Table of Contents

DIGICOM
përtej shpejtësisë

1. Introduction to the F-Secure app

The F-Secure app covers all your security and privacy protection needs.

The F-Secure app includes all the protection features you need in just one single app. It is built on the award-winning antivirus protection technology by F-Secure. It's up to you to decide what features you want to include in your subscription. Later, if the need arises, you can extend the range of protection features on the app without having to reinstall the app.

F-Secure Total gives you comprehensive protection both for the security of your devices and for your privacy. It also helps you avoid identity theft. As we share more and more of our personal lives online nowadays, we not only need to protect our devices, but our personal information as well.

The internet is an important part of our daily lives. We want to stay connected with our loved ones, do our banking and shopping online and search the internet for information by asking search engines questions.

With the amount of personal data we handle every day on our smartphones, tablets, and computers, it's important to keep all our devices protected, our information private, and our personal information safe.

With F-Secure Total, you can do the following:

- Protect yourself and your entire family and friends online
- Protect your browsing, online banking and shopping
- Secure your connection in wireless networks
- Stop tracking attempts online
- Protect yourself and your devices against malware and other online threats
- Access geo-blocked content
- Protect your own and your family's personal information against cyber crime

2. System requirements

This topic lists the operating system versions supported by the F-Secure app.

The F-Secure app supports the following operating systems:

For Windows computers:

- Windows 11
- Windows 10 with the latest updates installed (all 64-bit editions; 32-bit editions are not supported)

- Devices running the Windows on ARM64 operating system, although VPN functionality is currently not supported on ARM devices

For Mac computers:

- macOS 15 (Sequoia)
- macOS 14 (Sonoma)
- macOS 13 (Ventura)
- macOS 12 (Monterey)
- Intel and Apple Silicon processors are both supported

For smartphones and tablets:

- Android 10.0 or newer
- iOS 17.0 or newer

Note: Chromebook devices are currently not supported.

3. Installing the product on your device

- You will receive a welcome email from digisafe F-Secure with all the details, including credentials username and password and also the link to download the app. Click the link and you will be redirected to download page where you can download the app depending on the platform you are on (Windows, MacOS, IOS or Android).
- When the installation is complete, open the app.
- If you agree to the End User License Terms, select **Accept and continue**. You may be asked to log in to your account when you start the app for the first time.
- As you are setting up protection for yourself, select **Continue** to finalize the protection for the device.
- Login with the credentials provided on the email. After successfully logged in, you will be prompted to change the password.

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

4. Protecting your children with Family Rules

With Family Rules, you can limit your children's daily and nighttime device use as well as their 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 the content filtering, you can ensure your children view only appropriate content on their devices by restricting what web pages they can access.

With the device use limits, you can schedule the time that your children can spend online. You can specify the daily device use times for weekdays and weekends separately. You can also limit the device use during nighttime for school nights and weekend nights.

Note: Each device having the F-Secure app should have its own profile. When installing the app on a child's device, assign a child profile for the device. Only then can you use Family Rules to limit the child's device use.

Note: The Family Rules settings can be edited only on the parent's device or through the online management portal.

4.1 Protecting your child's device

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

Note: Each device having the F-Secure app should have its own profile. When installing the app on a child's device, assign a child profile for the device. Only then can you use Family Rules to limit the child's device use.

To set up protection for your child:

1. Open the F-Secure app.
2. On the main view, select **People & Devices**.
3. On the **People & Devices** view, select **+ Add device**.
4. Select **My child's device** > **Continue**.

Note: If you have previously already added child profiles, they are listed here. To add a new child profile, select **New child profile**.

5. Select how you want to deliver the installation link to the device you want to protect and then select **Send link**.
6. Open the message with your child's device and follow the installation instructions.
7. Select **Install from app store** to go to the app store and select **Install** to start the installation.
8. When the installation is complete, select **Open** to start the application.

The welcome page opens.

9. Agree to the End User License Terms by selecting **Accept and continue**.
10. When prompted, log in to your account.
11. As you are setting up protection for your child, select **Install for a child?**

Note: If you have previously already added child profiles, they are listed here. From the **Set up protection for** drop-down, select **New child profile** and then select **Continue**.

The **Create new child profile** view opens.

12. Enter the name of the child, select the age group the child belongs to, and then select **Next**.

The **Family Rules settings** view opens.

13. Select **Next**.

The **App Control** view opens.

14. Select **Turn on App Control** and do the following:
    1. Select the default setting for all new apps that will be installed on the device: **Time-limited** or **Blocked**.
    2. Select the setting for the apps that are already installed on the device: **Time-limited**, **Always allowed** or **Blocked**.
    3. Select **Next**.

The **Daily Time Limits** view opens.

15. Turn on **Daily Time Limits**, use the sliders to limit the daily use time of the apps that you have selected as Time-limited on weekdays and weekends, and select **Next**.

The **Bedtime** view opens.

16. Turn on **Bedtime** by using the sliders to limit the nighttime use of apps or device on school nights and weekend nights, and select **Next**.

