powered by BOXX INSURANCE

BOXX CYBER PROTECT

APP USER GUIDE

VERSION 1.0

Contents

Chapter 1: Introduction to BOXX CYBER PROTECT 3

Chapter 2: Installing BOXX CYBER PROTECT....5

2.1 Installing BOXX CYBER PROTECT on your mobile device....5
2.2 Checking the app is working....5

Chapter 3: Protecting your identity online....6

3.1 Adding items for monitoring....6
3.2 Editing and deleting monitored items....7

Chapter 4: Storing and protecting your passwords....8

4.1 Getting started with Password Vault....9
4.1.1 About the master password....9
4.1.2 About the recovery QR code for the master password....10
4.1.3 Using biometric authentication to unlock Password Vault....12
4.2 Using Password Vault....13
4.2.1 What makes a good password....13
4.2.2 Storing entries....14
4.2.3 Editing entries....15
4.2.4 Accessing your old passwords....16
4.3 Using Autofill....17
4.3.1 Autofill and built-in browser password managers....17
4.3.2 Turning on Autofill....17
4.4 Connecting devices....18
4.4.1 Connecting your devices to sync your Password Vault data across both devices....18
4.5 Unlocking and locking Password Vault....19

Chapter 5: Protecting people and devices....20

5.1 Protecting your own device....20
5.2 Protecting your child's device....21
5.2.1 Editing Family Rules settings....21
5.3 Sharing protection with a family member or friend....23
5.3.1 Did you receive an invitation to protect your devices?....23

Chapter 6: Privacy VPN....25

6.1 Turning on and off the VPN connection....25
6.2 Marking a local WiFi network as trusted....25

Chapter 7: Protecting your web browsing....27

7.1 Setting Safe Browser as the default or primary browser....27
7.2 Protecting online banking and shopping....28
7.2.1 Using Safe Browser for online banking and shopping....28
7.3 Returning from or entering a blocked website....28

Chapter 1

Introduction to BOXX CYBER PROTECT

BOXX CYBER PROTECT is an easy-to-use app for all your security and privacy protection needs.

BOXX CYBER PROTECT is an all-in-one package that includes everything you need to protect your privacy and devices from online threats. It is built on award-winning antivirus protection technology. The product covers you comprehensively as follows:

- **Protects your devices against harmful content**

The app protects you against viruses, trojans, ransomware, and other harmful apps that may collect, steal or lock personal data, credit card numbers, banking credentials, and additional valuable information.

- **Protects your browsing, online banking and shopping**

The app can protect your online banking and shopping sessions by preventing harmful software or sites from collecting and sending out personal details that you enter, including credit card numbers, user account information, and passwords. It blocks websites that try to scam you out of your money or personal information with Browsing protection. It automatically keeps you from malware and phishing sites protecting your security and privacy.

On mobile devices, Banking protection is enabled within Safe Browser.

- **Secures your internet connection with Privacy VPN**

The app protects your privacy and encrypts your internet connection with a fast and unlimited VPN to prevent hackers, trackers, and intrusive companies from spying on your online activities, even on unsecured public WiFi networks at hotels, restaurants and airports.

This integrated VPN technology adds another layer of security and privacy while browsing.

- **Prevents online identity theft**

The app helps to respond to account takeover and identity theft threats.

It protects your online identity by storing your passwords securely and letting you access them easily from any device with Password Vault, a handy password manager. Password Vault makes it easy for you to create strong and unique passwords, and you can synchronize them across all your devices. Its password analysis feature lets you know if you are using common, weak or even reused passwords.

With ID Monitoring, you get real-time breach alerts when an online service you use gets hacked, and your personal information is at risk. With a combination of human intelligence and dark web monitoring, we recover breach data before it ends up in the dark web on average from four to six months faster than the rest of the market.

It lets you protect your entire family and friends.

The app has been designed to protect your entire family, from small children to adults, adjusting to personal protection needs with a single app.

With the app, you can easily manage your subscription, licenses and users protected with your subscription. The People & Devices view gives you an overview of the people and their devices that you, as the subscription owner, have protected with your subscription. The users that you invite to your group will have a user account of their own.

All child profiles are managed using your account. The app lets parents set healthy boundaries for children’s device use without forgetting the core online security and privacy. The app ensures that children can safely explore the internet, install apps, and communicate with friends and family.

Alternatively, you can use the online management portal to protect your group’s devices.

Chapter 2

Installing BOXX CYBER PROTECT

You can download and install BOXX CYBER PROTECT from the invitation email you have been sent.

You can also use the portal to send an installation link to a device by email or SMS, making it easy to deliver BOXX CYBER PROTECT to a device that you want to protect.

2.1 Installing BOXX CYBER PROTECT on your mobile device

This topic provides instructions on installing BOXX CYBER PROTECT on your smartphone or tablet.

