



StarHub CyberProtect QuickStart Guide for Computer

(Windows / macOS)

MARCH 2026

Table of contents

About	4
StarHub CyberProtect account	4
StarHub CyberProtect Portal	4
CyberProtect application	5
System requirements for Microsoft Windows	6
System requirements for Apple macOS	6
Welcome to StarHub CyberProtect	7
Install CyberProtect Now	7
Forget password	8
Getting started with CyberProtect	9
Adding new device on StarHub CyberProtect portal	9
Sharing protection with a family or friend	12
Restricting online content for your children	15
Setting up content filtering for a child	16
Content categories	17
Device Protection	18
Protecting your device against Virus & Threats	18
Protecting your computer with real-time scanning	18
Run virus scanning manually	19
Exclude files or folders from scanning	23
View and restore quarantined items	24
Using gaming mode (for Windows only)	26
Protection status icons	27
Scam Protection	28
Protecting your web browsing	28
Protecting online banking and shopping	28
Changing Banking Protection settings	29
Shopping Safely Online	30
Browsing safely with Safety ratings	31
Enabling browser extension for Safari (For Mac only)	32
Returning from or entering a blocked website	33
Blocking advertisements on websites	34
Rejecting non-essential cookies	34
VPN	35
What are the virtual locations for CyberProtect VPN?	36
Changing your virtual location?	37
Connecting to other devices in the same network	37

Allowing applications to bypass VPN (For Windows only).....	37
Blocking internet access when VPN is disrupted or is being established	38
Changing the VPN protocol used.....	38
Technical Support.....	40
Contact us	40
Using the support tool	40
CyberProtect features per platform.....	41

About

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

- We explain about the CyberProtect app.
- We introduce StarHub CyberProtect, the user credential, the management portal for CyberProtect apps, and what you can do within the portal.
- We also explain the on-boarding journey for StarHub customer, which is the steps to taking 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 with the StarHub CyberProtect Portal. StarHub CyberProtect Portal allows you to conveniently manage the security of your devices.

CyberProtect is powered by F-Secure, a customized build of F-Secure TOTAL made exclusively for StarHub customer. 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

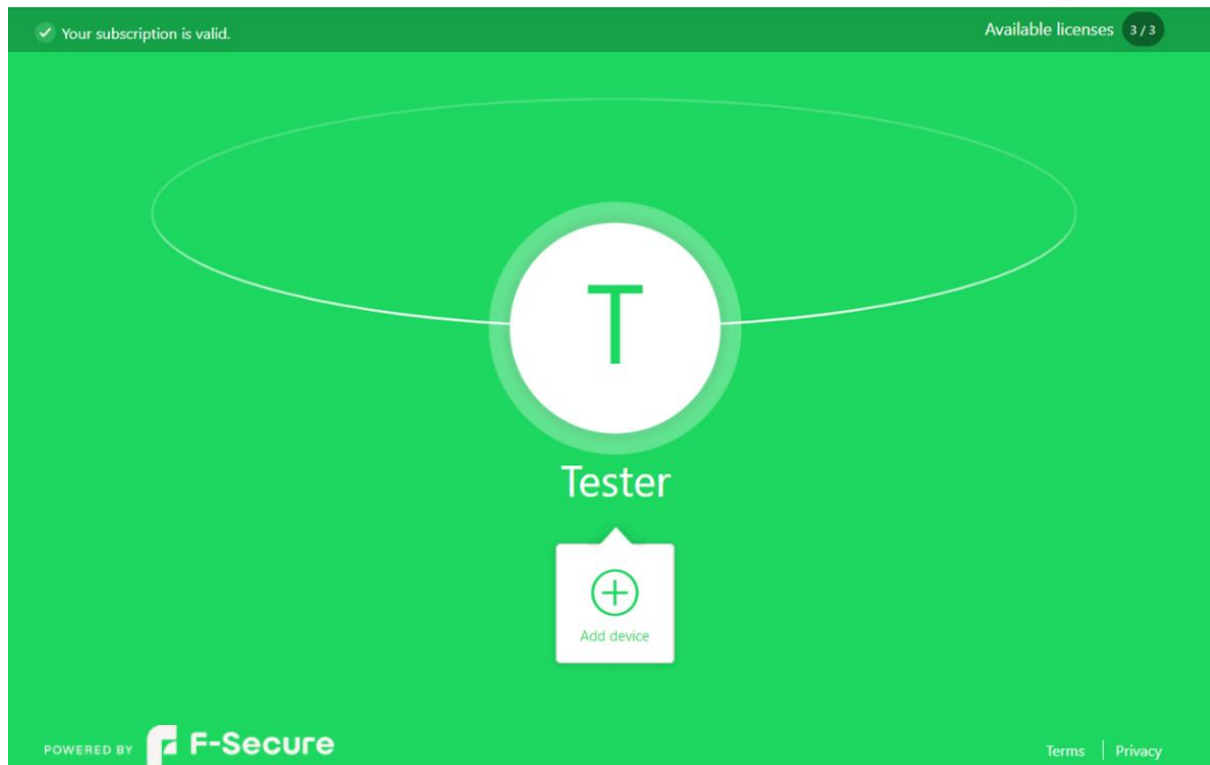
StarHub CyberProtect Portal is the home of your protection. It is an easy-to-use online management portal that you can use to send CyberProtect installation links to target devices, to release licenses from the devices that do no longer need protection in your StarHub CyberProtect Portal group, and to 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 applications on all your devices to protect your security 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 only safe web sites can be accessed.
- Banking Protection, which protects your online banking activities by securing the connection when you access an online banking portal.
- 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 for Microsoft Windows

Operating Systems supported:

- Windows 11.
- Windows 10 version 21H2 (build 19044) or newer
- Windows 11 on ARM64 version 24H2 (build 26100) or later

Recommended system requirements:

- Minimum: 2GB RAM, dual-core CPU, 3GB of free disk space
- Recommended: 4GB RAM, quad-core CPU, 5GB of free disk space

Supported Browsers:

- Google Chrome.
- Mozilla Firefox.
- Microsoft Edge.

System requirements for Apple macOS

Operating systems supported:

- macOS version 26 "Tahoe"
- macOS version 15 "Sequoia"
- macOS version 14 "Sonoma"
- macOS version 13 "Ventura"
- macOS version 12 "Monterey"

Recommended system requirements:

- Intel / Apple Silicon processor
- 1GB of free disk space
- 8 GB or more of memory is recommended
- Internet Connection: An Internet connection is required to validate your subscription and receive updates

Supported Browsers:

- Google Chrome.
- Mozilla Firefox.
- Microsoft Edge.
- Safari.

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

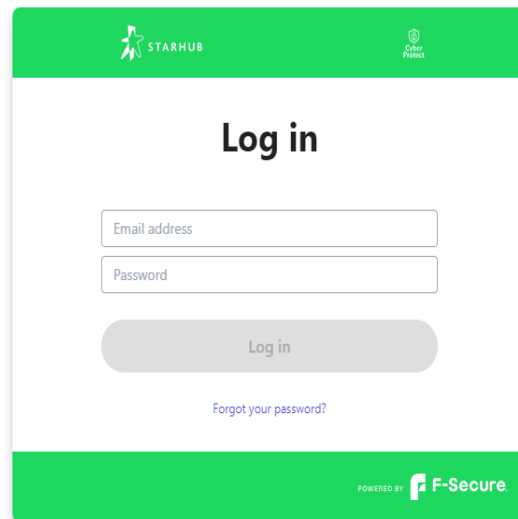
Install CyberProtect Now

It is a login-less installation link, application installed do not requires user login credential to activate, except iOS.

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

First time login

1. Login management portal with temporary password provided username is always your e-mail address.
2. Portal will prompt to set your own password on first login.