The **Content Filtering** view opens.

17. Turn on **Content Filtering**, select the categories of web content you wish to block, and select **Next**.
18. To allow the app to access files, select **Allow** > **Allow**.
19. To allow the app to block apps and limit device use, and to prevent children from removing protection or uninstalling, you need to turn on accessibility:

Note: The following steps depend on the device model you use. Consult your device manual for more information.

1. Select **Allow**. The **Turn on accessibility** window opens.

2. Select **Continue**.
3. Select **Installed services**.
4. Select **F-Secure TOTAL** > **Off** > **Allow** to allow the app to have full control of your child's device.

Your child's device is now protected.

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

4.2 Making changes to existing child profile settings

At times you need to make changes to the family rule settings that you have set for a child.

As your children become older, you may need to change the age group they belong to. The time limits may also need some adjustments. Or you may not need the child profile any longer and want to remove it.

Important: For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

To edit the settings of a child profile:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

On the **Child profile** view, you can add new devices as well as make changes to the existing devices, family rule and profile settings of the child.

3. On the **Child profile** view, select the device you want to edit, and on the **Device** view you can do the following:
   - edit the device name
   - release the license allocated for the device.

Note: You need to log in to your account to confirm the license release.

4. On the **Child profile** view, you can immediately see which **FAMILY RULES** settings have been turned on and which are off. You can edit the following settings:
   - App Control (Android only)
   - Daily Time Limits (excluding devices running on iOS)

- Bedtime
- Content Filtering.

5. On the **Child profile** view, you can make the following changes to the **Profile settings**:
   - edit the child's name
   - move the child to another age group
   - remove the child's profile.

Note: You need to log in to your account to confirm the profile removal.

4.3 Editing App Control settings

This topic describes how to make changes to current App Control settings (Android only).

With App Control, you can select which apps are always allowed, which are limited by daily time limits and bedtime settings, and which are always blocked on the child's devices.

If App Control is turned off, daily time limits and bedtime settings no longer apply to specific apps but restrict the use of the whole device. Calling and SMS messages are always allowed.

Important: For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

If you want to edit the App Control settings for your child's profile, do as follows:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **App Control**.

The **App Control** view opens. If **App Control** is turned off, use the switch to turn it on.

4. To see a list of current devices which use **App Control**, select **Which devices App Control works on**.

Note: App Control is supported only by devices running on Android.

5. Under **DEFAULT SETTING**, you can define how a newly-installed app is treated by App Control:

- **Time-limited** - This means that the app use is restricted by daily time limits and bedtime limits.
- **Always blocked** - This means that the app cannot be used at all.

6. Under **ALL CURRENT APPS**, you can see the apps that have already been installed on the device. For each app, you can define separately how it is treated by App Control:
    - **Time-limited** - This means that the app use is restricted by daily time limits and bedtime limits.
    - **Always allowed** - This means that the app use is not restricted by daily time limits nor bedtime limits.
    - **Always blocked** - This means that the app cannot be used at all.
7. To save the changes, select **Save**.

4.4 Editing daily time limit settings

This topic describes how to make changes to current daily device use times.

You can control when and for how long a child can use the device.

Important: For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

If you want to edit the daily time limit settings for your child's profile, do as follows:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **Daily Time Limits**.

The **Daily Time Limits** view opens. If **Daily Time Limits** is turned off, use the switch to turn it on.

4. On the **Daily Time Limits** view, set the maximum number of hours that your child is allowed to use the device on weekdays and at weekends:
    1. For **Weekdays**, use the slider to change the maximum time allowed per day.
    2. For **Weekends**, use the slider to change the maximum time allowed per day.

Note: If you do not want to limit the amount of time that the child uses the device each day, drag the slider as far to the left as possible to set the allowed number of hours to **Unlimited**.

5. To save the changes, select **Save**.

4.5 Editing bedtime settings

This topic describes how to make changes to current bedtime settings.

Use the bedtime settings to prevent the use of the device during night time. Calling and SMS messages are always allowed. You can set a different bedtime for school nights—from Sunday night to Thursday night—and weekend nights—from Friday night to Saturday night.

With Android devices, turn on App Control to choose which individual apps are affected by the bedtime settings.

Important: For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

If you want to edit the bedtime settings for your child's profile, do as follows:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **Bedtime**.

The **Bedtime** view opens.

4. On the **Bedtime** view, prevent the nighttime use of the device as follows:
    1. Turn on the **School nights** setup pane and drag the slider to set the time when bedtime starts and ends.
    2. Turn on the **Weekend nights** setup pane and drag the slider to set the time when bedtime starts and ends.
5. To save the changes, select **Save**.

4.6 Editing content filtering settings

This topic describes how to make changes to current content filtering settings.

You can keep your children safe from the many threats on the internet by limiting the types of content they can view while browsing the web.

You can block access to websites and pages that contain unsuitable content.

Important: For technical reasons, when you edit the family rules set up earlier, you must turn Privacy VPN off and on again on the applicable mobile device **after 24 hours** for the new settings to take effect.