1. Click on “Install Cyber BOXX Protect” in the welcome email you have been sent
2. Install Cyber BOXX Protect from your app store using the link in the welcome email
3. Once the app is installed on your device, launch the app and complete the app set-up step
4. Enter the log-in details you were sent in the welcome email (your email address and the One Time Password provided in the invitation email)
5. Configure notification settings

2.2 Checking the app is working

The app is working and protecting you and your device when you see a green tick and the text “Your device is protected” in the main app view.

If the protection is turned off, a red exclamation mark appears in the middle of the shield with the text “Your device is not protected.” On the main app view, a notification prompts you to turn on Viruses & Threats protection. Select Turn on to activate the protection.

If it has been a while since the device was last scanned, you can manually activate a virus scan:

1. On the main app view, select Viruses & threats. The Virus & Threat protection view opens.
2. Tap on Scan to activate a virus scan.

Once the scan is completed, you can see the results of the scan on the page.

Chapter 3

Protecting your identity online

With ID Monitoring, you can add your email addresses and other personal information for monitoring and receive guidance on what to do if your information leaks in a data breach.

The notification email includes information on what personally identifiable information (PII) has been associated with the breach; what the violation was; what company or entity was breached; when the breach took place; and what other pieces of PII have been associated with the monitored email address, such as passwords, credit card numbers, street address, and so on.

Note: When you create your account, your email address is automatically added for monitoring. You will receive a confirmation email to the address in question, and you need to confirm the email address before you can access the detailed information about the breaches and leaked data, if any, associated with this email address.

3.1 Adding items for monitoring

This topic describes how to add items for monitoring.

The first item you add for monitoring must be your email address. Only after having added the email address for monitoring can you add other items, such as usernames and credit card numbers for monitoring. This address will also be the email address to which we send notifications if your information appears in a data breach.

Note: When you create your account, your email address is automatically added for monitoring. You will receive a confirmation email to the address in question, and you need to confirm the email address before you can access the detailed information about the breaches and leaked data, if any, associated with this email address.

To add more items for monitoring:

1. Open the app and select ID Monitoring.
2. In the ID Monitoring view, select Monitored Items. The Monitored Items view opens.
3. Select + Add item.

The Add new dialogue opens, listing all the available item types to choose from. Note that if you still need to add an email address for monitoring, the product asks you first to add an email address for monitoring. Only after that can you add other types of items for monitoring.

4. Select the type of item you want to add for monitoring. The New Monitored Item view opens.
5. Enter the requested information and select Add.

Monitoring immediately looks for breaches with your data and shows you the search result. Note that to see more detailed information about your leaked data, if any, and the recommended actions, make sure that you have confirmed your email address.

6. If you still need to confirm your email address, open the confirmation email, and select the link to verify that this is your email address.
7. To see the details of your exposed personal information and what you should do, tap on the specific breach listed in the ID Monitoring view.

Important: If your information has been exposed to a data breach, we urge you to execute the recommended actions as soon as possible to eliminate the risk of your information being misused.

3.2 Editing and deleting monitored items

This topic describes how to edit a monitored item and how to delete an item from monitoring.

Note: You cannot directly edit an item added for monitoring. If you need to edit an existing monitored article, delete the item and add it again for monitoring.

To delete a monitored item:

1. Open the app and select ID Monitoring.
2. In the Monitoring view, select Monitored Items.

The Monitored Items view opens, listing all your currently monitored items.

3. To delete an item from the list, select the three dots next to the article and then select Delete. The Delete Monitored Item? Dialog opens.
4. To confirm that you want to stop monitoring the item, select Delete. The item disappears from the monitored items.

Note: To edit your contact email address or to delete it from monitoring, you need to delete all other monitored items, if any, before you can edit or delete the contact email address.

Storing and protecting your passwords

Password Vault stores and protects your personal information, such as passwords, credit card numbers, and PIN codes.

Password Vault gives you an easy way to ensure that your online services account credentials, credit card details, and other important information stay safe and conveniently accessible.

The main benefits of the Password Vault feature are:

- **Password storage:** Store all your passwords, login details, PIN codes, credit card details, and online banking credentials securely.

- **Create passwords:** Generate stronger, unique passwords for all your services and accounts.

- **Autofill:** Get your passwords automatically entered on login pages in your web browser to make it easier and quicker to access your account.

- **Connecting device:** You can connect your devices to synchronize your passwords securely across them all.

With Password Vault, all the data is encrypted, and the only way to access it is with your master password. No one can access your data. Furthermore, the service is anonymous, which means there is no way for anyone else to link you to your data. There is no web browser access to your data, so nobody can access it without stealing your device.

Password Vault stores your data, such as usernames, passwords and credit card details, on the computer or mobile device you use to run the app.

