

Top tips for staying secure online

Top tips to ensure you are doing all you can to secure you and your family online

PAGE 3 OF 7

Install the latest software and app updates

Applying security updates promptly will help protect your devices and accounts from cyber criminals.



You should apply updates to your apps and your device's software as soon as they are available.

Updates include protection from viruses and other kinds of malware, and will often include improvements and new features.

If you receive a prompt to update your device (or apps), don't ignore it. Applying these updates is one of the most important (and quickest) things you can do to keep yourself safe online.

You should also turn on 'automatic updates' in your device's settings, if available. This will mean you do not have to remember to apply updates.

Note that:

- updating your device may take some time and requires a reliable internet connection, so it's best to do it at home where you can access your wi-fi (and keep your device plugged in)
- [older devices](#) will eventually stop receiving updates updates

Keeping your phones, tablets and computers up to date

For detailed instructions about how to keep these devices up to date, refer to the support area within the manufacturers' official websites. If you're advised to back up your data, you can refer to the [NCSC's guidance on how to do this](#).

To get you started, we've included links to popular devices.

- [Update your iPhone, iPad or iPod touch](#)
- [Update your Mac computer](#)
- [Update your Windows 10 or Windows 11 laptop/PC](#)
- [Update your Android device \(Samsung, Google Pixel, Huawei phones and tablets etc\)](#)

Updating devices automatically

- [Update Android apps automatically](#)
- [Turn automatic updates on/off on Apple devices \(middle of page\)](#)

Keeping 'smart' devices up to date

For instructions about how to keep smart devices up to date (such as smart speakers, fitness trackers and security cameras), refer to the support area within the manufacturer's official website, and look for information about updating your device.

To get you started, we've included links to popular smart devices.

- [Amazon devices \(Fire Tablets, Kindle E-readers, Alexa Devices, Fire TV\)](#)

- [Apple Watch](#)
 - [Fitbit devices](#)
 - [Garmin devices](#)
 - [Google Nest or Home speakers](#)
 - [Ring doorbells](#)
-

When your device no longer receives updates

Manufacturers eventually stop providing updates for older devices. If you continue to use a device that's no longer supported:

- ✘ it won't receive updates that contain new features and performance improvements
- ✘ it won't receive the security updates from the manufacturer (and without these your phone is less secure)

You don't need to buy the latest (or most expensive) model to stay safe, but if possible, **avoid** buying and using phones that are no longer supported. You can check online to find if a specific model still receives updates from the manufacturer. Here are the details for iPhone, Chrome, and Pixel/Nexus devices.

- [Supported iPhone models](#)
- [Chrome OS \(e.g. Chromebooks\)](#)
- [Pixel devices](#)

If you have another type Android device (such as those manufactured by Samsung or Huawei), you'll have to [check with the manufacturer](#).

PUBLISHED

17 December 2018

REVIEWED

21 December 2021

VERSION

2.0

WRITTEN FOR

[Individuals & families](#)