



StarHub CyberProtect QuickStart Guide for Mobile

(Android / iOS)

MARCH 2026

Table of contents

About	4
StarHub CyberProtect account.....	5
StarHub CyberProtect Portal.....	5
CyberProtect application	6
System requirements.....	6
Welcome to StarHub CyberProtect	7
First time login.....	8
Forgotten password.....	8
Getting started with CyberProtect	9
Adding a new device.....	9
Sharing protection with a family or friend.....	10
Protecting online content for your children	11
Setting up content filtering for a child.....	11
Content Categories.....	12
Device Protection	14
Protecting your device against viruses and threats (for Android only)	14
Scan and remove virus manually (for Android only)	14
Device Security.....	15
Scam Protection	16
Protecting your web browsing	16
Setting up the Chrome Protection extension (for Android only)	16
Setting up the Browsing extension in Safari (for iOS only)	17
Running into a blocked website	19
Rejecting non-essential cookies (for iOS only)	19
Blocking advertisements on websites (for iOS only)	19
Protecting yourself against text message scams.....	20
Making sure your WiFi connection is safe	20
VPN.....	21
Turning on the VPN connection	21
What are the virtual locations for CyberProtect VPN?.....	22
Changing your virtual location	23
Connecting to other devices in the same network	23
Allowing applications to bypass VPN (For Android only).....	23
Blocking internet access when VPN is disrupted or is being established (For Android only)	24
Changing the VPN protocol used.....	25

Technical support	25
Sending logs to support	26
Contact us	26
StarHub CyberProtect Features Per Platform	27

About

This documentation provides instructions and information on using the product. In brief, here is what we cover:

- We explain the CyberProtect app.
- We introduce StarHub CyberProtect, the user credentials, the management portal for CyberProtect apps, and what you can do within the portal.
- We also explain the onboarding journey for StarHub customers, covering the steps to take CyberProtect into use.

CyberProtect is a comprehensive security service that offers protection on multiple devices with a single subscription. With CyberProtect, you can protect yourself and your loved ones against all threats on a computer, smartphone, or tablet.

To fully utilize CyberProtect, you need a registered account in the StarHub CyberProtect Portal. StarHub CyberProtect Portal allows you to conveniently manage the security of your devices.

CyberProtect is powered by F-Secure and is a customized build of F-Secure TOTAL made exclusively for StarHub customers. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd. Nobody knows cyber security like F-Secure. For three decades, F-Secure has driven innovations in cyber security, defending tens of thousands of companies and millions of people.

StarHub CyberProtect account

To use CyberProtect, you need a StarHub CyberProtect account (username and password) to access StarHub CyberProtect Portal and to activate the installed CyberProtect applications.

StarHub CyberProtect Portal

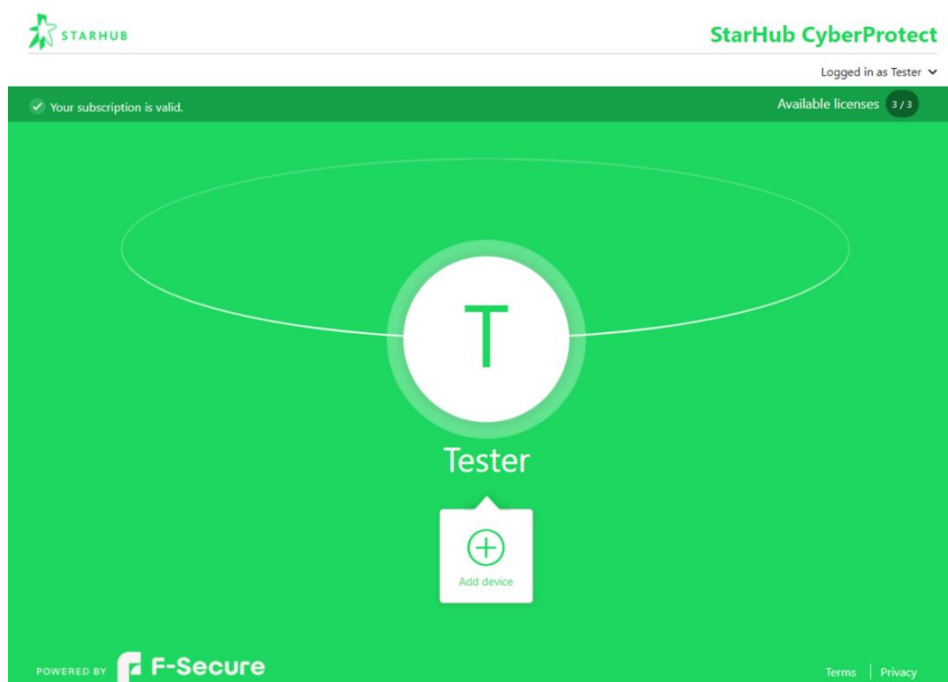
StarHub CyberProtect Portal is the home of your protection. It is an easy-to-use online management portal that you can use to send CyberProtect installation links to your devices, to release licenses from the devices that do no longer need protection in your StarHub CyberProtect Portal group, and to manage your subscription.