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

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select the child profile you wish to edit.

The **Child profile** view opens.

3. Under **FAMILY RULES**, select **Content Filtering**.

The **Content Filtering** view opens. If **Content Filtering** is turned off, use the switch to turn it on to block the content you don't want children to have access to.

4. Enable Safe Search to hide undesired content from search results.

Note: Safe Search supports the following search engines on Windows and Mac computers: Google, Bing, DuckDuckGo, Yahoo and YouTube. On Android and iOS devices Safe Search supports the following search engines: Google, Bing, and DuckDuckGo when using Safe Browser.

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

Note: Click on the content category to see more detailed information about it.

6. To save the changes, select **Save**.

4.7 Content categories

You can block access to several types of content.

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 websites. 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 catalogs 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 allow or instruct people on how to bypass network filters, including web-based translation sites that allow people to do so. For example, sites that provide lists of public proxies that can be used to bypass possible network filters.

Unknown

Websites that are new or unknown to our web filters. The content of these websites cannot be confirmed.

5. Sharing protection with a family member or friend

This topic describes how to share the protection with a family member or a 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.

Note: Note that if the person you want to invite to your group has already been added to your group or belongs to another My F-Secure 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 F-Secure 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 F-Secure account after which you can then use the email address in the invitation.

To share protection with someone else:

1. On the main view, select **People & Devices**.
2. On the **People & Devices** view, select **+ Add device**.
3. Select **Someone else's device** > **Continue**.
4. To invite a user to your group:
    1. Enter the first name of the user.
    2. Enter the last name of the user.
    3. Enter the email address of the user.
    4. 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.

5.1 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 in which you are invited 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 through 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 **Log in**.

The **Change your password** window opens.

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

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

You can now manage your own devices and their protection either through the online management portal or through the product's **People & Devices** view. As an invited user, you can manage your account as follows:

- 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 at any time.
- 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.

5.2 Stop sharing protection with a family member or friend

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

If you want to stop sharing protection with a family member or a friend, you can remove the sub-user from your My F-Secure group.

To remove a sub-user:

1. On the main view, select **People & Devices**.
2. Select the sub-user you want to stop sharing protection.
3. Select **Remove from group**.
4. To confirm the removal, you need to log in to your F-Secure account. Select **Log in**, enter your account credentials and then select **Log in**.

The **Remove from group** window opens.

5. Select **Remove**.

The sub-user is removed from your My F-Secure group and is no longer protected by your subscription.

Alternatively, you can stop sharing protection and remove sub-users through the My F-Secure portal.

5.3 Releasing a license from a device

This topic describes how to release a license that is no longer needed for a device.

If you have a device that no longer needs a license, we recommend that you release the license. Only then can the license be used on another device. For example, if you buy a new computer, phone or tablet and the old one is no longer used, you need to release the license used by the old device before the license can be assigned to the new device.

To release a license from a device:

1. Open the F-Secure app.
2. On the main view, select **People & Devices**.
3. Select the user from whom you want to release the license.

A list of protected devices of the user is shown.

4. Select the device that you want to release a license from.

Basic details about the device are shown.

5. Select **Release license**.

Note: To confirm the license release, you may need to log in to your account. Select **Log in**, enter your account credentials and then select **Log in**.

The **Release license** window opens.

6. Select **Release license**.

This frees up the license that you can now use on another device.

Alternatively, you can release a license that is no longer needed through My F-Secure.

Note: Releasing a license from a device does not uninstall the security app from the device. To uninstall the app, you have to do it manually from the device.

6. Device Protection

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

When scanning is turned on, the app scans the device daily automatically. You can also scan the device manually at any time.

We recommend that you scan your device for threats whenever the product asks you to do so.

The app also scans installed programs and inserted memory cards for viruses, spyware, and riskware automatically.

Note: The battery optimization features on some Android devices may stop the app from running in the background. When this happens, or if you stop the app manually, your device is not protected against threats. To avoid this issue, check the battery usage permissions on your device and make sure that the app has the required permissions to always stay running.

6.1 Running a manual scan

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

To manually scan files on your device:

1. On the main view of the app, select **Device Protection**.
2. Select **Scan**.

The scan starts.

3. After the scan has completed, the product shows the following information:
   - Total files checked - the number of files that were scanned
   - Total apps checked - the number of applications that were scanned

Tip: By selecting **Scan history**, you can view the list of both manual and automatic scans run. Tap the desired scan to see more information about the scan results.

6.2 Turning automatic scanning on

You can set the app to scan your device for viruses and other threats automatically.

When turned on, the app automatically scans the device daily and every time a new app is installed.

To make sure that automatic scanning is enabled on your device, do the following:

1. On the main view of the app, select **Device Protection**.

2. Select ⚙ in the top-right corner, and make sure that the **Antivirus is ON** setting is turned on.

The app automatically scans new apps and files daily.

If you want the app to scan your device even when the device is on a metered network connection, make sure the **Metered scan ON** setting is turned on.

Note: Turning this option on may result in extra costs.