STARHUB Cyber Protect

Log in

Email address

Password

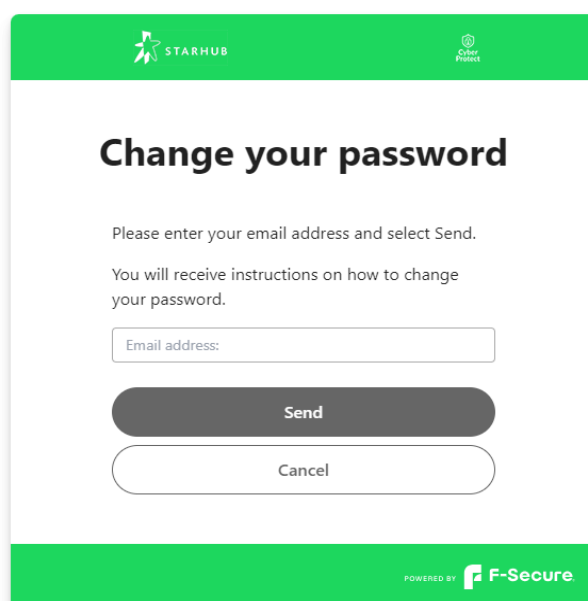
Log in

[Forgot your password?](#)

POWERED BY F-Secure

Forget password

1. Click **Forget password** on Login page.
2. Enter your e-mail address registered to reset password.
3. Follow instructions to reset your password in e-mail received.



STARHUB Cyber Protect

Change your password

Please enter your email address and select Send.
You will receive instructions on how to change your password.

Email address:

Send

Cancel

POWERED BY F-Secure

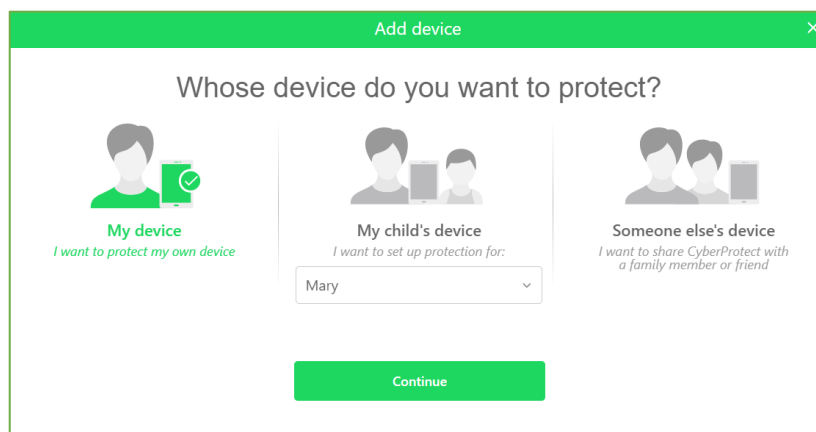
Getting started with CyberProtect

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.

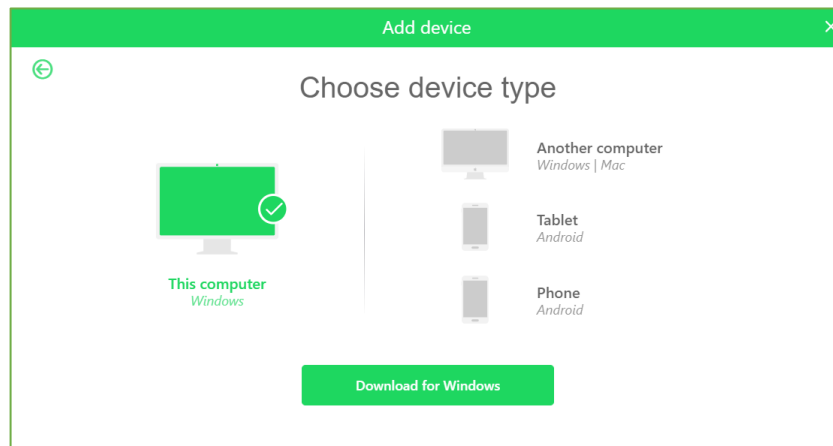
You can download and install CyberProtect through StarHub CyberProtect Portal. You can also use StarHub CyberProtect Portal to send the installation link to a device by email or text message, making it easy for you to deliver CyberProtect to a device that you want to protect.

Adding new device on StarHub CyberProtect portal

1. Log in to **StarHub CyberProtect Portal** with your account (username and password), or Open the **CyberProtect app** and select the **People** tab, **People & Devices** view opens.
2. Select **+ Add device**.
3. Choose whose device you want to protect, then select **My device > Continue**.



4. Select how you want to deliver the installation link to the device you want to protect and then select **Send Link**.
 - Select **This computer** to install CyberProtect on your current computer.



- 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.
5. Open the message with your device and select **Install now**.
 6. Select **Download for Windows PC / Download for Mac** to download the product installer.
 7. Launch the downloaded installation package.

The setup page opens. You need administrative rights to start the installation.

8. Once the product setup window is displayed, select **Accept and continue** after you read and agree to the End User License Terms.
9. Follow the instructions shown onscreen to complete the installation.
10. When the installation is completed, log in to your account, if prompted, and select **Continue** to finalize the protection for the device.
11. CyberProtect notifies you if your browser extension is not yet in use.

To add the browser extension, select **Set up** on the notification shown on the product main page and follow the instructions shown onscreen.

Note: *If you don't see the browser extension notification, the extension is already in use.*
12. You may need to restart your computer to validate your subscription and download the latest updates.
13. After the installation is complete, choose **Open** to start the application and to activate the product.

The product does not protect your device before you activate it.

Note: *If you are installing the product on your child's device, you are prompted to set up Family Rules.*

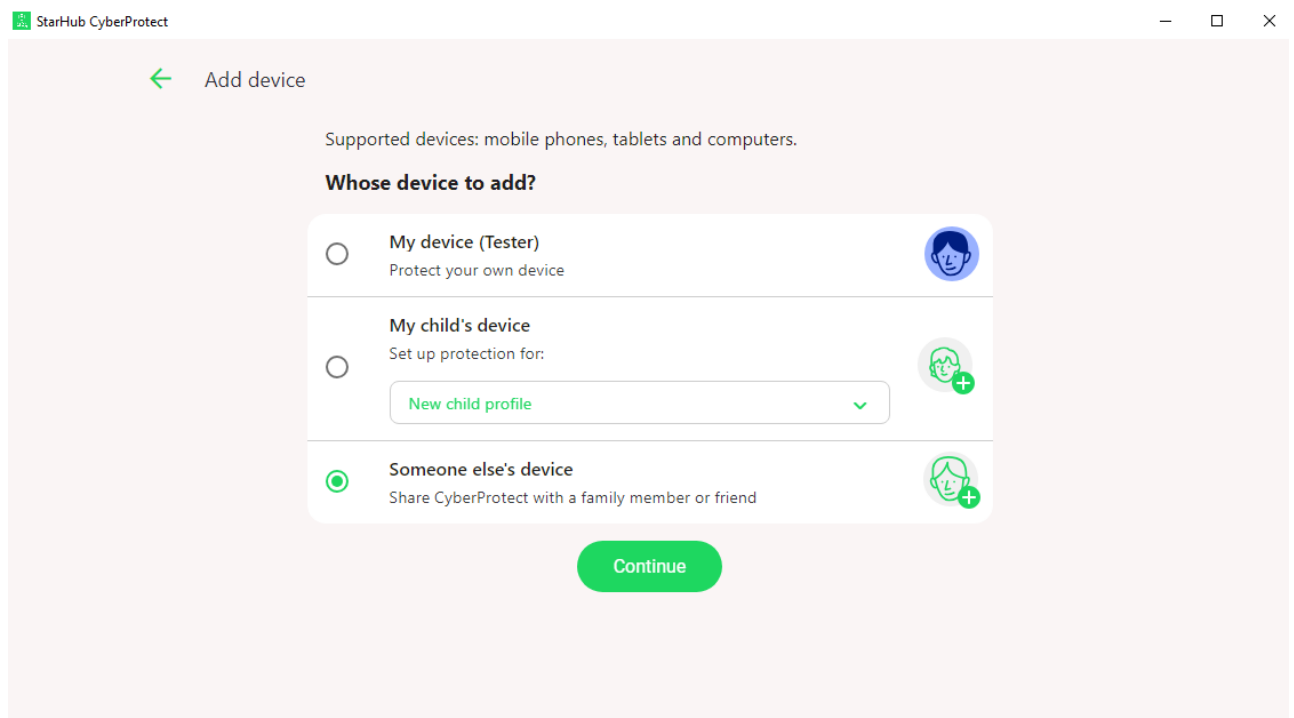
You have now set up protection for your own device. To view and manage the protection of the above device, go to the product's People & Devices view, or log in to your account to access the online management portal.