Your passwords are stored in an encrypted format, and nobody can access them unless they know your master password and get access to your device.

You can sync your passwords across your devices. We do not provide access to passwords through our servers for security reasons. We recommend you sync your passwords with another device running the app if you lose or break your device. No matter what happens to one of your devices, sync ensures that you always have access to your passwords on the other devices.

4.1 Getting started with Password Vault

This topic describes how to take Password Vault into use on the device you are currently using.

When you take Password Vault into use, the first thing you need to do is to create a master password. The master password is the only one you need to remember once you have set up Password Vault.

To set up Password Vault:

1. Open the app and select Password Vault.
2. Select I'm a new user.

Note: If you already use the app on another device, you can connect the devices to sync your passwords by selecting I am an existing user.

3. Create a strong master password and select Continue.
4. Repeat the master password and select Confirm.
5. Create a recovery QR code by selecting Save. The code is saved as an image in your Photos.

Important: We strongly recommend that you immediately create a recovery QR code for the master password. It is the only way to regain your master password if you forget it.

6. If you want to use biometric authentication, for example, Touch ID, to access your Password Vault faster, make sure that Use Touch ID to unlock is turned on and select Save. Note that if you don't want to take the biometric authentication into use now, you can do it later from Password Vault settings.

Remember: Do not, however, forget your master password. From time to time, you'll need to enter your master password to unlock Password Vault.

You are now ready to add your first password to Password Vault.

If you did not yet create a recovery QR code for the master password, the notification to generate the code will be shown to you until you create it.

4.1.1 About the master password

The master password is critical as it gives you access to your Password Vault data.

When you set up Password Vault, the first thing you need to do is to create a master password. The master password is the only password that you need to remember once you have taken Password Vault into use.

Choose a hard-to-guess master password or passphrase that you can remember, as Password Vault will not be able to reset your master password if you forget it. The fact that there is no way to reset a forgotten master password has been a conscious decision to increase your security and privacy and protect your data.

You are prompted to create a recovery QR code at the end of setting up Password Vault. We strongly recommend that you create the code, as it is the only way of regaining access to your Password Vault data should you forget your master password.

Changing the master password

This topic describes how you can change your master password for Password Vault on any device.

To change your master password:

1. Open the app and select Password Vault.
2. Select the settings icon from the screen's top-right corner. The Password Vault settings view opens.
3. Select Change Master Password.
4. Enter your old master password and select Continue.
5. Enter a strong new master password.
6. Repeat the new master password and select Confirm.

Note: If you are using biometric authentication, provide the requested authentication.

7. Since you have changed your master password, you must create a new recovery QR code. Select Create now and then select Save as an image.

The code is saved to the default location on your device.

Your master password has now been changed. Once you have changed your master password on one device, you must use the new password on all your connected devices.

Note: If you change the master password for any reason, you must create a new recovery QR code. Any old code will no longer be valid. Therefore, ensure that the recovery QR code is always up to date and valid for your current master password.

4.1.2 About the recovery QR code for the master password

The recovery QR code for the master password is a unique and personal code that is the only way of regaining access to the Password Vault data should you forget your master password.

Important: We strongly recommend that as a final step when taking Password Vault into use, you create a recovery QR code for your master password.

For security reasons, we cannot restore any master passwords, as this would mean accessing your master password, which could be considered a security risk.

The recovery QR code is strongly encrypted and can only be decrypted on one of your connected devices. This means that it cannot be decrypted on any other user device.

There are a few important things to note about the recovery QR code:

- Every time you change your master password, you must create a new recovery QR code.

- You always need the latest recovery QR code to regain access to your Password Vault data.

- If you connect new devices, the app may ask you to create a new recovery QR code. If this is the case, make sure you create a new recovery QR code, as the old code will not work anymore.

- We recommend saving the recovery QR code as an image and printing a copy for safekeeping. The recovery QR code print-out should not be stored in the exact location of your device.

Note: If you change the master password for any reason, you must create a new recovery QR code. Any old code will no longer be valid. Therefore, ensure that the recovery QR code is always up to date and valid for your current master password.

Creating a recovery QR code for the master password

This topic explains how to create a recovery QR code for the Password Vault master password.

Important: We strongly recommend that you immediately create a recovery QR code for the master password. It is the only way to regain your master password if you forget it.

To create a recovery QR code for your master password:

1. Open the app and select Password Vault.
2. Select the settings icon from the screen's top-right corner. The Password Vault settings view opens.
3. Select Create Recovery Code, and do one of the following:

- If you have biometric authentication in use, provide the requested authentication. Alternatively, select Use the password and enter your master password.

- Enter your master password and select Confirm to create a recovery QR code.

The recovery code image is automatically created.

4. Select Save.

The code is saved to the default location on your device. This is usually the Photos folder.