6.3 Using metered network connections

A metered network connection is one which has a limit on how much data you can use.

When turned on, the app scans even while on a metered connection. This may result in increased data traffic and extra costs.

To allow scanning while on a metered network connection, do the following:

1. On the main view of the app, select **Device Protection**.
2. Select ⚙ in the top-right corner, and make sure that the **Metered scan ON** setting is turned on.

6.4 Checking the scanning results

Once a scan is complete, you can check the results.

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

To assess the detected file, do the following:

1. In the **Device Protection** view, select the notification under **Scan**.

The Scan details page opens.

2. To remove the file or files, select **Remove all detections** to remove them at the same time from your device.
    - To see more details, still on the **Scan details** page, 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
  - 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 website: Threat Descriptions.

6.5 Viewing app permissions on your device

Device Protection gives you an overview of the permissions that apps installed on your device are currently using.

We recommend that you regularly check the permissions that are allowed for your installed apps. Some apps may request permissions that are necessary for features that you never use, for example. In addition, checking the app permissions is a good way to see if any apps have extensive access to your device data and functions, which may affect your privacy.

1. On the main view of the app, select **Device Protection**.
2. Under **App privacy overview**, select the filter icon and then **By app** to view the currently allowed permissions by app.
3. Select an app to see more details of the allowed permissions for that app.

This shows you a list of all the device permissions that are allowed for the app, with a brief description of each permission.

4. Select **Manage permissions** to go to your device settings and change the permissions for the selected app.

Here you can revoke permissions from the app if you think they are not needed. However, note that revoking permissions may affect the app functionality.

7. Scam Protection

This section explains how the app can ensure safe browsing on the internet, as well as safe online banking. The app also protects you against other common scams.

By using Chrome Protection or the built-in Safe Browser, 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.

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

Note: When you use the built-in Safe Browser, there can be a slight delay before the app blocks redirected malicious pages. In most situations the delay is not noticeable, but it may be a few seconds.

7.1 Setting up the Chrome Protection extension

The app requires certain permissions to provide protection on the Chrome browser. When you approve these permissions, the app protects your web browsing on Chrome and shows you security information while you browse the internet.

Note: The browser extension uses the address of the website to check its reputation and determine the safety of the page. It does not check any content, links, or scripts that are present on the page.

To start using Chrome Protection:

1. Open the F-Secure 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 F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Chrome Protection**.
4. Select ⚙ in the top-right corner of the screen to open the settings.
5. Select which types of sites should show or hide the 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.

7.2 Allowing blocked websites

You can manually allow websites that the product has blocked if you are sure that they are safe.

To allow a blocked website:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Allowed websites**.
4. Select **Add allowed website**.
5. Enter the address of the website you want to add, then select **Allow this website**.

To allow all subdomains of a website, enter the main domain. For example, if you enter example.com, this will allow test.example.com and sample.example.com in addition to www.example.com.

The product does not support the use of wildcard characters, for example *.

The website is now listed as an allowed website.

To remove a website from the list, select the website and then select **Remove**.

7.3 Showing safety ratings for websites

You can select when safety ratings are shown as an overlay icon in the app settings.

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

This opens the settings view.

3. Switch on **Overlay icon** to show the safety ratings of websites that you visit.

The overlay icon also shows you when you are visiting a banking website and whether shopping websites that you visit can be trusted or not.

When the overlay icon is in use, you can select the icon in the browser to see more information on the rating for the current website.

7.4 Setting Safe Browser as the default browser

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

Setting Safe Browser as the default browser 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 other browsers.

If you are taking Safe Browser into use on your own device, there is no need to remove other browsers.

To set up Safe Browser as the default browser:

1. On your device, select **Settings** > **Apps** > **Choose default apps**.

The **Default apps** view opens.

2. Select **Browser app**.

The **Default browser app** view opens.

3. Select **F-Secure** as the default browser app.

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

Using Safe Browser for online banking and shopping

You can do your online banking and shopping safely only if you use the built-in Safe Browser.

Once Safe Browser is turned on, all other network connections are put on hold temporarily while doing your online banking and shopping.

To access Safe Browser and protect your browsing:

1. Open the F-Secure app.
2. On the main view of the app, select **Scam Protection**.
3. Select **Safe Browser**.
4. Browse to an online banking or shopping site and carry out your transaction.

When you enter an online banking or shopping site, a notification appears in the browser, saying **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.

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 when using Safe Browser or Chrome with Chrome Protection switched on, 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**.

7.5 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.

Note: This feature is currently in the beta development phase, meaning that some functionality issues are to be expected.

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 F-Secure 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** .

7.6 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.

WiFi Protection checks various security aspects of your connection whenever you connect your device to the network over WiFi. This checks include the certificates and encryption for the connection as well as testing network requests for any unexpected or suspicious changes. Once the connection is checked, WiFi Protection notifies you whether or not it is safe to use.

WiFi Protection uses notifications to show you if your WiFi connection is safe or not. If the app does not have permission to show notifications on your device, you are asked to allow that permission when you go to the **WiFi Protection** view.