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.

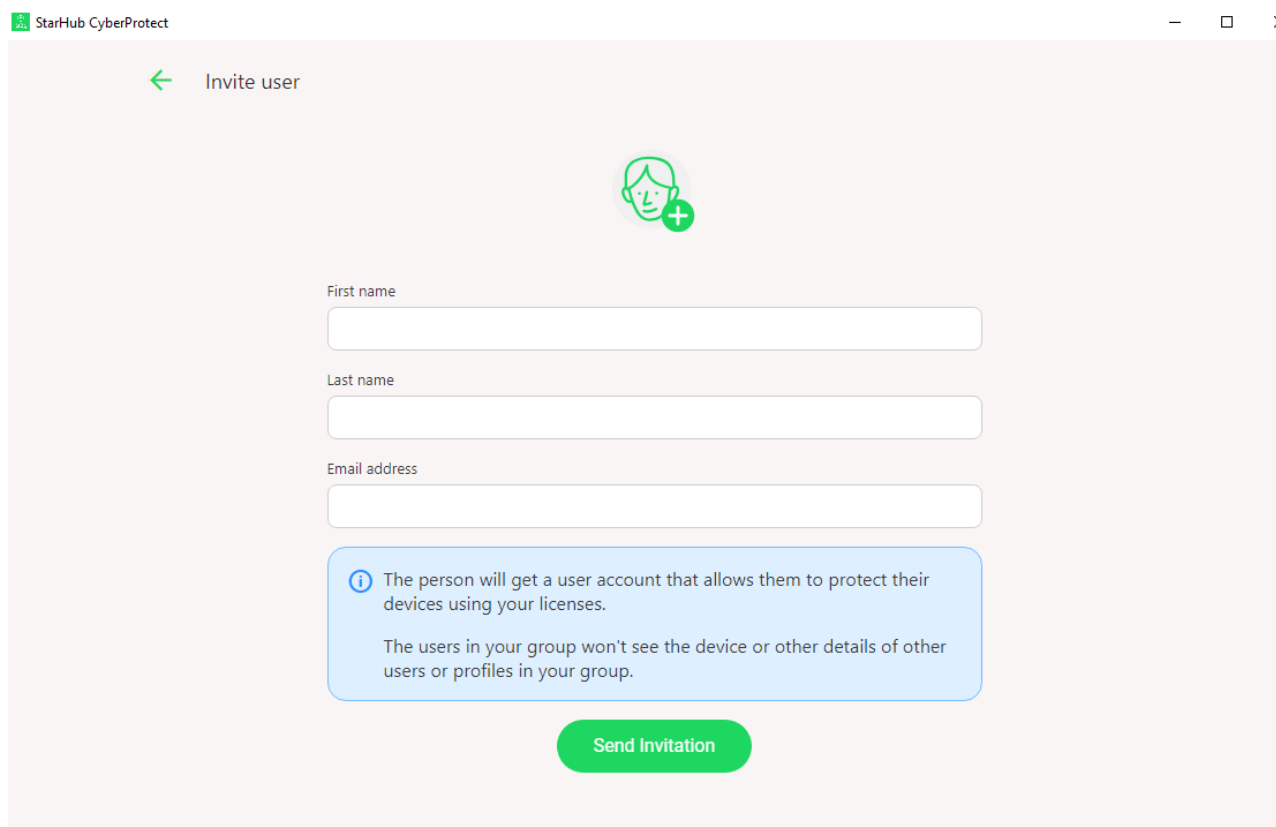
To share protection with someone else:

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.



The image shows a screenshot of the StarHub CyberProtect application window. The window has a title bar with the text "StarHub CyberProtect" and standard window controls (minimize, maximize, close). Inside the window, there is a header area with a green back arrow and the text "Invite user". Below this, there is a green circular icon with a white plus sign and a stylized face. The main content area contains three input fields: "First name", "Last name", and "Email address". Below these fields is a blue information box with a white 'i' icon and the following text: "The person will get a user account that allows them to protect their devices using your licenses. The users in your group won't see the device or other details of other users or profiles in your group." At the bottom of the form is a green button labeled "Send Invitation".

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 CyberProtect 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.

Restricting 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.

Note: Editing the Family Protection settings requires administrator privileges. You can edit the settings separately for each user account on the computer.

Setting up content filtering for a child

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

To set up protection for your child:

1. Open the CyberProtect app.
2. On the main view, select **Family Protection**.
This opens the **Family Protection** settings.
3. Select **Edit settings**.
4. Select the user account that you want to edit.
5. Switch on **Content filtering**.
6. 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.

You can also allow specific websites, even if content filtering would block them based on their content type:

- i. Select **View website exceptions**.
This opens a new view that lists the websites you want to allow.
- ii. Select **Add new**.
- iii. Enter the address of the website that you want to allow.
- iv. Select **OK**.

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

Note: Browsing Protection uses browser extensions to protect your web browsing, online banking and shopping, and to show you security information while you browse the internet. Therefore, make sure that the browser extensions are in use.

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 Virus & Threats

The app scans your device for viruses, harmful content, and other threats to your device or your data. To prevent malware infections like viruses, trojans, spyware, and ransomware, all files and applications are automatically scanned. In addition to the clearly bad files or applications, CyberProtect scans for potentially unwanted applications which may behave in an undesirable way on your device like aggressive marketing tools.

Files are scanned in real-time, on-demand (manual scanning) or triggered upon certain events like installation of an application. Once a malware or a potentially unwanted application is discovered, you will be immediately instructed to remove it. The scanning logic depends on the underlying operating system.

Protecting your computer with real-time scanning

Real-time scanning protects the computer by scanning all files when they are accessed and by blocking access to those files that contain malware.

When your computer tries to access a file, Real-time scanning scans the file for malware before it allows your computer to access the file. If Real-time scanning finds any harmful content, it puts the file to quarantine before it can cause any harm. Files on removable drives such as CDs, DVDs, and portable USB drives take a longer time to scan.

Note: *Compressed files, such as .zip files, are not scanned by real-time scanning.*

Real-time scanning may slow down your computer if:

- you have a computer that does not meet the system requirements, or

- you access a lot of files at the same time. For example, when you open a directory that contains many files that need to be scanned.

We recommend that you keep Virus protection turned on all the time. You can also scan files manually and set up scheduled scans if you want to make sure that there are no harmful files on your computer or to scan files that you have excluded from the real-time scan.

To make sure that real-time scanning is on:

1. Open CyberProtect, on the main view of the product, select **Device Protection**.
2. On the **Device Protection** view, select **Settings**.
3. Select **Edit settings**. Turn on **Virus Protection**.