5. Go to the folder, select the image, and send it to a service from which you can print it.

Note: We recommend you save the code as an image and print the file out for safekeeping rather than store it in a cloud storage service.

Related information

Using biometric authentication to unlock Password Vault

If your mobile device supports biometric authentication, you can use, for example your fingerprint to unlock Password Vault.

Using the recovery QR code to recover a forgotten master password

This topic explains how to recover your master password using the recovery QR code.

Important: You can recover your master password only if you have previously created a recovery QR code for your master password.

To recover your master password with the recovery QR code:

1. Open the app and select Password Vault.
2. On the login screen, select Forgot Master Password?
3. Do one of the following:

- Select Import image, and then select the code image from the folder to which you saved it.

- Select Scan Recovery Code, and scan the print-out of the code.

Your master password appears on the screen.

4. Copy the master password to the clipboard and paste it to the Master Password field on the login page.
5. Select Unlock.

Password Vault opens.

4.1.3 Using biometric authentication to unlock Password Vault

If your mobile device supports biometric authentication, you can use, for example, your fingerprint to unlock Password Vault.

Note: Before using biometric authentication to unlock Password Vault, you must first register your fingerprint.

Consult your device user manual to find out how to take biometric authentication into use on your device.

In Password Vault, you can take biometric authentication into use when you create your master password or later on by selecting biometric authentication to unlock in the Password Vault login view.

Remember: Do not, however, forget your master password. From time to time, you'll need to enter your master password to unlock Password Vault.

Important: We strongly recommend that you immediately create a recovery QR code for the master password. It is the only way to regain your master password if you forget it.

4.2 Using Password Vault

With Password Vault, you can create and edit password and payment card entries, let the app generate strong passwords for your online services, and access your password history.

4.2.1 What makes a good password

The general recommendation for a good password is that it should be unique and contains a combination of letters, numbers, and special characters. It is easy for you to remember but hard for anyone else to guess.

In addition to these general guidelines, several other approaches improve the safety of your accounts for online services:

- Use generated passwords. When you use a password generated by Password Vault, no memorization system or other clues can be used to break the password.

- Change your password. It's a good idea to change your passwords now and again, but if nothing else, change your password immediately for any service that notifies you of a potential data breach.

- Whenever feasible, use different email addresses for different online services. This means that if your email account is hacked, it won't put all of your online accounts at risk.

- Avoid using your email address as a username whenever possible. Many services automatically create your account with your email address as a username; if not, use something else.

Why do you need to use different passwords for each service and account?

Security experts generally recommend using strong, unique passwords for each of your online services and accounts.

Strong passwords containing several different characters are compulsory for some online services - the password you enter when you sign up is only accepted if it is longer or complex enough.

However, even if you come up with a highly complex password that is virtually impossible for anyone else to guess, the safety of your account to online services is at risk if you use that same password for each account. For example, if hackers gain access to the login details for one of your services, they can then use that information to access any of your other online accounts where you have used the same password. Using a unique password for each account means that your additional charges are not at risk, even in the event of a data breach in one of the services you use.

4.2.2 Storing entries

Step-by-step instructions on creating entries in the app and how to let the app generate strong passwords for your online services.

Storing a new password on a mobile device

You can store new passwords in the app on your mobile device.

To store a new password:

1. Open the app and select Password Vault.
2. Select + Add.
3. Select Password.
4. In the Title field, give your entry a descriptive name.
5. To customize the entry icon on the left, tap on it and select a background colour and a symbol for the entry. Once done, confirm your selection by selecting Done.
6. In the Username field, enter your username for the app or online service.
7. In the Password field, create a strong password or passphrase.

Tip: Select the dice icon to open the Generate password view, where you can let the app generate a strong, random password for you. Tap the dice icon until you are satisfied with the generated password. To save the password, select Done.

8. In the Web address field, enter the web address (URL) of the online service login page.
9. In the Notes field, enter any additional information.
10. To save the entry, select Done.

The new credentials have now been added to Password Vault.

Important: If you change or generate a password in Password Vault, remember to change your password also in the online service or application in question.

Storing payment card information on a mobile device

You can safely store any payment cards details, such as credit and debit card details, in the app on your mobile device.

To store your payment card details:

1. Open the app and select **Password Vault.**
2. Select + Add.
3. Select a Credit card.
4. To customize the entry icon on the left, tap on it, choose one of the available payment card symbols, and select Done.
5. In the Title field, enter the name of the payment card.

6. In the Cardholder name field, enter your name as it is on the payment card.
7. In the Credit card number field, enter your card number.
8. In the PIN field, enter the personal identification number associated with the card
9. In the Expiry Date field, enter the card's expiration date in the format MM/YY.
10. Enter your card's verification code (CVV) in the Verification code field.
11. In the Web address field, enter the service's web address (URL).
12. In the Notes field, enter any additional information.
13. To save the new entry, select Done.

