has activado la VPN de privacidad, puedes activarla de la siguiente manera:

1. Abra la aplicación y seleccione VPN de privacidad. Se abrirá la vista Privacidad VPN.
2. Para activar la VPN de privacidad, toque el centro de la pantalla. Su actividad en línea está ahora protegida.

Nota: Para desactivar la VPN de privacidad, toque el centro de la pantalla.

Puede ver estadísticas sobre cómo VPN de privacidad ha protegido su tráfico en la vista de VPN de privacidad. Los datos también muestran cuántos rastreadores y sitios web dañinos ha bloqueado VPN de privacidad.

6.2 Marcar una red WiFi local como de confianza

Con VPN de privacidad, puede marcar su red local favorita como de confianza para permitir conexiones a otros dispositivos dentro de la misma red mientras la VPN está activada.

Para marcar la red WiFi local como de confianza:

1. Abra la aplicación y seleccione VPN de privacidad. Se abrirá la vista Privacidad VPN.
2. Selecciona el icono de configuración en la esquina superior derecha.

Se abre la vista de configuración de VPN de privacidad, que muestra la red local actual que está utilizando.

3. Selecciona Redes WiFi de confianza.

Se abre la vista Redes WiFi de confianza.

4. Seleccione la casilla Red actual y, a continuación, Guardar. Su red actual está ahora marcada como de confianza.

Importante: Nunca marques como de confianza las redes que no requieran contraseña.

Capítulo 7

Protección de la navegación web

Esta sección explica cómo la aplicación puede garantizar una navegación segura en Internet, así como una banca en línea segura.

Con Navegación segura, puedes utilizar Navegador Seguro, un navegador personalizado dentro de la aplicación que puedes establecer como navegador predeterminado en tu dispositivo. Navegador Seguro evita que accedas accidentalmente a sitios web dañinos y te ofrece más seguridad al realizar operaciones bancarias en línea.

Al utilizar Navegador Seguro, se comprueba automáticamente la seguridad de un sitio web antes de acceder a él. El producto bloquea el acceso si el sitio está clasificado como sospechoso o dañino. La calificación de seguridad de un sitio web se basa en el análisis de nuestro servicio de reputación de sitios web.

Nota: Sin embargo, sigue siendo posible entrar en un sitio web bloqueado incluso después de ver el mensaje de advertencia, aunque esto sólo se recomienda si sabe con certeza que el sitio es seguro. El sitio se detiene de nuevo al reiniciar el producto o al apagar y volver a encender Navegador Seguro.

Navegador Seguro también aumenta la seguridad cuando entras en un sitio de banca en línea, impidiendo que software dañino distribuya tu información privada.

El uso del Navegador seguro es especialmente importante si el dispositivo pertenece a un niño. El Navegador seguro se utiliza junto con las Reglas familiares, por lo que, para proteger completamente el dispositivo de un niño, se recomienda configurar el Navegador seguro como navegador principal y activar las Reglas familiares.

Para empezar a utilizar Navegador Seguro:

1. Abra la aplicación y seleccione Navegación segura. Se abre la vista Navegación segura.
2. Seleccione Navegador seguro.

7.1 Establecer Navegador Seguro como navegador predeterminado o principal

Este tema explica cómo configurar Navegador Seguro como navegador predeterminado o principal.

Para empezar a utilizar Navegador Seguro y sacar el máximo partido del producto, configure Navegador Seguro como navegador predeterminado o principal en el dispositivo.

Esto es especialmente importante si el dispositivo pertenece a un niño y desea proteger su actividad en línea. Como medida de seguridad, también puedes plantearte eliminar los demás navegadores del dispositivo del niño para asegurarte de que no pueda acceder a otros sitios utilizando navegadores diferentes.

Si está utilizando Navegador Seguro en su dispositivo, no es necesario eliminar otros navegadores. Sin embargo, asegúrese de utilizar siempre Navegador Seguro si desea que Safe Browsing evalúe la seguridad de los sitios web que visita y evite el acceso accidental a sitios web dañinos.

Para configurar Navegador Seguro como navegador predeterminado:

1. Vaya a Ajustes > Safari > Aplicación de navegador predeterminada en su dispositivo.
2. Seleccione BOXX Cyber Protect.

Para comprobar que se ha activado el Navegador Seguro, abra esta página de prueba en su navegador: https://unsafe.fstestdomain.com. Si la página se bloquea, Navegador Seguro se ha configurado correctamente.

7.2 Proteger la banca y las compras en línea

La aplicación puede proteger sus sesiones de banca y compras en línea impidiendo que programas o sitios dañinos recopilen y envíen los datos personales que introduzca, incluidos números de tarjetas de crédito, información de cuentas de usuario y contraseñas.

Cuando Navegador Seguro está activado y entras en un sitio de banca o compras online, la aplicación lo detecta automáticamente. Pone todas las demás conexiones de red en espera, excepto los sitios que necesitas para realizar tu transacción (que han sido verificados como seguros por BOXX Cyber Protect).

El resto de conexiones sólo se restablecen cuando finaliza la sesión en el sitio bancario. Esta capa de seguridad adicional impide que programas dañinos envíen tus datos privados.

Nota: La protección de tus operaciones bancarias y compras en línea solo funciona cuando utilizas Navegador Seguro. La aplicación no puede proteger tus sesiones de banca o compras online si utilizas cualquier otro navegador.

7.2.1 Uso de Navegador Seguro para banca y compras en línea

Una vez activada la Navegación Segura en la aplicación, el resto de conexiones de red se suspenden temporalmente.

Para acceder al Navegador Seguro y activar la protección de Navegación y Banca:

1. Abra la aplicación y seleccione Navegación segura. Se abrirá la vista Navegación segura.
2. Seleccione Navegador seguro.
3. Navegue por un sitio de banca o compras en línea y complete su transacción.

Cuando entras en un sitio de banca o compras online, aparece una notificación en la aplicación que dice Has entrado en un sitio bancario de confianza. Esto significa que la protección está funcionando.

También puede simular el aspecto de la notificación seleccionando el enlace. ¿Qué aspecto tiene la notificación? En la página Pago y banca seguros.

7.3 Volver de un sitio web bloqueado o entrar en él

Este tema explica qué hacer si accidentalmente accede a un sitio dañino utilizando el Navegador Seguro.

Supongamos que accedes accidentalmente a un sitio web dañino cuando utilizas Navegador Seguro. En ese caso, la aplicación bloquea automáticamente el acceso y muestra una página en la que se le informa de que el sitio web al que acaba de acceder es peligroso. Hay dos cosas que puedes hacer después de esto:

1. Si desea volver a la página original que abandonó, seleccione Volver a la página.
2. Si sabes que el sitio es seguro y quieres entrar en él aunque el Navegador Seguro lo haya bloqueado, sigue el enlace Quiero entrar en este sitio web de todos modos de la página

BOXX INSURANCE

PREDECIR.
PREVENIR.
ASEGURAR.

www.boxxinsurance.com