Keeping Your Data Safe

Table of Contents

Keeping Your Data Safe

New Online Safety Bill Passed as Law by UK Government

As of September 20th 2023, the UK Government has approved into law a new online safety bill, designed to protect children and adults online. This will make social media companies more responsible for the safety of their users.

It will protect children by making social media platforms:

- remove illegal content quickly or prevent it from appearing in the first place. This includes removing content promoting self-harm.
- prevent children from accessing harmful and age-inappropriate content.
- enforce age limits and age-checking measures.
- ensure the risks and dangers posed to children on the largest social media platforms are more transparent, including by publishing risk assessments.
- provide parents and children with clear and accessible ways to report problems online when they do arise

Underage children will be kept off social media platforms

The online safety laws will mean social media companies will have to keep underage children off their platforms. Social media companies set the age limits on their platforms and many of them say children under 13 years of age are not allowed, but many younger children have accounts. This will stop. Different technologies can be used to check people's ages online. These are called age assurance technologies.

The new laws mean social media companies will have to say what technology they are using, if any, and show they are enforcing their age limits.

For further information on the new law, please follow the UK Government link below;
https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill?gclid=EAIaIQobChMI7suer7C5gQMVjvftCh1XoAriEAAYASAAEgKyePD_BwE&gclsrc=aw.ds#full-publication-update-history

Security Best Practises

Update all Devices

Install the latest software and app updates - Software and app updates contain vital security updates to help protect your devices from cyber criminals.

Backup all Data

You should back up your data regularly. If you're using an external storage device, keep it somewhere other than your main workplace – encrypt it, and lock it away if possible. That way, if there's a break-in, fire, or flood, you'll minimise the risk of losing all your data.

- Check your back-up. You don't want to find out it's not worked when you need it most. Make sure your back-up isn't connected to your live data source, so that any malicious activity doesn't reach it.

- The same goes for mobile phones. Most come with capabilities to backup to Cloud. This should be set up and regularly backed up. Further information and how-to's here

Keeping Your Data Safe

Be Wary of Suspicious Emails

You need to know how to spot suspicious emails. Look out for signs such as bad grammar, demands for you to act urgently and requests for payment. New technologies mean that email attacks are becoming more sophisticated. A phishing email could appear to come from a source you recognise. If you're not sure, speak to the sender.

Antivirus

Install anti-virus and malware protection and keep it up to date - You must make sure the devices you and your employees use at home, or when you're working away, are secure. Anti-virus software can help protect your device against malware sent through a phishing attack. Anti-virus is not necessarily required on smart phone or tablets if apps have been installed via Google Play or Apple's AppStore as they are screened when added to the stores.

Protect Your Device When it's Unattended

Lock your screen when you're temporarily away from your desk to prevent someone else accessing your computer. If you do need to leave your device for longer, put it in a secure place, out of sight.

Make Sure your Wi-Fi Connection is Secure

Using public Wi-Fi, or an insecure connection, could put personal data at risk. You should make sure you always use a secure connection when connecting to the internet. If you're using a public network, consider using a secure Virtual Private Network (VPN). VPN software can be found on all app stores for the various smart device, recommendations later in this document.

Children and Mobile Phones - Good Safety and Awareness Practices

Setting Boundaries

It's important to set boundaries and limits with your kids. Talk to them about the boundaries themselves, and your reasons for setting them. These boundaries could include screen time limits, restrictions on what apps they can use or where they can use their phone.

By setting these limits, you can encourage children to still enjoy activities that stimulate their minds in other ways, such as sports, board games or reading. It also allows you to reclaim family time and ensure your child isn't using age-inappropriate apps.

Utilize Parental Controls

Parental controls allow you to see exactly what sites and apps your child is accessing on their smartphone, tablet, or computer. It also lets you see how long they are spending on these devices.
While there are many parental control apps to choose from, the standard choice is Google Family Link. Free to use, Google Family Link works with both Apple and Android devices.

While you still may want to use a parental control app to check what your child is doing online, it's always good to engage with them directly as well. By encouraging them to share what they are doing on their phone, you may get a better insight into risks such as cyberbullying or their social network use.

Teach Children Phone Security

By teaching your child a few security measures now, you will help them keep their devices secure in the long run. Examples include:

- Don't connect to public wi-fi as that may give hackers access to your child's phone and information.
- Don't share passwords with friends or strangers.
- Don't overshare online – once a photo or video is out there, it can't be taken back.
- Keep your phone close in your bag or on-hand rather than leaving it in public places where it can be stolen.
- Password protect the phone so that if it is stolen, personal photos or messages can't be easily accessed.

Keeping Your Data Safe

Password Security

Use Strong Passwords and Multi-Factor Authentication

Make sure you use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored. They must be difficult to guess. The National Cyber Security Centre (NCSC) recommends using three random words.

Where possible, you should consider using multi-factor authentication. Multi-factor authentication is a security measure to make sure the right person is accessing the data. It requires at least two separate forms of identification before access is granted. For example, you use a password and a one-time code which is sent by text message. Online banking login is a prime example of this.

Email Security: Different Password

Use a strong and separate password for your email account. Your email address is often used as backup access for forgotten passwords for other accounts. An intruder or criminal may be able to

- Access private information about you (including your banking details)
- Post emails and messages pretending to be from you (and use this to trick other people)
- Reset all your other account passwords (and get access to all your other online accounts)

Password Managers

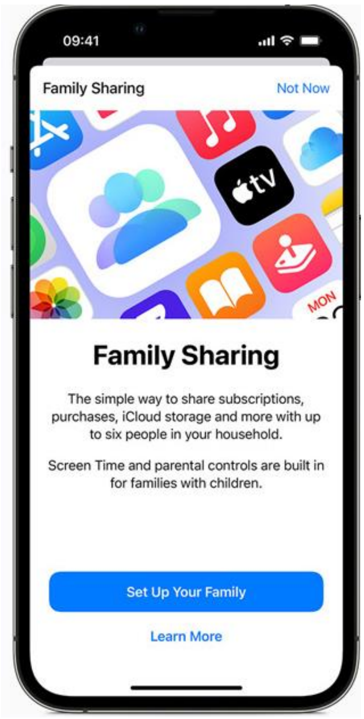
Using a password manager can help you create and remember passwords. Further information on password managers is at the end of this document.

Keeping Your Data Safe

How-to's and Recommendations

Apple Family Sharing

Family Sharing lets you and up to five other family members share access to amazing Apple services like Apple Music, Apple TV+, Apple News+ and Apple Arcade. Your group can also share iTunes, Apple Books and App Store purchases, an iCloud storage plan, and a family photo album. You can even help locate each other's missing devices.