    Your payment card entry has now been added to **Password Vault.**

4.2.3 Editing entries

Step-by-step instructions on how to edit entries in the app.

Editing an existing entry

You may need to edit a Password Vault entry at some point.

To edit an entry:

1. Open the app and select Password Vault.
2. Select the entry that you want to edit.
3. Select the pen icon to open the Edit view.
4. Make the required changes.
5. To save the changes, select Done.

Generating a password with Password Vault

Password Vault can generate a strong password for you when you need to change a password.

You can choose the length and complexity of the password.

To change a password:

1. Open the app and select Password Vault.
2. Go to the entry whose password you want to change and select the pen icon.
3. In the Password field, select the dice icon.
4. In the Generate password view, you can do the following:

    - Drag the slider from side to side to select the number of characters you want in your password.
    - Select the type of characters (lower and upper case letters, numbers and special characters) you want in your password.
    - Tap the dice icon below the generated password if unsatisfied with the password.

5. To take the generated password into use, select Done.
6. To save the entry, select Done.

Important: If you change or generate a password in Password Vault, remember to change your password also in the web service or application in question.

You can store new passwords in the app on your mobile device.

Deleting an entry

You can delete Password Vault entries that you don’t need any longer.

To delete an entry:

1. Open the app and select Password Vault.
2. Select the entry that you want to delete.
3. Select the pen icon to open the Edit view.
4. To delete the entry, select the trash can icon.
5. To confirm the deletion, select Delete.

4.2.4 Accessing your old passwords

The Password History log contains your previous passwords, if any, for the online service in question.

After changing a password in Password Vault, you may still need to log in to the online service with the old password. Also, quite often, before being able to change a password for a service, you need to enter the old password.

To access the previous passwords:

1. Open the app and select Password Vault.
2. Open the entry whose previous passwords you want to view.
3. Select Password history.

Note: If you cannot see Password history in the entry, there are no previous passwords available for that particular online service.

The Password history view opens.

4. Select the open-eye icon in the top-right corner to view the hidden passwords.

Note: If you want, you can delete the password history by selecting first the trash icon in the top-right corner and then Clear in the Clear password history dialog.

5. To close the Password history view, select the x icon in the top-left corner.

4.3 Using Autofill

With Password Vault, you don't have to enter usernames and passwords manually.

You need to have the username, password and web address of the service saved in Password Vault for Autofill to work. When you log in to an app or website with credentials saved in Password Vault, you can have the app enter your username and password automatically.

4.3.1 Autofill and built-in browser password managers

This topic explains built-in browser password managers and how these may affect Autofill in Password Vault.

As most browsers have a built-in password manager, passwords may get saved to the browser automatically. To keep your passwords safe, the best practice is to avoid saving passwords in your browser.

Passwords saved in the browser may also cause issues with Autofill in Password Vault, as the app cannot identify the passwords correctly for the service being logged into.

Before taking Autofill into use in Password Vault, we, therefore, recommend the following:

- Turn off the built-in password manager in the browser that you use.
- Make sure that all the passwords in the built-in password manager are stored in Password Vault. Move your passwords to Password Vault if you have not already done so.
- Once the built-in password manager is turned off, to ensure that none of your passwords remain in the built-in password manager, you may also have to clear the data in the browser.

4.3.2 Turning on Autofill

With Autofill, you can log in to apps and websites without manually entering usernames and passwords.

You need to have the username, password and web address of the service saved in Password Vault for Autofill to work. When you log in to an app or website with credentials saved in Password Vault, you can have the app enter your username and password automatically.

To turn on Autofill on your iPhone or iPad:

1. Go to your device Settings > Passwords & Accounts.
2. Under Passwords & Accounts, select AutoFill Passwords.
3. Under AutoFill Passwords, turn on AutoFill Passwords if it is turned off.
4. Under Allow filling from, select Password Vault.

You can now use Autofill on your device.

Logging in to an app or website

For Password Vault 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.

To log in to an app or website on your iPhone or iPad:

1. Open the app or the website login page and tap the username field. Passwords appear on top of your device keyboard.
2. Select Passwords.
3. Select Password Vault.
4. Unlock Password Vault.
5. Select the entry needed.
6. Select Login.

You are now logged in to the app or web service.

4.3 Connecting Devices

You can connect your devices to synchronize your Password Vault data.

To sync your Password Vault data across all your devices, you need to connect the devices with the app installed.

If you have the app on a single device, your Password Vault data is stored on that device only. The app has been designed so that connecting your devices lets you have your data readily available and always up to date on your other devices. When you have your data also on another device, there is no need to worry if a device gets lost, stolen or damaged; your data will still be intact on one of your other devices.