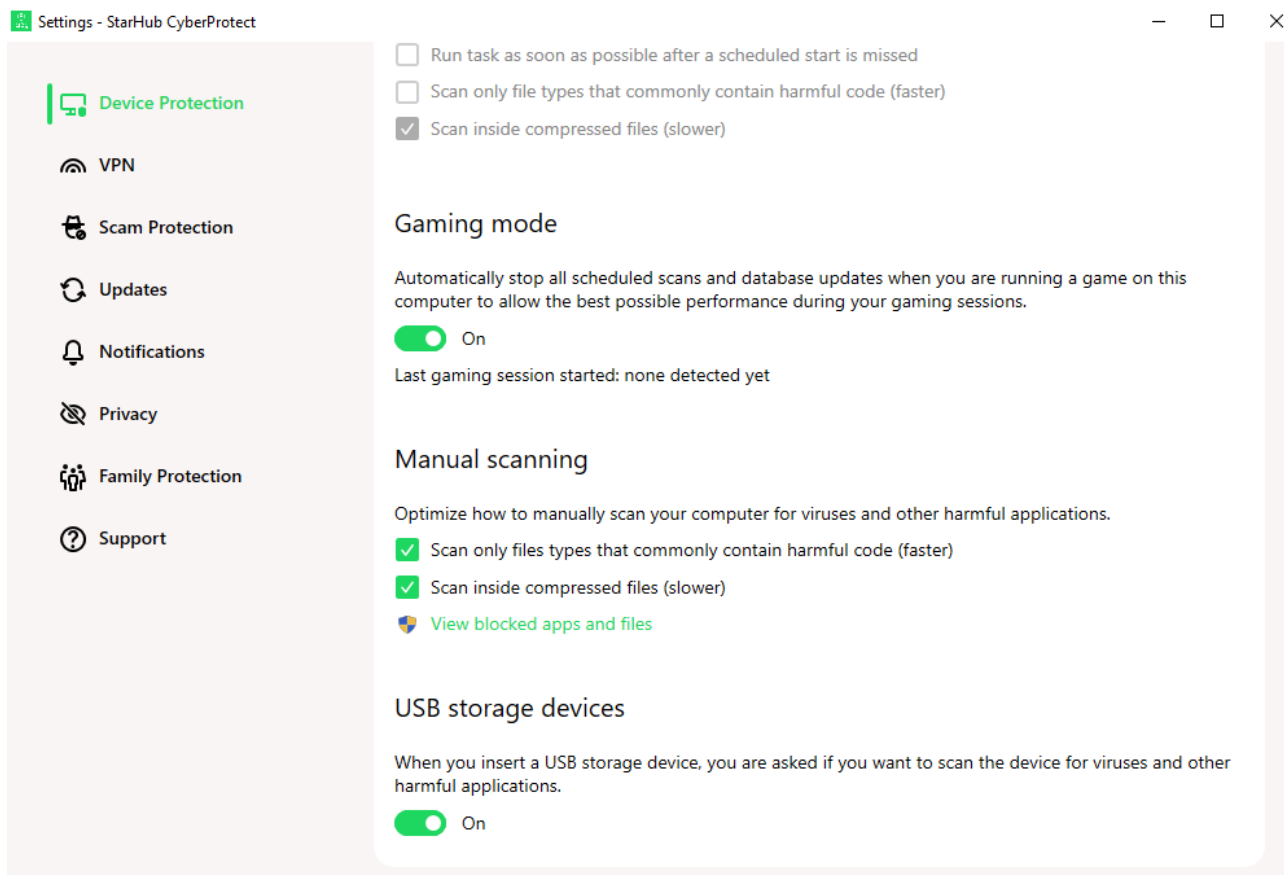
Run virus scanning manually

You can scan your entire computer to be completely sure that it has no harmful files or unwanted applications. The full computer scan scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan can take a long time to complete.

You can also scan only the parts of your system that contain installed applications to find and remove unwanted applications and harmful items on your computer more efficiently.

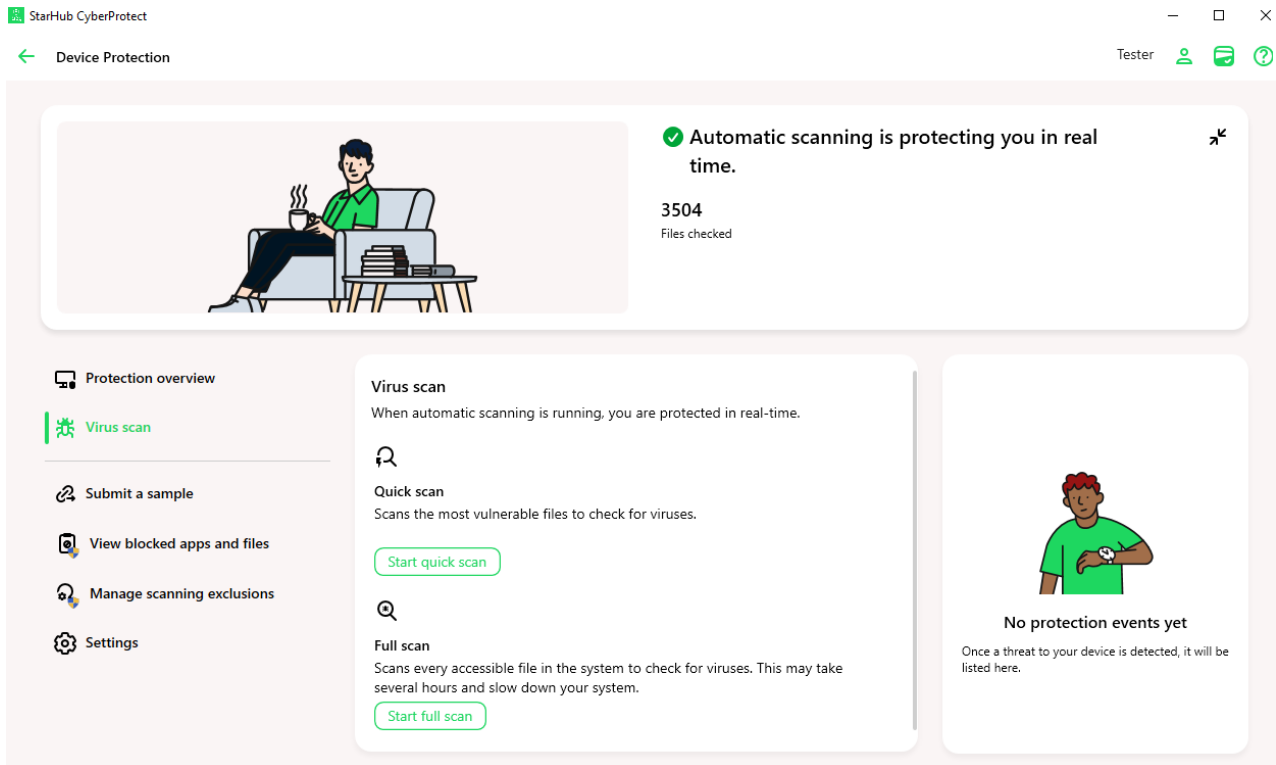
To scan your computer, follow these instructions:

1. If you want to optimize how the manual scanning scans your computer, select **Device Protection > Settings**.
 - a. In **Settings**, select **Manual scanning**.
 - b. Select **Scan only file types that commonly contain harmful code (faster)** if you do not want to scan all files.
 - i. The files with the following extensions are examples of file types that are scanned when you select this option: **com, doc, dot, exe, html, ini, jar, pdf, scr, wma, xml, zip**.
 - c. Select **Scan inside compressed files** to scan files that are inside compressed archive files, for example zip files. Scanning inside compressed files makes the scanning slower. Leave the option unchecked to scan the archive file but not the files that are inside it.
 - d. Select **OK** to close the **Settings** window.



2. Open CyberProtect, on the main view of the product, select **Device Protection**.
3. On the **Virus scan** view, select either **Quick scan** or **Full scan**.
 1. **Quick scan** scans only the parts of your system that contain installed applications and then locations where viruses are commonly found, including your document folders. It can find and remove unwanted applications and harmful items on your computer in a shorter time.

2. **Full computer scan** scans all internal and external hard drives for viruses, spyware, and potentially unwanted applications. It also checks for items that are possibly hidden by a rootkit. The full computer scan can take a long time to complete.