You can also set the app to show you notifications of open WiFi connections (connections that do not require any password) as well as safe and unsafe connections.

Note: To identify open WiFi connections on devices with Android older than version 12, the app requires the Location permission and that the location service is switched on in your device.

To make sure your WiFi connections are safe:

1. Open the F-Secure 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.

8. VPN

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

VPN protects your connection in a WiFi network by making your data unreadable for outsiders. It even prevents anyone from changing your data or hijacking your network traffic.

When you browse the internet, data collection companies track your online activities and sell your data to advertisers. VPN blocks these tracking attempts from HTTP traffic so you can browse anonymously and undisturbed.

You can easily see how your privacy has been protected on the **Privacy VPN** view. It shows you the volume of your internet traffic that has been protected.

When you take the product into use, the app asks your permission to set up a VPN connection. You need to allow this so that VPN can monitor network traffic. Later, you can turn VPN on or off on the main view of the app.

Important: If you have any other VPN software, such as F-Secure FREEDOME VPN, installed on your device, make sure that you don't have both VPNs turned on at the same time. If you have FREEDOME VPN turned on and then turn Total's VPN on, the network stops working until you turn off one of the VPN connections.

8.1 Turning on the VPN connection

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

To turn on VPN:

1. Open the F-Secure app.
2. Under **Privacy VPN**, select the toggle switch to turn VPN on.

When you are turning VPN on for the first time after installing the app, the "Setting up VPN" window 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 **Privacy VPN**, tap the toggle switch.

8.2 Marking a local WiFi network as trusted

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 marking the network as trusted.

To mark a network as trusted:

1. Open the F-Secure app.
2. On the main view, select **Privacy VPN**.

3. Select ⚙ in the top-right corner.

The **Privacy VPN settings** view opens.

4. Select **Trusted networks**.

If you have not allowed location permissions for the app, you have to allow those first.

    1. Select **Allow permissions**.

You are asked if you want to allow the app to access your device's location.

    2. Select **Allow** and then select **While using this app**.

The **Trusted networks** view opens.

5. Select **Current network**.

Your current network is now marked as trusted.

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

8.3 Changing your virtual location

Using a virtual location protects your privacy and lets you access your favorite streaming services when abroad.

By default, the app uses the location that gives you the best possible connection. This is usually the location closest to you, but this may vary, for example, depending on the amount of network traffic.

Companies use IP geolocation to block access to their content in certain countries. With VPN, you may be able to access some of these services by changing your virtual location.

To change your virtual location:

1. Open the F-Secure app.
2. Tap on **Privacy VPN**.

The **Privacy VPN** view opens, showing the location you are currently connected.

3. Tap on the current location to open the **Choose a location** view, and select the virtual location you want.

The app immediately connects to the location and takes you back to the **Privacy VPN** view.

Your device will still know its real location, even without GPS, and apps may have permission to use it.

8.4 Allowing applications to bypass VPN

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 F-Secure app.
2. On the main view, select **Privacy VPN**.
3. Select ⚙ in the top-right corner.

The **Privacy 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.

8.5 Using tracking protection

Tracking protection ensures your privacy while you browse the web, although you may have to switch it off for some apps or websites to work properly.

When you go to a website or use an app that tries to track you, VPN hides your IP address, blocks tracking cookies, and prevents apps from sending information about you to data collection sites.

Tracking protection removes all cookies set by known advertising networks, preventing the ad networks from tracking individual visitors from site to site. It also prevents communication with any tracking domains identified by F-Secure's reputation analysis.

However, many websites and services use encrypted communications (HTTPS/TLS/SSL) to transfer content, and in those cases VPN cannot decrypt the full address of linked content to reliably determine whether it is a tracking cookie or legitimate content. This means that some pages might load slowly or have missing content.

In addition, some apps may stop working due to an incorrectly blocked connection. This issue may appear if you are buying something online and the purchase flow is cut off during the transition between the online shop and your banking app, for example.

By default, tracking protection is turned on. If an app that you trust is not working or websites take a long time to load, you can try turning tracking protection off:

1. Open the F-Secure app.
2. On the main view, select **Privacy VPN**.
3. Select ⚙ in the top-right corner.

The **Privacy VPN settings** view opens.

4. Select the **Tracking protection** switch to turn the feature off.

The app does not aim to block anything going from your browser to the site you are visiting. because blocking cookies from the site you visit easily breaks login sessions, stored preferences, and other valuable features.

The anti-tracking statistics in the app only show the total amount of data that was blocked and the number of cookies that were filtered to prevent tracking. We are not able to provide more accurate data about what was blocked to our users since we do not log any traffic for privacy reasons.

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 on when you set up the VPN connection.

To turn Killswitch off:

1. Open the F-Secure app.
2. On the main view, select **Privacy VPN**.
3. Select ⚙ in the top-right corner.

The **Privacy VPN settings** view opens.

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

Browsing protection blocking suspicious and malicious websites

Browsing protection is turned on by default when you set up the VPN connection.