Install the product on other devices

You can add new computers, smartphones, and tablets to your account and send the installer to the new devices. When you install the product on a new device, the device appears in your account within the portal.

Manage your subscriptions

You can view your subscription status, expiration date, used licenses, and available licenses online. You can also transfer the product from one device to another if you replace one of your current devices with a new one.



Login [StarHub CyberProtect Portal](#).

CyberProtect application

Install the CyberProtect app on all your devices to protect your data and privacy. CyberProtect supports devices running on Windows, Mac, Android, and iOS operating systems.

CyberProtect also protects you and your loved ones while browsing the internet, with technology like:

- Browsing Protection, which uses advanced cloud-based web reputation checking to verify the web pages and make sure you only access safe websites.
- Banking Protection, which protects your online banking activities by securing the connection when you access an online banking site.
- To use the most up-to-date protection, you can opt to participate in the Security Cloud, an advanced and cooperative cloud-based scanning technology that checks the reputation of any file found on the device. This offers the fastest response time against new threats and protects against both existing and future threats.

System requirements

StarHub CyberProtect supports the following operating system versions for smartphones and tablets:

- Android OS 11 - 16.
- iOS 18 - 26.

Welcome to StarHub CyberProtect



Get it working in just 2 simple steps

Hello test1204,

Activate CyberProtect now to protect up to 3 devices against cyber threats.

🔑 All it takes is 2 steps:

Step 1 Install the CyberProtect app and login with your credentials

Email: @f-secure.com

Temporary password:

Step 2 Set up CyberProtect for your devices

On the CyberProtect App, select the People tab > People & Devices > select + Add device.

[Install CyberProtect now](#)

Important info on Welcome E-mail

- Username
- Temporary password
- Subscription information
- CyberProtect portal
- Download Installer

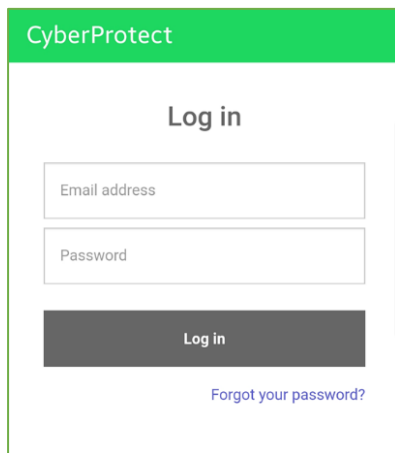
Install CyberProtect Now

The installation link does not require you to log in to activate the installed app, except for iOS.

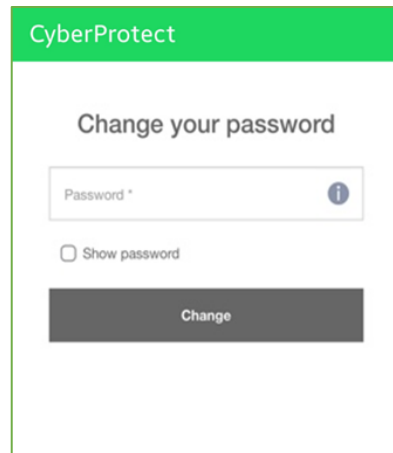
1. Click **Install CyberProtect Now** to open the Download Installer page.
2. Select **Install app on Appstore** to download and install the app on your device.
3. Launch the CyberProtect app. It is activated automatically (no login required).

First time login

1. Log in to the management portal with the temporary password provided. Your username is always your email address.
2. The portal will prompt you to set your own password after you log in for the first time.