Family Sharing

Not Now

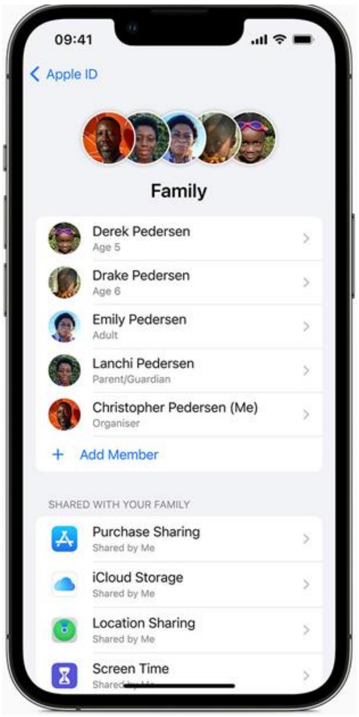
Family Sharing

The simple way to share subscriptions, purchases, iCloud storage and more with up to six people in your household.

Screen Time and parental controls are built in for families with children.

Set Up Your Family

Learn More



Apple ID

Family

Derek Pedersen
Age 5

Drake Pedersen
Age 6

Emily Pedersen
Adult

Lanchi Pedersen
Parent/Guardian

Christopher Pedersen (Me)
Organiser

+ Add Member

SHARED WITH YOUR FAMILY

Purchase Sharing
Shared by Me

iCloud Storage
Shared by Me

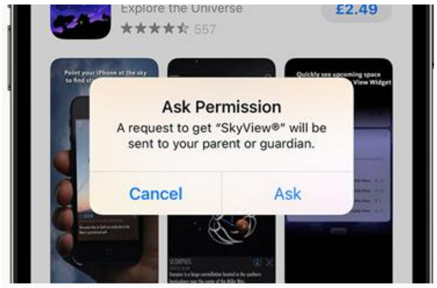
Location Sharing
Shared by Me

Screen Time

One adult in your family — the organiser — invites all the other members to join and sets up accounts for anyone under 13. Once family members join, Family Sharing is set up on everyone's devices automatically. The group then chooses which services and features they'd like to use and share

Making purchases is easy. So is setting limits.

When your family sets up purchase sharing, all new Apple Books and App Store purchases will be billed to the organiser's account. But if Ask to Buy is turned on for children in the family, the organiser can still call the shots. When a child initiates a purchase, an alert is sent to the organiser, who can review the download and approve or decline it from their own device. This applies to both purchases and free downloads.



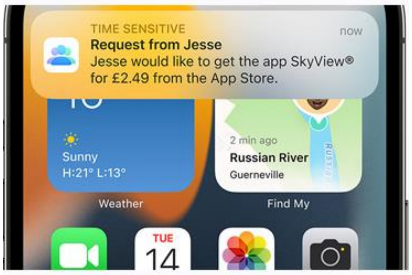
Explore the Universe £2.49

Ask Permission

A request to get "SkyView®" will be sent to your parent or guardian.

Cancel Ask

They ask to buy.
Before your children can make a purchase, they must ask your permission.



TIME SENSITIVE now

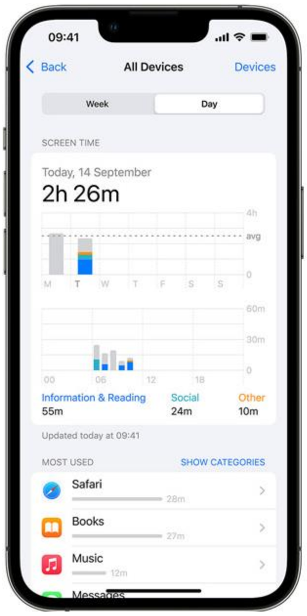
Request from Jesse
Jesse would like to get the app SkyView® for £2.49 from the App Store.

You reply from anywhere.
A notification appears on your device. You can review the request, then approve or decline it.

Keeping Your Data Safe

Screen Time Usage

Screen Time can give you a better understanding of how much time your kids spend using apps, visiting websites, and on their devices overall. When you use Screen Time with Family Sharing, you can review your kids' activity reports and set time limits for specific apps from your own device. You can also name another family member as a parent/guardian, so that you're always on the same page when it comes to your kids and their screen time.



09:41

Back All Devices Devices

Week Day

SCREEN TIME

Today, 14 September

2h 26m

Information & Reading 55m

Social 24m

Other 10m

Updated today at 09:41

MOST USED SHOW CATEGORIES

Safari 28m

Books 27m

Music 12m

Messages

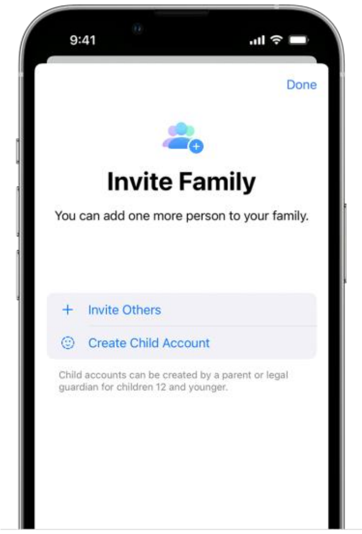
TIME SENSITIVE now

Time Check

5 minutes remaining for Games today.

Start a Family Group

One adult in the family — the family organizer — can set up Family Sharing for the group from their iPhone, iPad, iPod touch, or Mac. If purchase sharing is turned on, the family organizer pays for family members' purchases and must have a valid payment method on file.3



9:41

Done

Invite Family

You can add one more person to your family.

+ Invite Others

Create Child Account

Child accounts can be created by a parent or legal guardian for children 12 and younger.

On your iPhone, iPad, or iPod touch

1. Go to Settings.
2. Tap your name.
3. Tap Family Sharing, then tap Set Up Your Family.
4. Follow the onscreen instructions to set up your family and invite your family members.

Invite People to Join your Family

If you choose to invite people later or want to add another member to your family, you can send an invitation via Messages, email, or in person. If you have multiple Apple IDs, you can invite each of your accounts to the group, so you can share purchases from your other Apple IDs with your family.

On your iPhone or iPad with iOS 16 or later

1. Go to Settings.
2. Tap Family.
3. Tap Add Member
4. If your child doesn't have an Apple ID, tap Create an Account for a Child. But if your child already has an Apple ID, tap Invite People. They can enter their Apple ID password on your device to accept the invitation.

5. Follow the onscreen instructions to set up parental controls, location sharing, and more.

How to Create an Apple ID for your Child

Children under the age of 13 can't create an Apple ID on their own. (This age varies by region.) But if you're the family organizer or a guardian, you can create an Apple ID for your child.