Warning: If you only have the app on one mobile device and carry out a factory reset, the reset also wipes all your Password Vault data from the device. After this, there is no way to get the data back.

4.4.1 Connecting your devices to sync your Password Vault data across both devices

If you already use Password Vault on another device or app, you can connect the devices and sync your data to have your data readily available and always up to date on your other device.

Make sure that you have both devices at hand and that you have the app already installed on the other device as well.

To connect your devices and sync your Vault data across both devices:

1. Open the app on the device containing your Password Vault data and select Password Vault.
2. Select the settings icon from the screen's top-right corner. The Password Vault settings view opens.
3. Select Connect Devices.

The Connect devices view opens.

4. Select Generate sync code.

A sync code is automatically generated and valid for 60 seconds at a time. A new code is generated immediately after the current code expires.

5. Open the app on the other device you want to connect, sync your data, and select Password Vault.
6. Select I am an existing user.

The Connect devices view opens.

7. Enter the sync code generated in Step 4 into the Sync code field and select Connect.
8. When prompted, enter the master password you use on the device where you generated the sync code and select Confirm.
9. Finally, select Save if you want to start using biometric authentication to unlock Password Vault.

Your data has now been synchronized between these two devices. If you have more devices to be connected, repeat the above steps with each device. Note that you can generate the sync code on any connected device

4.5 Unlocking and locking Password Vault

When you are not using Password Vault, we recommend you lock it to add an extra layer of security.

To unlock and lock Password Vault, do the following:

- To unlock, enter your master password and select Unlock or touch the sensor on your phone if you use biometric authentication.

- To lock, select the settings icon and then Lock now from Password Vault settings.

Note: By default, Password Vault locks itself automatically after fifteen minutes. In the Password Vault settings, you can set the time after which Password Vault locks itself automatically. The time intervals are immediate, 5 minutes, 15 minutes, 30 minutes, 1 hour, 10 hours, and 1 week.

Chapter 5

Protecting people and devices

This section provides information on how to use the product to protect your own devices as well as the devices of your family and friends.

The People & Devices view gives you an overview of the people and their devices that you, as the subscription owner, have protected with your subscription. To see detailed information about a user, select the user, and a user-specific view opens, giving you an overview of the protection of the user.

On the People & Devices view, you can add more users and devices to your group by sending the product installation link to the user's device by email or SMS.

The users that you invite to your group will have a user account of their own. All child profiles are managed using your account.

Note: Alternatively, you can use the online management portal to protect your group's devices.

5.1 Protecting your own device

This topic describes how to start protecting your device.

To set up protection for your device:

1. Open the app and select People & Devices. The People & Devices view opens.
2. Select + Add device.
3. Select My device > Continue.
4. Select how you want to deliver the installation link to the device you want to protect, then select Send link.
5. Open the message with your device and follow the installation instructions.
6. Select Install from the app store to go to the app store and select Get to start the installation.
7. After the installation, select Open to start the application. The Welcome to BOXX Protect SAFE page opens.
8. If you agree to the End User License Terms, select Accept and continue.
9. As you set up protection for yourself, select Continue to finalize the security for the device.

Important: To protect your device and connections, the app requires that you allow access to photos, media and files on your device.

You have now set up protection for your device. To view and manage the protection of the above device, select People & Devices, or log in to your account to access the online management portal.

5.2 Protecting your child's device

This topic describes how to start protecting your child's devices.

To set up protection for your child:

1. Open the app and select People & Devices. The People & Devices view opens.
2. Select + Add device.
3. Select My child's device > Continue.
4. Select how you want to deliver the installation link to the device you want to protect, then select Send link.
5. Open the message with your device and follow the installation instructions.
6. Select Install from the app store to go to the app store and select Get to start the installation.
7. After the installation, select Open to start the application. The Welcome to BOXX Protect SAFE page opens.
8. Agree to the End User License Terms by selecting Accept and continue.
9. As you set up protection for your child, select Install for a child.
10. From the Set up protection for drop-down, select New child profile and then select Continue. The Create new child profile view opens.
11. Enter the child's name, select the age group the child belongs to, and then select Next. The Family Rules settings view opens.
12. Turn on Bedtime by using the sliders to limit the night-time use of apps or devices on school nights and weekend nights, and select Next.

The Content Filtering view opens.

13. Turn on Content Filtering, select the categories of web content you wish to block and select Next.

Your child's device is now protected.

For ease of use, you can manage your child's online activity on your device. This is a versatile way to make changes and add or remove restrictions on the fly without having your child's device physically with you.

5.2.1 Editing Family Rules settings

This section describes how to make changes to the current Family Rules settings.

Setting a bedtime

By setting a bedtime, you can ensure that your child gets to sleep when they should.