To turn Browsing protection off:

1. Open the F-Secure app.
2. On the main view, select **Privacy VPN**.
3. Select ⚙ in the top-right corner.

The **Privacy VPN settings** view opens.

4. Select the **Browsing protection** switch to turn the feature off.

9. Password Vault

With Password Vault, you can improve your security by creating strong and unique passwords. It also allows you to sync your passwords across all your devices which means that you have your passwords available to you no matter which one of your devices you are using. This makes signing in to your online accounts easier and safer.

9.1 Getting started with Password Vault

This topic describes how to take Password Vault into use on the device your 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 password that you need to remember once you have set up Password Vault.

To set up Password Vault:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select **I'm a new user.**

Note: If you want to access your Password Vault created on another device or app, you can connect the devices to sync your passwords by selecting **I am an existing user**.

4. Create a strong master password and select **Continue**.
5. Repeat the master password and select **Confirm**.
6. Create a recovery QR code by selecting **Save as image**. The code is saved as an image to your Gallery. If your device is running on Android 9 or earlier, you must allow Password Vault to access your photos, media, and files on your device.
7. If your device supports biometric authentication, for example fingerprint, and you have set it up, you can access your Password Vault faster by enabling **Use biometric authentication to unlock** and selecting **Save**. Note that if you don't want to take the biometric authentication into use now, you can do it later in the Password Vault settings.

8. Set up autofill to access your online services without having to enter your username and password manually:

    1. In Password Vault, select ⚙ > **Autofill**.
    2. Turn on **Autofill** and select the required autofill service from the device settings.

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

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 create the code will be shown to you until you create it.

9.2 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.

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 F-Secure app.
2. On the main view, select **Password Vault**.
3. Select **+ Add** > **Password**.

The entry details open.

4. In the **Title** field, give your entry a descriptive name.
5. To change the entry icon on the left, tap on it and select a background color and a symbol for the entry. Once done, confirm your selection by selecting ✓.
6. In the **Username** field, enter the username that you use for the app or online service.
7. In the **Password** field, create a strong password or passphrase.

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

8. In the **Web address** field, enter the web address (URL) of the online service login page.

Note: The format of the web address must be https://example.com.

9. In the **Notes** field, enter any other information you want to add.

10. To save the entry, select ✓ .

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.

9.3 Storing payment card information on a mobile device

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

To store your payment card details:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select + **Add** > **Credit card**.

The entry details open.

4. To change the entry icon on the left, tap on it, choose a color and one of the available payment card symbols, and select ✓ .
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 ID number linked to the card.
9. In the **Expiry Date** field, enter the date (in format MM/YY) until which the card is valid.

10. In the **Verification code** field, enter your card's 3- or 4-digit security code that helps protect you from credit card fraud.
11. In the **Web address** field, enter the web address (URL) of the service.
12. In the **Notes** field, enter any other information you want to add.
13. To save the new entry, select ✓ .

Your payment card details have now been stored to Password Vault.

9.4 Editing existing data

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

To edit an entry:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry that you want to edit.

The entry details open.

4. Select ✎ to edit the entry details.
5. Make the required changes.
6. Select ✓ to save the changes.

Deleting entries

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

To delete an entry:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry that you want to delete.

The entry details open.

4. Select ✎ to edit the entry details.

5. To delete the entry, select 🗑 > **Delete**.

Letting the app generate a new password for an existing entry

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

You can choose the length and complexity of the password.

To generate a password:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry whose password you want to change.

The entry details open.

4. Select ✏ to edit the entry details.
5. In the **Password** field, select 🎲 .
6. 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.
    - Select 🎲 **Generate** to generate a new password.
7. To take the generated password into use, select ✓ > .

Accessing your old passwords

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

After you have changed 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 F-Secure app.
2. On the main view, select **Password Vault**.
3. Select the entry whose previous passwords you want to view.

The entry details open.

4. In the entry details, select **Password history**.

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

The **Password history** view opens.

5. To view a hidden password, select 👁 next to the password.

Note: You can copy the desired password to clipboard by selecting ⧉ .

6. To close the **Password history** view, select the arrow in the top-left corner.

If you want, you can delete the password history by selecting 🗑 .

9.5 Connecting devices to sync your Password Vault data across all your devices

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

Make sure that you have the devices you want to connect at hand and that you have the app already installed on both devices.

To sync your data across both devices:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. From the top-right corner of the screen, select ⚙ .

The **Password Vault settings** view opens.

4. Select **Connect Devices**.

The **Connect devices** view opens.

5. Select **Generate sync code**.

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

6. Open the app on the device with which you want to connect and sync your data, and select **Password Vault**.
7. Depending on whether the other device is a mobile device or a desktop device, do one of the following:
   - **On a mobile device**:
     1. Select **I am an existing user**. The **Connect devices** view opens.
     2. Enter the sync code generated in the first device and select **Connect**.
   - **On a desktop device**:
     1. Select **Connect Devices**.
     2. Enter the sync code generated in the first device and select **Connect devices**.
8. When prompted, enter your master password that you use on the device in which you generated the sync code and select **Confirm**.
9. Finally, if you want to start using biometric authentication to unlock Password Vault, select **Save**.