On your iPhone, iPad or iPod touch

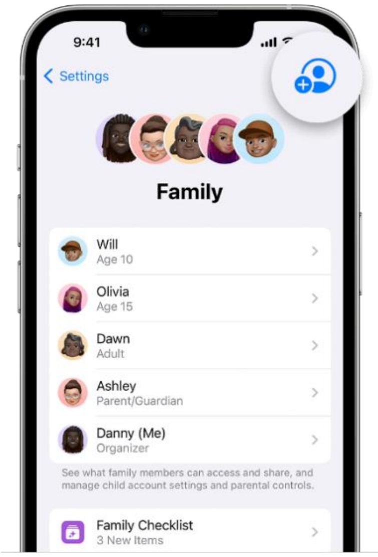
To verify that you're an adult, you need a credit card. On your iPhone, you can also use a driving licence or state ID added to Wallet where available.

In iOS 16 or iPadOS 16 or later

1. Go to Settings > Family.
2. Tap the Add Member button
3. Tap Create Child Account, then tap Continue.
4. Enter the child's name and birth date. Make sure you enter the correct date of birth – you can't change it later.
5. Follow the onscreen instructions to finish setting up the account. For your child's Apple ID, you can use their email address, the suggested @icloud.com address or their Game Center nickname.

In iOS 15 or iPadOS 15 or earlier

1. Go to Settings.
2. Tap your name, then tap Family Sharing.
3. Tap Add Member.
4. Tap Create an Account for a Child, then tap Continue.
5. Follow the onscreen instructions to finish setting up the account. You can use the child's email address for their Apple ID, or their Game Center nickname. Make sure you enter the correct date of birth – you can't change it later.



9:41

Settings

Family

Will
Age 10

Olivia
Age 15

Dawn
Adult

Ashley
Parent/Guardian

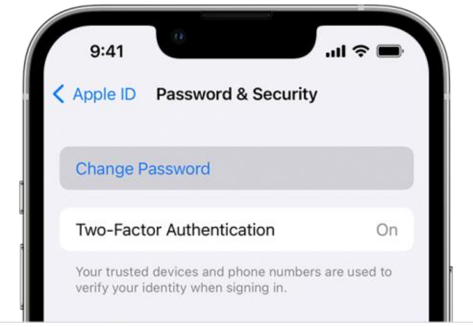
Danny (Me)
Organizer

See what family members can access and share, and manage child account settings and parental controls.

Family Checklist
3 New Items

Change your Apple ID password on your iPhone, iPad, iPod touch or Apple Watch

1. Tap Settings > your name > Password & Security.
2. Tap Change Password.
3. Enter your current password or device passcode, then enter a new password and confirm the new password. Forgotten your password?
4. Tap Change or Change Password.



9:41

Apple ID Password & Security

Change Password

Two-Factor Authentication On

Your trusted devices and phone numbers are used to verify your identity when signing in.

Change your child's Apple ID password

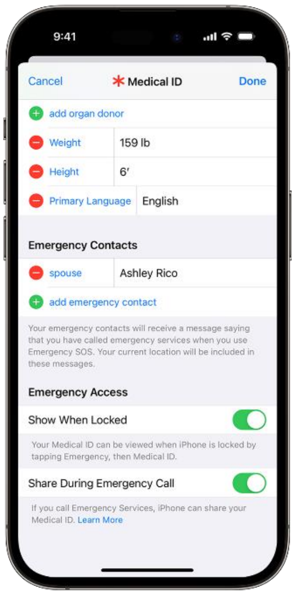
If you have an iPhone or iPad with the latest version of iOS or iPadOS and two-factor authentication turned on for your Apple ID, you can change the Apple ID password for a child account in your Family Sharing group.

1. Tap Settings > Family > your child’s account.
2. Tap Apple ID & Password.
3. Tap Change [Child’s Name] Password.
4. Enter your device passcode and follow the onscreen instructions.

Keeping Your Data Safe

Set Up Emergency Contacts

With Emergency SOS, you can quickly and easily call for help and alert your emergency contacts.



Cancel | * Medical ID | Done

⊕ add organ donor

⊖ Weight	159 lb
⊖ Height	6′
⊖ Primary Language	English

Emergency Contacts

⊖ spouse	Ashley Rico

⊕ add emergency contact

Your emergency contacts will receive a message saying that you have called emergency services when you use Emergency SOS. Your current location will be included in these messages.

Emergency Access

Show When Locked ●

Your Medical ID can be viewed when iPhone is locked by tapping Emergency, then Medical ID.

Share During Emergency Call ●

If you call Emergency Services, iPhone can share your Medical ID. Learn More

Add emergency contacts

1. Open the Health app and tap your profile picture 👤.
2. Tap Medical ID.
3. Tap Edit, then scroll to Emergency Contacts.
4. Tap the Add button ⊕ to add an emergency contact.
5. Tap a contact, then add their relationship.
6. Tap Done to save your changes.

Remove emergency contacts

1. Open the Health app and tap your profile picture 👤.
2. Tap Medical ID.
3. Tap Edit, then scroll to Emergency Contacts.
4. Tap the Delete button ⊖ next to a contact, then tap Delete.
5. Tap Done to save your changes.

Call the emergency services

Make the call on iPhone 8 or later:

In iOS 16.3, you release the buttons after the countdown to make an emergency services call.

1. Press and hold the side button and one of the volume buttons until the Emergency SOS slider appears.
2. Drag the Emergency Call slider to call the emergency services. If you continue to hold down the side button and volume button, instead of dragging the slider, a countdown will start and an alert will sound. If you release the buttons after the countdown, your iPhone will call the emergency services automatically.

Make the call on iPhone 7 or earlier:

1. Press the side (or top) button five times rapidly. The Emergency Call slider will appear.
2. Drag the Emergency SOS slider to call the emergency services.

After the call has ended, your iPhone will send your emergency contacts a text message with your current location, unless you choose to cancel. If Location Services is turned off, it will turn on temporarily. If your location changes, your contacts will get an update and you'll receive a notification about 10 minutes later.

Data Backup

1. Go to Settings > [your name] > iCloud > iCloud Backup.
2. Turn on iCloud Backup.
3. iCloud automatically backs up your iPhone daily when iPhone is connected to power, locked, and connected to Wi-Fi.

Note: On models that support 5G, your carrier may give you the option to back up iPhone using your cellular network. Go to Settings > [your name] > iCloud > iCloud Backup, then turn on or off Backup Over Cellular.

4. To perform a manual backup, tap Back Up Now.
5. To view your iCloud backups, go to Settings > [your name] > iCloud > Manage Account Storage > Backups. To delete a backup, choose a backup from the list, then tap Delete & Turn Off Backup.

Note: If you turn on an app or feature to use iCloud syncing (in Settings > [your name] > iCloud > Show All), its information is stored in iCloud. Because the information is automatically kept up to date on all your devices, it’s not included in your iCloud backup. (See the Apple Support article What does iCloud back up?)