With the bedtime setting, you can set a different bedtime for school nights—from Sunday night to Thursday night—and weekend nights—from Friday night to Saturday night

To set bedtimes, do the following:

1. Open the app and select People & Devices. The People & Devices view opens.
2. Select the child's device from the list.
3. Under FAMILY RULES, if Bedtime is Off, select Bedtime.
4. On the Bedtime view, prevent the use of the device at night as follows:

- For School nights, turn on the School nights setup pane.
- Drag the slider to set the time when bedtime starts and ends.
- For Weekend nights, turn on the Weekend nights setup pane.
- Drag the slider to set the time when bedtime starts and ends.
- Select Save.

Bedtime limits are now set up.

Note: Making phone calls and sending SMS messages are always allowed.

Blocking web content

With Content Filtering, you can ensure that your child only sees appropriate content on their device.

Content Filtering works by restricting the websites that your child might access. The types of websites that your child can access are based on the profile set up for your child and the age group selected.

For this reason, Content Filtering only works if you set Safe Browser as the default or primary browser on your child's device.

Note: We also recommend disabling Safari and other browsers on a child's device to prevent them from accessing websites from other browsers. Setting a password to protect the app settings is also a good idea. This way, you can do everything you can to ensure your child is safe online.

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

1. Open the app and select People & Devices. The People & Devices view opens.
2. Select the child's device from the list.
3. Under FAMILY RULES, ensure that Content Filtering is turned On.

- If Content Filtering is Off, select Content Filtering and use the slider to turn it on, then choose Save.

4. Under BLOCKED CONTENT CATEGORIES, check that the content categories you don't want your children to access are blocked.

Note: Tap a content category to see more detailed information about it.

5. When you are sure that you have selected all of the content categories that you want to block, select Save.

If your child tries to access a website containing any content categories blocked by Content Filtering, the browser blocks it.

Remember: To use Content Filtering; the app requires you to set up a child profile first.

5.3 Sharing protection with a family member or friend

This topic describes sharing protection with a family member or a friend.

When you invite family members or friends to your group, the invited persons get a user account that allows them to protect their devices using your licenses.

To share protection with someone else:

1. Open the app and select People & Devices. The People & Devices view opens.
2. Select + Add device.
3. Select Someone else's device > Continue.
4. To invite a user to your group:

- Enter the first name of the user.
- Enter the last name of the user.
- Enter the email address of the user.
- Select Send invitation.

This person receives the invitation email and now has an account that allows them to protect their devices using your licenses. The users in your group won't see the devices or other details of other users or profiles in the group.

Note that if the person you want to invite to your group has already been added to your group or belongs to another My BOXX Cyber Protect group, you will see a message in the invitation dialog saying that the person already belongs to your group or another group. This means that the email address used in the invitation has already been activated for a BOXX Cyber Protect account.

You can solve this by using another email address, if any, to invite the user to your group, or you can ask this user to delete the existing BOXX Cyber Protect account, after which you can use the email address in the invitation.

5.3.1 Did you receive an invitation to protect your devices?

This topic describes how to start protecting your devices if you have received an invitation from your friend.

When your friend shares the protection with you, you'll receive an email inviting you to use their licenses to protect your PC, Mac, smartphone and tablet for free. We have already created an account for you, and you can find your account details in the message.

To start protecting your devices:

1. Open the invitation email and read it carefully. Take note of your account details.
2. Select Start now.

Your account login page opens.

3. Enter your account login credentials sent to you in the invitation email and select login. The Change your password window opens.

4. Create a new strong password for your account, select Change, and then choose Continue.

Your online management portal opens. Start protecting your devices by selecting Add device to install the product on one of your devices.

You can now manage your devices and their protection through the online management portal or the product's People & Devices view. As an invited user, you can manage your account in the following ways:

- Protect more of your own devices if the subscription allows.
- You can change the name of the device being protected.
- You can release the license in use. Note that the subscription owner, or the person who invited you to share the protection, can remove your licenses anytime.
- You can leave the group at any time.
- You can make changes to your account settings, such as changing the account password and taking 2-step verification into use.

Chapter 6

Privacy VPN

This section provides information on how to use the product to protect your own devices as well as the devices of your family and friends.

The People & Devices view gives you an overview of the people and their devices that you, as the subscription owner, have protected with your subscription. To see detailed information about a user, select the user, and a user-specific view opens, giving you an overview of the protection of the user.

On the People & Devices view, you can add more users and devices to your group by sending the product installation link to the user's device by email or SMS.

The users that you invite to your group will have a user account of their own. All child profiles are managed using your account.

Note: Alternatively, you can use the online management portal to protect your group's devices.

6.1 Turning on and off the VPN connection

You can turn on and off the VPN connection on the product's main page.

When you install the product on your mobile device, the app asks you for permission to set up a VPN connection. If you did not turn on privacy VPN, then you can turn it on in the following way:

1. Open the app and select Privacy VPN. The Privacy VPN view opens.
2. To turn Privacy VPN on, tap the center of the screen. Your online activity is now protected.