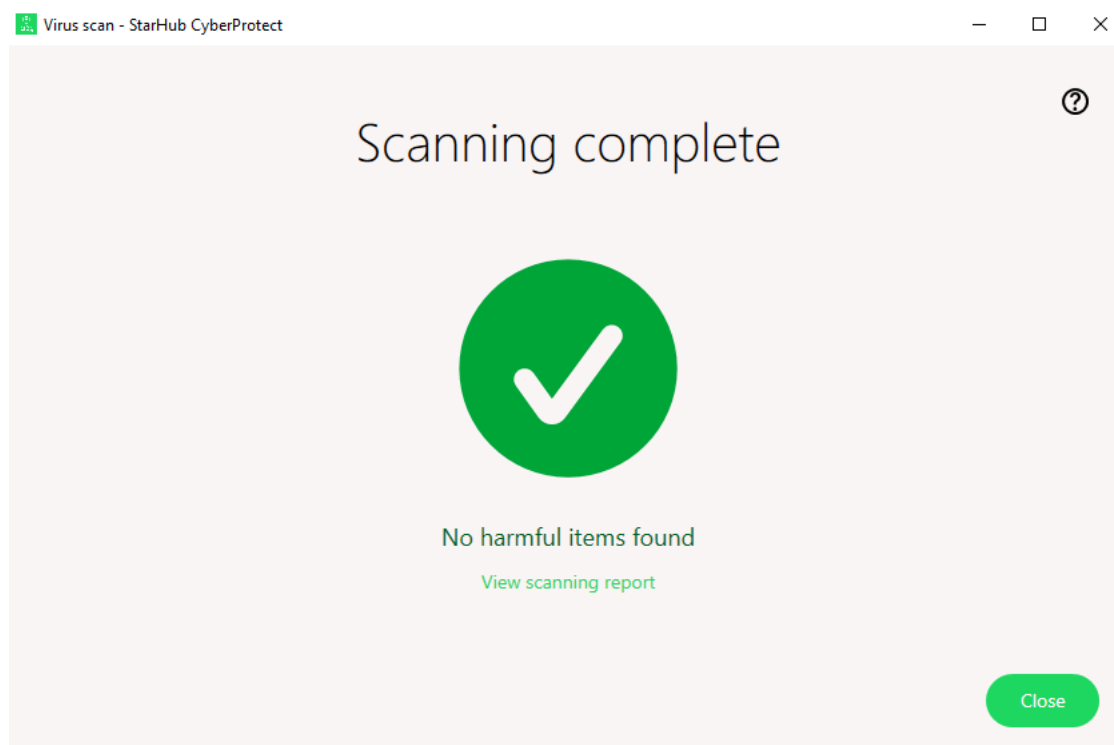
4. If the scan finds any harmful items, it shows you the list of harmful items that it detected.
- Click the detected item to choose how you want to handle the harmful content.
 - Select **Remove**, then **Yes** to start the cleaning process.

Option	Description
Clean up	Clean the files automatically. Files that cannot be cleaned are quarantined.
Quarantine	Store the files in a safe place where they cannot spread or harm your computer.
Delete	Permanently remove the files from your computer.
Skip	Do nothing for now and leave the files on your computer.
Exclude	Allow the application to run and exclude it from future scans.

Note: Some options are not available for all harmful item types.

5. The scan shows the results and the number of harmful items that were cleaned.

Note: The scan may require that you restart your computer to complete the cleaning process. If the cleaning requires a computer restart, select Restart to finish cleaning harmful items and restart your computer.



Exclude files or folders from scanning

When you exclude files or folders from scanning, they are not scanned for harmful content. To leave out files or folders from scanning:

1. Open CyberProtect, on the main view of the product, select **Device Protection**.
2. On the **Manage scanning exclusions** view, select **App and file control**.

Note: You need administrative rights to change these settings.

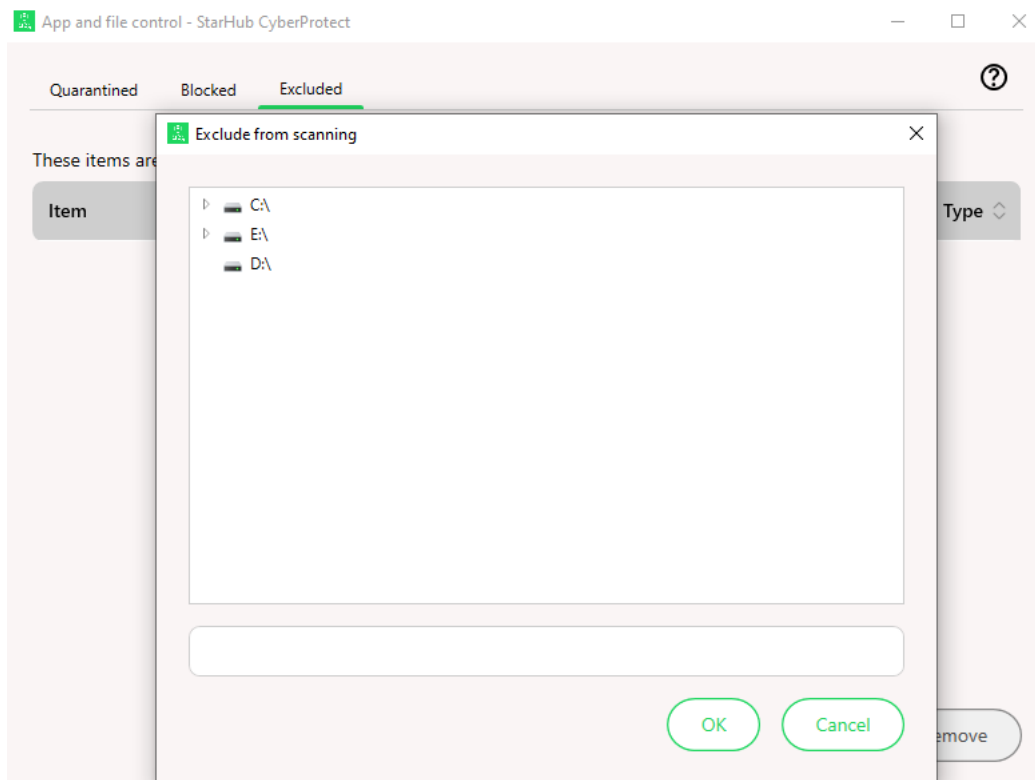
3. Select the **Excluded** tab.

This view shows you a list of excluded files and folders.

4. Select **Add new**.

5. Select the file or folder that you do not want to include in scans. Select **OK**.

The selected files or folders are left out from the future scans.