Keeping Your Data Safe

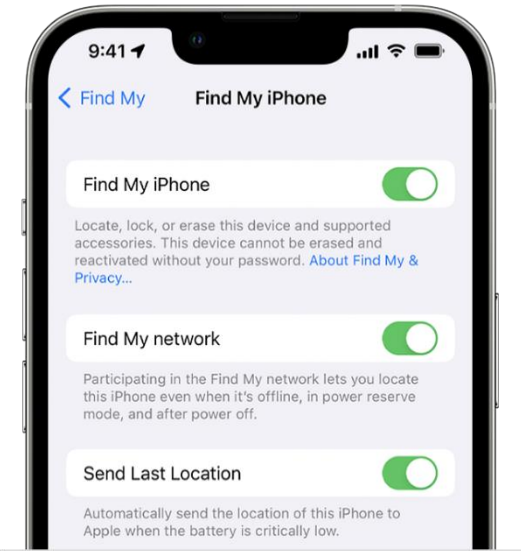
Link - https://support.apple.com/en-gb/guide/iphone/iph3ecf67d29/ios

Set Up Remote Locate/Wipe/Lock Features

Crucial for if a phone has been lost or stolen, the remote locate, wipe and lock features on Smartphones will ensure the data on your phone is easily wiped or your phone relocated. This section will show how to enable this.

How to turn on Find My for your iPhone, iPad or iPod touch

1. Open the Settings app.
2. Tap your name, then tap Find My.
3. If you want friends and family to know where you are, turn on Share My Location.
4. Tap Find My [device] and then turn on Find My [device]
5. To see your device even when it's offline, turn on Find My network*
6. To have the location of your device sent to Apple when the battery is low, turn on Send Last Location.
7. If you want to be able to find your lost device on a map, make sure Location Services is turned on. To do this, go to Settings > Privacy & Security > Location Services and turn on Location Services.



Find My iPhone

Locate, lock, or erase this device and supported accessories. This device cannot be erased and reactivated without your password. About Find My & Privacy...

Find My network

Participating in the Find My network lets you locate this iPhone even when it's offline, in power reserve mode, and after power off.

Send Last Location

Automatically send the location of this iPhone to Apple when the battery is critically low.

* The Find My network is an encrypted, anonymous network of hundreds of millions of Apple devices that can help you locate your device.

How to add your AirPods, Apple Watch or Beats product to Find My

If your AirPods, Apple Watch or supported Beats product are paired with your iPhone, they're automatically set up when you turn on Find My iPhone.

To make sure you can find your devices even if they're powered off or disconnected, check that Find My network is turned on.

Turn on Find My network for AirPods Pro or AirPods Max

1. Go to Settings > Bluetooth.
2. Tap the More Info button ⓘ next to your device in the list.
3. Scroll down to Find My network.
4. Make sure Find My network is turned on.

Turn on Find My network for Apple Watch

1. On your Apple Watch, open Settings.
2. Tap your name.
3. Scroll down until you see your Apple Watch.
4. Tap your watch name, then tap Find My Watch.
5. Make sure Find My network is turned on.

Erase a device on iCloud.com

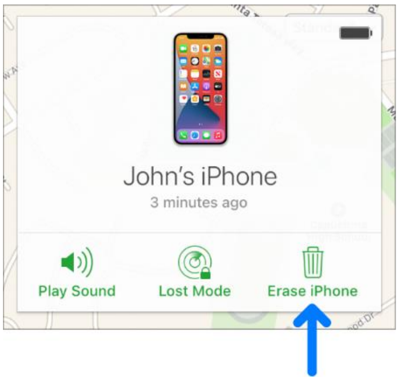
To sign in to Find Devices, go to icloud.com/find.

What happens when you erase a device in Find Devices?

1. A confirmation email is sent to your Apple ID email address.
2. Activation Lock remains on to protect it. Your Apple ID and password are required to reactivate the device.

3. If you erase a device that has iOS 15, iPadOS 15 or later installed, you can use Find Devices to locate or play a sound on the device. Otherwise, you will not be able to locate or play a sound on it. You may still be able to locate your Mac or Apple Watch if it is near a previously used Wi-Fi network.

Remotely erase your device or a family member's device



1. In Find Devices on iCloud.com, click All Devices, then select the device you want to erase.
2. If you do not see All Devices, it is because you have already selected a device. Click the name of the current device in the center of the Find Devices toolbar to see the Devices list, then select a new device.
3. Click Erase [device].
4. A confirmation email is sent to your Apple ID email address.
5. Activation Lock remains on to protect it. Your Apple ID and password are required to reactivate the device.
6. If you erase a device that has iOS 15, iPadOS 15 or later installed, you can use Find Devices to locate or play a sound on the device. Otherwise, you will not be able to locate or play a sound on it. You may still be able to locate your Mac or Apple Watch if it is near a previously used Wi-Fi network.

Cancel an erase

If your device is offline, the remote erase happens the next time it is online. If you find the device before it is erased, you can cancel the request.

1. In Find Devices on iCloud.com, click All Devices, then select the device.
2. If you do not see All Devices, it is because you have already selected a device. Click the name of the current device in the centre of the Find Devices toolbar to see the Devices list, then select a new device.
3. Click Stop Erase Request, then enter your Apple ID password.

Secure AirDrop

AirDrop is used to share and receive photos, documents, and more with other Apple devices that are nearby. Negate unwanted photos or documents by securing your Apple devices.

Keeping Your Data Safe

To choose who can see your device and send you content in AirDrop:

1. Go to Settings, then tap General.
2. Tap AirDrop, then choose an option.

You can also set your AirDrop options in Control Centre:

1. On iPhone X or later, swipe down from the upper-right corner of the screen to open Control Centre. Or follow the same motion to open Control Centre on your iPad with iOS 12 or later or iPadOS. On your iPhone 8 or earlier, swipe up from the bottom of the screen.
2. Press firmly or touch and hold the network settings card in the upper-left corner.
3. Touch and hold the AirDrop button, then choose one of these options:
   a. Receiving Off: You won't receive AirDrop requests.
   b. Contacts Only: Only your contacts can see your device.
   c. Everyone: All nearby Apple devices using AirDrop can see your device. When you set your AirDrop option to Everyone in iOS 16.2 or later, your option reverts to Contacts Only after 10 minutes.