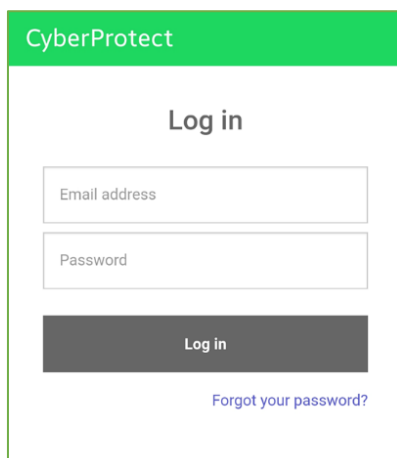
The screenshot shows the 'Log in' screen of the CyberProtect management portal. It features a green header with the 'CyberProtect' logo. Below the header, the title 'Log in' is centered. There are two input fields: 'Email address' and 'Password'. A dark grey 'Log in' button is positioned below the fields. At the bottom, there is a blue link that says 'Forgot your password?'.



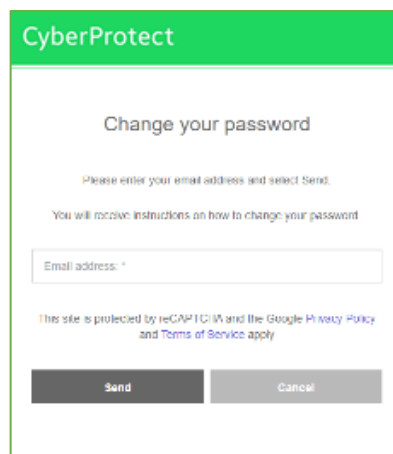
The screenshot shows the 'Change your password' screen of the CyberProtect management portal. It features a green header with the 'CyberProtect' logo. Below the header, the title 'Change your password' is centered. There is a 'Password *' input field with an information icon. Below the field is a checkbox labeled 'Show password'. A dark grey 'Change' button is at the bottom.

Forgotten password

1. Click **Forgot your password** on the login page.
2. Enter your email address.
3. Follow the instructions in the email that you receive to reset your password.



This is a duplicate of the 'Log in' screen described in the previous block, showing the 'Email address' and 'Password' fields, the 'Log in' button, and the 'Forgot your password?' link.



The screenshot shows the 'Change your password' screen after clicking 'Forgot your password'. It features a green header with the 'CyberProtect' logo. Below the header, the title 'Change your password' is centered. The instructions read: 'Please enter your email address and select Send. You will receive instructions on how to change your password.' There is an 'Email address: *' input field. At the bottom, there are two buttons: 'Send' and 'Cancel'. A small note at the bottom states: 'This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.'

Getting started with CyberProtect

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.

You can download and install CyberProtect through StarHub CyberProtect Portal. You can also use StarHub CyberProtect Portal to send the installation link to a device by email or text message, making it easy for you to add CyberProtect to a device that you want to protect.