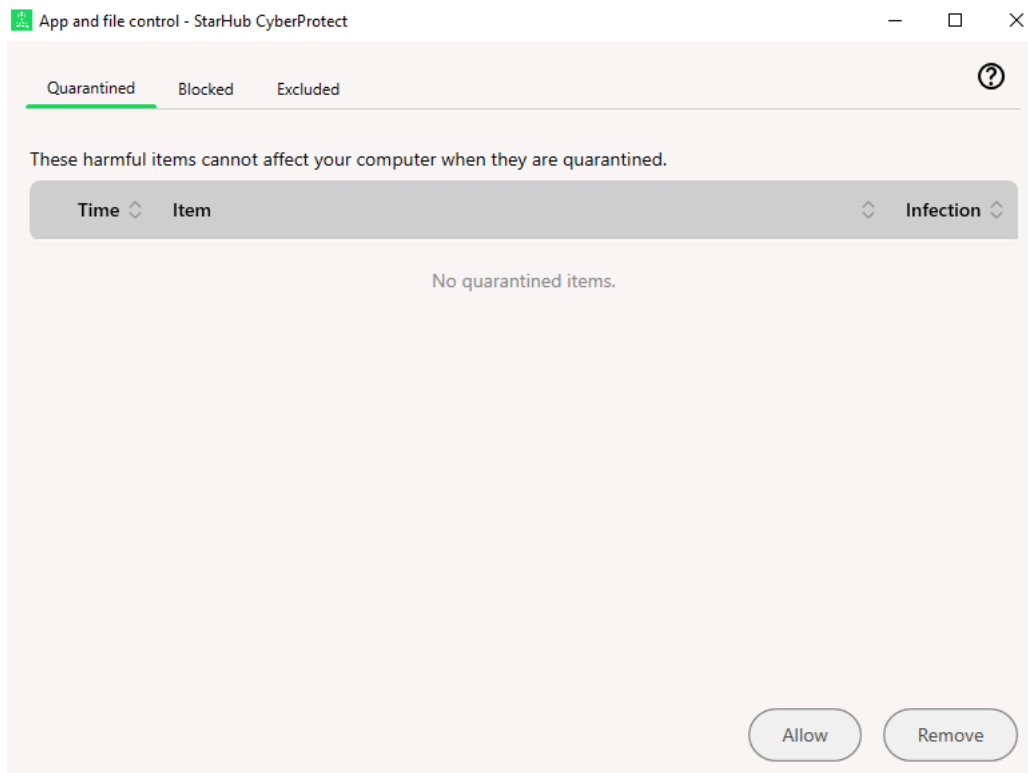
View and restore quarantined items

You can view more information on items placed in quarantine.

Quarantine is a safe repository for files that may be harmful. The product can place both harmful items and potentially unwanted applications in quarantine to make them harmless. You can restore applications or files from quarantine later if you need them. If you do not need a quarantined item, you can delete it. Deleting an item in quarantine removes it permanently from your computer.

To view information on items placed in quarantine:

1. Open CyberProtect, on the main view of the product, select **Device Protection**.
2. On the **Manage scanning exclusions** view, select **App and file control**.
Note: You need administrative rights to change these settings.
3. Select the **Quarantined** tab.
This list shows you the name, date of detection, and infection type for each quarantined item.
4. Double-click a quarantined item to see more information.
For single items, this shows you the original location of the quarantined item.



You can restore the quarantined items that you need.

You can restore applications or files from quarantine if you need them. Do not restore any items from quarantine unless you are sure that items pose no threat. Restored items move back to the original location on your computer.

To restore quarantined items:

1. Open CyberProtect, on the main view of the product, select **Device Protection**.
2. On the **Manage scanning exclusions** view, select **App and file control**.
Note: You need administrative rights to change these settings.
3. Select the **Quarantined** tab.
4. Select the quarantined item that you want to restore.
5. Click **Allow**.
6. Click **Yes** to confirm that you want to restore the quarantined item.

The selected item is automatically restored to its original location. Depending on the type of infection, the item may be excluded from future scans.

Note: To view all the currently excluded files and applications, select the **Excluded** tab in the **App and file control** view.

Using gaming mode (for Windows only)

The automatic gaming mode requires that you have Windows 10 version 1809 ("October 2018 Update") or later running on your computer.

The gaming mode is enabled in the product by default. As soon as the product detects that you are running a game on your computer, it automatically stops all scheduled scans and suspends product and database updates. This reduces the product's impact on your computer and network use. It frees up more system resources for computer games while still maintaining the essential functionality of the product. The gaming mode turns off automatically when you stop playing the game.

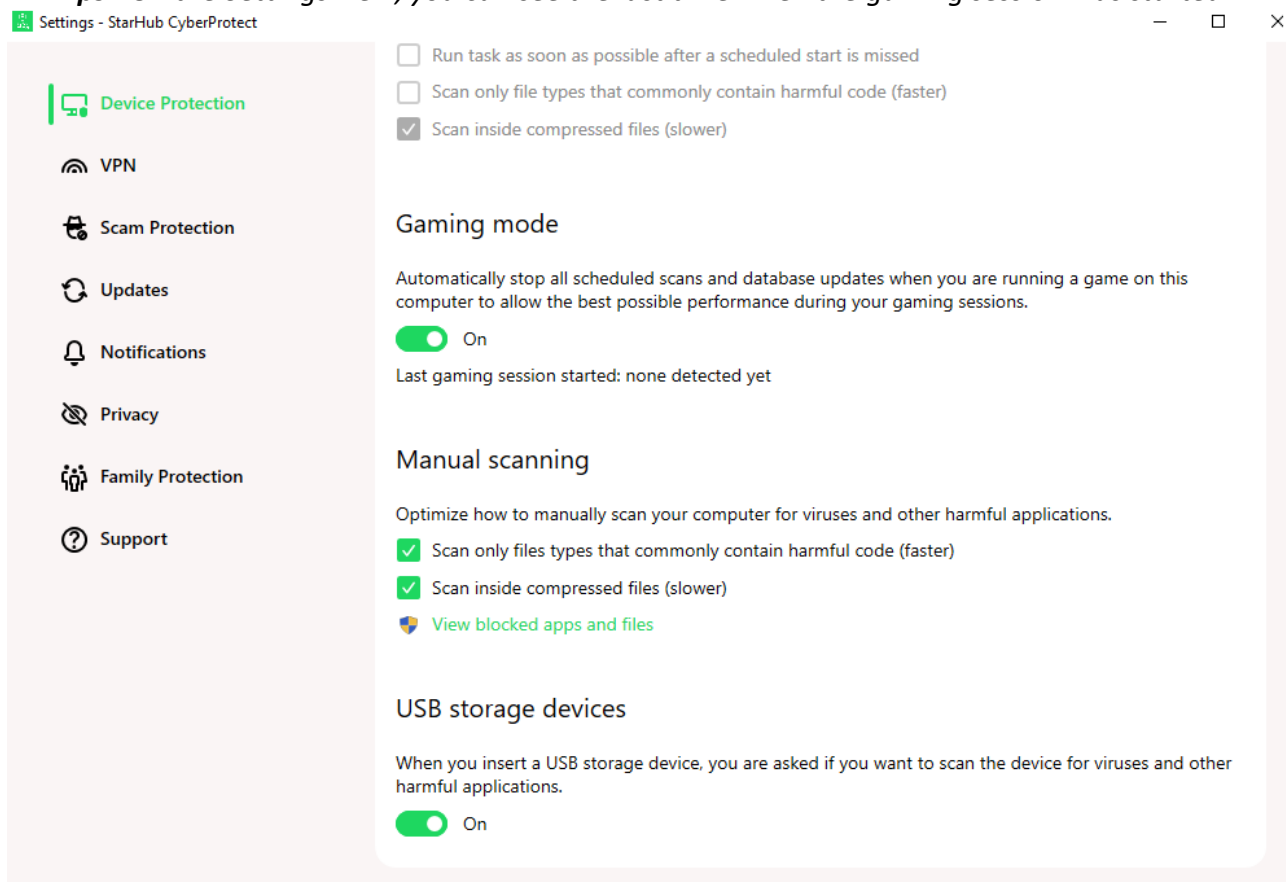
If you don't want the gaming mode to turn on automatically, turn it off in the following way:

1. Open CyberProtect on the main view of the product, select the  menu button.
2. Select **Settings > Scanning settings**.
3. Select **Edit settings**.

Note: You need administrative rights to change some of the settings.

4. Turn off gaming mode. Now the gaming mode will not turn on automatically.

Tips: On the Settings view, you can see the last time when the gaming session was started.



Sometimes, however, Windows may fail to recognize a game, and the gaming mode will not activate. If this occurs, you can manually add detection for that game in the Xbox Game Bar in the following way:

1. Launch the game.
2. Press **Windows key + G**.
The **Game Bar** opens.
3. From the Game Bar, select **Settings > General** and select then the **Remember this is a game** checkbox. If you don't see the setting, Game Bar already recognizes the game.

From now on, the product will always activate the gaming mode as soon as you launch the game. You can use this setting with games bought from any games store.

Protection status icons

The protection status icon shows you the overall status of the product and its features.

Status Icon	Status Name	Description
	OK	Your device is protected. Features are turned on and working properly.
	Warning	Your device is not fully protected. The product requires your attention, for example, it has not received updates in a long time, or a security feature is turned off.
	Danger	Your device is not protected. The product requires immediate action, for example a critical feature is turned off or your subscription has expired.