If you see Receiving Off and can't tap to change it:

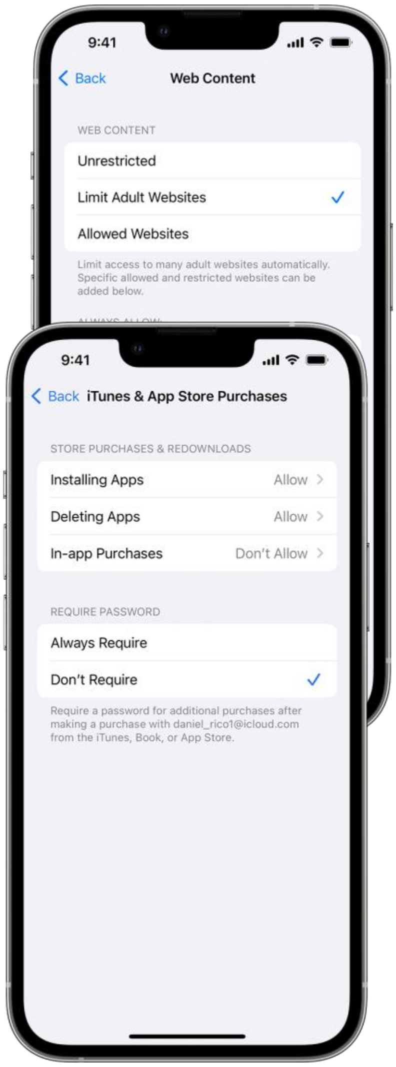
1. Go to Settings > Screen Time.
2. Tap Content & Privacy Restrictions.
3. Tap Allowed Apps and make sure that AirDrop is turned on.

Keeping Your Data Safe

Filter Web Content

iOS and iPadOS can filter website content automatically to limit access to adult content in Safari and other apps on your device. You can also add specific websites to an approved or blocked list, or you can limit access to only approved websites.

1. Go to Settings and tap Screen Time.
2. Tap Content & Privacy Restrictions and enter your Screen Time passcode.
3. Tap Content Restrictions, then tap Web Content.
4. Choose Unrestricted Access, Limit Adult Websites or Allowed Websites.



9:41

< Back Web Content

WEB CONTENT

Unrestricted

Limit Adult Websites ✓

Allowed Websites

Limit access to many adult websites automatically. Specific allowed and restricted websites can be added below.

9:41

< Back iTunes & App Store Purchases

STORE PURCHASES & REDOWNLOADS

Installing Apps	Allow >
Deleting Apps	Allow >
In-app Purchases	Don't Allow >

REQUIRE PASSWORD

Always Require

Don't Require ✓

Require a password for additional purchases after making a purchase with daniel_rico1@icloud.com from the iTunes, Book, or App Store.

Prevent iTunes & App Store Purchases

You can also prevent your child from being able to install or delete apps, make in-app purchases and more. To prevent iTunes & App Store purchases or downloads:

1. Go to Settings and tap Screen Time.
2. Tap Content & Privacy Restrictions. If asked, enter your passcode.
3. Tap iTunes & App Store Purchases.
4. Choose a setting and set to Don't Allow.

You can also change your password settings for additional purchases from the iTunes & App Store or Book Store. Follow steps 1–3, then choose Always Require or Don't Require.

Prevent Explicit Content and Content Ratings

You can also prevent the playback of music with explicit content and films or TV programmes with specific ratings. Apps also have ratings that can be configured using content restrictions.

To restrict explicit content and content ratings:

1. Go to Settings and tap Screen Time.
2. Tap Content & Privacy Restrictions, then tap Content Restrictions.
3. Choose the settings you want for each feature or setting under Allowed Store Content.

Here are the types of content you can restrict:

- Music, Podcasts, News, Fitness: prevent the playback of music, music videos, podcasts, news and workouts containing explicit content
- Music Videos: prevent finding and viewing music videos
- Music Profiles: prevent sharing what you're listening to with friends and seeing what they're listening to
- Films: Prevent films with specific ratings
- TV Programmes: prevent TV programmes with specific ratings
- Books: Prevent content with specific ratings
- Apps: Prevent apps with specific ratings
- App Clips: prevent app clips with specific ratings

Android

Set up a Child Account on an Android Device – Using Family Link

For kids and teens - Family Link supervision can run on Android devices with version 7.0 (Nougat) and higher. Devices running Android versions 5.0 and 6.0 (Lollipop and Marshmallow) may also be able to have Family Link settings applied to them.

For parents - Parents can run Family Link on Android devices running versions 5.0 (Lollipop) and higher, and iPhones running iOS 11 and higher.

1. Download the Family Link app from the Google Play Store.

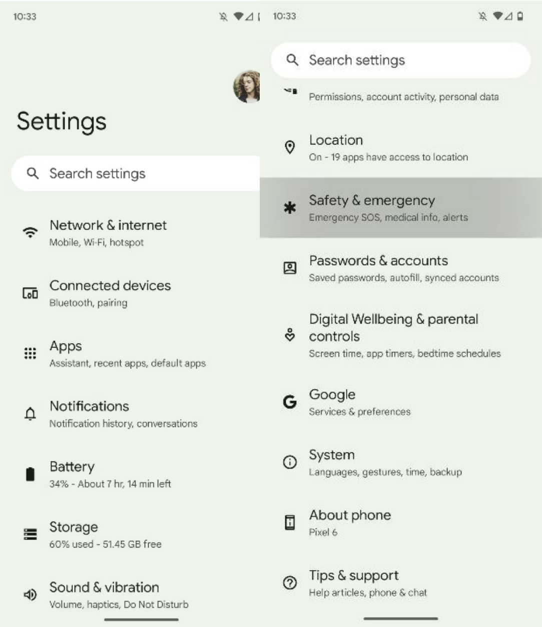
Keeping Your Data Safe

2. Open the Family Link app .
3. If you don't have the Family Link app, visit the [Family Link setup page]() to get started.
4. At the top left, tap Menu ≡ › Add child .
5. Follow the on-screen instructions.
6. When you're done, you'll get an on-screen confirmation.

Android 12 and 13

Add emergency contacts

1. Open the Settings app.
2. Scroll down and tap Safety & emergency.
   This menu can be found in the Advanced Settings menu on earlier versions of Android (Android 11 and earlier).
3. Tap Emergency contacts.
4. Tap Add contact.
5. Select emergency contacts from your contact list.
   If you wish to add someone who isn't on your contacts list, add them through the Contacts app first.