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 of your connected devices.

9.6 Setting up autofill to access apps and websites faster

You can quickly access apps and websites without having to enter your login credentials manually.

Note: In some device models, all apps may not fully support Autofill.

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 that are saved in Password Vault, you can have the app enter your username and password automatically.

To set up autofill on your Android device:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.

3. From the top-right corner of the screen, select ⚙.

The **Password Vault settings** view opens.

4. Select **Autofill**.

The **Autofill** view opens.

5. Turn on **Autofill**.

Your device's **Autofill service** view opens.

6. Select **F-Secure** as your autofill service, and then select **OK** to confirm you selection.

You can now access your apps and online services without having to enter your login credentials manually.

9.7 Changing the master password

This topic describes how you can change your Password Vault master password.

To change your master password:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. From the top-right corner of the screen, select ⚙.

The **Password Vault settings** view opens.

4. Select **Change Master Password**.
5. Enter your old master password and select **Continue**.
6. Enter a strong new master password.
7. Repeat the new master password and select **Confirm**.

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

8. Since you have changed your master password, you need to create a new recovery QR code. Select **Create now** and then select **Save as 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: When you change the master password for any reason, you need to create a new recovery QR code. Any old code will no longer be valid. Therefore, make sure that the recovery QR code is always up to date and valid for your current master password.

9.8 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 for you to regain your master password if you forget it.

To create a recovery QR code for your master password:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. From the top-right corner of the screen, select ⚙.

The **Password Vault settings** view opens.

4. Select **Create Recovery Code**, and do one of the following:
   - If you have biometric authentication in use, provide the requested authentication. Alternatively, select **Use 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.

5. Select **Save as image**.

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

6. Go to the folder, select the image, and send it to a service from where you can print it out.

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

Using the recovery QR code to recover your forgotten master password

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

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

To recover your master password with the recovery QR code:

1. Open the F-Secure app.

2. On the main view, select **Password Vault**.
3. On the login screen, select **Forgot Master Password?**.

The **Forgot Master Password?** view opens.

4. Select **Import**.
5. Find and open the recovery QR code image file which you have created earlier.

Your master password appears on the screen.

6. Enter your master password and select **Unlock**.

Password Vault opens.

9.9 Unlocking and locking Password Vault

This topic shows you how to unlock Password Vault.

Important: To keep you passwords and personal information safe, we recommend that you lock Password Vault whenever you are not using it.

To unlock Password Vault, do the following:

1. Open the F-Secure app.
2. On the main view, select **Password Vault**.
3. Enter your master password and select **Unlock** or, use biometric authentication to unlock Password Vault.

Note: By default, Password Vault locks itself automatically after five minutes. To set the time after which Password Vault locks itself, go to **Password Vault settings** ⚙ > **Lock automatically after**, and select the time. The options are immediately, 5 minutes, 15 minutes, 30 minutes, 1 hour, 10 hours, and 1 week.

4. To lock Password Vault manually, select **Password Vault settings** ⚙ > **Lock now**.

Using biometric authentication to unlock Password Vault

On certain mobile device models, you can use biometric authentication to unlock Password Vault.

To be able to use your fingerprint to unlock Password Vault, you first need to register your fingerprint. Consult the device user manual to find out how to take fingerprint recognition into use in your device.

In Password Vault, you can take biometric authentication into use when you create your master password, or later on in the Password Vault settings or login page.

Important: Do not, however, forget your master password as you need it, for example, after every software upgrade.

Also, we strongly recommend that you create a recovery QR code for your master password. It is the only way you can access your data if you forget your master password.

10. ID Monitoring

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

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

You can add up to 10 items of each type for monitoring; that is, 10 email addresses, 10 payment cards, 10 phone numbers, etc.

10.1 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 F-Secure sends notifications if your information appears in a data breach.

To add more items for monitoring:

1. Open the F-Secure app.
2. On the main view, select **ID Monitoring**.
3. In the **ID Monitoring** view, select **Add an entry**.

The **Add new** dialog opens, listing all the available item types to choose.

4. Select the type of item you want to add for monitoring.
5. Enter the requested information and select **Save**.

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

6. If you have not yet confirmed your email address, open the confirmation email, and select the link to confirm that this is your email address.
7. To see the details of your exposed personal information and what you should do, select the specific breach listed in the **ID Monitoring** > **Breaches** view.

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

10.2 Editing and deleting monitored items

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

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

To delete a monitored item:

1. Open the F-Secure app.
2. On the main view, select **ID Monitoring**.
3. In the **ID Monitoring** view, select **Your data**.

The list of your monitored items opens.

4. To delete an item from the list, select ••• next to the item you want to remove and then select **Delete entry**.

A confirmation dialog opens.

5. 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.

10.3 Changing your contact email address

You will receive notifications to your contact email address as soon as any of your monitored items appears in a data breach.

The first email address that you add as a monitored item becomes automatically your contact email address.