Adding a new device

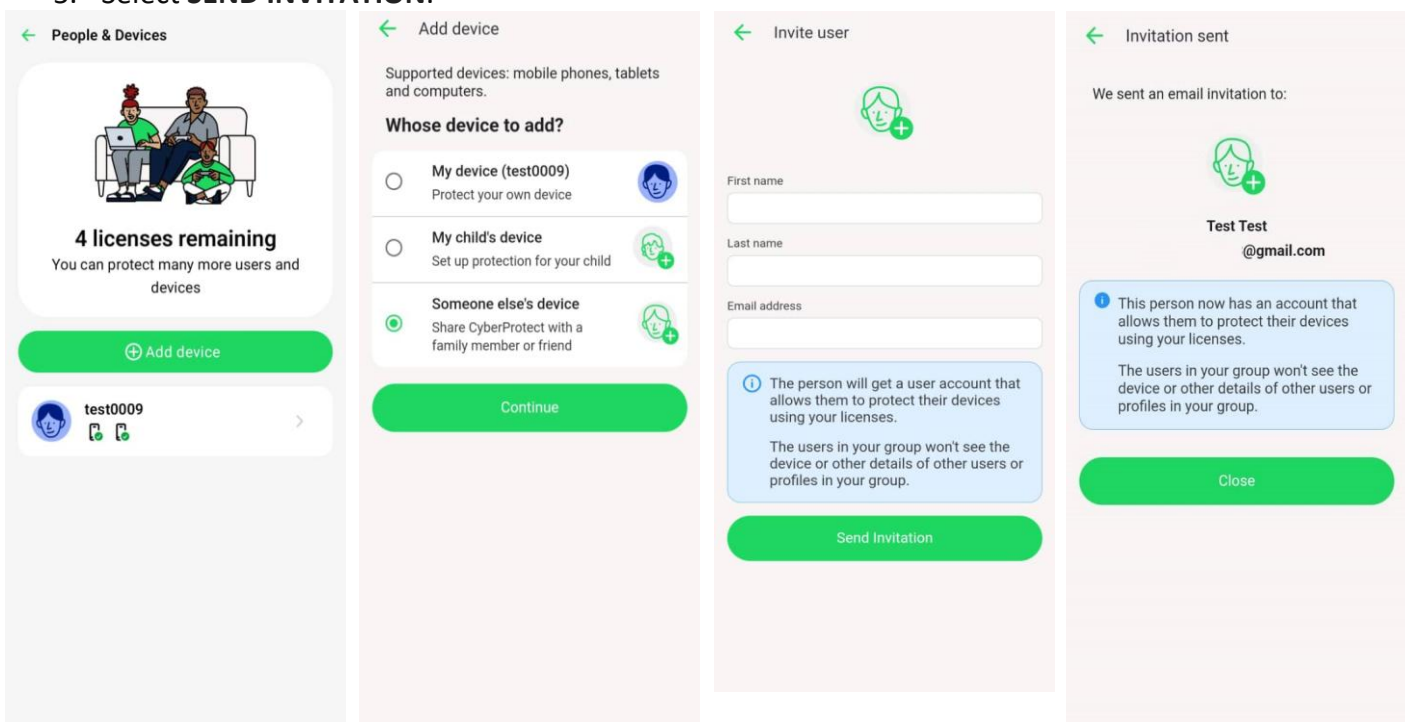
1. Log in to **StarHub CyberProtect Portal** with your account (username and password), or open the **CyberProtect app** and select **People & Devices**.
2. Select **+ Add device**.
3. Choose whose device you want to protect, then select **Continue**.
 - Select **This device** to install CyberProtect on your current device, then select **Install from app store** to go to the app store and start the installation.
 - To install the product on a different device:
 - a. Select the device type and then select **Continue**.
 - b. Select **Send by SMS** and enter the phone number for the device. If the device does not have a phone number, select **Send by email** and enter an email address that you can access on the device.
 - c. Select **Send**.
 - d. Follow the installation instructions that are sent to the device.
4. After the installation is complete, select **Open** to start the app and to activate the product. The product does not protect your device before you activate it.

Sharing protection with a family or friend

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

To share protection with someone else:

1. Open the CyberProtect app and select the **People & Devices** tab.
The **People & Devices** view opens.
2. On the **People & Devices** view, 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.
5. 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.

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

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

Protecting online content for your children

With Family Protection, you can limit your children's access to inappropriate content to prevent them from being exposed to undesirable material on the internet.

The internet is full of interesting websites, but you might not consider all content desirable or appropriate, especially for children. With content filtering, you can make sure your children only see appropriate content on their devices by restricting what web pages they can access.

Setting up content filtering for a child

With content filtering, you can limit the types of online content that your child can access.

When you first set up content filtering on your child's device, you are asked to set a PIN code that makes sure that your child cannot change the settings that you decide to use.

Note: Content filtering uses a VPN connection to block the unwanted content that you select. If you switch on the app's main VPN feature, content filtering does not work.

To set up protection for your child:

1. Open the **CyberProtect** app.
2. On the main view, select **Content filtering**.
3. Select **Get started**.
If you are setting up content filtering for the first time, the app asks you to create a Family Protection PIN.
 - I. Enter a PIN that you can remember easily, then select **Continue**.
 - II. Repeat the PIN that you entered, then select **Continue**.After you set or enter your Family Protection PIN, the **Content filtering** settings view opens.
4. Switch on **Filter online content**.
5. Select the content filtering profile.
You can select **Strict**, **Moderate**, or **Basic**. Each profile blocks a different set of content types. If you do not see the list of content types, scroll down to see which ones are blocked.
6. Select **Continue**.
The app asks you to allow VPN configurations. This is a necessary step, because Family Protection uses a VPN connection to block unwanted content.
7. Select **Continue**.
This opens a system alert that asks you if you want to allow VPN configurations for the app.
8. Allow the VPN configurations.