10:33

Settings

Search settings

Network & internet
Mobile, Wi-Fi, hotspot

Connected devices
Bluetooth, pairing

Apps
Assistant, recent apps, default apps

Notifications
Notification history, conversations

Battery
34% - About 7 hr, 14 min left

Storage
60% used - 51.45 GB free

Sound & vibration
Volume, haptics, Do Not Disturb

10:33

Search settings

Permissions, account activity, personal data

Location
On - 19 apps have access to location

Safety & emergency
Emergency SOS, medical info, alerts

Passwords & accounts
Saved passwords, autofill, synced accounts

Digital Wellbeing & parental controls
Screen time, app timers, bedtime schedules

Google
Services & preferences

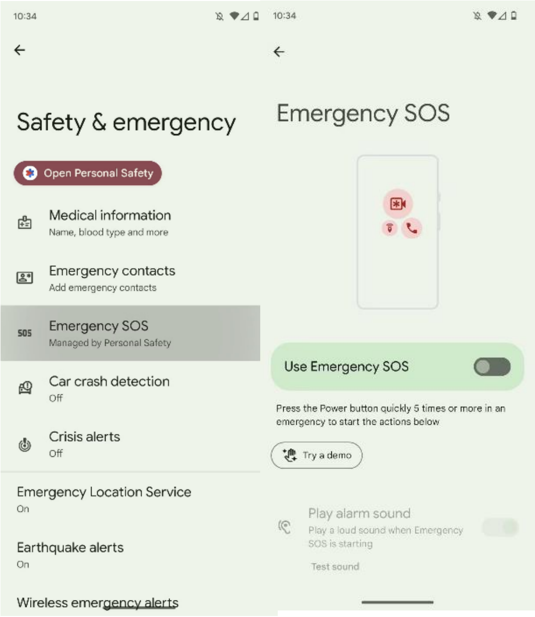
System
Languages, gestures, time, backup

About phone
Pixel 6

Tips & support
Help articles, phone & chat

Turn On Emergency Contacts

1. Open the Settings app on your phone.
2. Scroll down and tap Safety & Emergency. On earlier versions of Android, the Safety & Emergency menu can be found in the Advanced Settings menu.
3. Tap Emergency SOS.
4. Toggle the Use Emergency SOS slider.



10:34

Safety & emergency

Open Personal Safety

Medical information
Name, blood type and more

Emergency contacts
Add emergency contacts

Emergency SOS
Managed by Personal Safety

Car crash detection
Off

Crisis alerts
Off

Emergency Location Service
On

Earthquake alerts
On

Wireless emergency alerts

10:34

Emergency SOS

Use Emergency SOS

Press the Power button quickly 5 times or more in an emergency to start the actions below

Try a demo

Play alarm sound
Play a loud sound when Emergency SOS is starting

Test sound

How to Share Information with Emergency Contacts

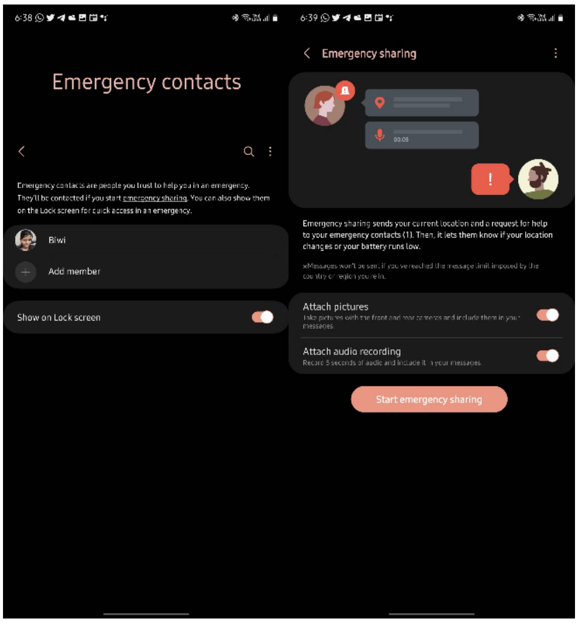
1. On the Emergency SOS menu, tap Share info with emergency contacts.
2. Tap Next to begin setup.
3. If you haven't created any emergency contacts, tap Add contact to create some. Tap Next after adding your contacts.
4. Toggle the switches to choose what information you want to share. To share only your location, tap Skip.
5. Tap Next to set location permission to Allow all the time in Google Maps.
6. Toggle the switches to choose what information you want to share. To share only your location, tap Skip.
7. Tap Next to set location permission to Allow all the time in Google Maps.

Keeping Your Data Safe

Samsung Phones (One UI)

Turn On Emergency Contacts

1. Open the Settings app.
2. Scroll down and tap Safety & Emergency. This option is in the Advanced Settings menu on One UI 3.
3. Select Emergency Contacts. Tap Add member and add your emergency contacts to the list. You can enable the same on the lock screen to access them quickly in an unfortunate situation.
4. Go back and select Emergency Sharing.
5. Enable the Attach pictures and Attach audio recording toggles
6. Go back and select Emergency SOS.
7. Enable Share info with emergency contacts toggle.



Emergency contacts

Emergency contacts are people you trust to help you in an emergency. They'll be contacted if you start emergency sharing. You can also show them on the Lock screen for quick access in an emergency.

Biwi

Add member

Show on Lock screen

Emergency sharing

Emergency sharing sends your current location and a request for help to your emergency contacts (1). Then, it lets them know if your location changes or your battery runs low.

*Messages won't be sent if you've reached the message limit imposed by the country or region you're in.

Attach pictures
Take pictures with the front and rear cameras and include them in your messages.

Attach audio recording
Record 5 seconds of audio and include it in your messages.

Start emergency sharing

Android Backup – Google One

To automatically back up your phone;

Important: To help protect your backed-up data, use a PIN, pattern or password screen lock instead of a swipe or Smart Lock.

You can set up your device to automatically back up your files.

1. Open your device's Settings app.
2. Select Google And then Backup.
   a. Tip: If this is your first time, turn on Backup by Google One and follow the on-screen instructions.
3. Tap Back up now.

Your Google One backup can take up to 24 hours. When your data is saved, 'On' will be displayed below the data types that you selected.

Link - https://support.google.com/android/answer/2819582?hl=en-GB

Lock & Erase

1. On a browser, go to android.com/find.
2. Sign in to your Google Account.
   a. If you have more than one device: At the top of the sidebar, select the lost device.
   b. If your lost device has more than one user profile: Sign in with a Google Account that's on the main or personal profile. Learn about user profiles.
3. The lost device gets a notification.
4. On the map, you'll get info about where the device is.
   a. The location is approximate and may not be accurate.
   b. If your device can't be found, you may find its last known location, if available.
5. If you get a prompt, tap Enable lock & erase.
6. Select what you want to do:
   a. Play sound: Rings your device at full volume for 5 minutes, even if it's set to silent or vibrate.
   b. Secure device: Locks your device with your PIN or password. If you don't have a lock, you can set one. To help someone return your device to you, you can add a message or device number to the lock screen.
   c. Erase device: Permanently deletes all data on your device, but may not delete SD cards. After you erase, Find My Device won't work on the device.

Find My Device App

1. On another Android phone or tablet, open the Find My Device app .

   a. If the other device doesn't yet have the app, get it on Google Play.

2. Sign in.
   a. If your own device is lost: Tap Continue as [your name].
   b. If you're helping a friend: Tap Sign in as guest and let your friend sign in.
3. From the listed devices, select the device you want to locate.
   a. You’ll find the same options listed in the above steps.
4. You may be prompted to provide the lock screen PIN for the Android device you want to locate. This applies to Android 9 or higher. If the device you want to find doesn’t use a PIN, or runs Android 8 or lower, you may be prompted for your Google password.
5. Follow the same steps on find, lock, or erase a device remotely.