Examples of status messages that you may see:

- **Google Chrome browser extension is not in use**
- **Mozilla Firefox browser extension is not in use**
- **Microsoft Edge browser extension is not in use**
- **Your subscription has expired**

Scam Protection

Protecting your web browsing

Safe browsing helps you use the Internet safely by preventing unintentional access to harmful web sites and adding extra security to your web browser during online banking sessions.

Browsing protection in CyberProtect makes sure that while you browse the web, the sites you go to are safe. Browsing protection does this by blocking web sites that contain suspicious and harmful content or steal your personal information, including credit card numbers, user account information, and passwords.

Protecting online banking and shopping

When Banking Protection is turned on, it automatically detects when you access online banking websites or other sites that contain sensitive information.

Banking protection adds another layer of security to prevent attackers from interfering with your confidential transactions and protects you against harmful activity when you access your online bank or make transactions online. Banking protection automatically detects secure connections to online banking websites and blocks any connections that do not go to the intended site.

Banking protection currently supports the following web browsers:

- Safari (macOS)
- Firefox
- Google Chrome
- Microsoft Edge (Chromium)

Using Banking Protection

When you access your bank's website or make online payments, Banking Protection activates and blocks all connections that are not necessary for online banking so that they cannot interfere with your confidential transactions. A **Banking Protection** frame appears around your computer screen with a green tick at the top. This indicates that **Banking Protection** is now active. While active, Banking Protection only allows connections that it considers safe, all other connections are blocked.

Once you close the browser or finish the banking session, you do not have to do anything. **Banking Protection** automatically detects that the banking session is over and closes the **Banking Protection** frame.

By default, Banking protection is enabled. If it is not enabled, turn on Banking protection in the following way.

- On macOS computer:
 1. Open the CyberProtect app.
 2. On the main view of the app, Select Scam Protection.
 3. Select settings.
 4. Select the lock icon in the bottom-left corner.
Note: You need administrative rights to change these settings.
 5. Select **Turn on Banking protection**.
- On Windows computer:
 1. Open the CyberProtect app.
 2. On the main view of the app, select Scam Protection.
 3. Select Settings > Edit settings.
 4. Turn on **Banking Protection**.

Note: Banking protection requires that browser extensions are in use.

Changing Banking Protection settings

You may want to change the product settings for Banking Protection when it is active, for example:

- If you do not want to interrupt your other active connections when Banking Protection is active, or
- If you do not want Banking Protection to clear the clipboard when the Banking Protection session ends.

While Banking Protection is on, access the settings as follows:

1. Select the green tick at the top of your screen, then select .
2. This opens the **Settings** menu for **Scam Protection**.
3. Modify the settings for **Banking Protection** to suit your need.

Note: If Banking Protection does not activate and you do not see the frame appear, check that the Browsing Protection extension is turned on in the web browser that you use.

Shopping Safely Online

Shopping Protection makes your online shopping sessions more secure by notifying you of fake and untrustworthy websites.

Note: Shopping Protection requires that the Browsing Protection extension is enabled in the web browser that you use.

By default, Shopping Protection is switched on to improve the safety of your online shopping. Upon entering a shopping website, a safety rating pop-up is displayed in the lower-right corner of the page to indicate how trustworthy the website is. If the shopping site is safe, the pop-up disappears after a few seconds and will not be shown again on the site during the shopping session. However, if the site is not safe, the pop-up warning will stay on the page until you leave the site.

You can adjust when the notifications are shown in the product settings, for example if you do not want to see notifications for safe shopping websites.

The safety rating pop-up is displayed also when you enter a shopping site by clicking a link, for example in an email or text message.

The safety ratings are also represented as informative icons on search results pages when you use popular search engines like Google, Bing, Yahoo, or DuckDuckGo. When you hover the mouse over the rating icon, you will see details about the safety of the website.

This information is also accessible via the browser extension icon in the browser toolbar. If you think that the website is incorrectly rated, you can suggest a new rating for the website.

To change the settings for Shopping Protection:

1. Open the CyberProtect app.
2. On the main view of the app, select Scam Protection.
3. Select Settings.
4. Select Edit settings.
5. Switch Shopping Protection on or off.
6. Select or clear Show notifications for safe shopping websites and Show notifications for suspicious shopping websites according to what notifications you want to see.

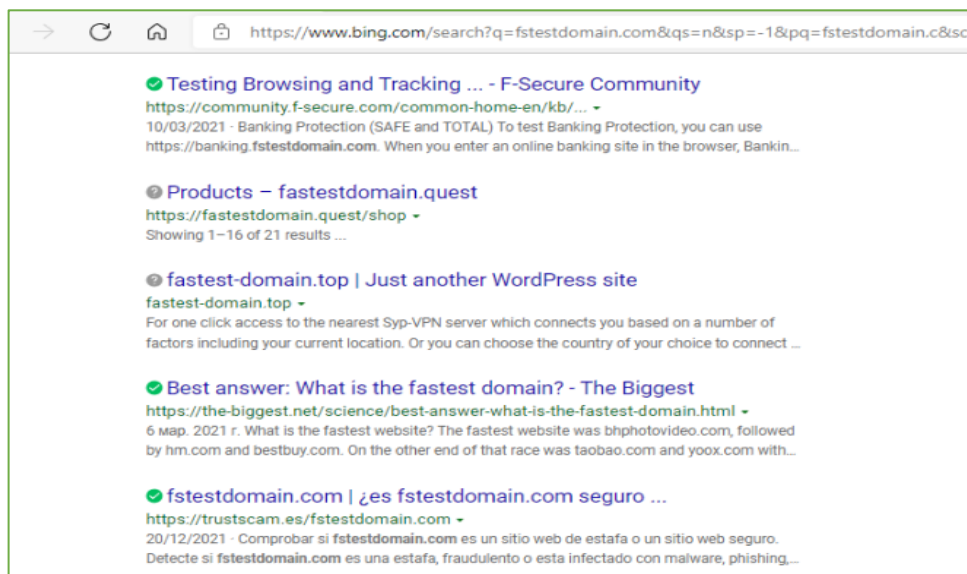
Browsing safely with Safety ratings

Browsing protection shows safety ratings for websites on search engine results. Color-coded icons show the safety rating of the current site. The safety rating of each link on search results is also shown with the same icons:

	The site is safe to the best of our knowledge. We did not find anything suspicious in the web site.
	The site is suspicious, and we recommend that you are careful when you visit this web site. Avoid downloading any files or providing any personal information.
	We have not analyzed the web site yet or no information is currently available for it.
	The access to this web site is never blocked.
	The site is harmful. We recommend that you avoid visiting this website. Alternatively, an administrator has blocked this site and you cannot visit it.

Safety ratings are available on the following search sites:

- Google
- Bing
- Yahoo
- DuckDuckGo



Enabling browser extension for Safari (For Mac only)

You must enable the browser extension for Safari to be able to use the browser safely. The product installs the browser extension automatically, and the only thing you need to do is to make sure that the extension is turned on.

To ensure that the browser extension for Safari is turned on:

1. Select the product icon in the menu bar.
2. Select **Scam Protection** from the menu.
3. Select Settings.
4. Select **Set up Safari Extension**.
5. Select Get > Install to install the extension from App Store.
6. In the **Extensions** dialog, make sure that **Secure Browsing** is selected.

You can now use Safari to browse the internet safely.

Checking that browser extensions are in use

Browsing protection **requires** browser extensions to be able to protect your web browsing, online banking, and shopping, and to show you security information while you are browsing the internet. Therefore, make sure that the browser extensions are in use.

When you open your browser, it displays a notification about the newly installed extension, and you may need to enable it. If you miss the notification, the main view of the product shows you if the browser extension has not yet been set up. The easiest way to set up the extension for your browser is to select Set up from the notification shown on the product's main view and follow the on-screen instructions.