You have now set up content filtering for your child. To change any of these settings later, select **Content filtering** on the main view of the app

Content Categories

Adult content	Websites that are aimed at an adult audience with content that is clearly sexual or containing sexual innuendo. For example, sex shop sites or sexually oriented nudity.
Disturbing	Websites that contain images, explanations, or video games that can be disturbing. This category contains information, images and videos that are disgusting, gruesome or scary, which can potentially disturb younger children.
Drugs	Websites that promote drug use. For example, sites that provide information on purchasing, growing, or selling any form of these substances.
Gambling	Websites where people can bet online using real money or some form of credit. For example, online gambling and lottery websites, and blogs and forums that contain information about gambling online or in real life.
Alcohol and tobacco	Websites that display or promote alcoholic beverages or smoking and tobacco products, including manufacturers such as distilleries, vineyards, and breweries. For example, sites that promote beer festivals and websites of bars and night clubs.
Illegal	Websites that contain imagery or information that is banned by law.
Illegal downloads	Unauthorized file sharing or software piracy web sites. For example, sites that provide illegal or questionable access to software, and sites that develop and distribute programs that may compromise networks and systems.
Violence	Websites that may incite violence or contain gruesome and violent images or videos. For example, sites that contain information on rape, harassment, snuff, bomb, assault, murder, and suicide.
Hate	Websites that indicate prejudice against a certain religion, race, nationality, gender, age, disability, or sexual orientation. For example, sites that promote damaging humans, animals, or institutions, or contain descriptions or images of physical assaults against any of them.
Weapons	Websites that contain information, images, or videos of weapons or anything that can be used as a weapon to inflict harm to a human or animal, including organizations that promote these weapons, such as hunting and shooting clubs. This category includes toy weapons such as paintball guns, airguns, and bb guns.
Dating	Websites that provide a portal for finding romantic or sexual partners. For example, matchmaking sites or mail-order bride sites.
Shopping and auctions	Websites where people can purchase any products or services, including sites that contain catalogues of items that facilitate online ordering and purchasing and sites that provide information on ordering and buying items online.
Streaming media	Websites and services that let users stream various kind of videos, often without age restrictions.

Social networks	Networking portals that connect people in general or with a certain group of people for socialization, business interactions, and so on. For example, sites where you can create a member profile to share your personal and professional interests. This includes social media sites such as Twitter.
Anonymizers	Websites that provide anonymous and untraceable communication via the Internet.
Unknown	Websites that are not categorized. You can use this category to block content that is unknown.

Device Protection

Protecting your device against viruses and threats (for Android only)

The app scans your device for viruses, harmful content, and other threats to your device or your data.

When scanning is turned on, the app scans the device daily automatically. The app also scans installed programs and inserted memory cards for viruses, spyware, and riskware automatically.

Scan and remove virus manually (for Android only)

You can also scan your device for viruses and other malicious code any time you want.

To manually scan files on your device:

1. Open the app and select **Device Protection**.
2. Select **SCAN**. The scan starts.
3. After the scan is finished, the product shows the following information:
 - Total files checked - the number of the files that were scanned
 - Total apps checked - the number of applications that were scanned
4. Once a scan is complete, you can check the results.
5. If the app detects a file containing a virus or other malicious code during scanning, a notification appears in the **Device Protection** view. You may see the following notification, for example:
 - 1 Detection - Potentially unwanted app
 - 1 Infection - Harmful app detected

6. To assess the detected file, open **Scan details** page:
 - a) In **Device Protection**, select the notification on the main view under **SCAN**.
 - b) To remove the file or files, select **Remove all detections** to remove them from your device at the same time.
 - c) To see more details, select the notification to see more about the details of the detection. You may see the following details:
 - App name
 - Package name
 - Problems detected
 - Size
 - d) Select **Remove** to remove the file. The file or files are removed completely from your device.

You can find descriptions and information on viruses, trojans, worms, and other forms of unwanted software in the F-Secure web site: [F-Secure Labs: Threat Descriptions](#).

Device Security

Device Protection alerts you if you have not set up a PIN or biometrics lock for your device.

Note: The available identification options, such as PIN code, facial recognition, or fingerprint recognition, vary according to your device model and version.

The app shows you a notification if the device lock is not in use. Follow the instructions given in the notification to resolve the issue.