Note: To turn the privacy VPN off, tap the center of the screen.

You can see statistics on how Privacy VPN has protected your traffic on the Privacy VPN view. The data also shows how many trackers and harmful websites Privacy VPN has blocked.

6.2 Marking a local WiFi network as trusted

With Privacy VPN, you can mark your favourite local network as trusted to allow connections to other devices within the same network while VPN is on.

To mark the local WiFi network as trusted:

1. Open the app and select Privacy VPN. The Privacy VPN view opens.
2. Select the settings icon in the top-right corner.

The Privacy VPN settings view opens, showing the current local network you are using.

3. Select Trusted WiFi networks.

The Trusted WiFi networks view opens.

4. Select the Current network checkbox and then Save. Your current network is now marked as trusted.

Important: Never mark networks that don’t require a password as trusted.

Chapter 7

Protecting your web browsing

This section explains how the app can ensure safe browsing on the internet, as well as safe online banking.

With Safe Browsing, you can use Safe Browser—a custom browser within the app that you can set as your default browser on your device. Safe Browser prevents you from accessing harmful websites accidentally and gives you extra security when banking online.

By using Safe Browser, the safety of a website is automatically checked before you access the site. The product blocks access if the site is rated as suspicious or harmful. The safety rating of a website is based on analysis from our website reputation service.

Note: However, it is still possible to enter a blocked website even after viewing the warning message, although this is only recommended if you know for sure that the site is safe. The site is stopped again when you restart the product or turn Safe Browser off and on again.

Safe Browser also increases security when you enter an online banking site by preventing harmful software from distributing any of your private information.

Using Safe Browser is particularly important if the device belongs to a child. Safe Browser is used in tandem with Family Rules, so to protect a child's device fully, it is recommended to set Safe Browser as the primary browser and enable Family Rules.

To start using Safe Browser:

1. Open the app and select Safe Browsing. The Safe Browsing view opens.
2. Select Safe Browser.

7.1 Setting Safe Browser as the default or primary browser

This topic explains how to set up Safe Browser as the default or primary browser.

To take Safe Browser into use and to get the most out of the product, set Safe Browser as the default or primary browser on the device.

This is particularly important if the device belongs to a child and you want to protect their online activity. As a safety measure, you can also consider removing the other browsers from the child's device to ensure that the child cannot access other sites using different browsers.

If you are using Safe Browser on your device, there is no need to remove other browsers. However, ensure that you are always using Safe Browser if you want Safe Browsing to evaluate the safety of the websites you visit and prevent accidental access to harmful websites.

To set up Safe Browser as the default browser:

1. Go to Settings > Safari > Default Browser App on your device.
2. Select BOXX CYBER PROTECT.

To test that Safe Browser has been enabled, open this test page in your browser: https://unsafe.fstestdomain.com. If the page is blocked, Safe Browser has been set up successfully.

7.2 Protecting online banking and shopping

The app can protect your online banking and shopping sessions by preventing harmful software or sites from collecting and sending out personal details that you enter, including credit card numbers, user account information, and passwords.

When Safe Browser is enabled and you enter an online banking or shopping site, the app automatically detects the site. It puts all other network connections on hold except for the sites you need to carry out your transaction (which have been verified as safe by BOXX Cyber Protect).

All other connections are restored only when the session on the banking site is over. This additional security layer stops harmful software from sending out your private details.

Note: Protecting your online banking and shopping only works when you use Safe Browser. The app cannot protect your online banking or shopping sessions if you use any other browser.

7.2.1 Using Safe Browser for online banking and shopping

Once Safe Browser is turned on in the app, all other network connections are put on hold temporarily.

To access Safe Browser and trigger Browsing and Banking protection:

1. Open the app and select Safe Browsing. The Safe Browsing view opens.
2. Select Safe Browser.
3. Browse an online banking or shopping site and complete your transaction.

When you enter an online banking or shopping site, a notification appears in the app that says You have entered a trusted banking site. This means that the protection is working.

You can also simulate what the notification looks like by selecting the link. What does the notification look like? On the Secure Payment & Banking page.

7.3 Returning from or entering a blocked website

This topic explains what to do if you accidentally access a harmful site using Safe Browser.

Suppose you accidentally access a harmful website when using Safe Browser. In that case, the app automatically blocks access and shows a page telling you that the website you have just tried entering is harmful. There are two things that you can do after this:

1. If you want to return to the original page that you left, select Go back on the page.
2. If you know that the site is safe and you still want to enter the site, even though Safe Browser has blocked it, follow the I want to enter this website anyway link on the pag

BOXX INSURANCE™

PREDICT.
PREVENT.
INSURE.

www.boxxinsurance.com