- If you use **Firefox**, select first **Install Firefox extension** under **Browser extensions** and then select **Add**. The extension will be added and enabled for Firefox.
- If you use **Chrome**, select first the **Open Chrome Web Store** link under **Browser extensions**. The Browsing Protection by F-Secure page opens in Chrome Web Store. If the extension has already been installed on Chrome but disabled, select the **Enable this item** link from the banner on top of the page. If the extension has not yet been installed, select **Add to Chrome > Add extension**. The extension will be added and enabled for Chrome.
- If you use **Microsoft Edge**, select first the **Open Edge Add-ons** link under **Browser extensions**. The Browsing Protection by F-Secure page opens in Edge Add-ons. If the extension has already been installed on Microsoft Edge but disabled, select **Turn on** to enable it. If the extension has not yet been installed, then select **Get > Add extension**. The extension will be added and enabled for Microsoft Edge.



Returning from or entering a blocked website

If you accidentally access a harmful website, the webpage blocked automatically and shows Browsing Protection block page.

There are two things that you can do after this:

1. If you want to enter the website, select **Allow website on this computer > Allow**.
Enter your administrator password and select **OK**.
The blocked website opens. Also, the product adds the website to the allowed websites list.
2. If you think that the blocked site is safe and should not be blocked at all, you can submit the website for analysis [here](#).



You shouldn't surf here

<http://unsafe.fstesting.net/>

StarHub CyberProtect has listed this website as harmful. We recommend you do not enter this website.

Don't think this is harmful?

[Report a false positive here](#)

 [Allow website on this device](#)

POWERED BY  **F-Secure.**

Blocking advertisements on websites

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

By default, Ad blocker is switched on to prevent loading content from common advertising servers. The top right corner of the Secure Browsing view shows you the number of advertisements that the product has blocked.

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 **Settings**.
4. Select the lock icon in the bottom-left corner.
You need administrative rights to change these settings.
5. Switch off **Ad blocker**.
When you reload the page in your browser, it will include advertisements.

Rejecting non-essential cookies

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:

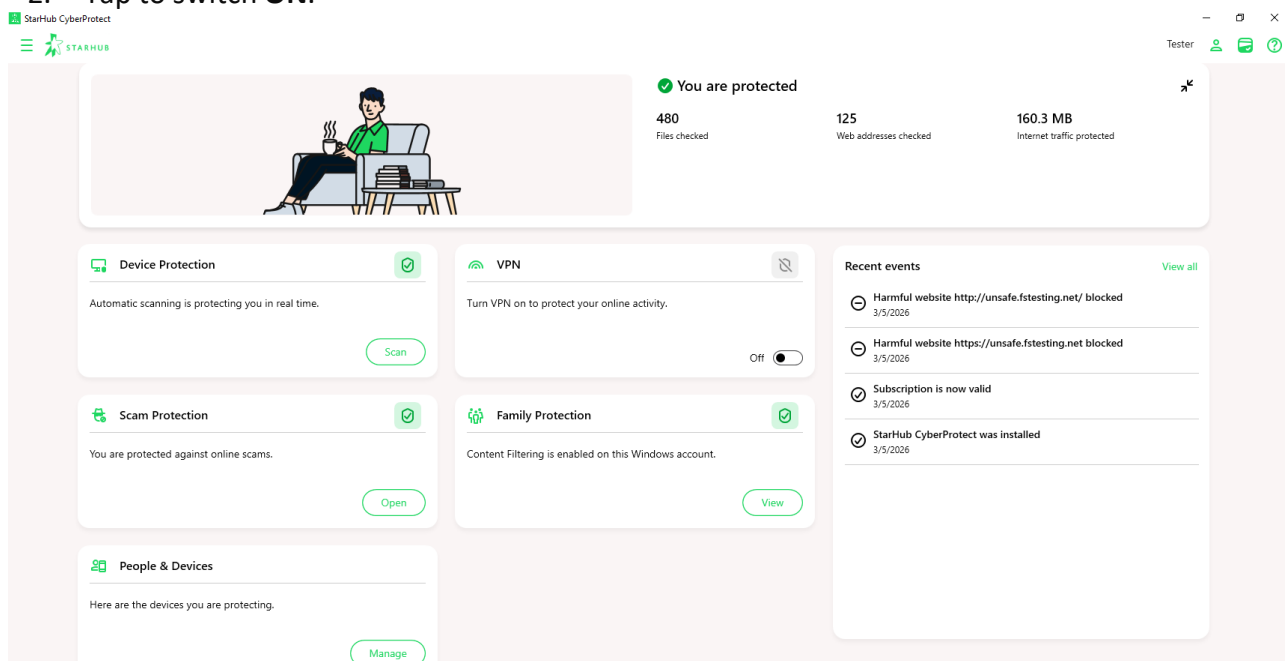
1. Open the CyberProtect app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Settings**.
4. Switch **Cookie Popup Blocker** on or off.

VPN

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.

To open VPN:

1. Open CyberProtect and locate **VPN**.
2. Tap to switch **ON**.



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. CyberProtect VPN lets you select a virtual location which gives your device an address in the selected country. In automatic mode, Cyberprotect VPN uses a server that is closest to you for the best possible network connection and speed.

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
- 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 users in certain countries from accessing their content. With CyberProtect VPN, you may be able to go around some of them by changing your virtual location in the following way:

1. Open the app.
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.

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 **Trusted networks**.

The **Trusted networks** view opens.

4. Under **Current networks**, select **Trust network** for the network that you want to trust.

Your current network is now marked as trusted.

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

Allowing applications to bypass VPN (For Windows 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.

To select the applications that can bypass VPN:

1. Open the CyberProtect app.
2. On the main view, select **VPN**.
3. Under **VPN bypass - Applications**, select **Select applications**.
A list of known applications are shown.
4. Select the applications that you allow to connect to the internet directly, and then select **Done**.

Note: If you want to browse for an application on your computer to allow it, select **Browse applications** and select the application.

The selected applications now bypass VPN.

Blocking internet access when VPN is disrupted or is being established

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 off when you set up the VPN connection.

To turn Killswitch on:

1. Open the CyberProtect app.
2. On the main view, select **VPN**.
3. Select **Settings**.
4. Under **Killswitch**, switch on **Killswitch** if you don't want to allow data traffic to bypass VPN.

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.

Depending on the version of the app that you have, it supports one of the following sets of VPN protocols:

- OpenVPN, OpenVPN (TCP), IKEv2
- Hydra, Wireguard, OpenVPN, OpenVPN (TCP) – Windows

- Hydra, Wireguard, IPSec - MAC

By default, the app uses either the OpenVPN or Hydra protocol, depending on your version of the app.

To change the VPN protocol:

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

Contact us

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

Using the support tool

Before contacting support, run the support tool to collect basic information about hardware, operating system, network configuration and installed software.

- To run the support tool on Windows computer:
 1. Open CyberProtect.
 2. On the main view, select the ☰ menu button.
 3. Select **Help & Support**.
 4. Select **Edit settings**.
***Note:** You need administrative rights to change the settings*
 5. Select **Run support tool**.
 6. Select **Run diagnostics** on the **Support Tool** window.
- To run the support tool on Mac computer:
 1. Go to the product folder under **Applications** and run the **Support Tool** application.
 2. Select **Run Diagnostics** on the **Support Tool** window.
 3. Enter the administrator password for your computer.
The support tool starts and displays the progress of the data collection.
 4. When the data collection is complete, select where you want to save the resulting **tar.gz** archive and then select **Save**.
The support tool opens a **Finder** window showing the saved file.
 5. Send the file to customer support when you are asked for it.
***Note:** You need administrative rights to change the settings*

The support tool starts and displays the progress of the data collection. When the tool has finished running, it saves the collected data to an archive on your desktop. You can provide the collected data (the diagnostics file) when contacting customer support.

CyberProtect features per platform

CyberProtect features across all 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