Keeping Your Data Safe

Parental Control & Monitoring Apps

Parental controls allow you to block and filter upsetting or inappropriate content. They work across your Wi-Fi, phone network, individual apps and devices. Parental controls can help you to: plan what time of day your child can go online and how long for. The below are some recommended options.

Qustudio Parental Control

- Device Limits - 5/10/15
- Free Version – Paid for enhanced features
- Geofencing
- Per-User Settings
- Remote Management
- Screen Time Management
- Social Network Monitoring
- Supports Android
- Supports iOS
- Supports macOS
- Supports Windows
- Web Filtering
- Well-designed web interface
- Comprehensive time restrictions
- App blocking on desktop and mobile platforms
- Cross-platform support
- Intuitive apps

Norton Family Premier

- Device Limits - None
- Per-User Settings
- Remote Management
- Screen Time Management
- Social Network Monitoring
- Supports Android
- Supports iOS
- Supports Windows
- Web Filtering
- Affordable
- Comprehensive web dashboard
- No limit on the number of monitored devices
- Easy setup and configuration
- Excellent geofencing tools
- House Rules encourage family dialogue about online safety

Keeping Your Data Safe

OurPact

- View – Capture automated periodic, on-demand or gallery views of your children’s online activity, all encrypted for safety.
- App Blocker – Block internet, text messages, and apps at-a-touch
- App Rules – Block & allow specific apps
- Block/Allow Websites – Prevent access to specific websites, including adult content, for safe internet browsing
- Block Texting - Block access or set rules for texting apps
- New App Alerts – Receive alerts when new apps are installed on your child’s device
- Block Schedules – Automate your family’s daily routine
- Screen Time Allowance – Set daily screen time limits for your kids
- Geofencing with Places – create GPS geofences around specific locations and receive real-time alerts when their kids leave and arrive at home, school or any set zone
- Find My Family – Allows parents to locate any family member using geolocation and geofences.

mSpy

- 100% invisible and undetected
- Tracks location
- Geofencing option available
- Monitors calls, SMS, and chosen apps

Password Managers

- Keeper - https://www.keepersecurity.com/affiliate/keeper-50off-unlimited.html?LSNSUBSITE=LSNSUBSITE
- NordPass - https://bi.cybernews.com/nordpass-p/
- RoboForm - https://bi.cybernews.com/roboform-uk/

Further details available - https://uk.cybernews.com/lp/best-password-managers-uk/?campaignId=18337685514&adgroupId=140872143306&adId=621920655313&targetId=kwd-15871195944&device=c&gunique=EAIaIQobChMI1KKVuobB_wIVEN7tCh1acAEPEAAYASAAEgKWv_D_BwE&gad=1&gclid=EAIaIQobChMI1KKVuobB_wIVEN7tCh1acAEPEAAYASAAEgKWv_D_BwE

Keeping Your Data Safe

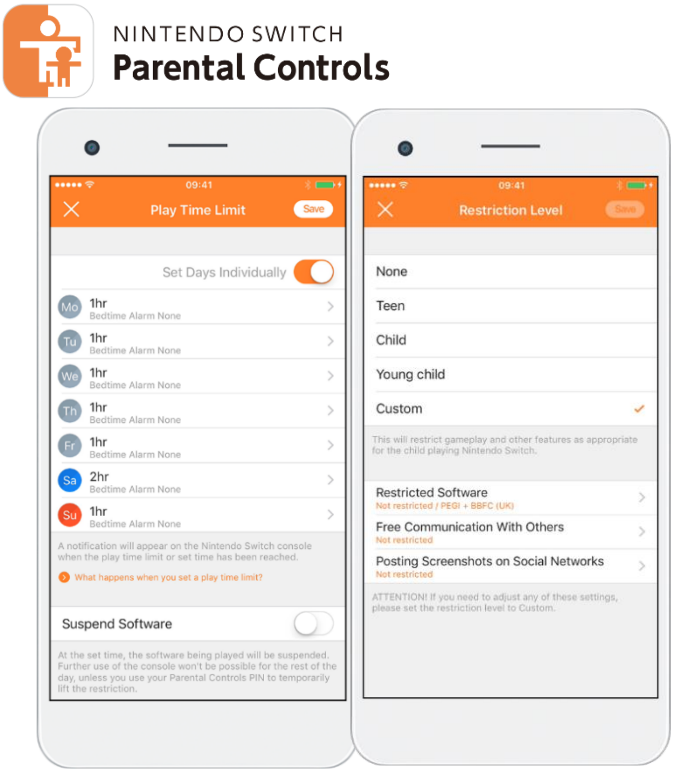
Media & Gaming

Nintendo Switch Parental Controls

The Nintendo Switch Parental Controls smart device app is a free smart device app which you can link with Nintendo Switch to easily monitor what and how your children are playing. If you do not have a smart device, you can also set certain restrictions on Nintendo Switch directly.

Features

- Gameplay time monitoring
- Monitor the game being played
- Age restrictions



09:41

Play Time Limit — Save

Set Days Individually ●

Mo 1hr
Bedtime Alarm None

Tu 1hr
Bedtime Alarm None

We 1hr
Bedtime Alarm None

Th 1hr
Bedtime Alarm None

Fr 1hr
Bedtime Alarm None

Sa 2hr
Bedtime Alarm None

Su 1hr
Bedtime Alarm None

A notification will appear on the Nintendo Switch console when the play time limit or set time has been reached.

What happens when you set a play time limit?

Suspend Software ○

At the set time, the software being played will be suspended. Further use of the console won't be possible for the rest of the day, unless you use your Parental Controls PIN to temporarily lift the restriction.

09:41

Restriction Level — Save

None

Teen

Child

Young child

Custom ✓

This will restrict gameplay and other features as appropriate for the child playing Nintendo Switch.

Restricted Software
Not restricted / PEGI + BBFC (UK)

Free Communication With Others
Not restricted

Posting Screenshots on Social Networks
Not restricted

ATTENTION! If you need to adjust any of these settings, please set the restriction level to Custom.

PlayStation 4 and 5

Parental controls and spending limits work alongside family management and playtime controls to help you manage your child's activity on PlayStation™Network.

How to set parental controls online

1. Sign into Account Management > Family Management.
2. Select the child family member you want to set restrictions for and select Edit to adjust each feature.

PS5 Console: Set Parental Controls

1. Go to Settings > Family and Parental Controls > Family Management.
2. Select the child family member you want to set restrictions for and select a feature to adjust.

PS4 Console: Set Parental Controls

1. Go to Settings > Parental Controls/Family Management > Family Management.
2. Select the child family member you want to set restrictions for and select a feature to adjust.