If you do not see a notification on the main view, or if you have dismissed the notification, you can also check the status in the **Device Protection** view:

1. On the main view of the app, select **Device Protection**.
2. Select any warnings you see under **Your device security**.
 - Select **Device lock** to see instructions on how to take the device lock into use.
3. Follow the instructions to resolve the issue.

Once you have resolved the issues, the warning message disappears from the **Device Protection** view.

Scam Protection

Protecting your web browsing

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

Setting up the Chrome Protection extension (for Android only)

Chrome Protection can protect your web browsing, online banking and shopping, and to show you security information while you are browsing the internet.

To enable the extension for Chrome:

1. Open the CyberProtect app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Chrome Protection**.

You are asked to allow permissions for the app. The app requires accessibility permissions to check the safety of websites that you visit, and permission to display content over other apps to show you the safety rating for websites.

4. Select **Continue** and follow the instructions on the screen to allow the required permissions.

Once you allow the permissions, your browsing on Chrome is protected.

When you go to a website in Chrome, an icon appears on the right edge of the screen to show you the safety rating of the website. Tap the icon to see more information about the safety rating. The icon dims after a little while, and you can hide it in the app settings if you want or drag it to any other edge of the screen. Harmful websites are blocked automatically.

To hide the Chrome Protection overlay icon:

1. Open the CyberProtect app.
2. Select Scam Protection.
3. Select Chrome Protection.
4. Select  in the top-right corner of the screen to open the settings.
5. Switch off **Overlay icon**.

Note: On some devices, updates to the Chrome browser or other system tools may reset the connection between Chrome Protection and the accessibility service on your Android device. As a result of this, the overlay icon is not shown, banking protection does not work, and unsafe pages are not blocked. To resolve this issue, go to the app permissions in your device settings and switch accessibility permissions for Chrome Protection off and on again.

Setting up the Browsing extension in Safari (for iOS only)

The browsing extension can protect your web browsing, online banking and shopping, and to show you security information while you are browsing the internet.

To enable the extension for Safari:

1. Open the CyberProtect app.
2. If you have not yet set up the extension for Safari, a notification about the extension is shown on the main view. Select **Set up**.
3. Enable the extension:

On iPhone:

1. Tap **AA**:



A pop-up button menu opens.

2. Tap **Manage Extensions** .

The **Manage Extensions** view opens.

3. Tap **Safe Browsing Extension** to enable the extension.
4. Tap **Done**.

On iPad:

5. Tap .

6. Tap **Safe Browsing Extension** to enable the extension.

You have now enabled the Safe Browsing extension for Safari.

4. Give the extension permission to protect on all websites:

1. Tap **AA** (on iPhone) or (on iPad).

2. Tap **Safe Browsing Extension**.

The **Safe Browsing Extension** permission options are shown.

3. Tap **Always Allow**.
4. Tap **Always Allow on Every Website**.

Note: If you wish, you can change this later in the device **Settings**.

5. Reload this page by tapping .

If you have any doubts about entering personal information on a website, you can still check the safety of the website manually:

1. On the browser, tap on the extension icon () next to the website address and select **Safe Browsing Extension** from the pop-up list. The result of the check is shown on the banner that opens on top of your browser.
2. To return back to the browser, select **Done**.

Running into a blocked website

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

If you accidentally access a harmful website, the app automatically blocks access to it and shows a page telling you that the website you have just tried entering is harmful.

If you think that the site is safe, you can report it as incorrectly rated by following the [Report a false positive here](#) link. To submit the site for analysis, on the **Submit a sample** page, select **URL sample**, fill in the required fields and select **Submit URL sample**.

Rejecting non-essential cookies (for iOS only)

The Cookie Popup Blocker feature helps protect your privacy while browsing by avoiding unnecessary cookies.

Websites use cookies for various purposes, such as storing information related to your session, identifying your account, or tracking the pages that you browse. While some cookies are often necessary to make a website usable, some can be used to collect data on your online activity. This is why different regional authorities have implemented legislation that requires websites to ask for consent on the use of cookies from anyone visiting that site.

Cookie Popup Blocker identifies known cookie consent providers on websites that you visit and automatically rejects non-essential cookies. However, not all websites use such providers, so the feature does not work on those websites.

To change the settings for Cookie Popup Blocker:

1. Open the CyberProtect app.
2. On the main view of the app, select **Scam Protection**.
3. Select the **Settings** icon  in the top-right corner of the screen.
This opens the settings view.
4. Switch **Cookie Popup Blocker** on or off.