To change your contact email address:

1. Open the F-Secure app.

2. On the main view, select **ID Monitoring**.
3. In the **ID Monitoring** view, select **Your data**.

The list of your monitored items opens.

4. If you haven't yet added the email address that you want to use as the new contact email address to the monitored items, do as follows:
    1. Select + > **Email** and then enter the email address and select **Save**.

An email with a confirmation link is sent to the address you entered.

2. Open the email and confirm your email address.

Once confirmed, the email address can be used as your contact email address.

5. In the **Your data** view, select ••• next to the email address and then select **Mark as primary contact**.

Your new contact email address is now in use.

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.

11. Technical support

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

If you have a question about the product or an issue with it, before contacting our customer support, go to F-Secure Community and see if you can find an answer to your question there.

11.1 Where can I find version information of the product?

If you need to contact us, our customer support may ask information about your product version.

To view the current version information:

1. Open the F-Secure app.
2. Select the profile icon 👤 in the top-right corner of the screen.
3. Select **About and help**.

The **About and help** view opens.

4. Under **About**, select **About the F-Secure app**.

The **About** view opens, showing various information about the product.

Apart from the product version information, the **About** view contains information, such as the license key, end user license terms, privacy policy, and third-party software.

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 F-Secure app.
2. Select the profile icon 👤 in the top-right corner of the screen.
3. Select **About and help**.

The **About and help** view opens.

4. Under **About**, select **About the F-Secure app**.

The **About** view opens, showing various information about the product.

5. Tap the version number seven times until the **SEND LOG** button is shown.
6. Select **SEND LOG** and then select your preferred email app.

The message opens in the email app with the recipient field prepopulated and the log(s) attached.

7. Describe the issue in more detail and send the message to our support.

Wait until our support contacts you.

11.2 Phone scams and what to do if you think you are targeted

Phone scams are unfortunately on the rise with scammers using social engineering to target their victims.

This topic is to help you identify these calls, and in the worst case—if you have been targeted—give you some information on what to do next.

What are phone scams?

Phone calls can start either as a cold call or via an advert or link that triggers a pop-up on your computer. These pop-ups then urge you to call the tech support number advertised; the pop-ups may appear suddenly and are not that easy to get rid of.

How can I recognize a phone scam?

These types of calls normally follow a certain pattern: The scammers usually claim that your computer has a problem, say a virus—when it actually doesn't—and then they trick you into paying for a service that doesn't exist either. They catch you off-guard and play on your emotions. Here's the basic scenario:

- Phone scammers claim to be from a well-known company, such as Microsoft, your bank, or even your network operator. As they use a reputable name, this puts you more at ease. They also seem knowledgeable and use technical terms, which make them seem legitimate and believable.
- As the risk seems real and you feel worried about possible computer viruses, you give the scammers access to your computer. They convince you to let them install an application that gives them access to your computer using remote access tools.
- Once the scammers have access to your computer, they pretend to fix the virus, and may also ask for your personal credentials. When the scammers have "fixed" the issue, they ask you to log into your online bank or ask you to fill in a form with your credit card details. The scammers charge you for the bogus service, which ends up being much more than you thought. In fact, it's difficult to know how much they really charge you.

What to do if you think you have been scammed

If you think you are being scammed and you recognize the scenario that we described above, do the following:

- Act without delay.
- Immediately contact your credit card company or bank, report the scam and cancel any bank or credit cards. If you act promptly, they even may be able to stop the transaction and reverse the charges.
- Report the scam to the appropriate authority.
- Change all your passwords on every website or service that you think might have been affected.
- Uninstall any unknown, third-party software.
- Run a full scan on your computer: Open your security product, then select **Device Protection** > **Full computer scan**.

Things to remember about unsolicited phone calls

- If you receive this type of a call, think: have I requested this?

Note: Normally, customer support calls you if you have already contacted them and created a support ticket.

- Remote sessions are commonly used in tech support as a way to assist you in solving issues.

Remember: Only allow remote sessions with people or companies you know and trust. Only ever allow remote sessions if you have contacted your service provider beforehand and have a valid support case with them. Also, guard your remote access data as you would guard any other password.

- Never give access to your device to people you don't know. Granting scammers remote access means that, in effect, you hand over the admin rights to your computer. Even if you have antivirus software installed, this can no longer protect you, as the scammers take control of your computer.
- Microsoft has informed its users that they never include phone numbers in their software's error messages or warning messages.
- Never freely hand over any personal credentials or credit card details.
- End the call immediately.
- These types of phone calls are illegal, and when in doubt, turn to the relevant authority that deals with fraud and report it.

How can the security product help?

With the security product installed, your computer is protected from viruses, trojans and ransomware. The Browsing protection, Banking protection, and Remote access tool protection features also add another layer of protection and make sure that you can browse and do your online banking safely.

If you have been targeted and you already have a security product installed, you can immediately run a full computer scan to help detect any applications that may have been installed by the scammers; these are called Potentially Unwanted Applications (PUAs). The product is not able to protect you from these types of phone scams, however.

Be vigilant and stay safe.