Further Help - https://www.playstation.com/en-gb/support/account/ps5-parental-controls-spending-limits/#set

YouTube

To hide potentially mature videos on the phone app, restricted mode can be enabled. Having an account will help to track history. To create an account, an age of 13 years or older is required.

Enable Restricted Mode

Go to Settings > General > Enable Restricted Mode

Note: Restricted mode is not 100% guaranteed to restrict all harmful videos.

Keeping Your Data Safe

YouTube Kids

YouTube Kids is a separate app and website created by YouTube that offers more filters and restrictions to help stop children coming across inappropriate content.

There are also additional parental control features available depending on your child’s age. You can choose between three age-based content settings:

- Preschool (Ages 4 and under)
- Younger (Ages 5–8)
- Older (Ages 9–12)

You can create individual user profiles for more than one child.

While the platform uses a range of different filters to stop adult content from playing, these aren’t always 100% effective. It’s always recommend supervising your child when they're watching videos or watching them to make sure they are suitable.

There are also no communication features available.

Keeping Your Data Safe

Home Security

Computer/Laptops

Backup

Computer Backup Software – www.idrive.com
Beginner's Guide to Computer Backups - https://uk.pcmag.com/onlinecloud-backup-services/8647/the-beginners-guide-to-pc-backup

Antivirus Software

- AVG – http://avg.com – Free, basic version available.
- Norton – http://norton.com
- McAfee - https://www.mcafee.com/consumer

Further details - https://uk.cybernews.com/lp/best-antivirus-software-uk/?campaignId=18368984628&adgroupId=140856403825&adId=635215681672&targetId=aud-1405169530316:kwd-11713941&device=c&gunique=EAIaIQobChMInL2orYjB_wIVCLztCh1clwbtEAAYAiAAEgINivD_BwE&gad=1&gclid=EAIaIQobChMInL2orYjB_wIVCLztCh1clwbtEAAYAiAAEgINivD_BwE

VPN Software

- NordVPN
- SurfShark
- TunnelBear

Broadband Routers & Wireless Network Safety

The standard home internet routers provide by local internet companies (JT Global, Sure etc.) are basic and provide little filtering or security options. It is recommended to replace these with one that provides more security in general. The below have been selected based on their ability to provide additional parental security.

Recommended Routers with Parental Controls

- Asus ROG Rapture GT-AX11000 – High Price
- TP-Link Archer AX20 – Good value
- TP-Link Archer AX50 – Good value
- Asus RT-AX68U
- Synology RT2600ac

Note: Most of these are available on Amazon.

Wireless Network Safety

Have cybersecurity in your home. The easiest way to protect yourself is to have cybersecurity for your home network(s). We recommend Total Security for the most comprehensive protection or Kaspersky Security Cloud to cover multiple devices.

WPA2 encryption should be active on your wireless network connection. This is the modern industry-standard for web security. But the important bit is that your data will be scrambled as it is sent and received. If someone intercepts this, they will not be able to unlock and read it.

Keeping Your Data Safe

Update your wireless network password. This is the Wi-Fi code you enter to connect your device to the internet. If you've made it something simple for convenience, upgrade it immediately. Convenience can be dangerous if it leaves you open to a malicious attack.

Change the default router password. As the heart of your internet data stream, having a strong router password is invaluable. This is different from your Wi-Fi password. Don't reuse passwords and always make each passcode a unique blend of uppercase, lowercase, numbers, and symbols.

Consider a dedicated 'guest' network to avoid unprotected device access. Your wireless network connects all your devices, including your smart speaker. One compromised device can lead to an attack on your speaker and the rest of your home. Routing guest traffic on a dedicated network will isolate any threats away from your devices.

Smart TV's

How can I make a smart TV more secure?

- If your TV is still in its support period, then you need to make sure you're getting each new patch. Check in your settings to see if automatic updates is turned on.
- Some TVs have passwords to access certain features of the TV and you should change this from the default.
- Buying a new TV when the patches stop coming in isn't realistic. TVs are expensive, but TV streamers aren't. If you're concerned, you could disconnect your TV from the internet and invest in a cheap TV streamer. They will have the same apps as your TV did and you can buy an up to date one that's still receiving security patches.
- Overall, if you're using an older TV, keep your eyes open for anything out of the ordinary. TVs aren't heavily targeted by cybercriminals but being generally wary of unusual requests for personal data is good practice when using any type of internet-connected device.

Smart Speakers

Become familiar with your smart speaker privacy and security settings. Dive into your device's app to explore your options. Google, Amazon, and Apple have been rolling out their own settings to lower safety risks for users.

- Mute the microphone when you don't want to be heard. Some devices have a physical switch, while others can be deactivated by voice command. This can prevent misfired wake phrases.
- Delete your command history to erase local and cloud storage of past recordings. This information is used to understand your voice better, however not regularly deleting this could risk your security. Commands can be deleted on most services either individually, in a time range, or in full.
- Opt-out of data sharing for "improving" voice services or "personalizing" your experience. Many times, these options are on by default. You'll have to turn these off yourself to halt the activity.
- Consider having different networks for your IoT devices and make sure these are separate from the home Wi-Fi you use for your personal devices (i.e., non IoT devices).

4 Smart Speaker Tips for Safe Usage

1. Don't speak any private information. This means credit card numbers, passwords, social security numbers, or any other data you wouldn't want a stranger to have. Treat the speaker like an eavesdropper and be wary of what you say around it.
2. Keep out of line-of-sight of windows. You'll want to avoid showing criminals (who might be spying on you) that you have a smart speaker system. Doing this might also reduce the risks of laser hacks (despite these being quite rare and highly unlikely).
3. Unplug your speaker when you're not at home. If it is not being used (due to no one being around) — the speaker should be off. Doing this removes a potential risk to your home security and is probably one of the most overlooked options for making sure you stay secure.
4. Always use a password manager for all those unique device passwords you've created. Well-protected passwords can be a safeguard against backdoor entry into your smart speaker.

Keeping Your Data Safe

Software, Tools and Apps

Safe Search Kids

https://www.safesearchkids.com/

- Great search engine, powered by Google but for kids.
- Safe Wiki, Images and Video pages
- Tips on Instagram, Roblox, WhatsApp security

Google Kids Space

Child friendly space, recommendations for app, books, and videos.

Useful Links

www.Unicef.org - Good section on cyberbullying, what it is, how to stop it.
https://learningathome.gov.je/digital-safety/ - Jersey Digital Safety Site
www.NSPCC.org.uk
www.Stopbullying.gov - Describes Cyber Bullying and its various forms

- Social media
- Text messaging, WhatsApp etc.
- Instant messaging over the internet
- Online forums, chat rooms
- Email
- Online gaming communities

How to Control Your Data on Facebook - https://www.which.co.uk/news/article/how-to-control-your-data-on-facebook-awOsD6f7pgHu

Documentaries

- The Social Dilemma (Netflix)
- The Great Hack