Blocking advertisements on websites (for iOS only)

Ad blocker blocks advertising content on the websites that you visit, making it harder to track you and improving your browsing experience.

If a page that you visit does not load correctly without advertisements, you can switch Ad blocker off temporarily:

1. Open the CyberProtect app.
2. On the main view of the app, select **Scam Protection**.
3. Select the **Settings** icon  in the top-right corner of the screen.

This opens the settings view.

4. Switch off **Block ads**.

When you reload the page in your browser, it will include advertisements.

Protecting yourself against text message scams

When you receive a text message (SMS) from an unknown sender, there is a risk that the message is a scam that includes links to harmful websites, for example.

Criminals often use text messages to trick people into sending them sensitive personal information or going to a harmful website. These messages can appear to be sent by a legitimate sender, for example a bank or courier service.

SMS Protection uses artificial intelligence (AI) to compare text messages that you receive with known scam messages, and it also checks the message content for any harmful links. SMS Protection automatically moves any identified scam messages to the junk folder of your messaging app.

Note: SMS Protection does not collect any personal data from your messages.

To set up SMS Protection:

1. Open the CyberProtect app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Message Protection > Get started**.

You are asked to allow permission to access your SMS messages and contacts, and you may also be asked to allow notifications.

4. Allow the requested permissions.

Once the necessary permissions are allowed, the app notifies you of any incoming messages that are identified as harmful. To see details about the detected messages, open the app and go to **Scam Protection > Message Protection > Scam reports**.

Making sure your WiFi connection is safe

When you use WiFi to connect your device to the network, WiFi Protection checks whether it is safe or if you should avoid using it.

Criminals can use non-securely configured WiFi hotspots to hijack or eavesdrop on your network communications, for example through man-in-the-middle attacks. This type of attack means that your internet connection can appear to work normally, but in fact the attacker can intercept your transferred data and redirect you to fake websites that appear to be genuine.

To make sure your WiFi connections are safe:

1. Open the CyberProtect app.
2. On the main view of the app, select **Scam Protection**.
3. Select **WiFi Protection**.

This opens the **WiFi Protection** view. When WiFi Protection is switched on, this view shows you statistics on the number of safe and unsafe WiFi connections.

4. Switch on **WiFi Protection**.
5. Switch on **Turn on VPN automatically** if you want to use VPN whenever you connect to an unsafe or open WiFi network.

This protects your personal information in cases where the security of the WiFi network may be compromised.

6. Select the notifications that you want to see.

Note: For iOS, you have to enable Automatic WiFi Protection via VPN Settings.

VPN

Turning on the VPN connection

Privacy is not about secrets. It's about your ability to control what information you want to give out. You don't want to give out your personal information, social security number, address, credit card number, or names of the family members to strangers. Typically, you exchange parts of your privacy for some value, and only in situations where you feel confident in doing so. It's about trust. Unfortunately, many misuse your trust for their own benefit only – your private information has value.

The app's virtual private network (VPN) creates a secure, encrypted connection from your device to the internet.

You can turn the VPN connection on or off from the main view of the app.

To turn on VPN:

1. Open the CyberProtect app.
2. Under **VPN**, select the toggle switch to turn VPN on.

When you turn VPN on for the first time after installing the app, the **Setting up VPN** view opens.

3. To allow the device to set up a VPN connection, select **Allow** > **OK**.

VPN is turned on, connecting the app to the location offering the best possible connection.

4. To turn VPN off again, under **VPN**, tap the toggle switch.

What are the virtual locations for CyberProtect VPN?

When you connect to the internet, your device is assigned an address that identifies where you are. The app automatically uses a server that is closest to you for the best possible network connection and speed. However, the app also lets you select a virtual location which gives your device an address in the selected country. When you decide to use a virtual location instead of your physical location, all online activity from your device goes through the chosen country, letting you use the internet as if you were in that country.

Note: Some services may block VPN connections. If you have issues accessing a specific service, try turning off VPN.

CyberProtect VPN currently provides the following virtual locations to choose from:

- Australia
- Austria
- Belgium
- Canada (Montreal, Toronto and Vancouver)
- Czech Republic
- Denmark
- Finland
- France
- Germany
- Ireland
- Italy
- Japan
- Mexico
- Netherlands
- Norway
- Poland
- Portugal
- Singapore
- South Korea
- Spain
- Sweden
- Switzerland
- United Kingdom

- USA (East coast, Northwest, South, Southeast and West coast)

Location may be subject to change.

Changing your virtual location

By default, CyberProtect VPN uses the server that is closest to you for the best possible connection.

Companies use IP geolocation to block access to their content from certain countries. With CyberProtect VPN, you may be able to go around some of them by changing your virtual location in the following way:

1. Open CyberProtect and go to Privacy VPN.
2. Select the **Location** button.
3. Select the virtual location that you want.

Your device may still know its real location through GPS, and apps may have permission to use it.

Connecting to other devices in the same network

You can mark your current network as trusted to allow connections to other devices within the same network while VPN is on.

For Android, this feature works only when the Killswitch feature is switched on. If Killswitch is switched off, you can access your local network without changing any settings.

To allow connections within the same network:

1. Open the CyberProtect app.
2. On the main view, select **VPN**.



3. Select  in the top-right corner.
The **VPN settings** view opens.
4. Switch on **Connect to local devices** or select **Trusted networks** for iOS

Note: Never allow local connections on networks that don't require a password.

Allowing applications to bypass VPN (For Android only)

You can select applications that can connect to the internet directly.

Some applications might not work with a VPN connection, for example to enforce location-based restrictions. If an app does not work properly, you can allow it to bypass VPN and check if it works then. However, doing this means that most of the data traffic for the app is not protected against tracking or other misuse. For example, if you allow a web browser to bypass VPN, all your activity on that browser is unprotected.

Note: Even when you allow an app to bypass VPN, it might not work. For example, domain name system (DNS) requests always go through VPN, and this may prevent the app from working properly.

To select the applications that can bypass VPN:

1. Open the CyberProtect app.
2. On the main view, select **VPN**.

3. Select  in the top-right corner.

The **VPN settings** view opens.

4. Select **VPN bypass**.

The VPN bypass view opens, listing applications that can be allowed to bypass VPN.

5. Select the applications that you allow to connect to the internet directly.

The selected applications now bypass VPN.

Blocking internet access when VPN is disrupted or is being established (For Android only)

Killswitch cuts off the internet access and blocks connections to other devices within the same network if the VPN connection drops for some reason.

By default, the Killswitch feature is turned on when you set up the VPN connection.

To turn Killswitch off:

1. Open the CyberProtect app.
2. On the main view, select **VPN**.

3. Select  in the top-right corner.

The **VPN settings** view opens.

4. Select the **Killswitch** switch to turn the feature off.

Changing the VPN protocol used

A VPN protocol is a set of rules that your device and the VPN server use to set up the connection.

The app supports the following VPN protocols:

- Hydra
- Wireguard
- OpenVPN (Android only)
- IKEv2 (iOS only)

By default, the app uses the Hydra protocol.

To change the VPN protocol:

1. Open the CyberProtect app.
2. On the main view, select **VPN**.

3. Select  in the top-right corner.

The **VPN settings** view opens.

4. Under **Protocol**, select the protocol you want to use.
5. Under **VPN protocol**, select the protocol you want to use.

Technical support

Here you can find information that can help you solve your technical issues.

Sending logs to support

This topic explains how to send log files to support if requested. At times, to be able to solve an issue, our technical support may need more detailed information about your device.

To create and send log files to support:

1. Open the CyberProtect app.
2. Select the profile icon  in the top-right corner of the screen.
3. Under **About**, select **App information**.
The **App information** view opens, showing various information about the product.
4. Select **Send log** and save the files to your device.
5. Reply to the email that you received from our technical support and add the saved log files to your reply as attachments.
6. Describe any other details about the issue and send the email to our support.

Wait until our support contacts you.

Contact us

Have a question? [Connect with us!](#)

StarHub CyberProtect Features Per Platform

StarHub CyberProtect features across operating systems supported Q1 2026.

	 Android	 iOS	 Windows	 Mac
Virus Protection	●	—*	●	●
Browsing and Phishing Protection	●	●	●	●
Banking Protection	●	●	●	●
Shopping Protection	●	●	●	●
Ad Blocker	—	●	●	●
Cookie Popup Blocker	—	●	●	●
Family Rules Content Filtering	●	●	●	●
Privacy Advisor	●	—	—	—
Device Lock Check	●	●	—	—
Outdated OS Check	—	●	—	—

* Not possible due to platform or Apple's restrictions