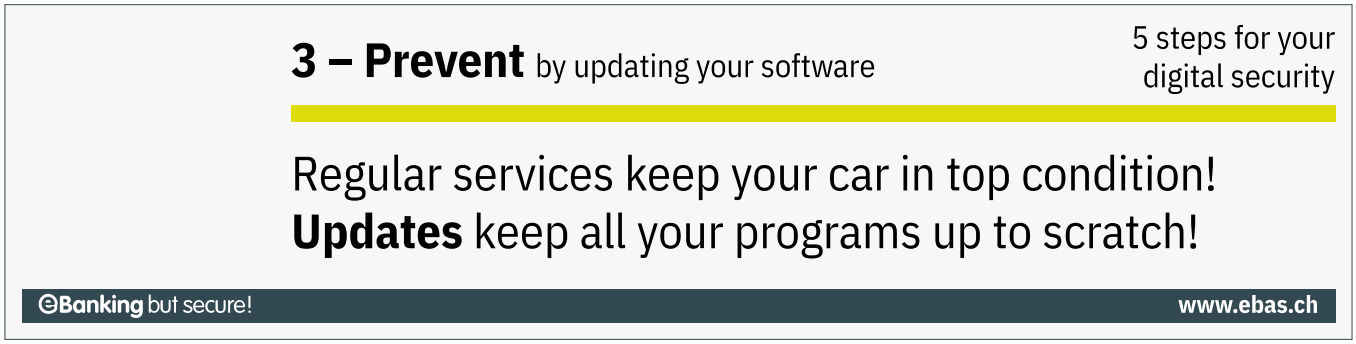
3 – Preventing with software updates

Who better to look after your programmes' security than their manufacturers? Maintain your system, software and apps, and make sure to regularly run the latest updates.

The most important points to remember:

- Only ever install software and apps you actually need, and make sure to exclusively download these from a manufacturer's page or an official store.
- Activate the automatic update feature not just for your operating system, but also all programs and apps installed.
- Only ever use the latest browser version to surf the Internet.



Outdated software often suffers from vulnerabilities, making it easy for attackers to take control of a device. Software manufacturers will correct any such vulnerabilities and offer patches in the shape of program updates.

Only ever install software and apps you actually need

Only install software and apps you actually need, and ensure that they originate from reputable sources, i.e. directly from manufacturers or an official store (e. g. Apple App Store or Google Play Store). You should also periodically check which software and apps you are still using and de-install any applications which are obsolete or which you no longer use. Every additional bit of software or app on your device constitutes yet another vulnerability.

Keep your devices up-to-date

Please ensure you always use the most up-to-date version of any software. The mainstay is an up-to-date operating system. But all other software installed (such as browsers like Mozilla Firefox or Google Chrome, or Adobe Acrobat Reader) must always be kept up-to-date, too. Usually, this is easily done and doesn't require much effort: Once you activate their respective update functions, these programs or your operating system will regularly look for the latest updates, often also installing these automatically.

Windows

In Windows 10, Windows updates are activated by default. For you, this means updates are downloaded and installed automatically as soon as they become available.

Under Advanced Options, you should also activate option “Give me updates for other Microsoft products when I update Windows”, so that other Microsoft products, such as Office, are also automatically updated.

Older Windows versions - End of life
You should no longer be working with Windows XP, Windows Vista and Office 2007 by now, as Microsoft has ceased support for this software. This means security updates are no longer made available to protect your computer against viruses, worms, Trojans and other malware.

Windows lifecycle (https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet)

macOS

Under macOS, system and software updates are provided centrally via the “Software Update” function. The automatic software update function is activated by default. In addition to the default settings, you should also activate the “Automatically keep my Mac up to date” option. To do so, click on “System preferences” in the “Apple” menu and then on “Software update” and “Automatically keep my Mac up to date”. For older systems than Mojave, you do as follows:

Select “System Preferences”, click the App Store, then select ”Download newly available updates in the background”. Updates available are also always displayed under the App Store symbol in the dock, indicated by the number of software updates available. Once you click on this, the App Store opens, and you can then install these updates.

Older macOS versions - End of life
Apple does not provide any timelines for their products’ “end of life”.

However, security updates are only ever published for their current macOS version plus two versions immediately preceding it. Older versions are no longer provided with any security updates and should therefore no longer be used.

Identify your Mac operating system. (https://support.apple.com/en-gb/HT201260)

Smartphone und Tablet

Most smartphone operating systems will notify users once any system updates are available. Check under “software update”, “mobile update” or similar in your system settings whether there is an automatic update function, and whether it has been activated. Apps installed can usually be updated via the store. Depending on your operating system, all apps or those specifically selected can even be updated fully automatically. Always make sure that you update both your operating system and all apps installed as soon as possible.

Older Android versions - End of life
Google does not provide any timelines for their products’ “end of life”.

Availability of updates varies depending on device and manufacturer.

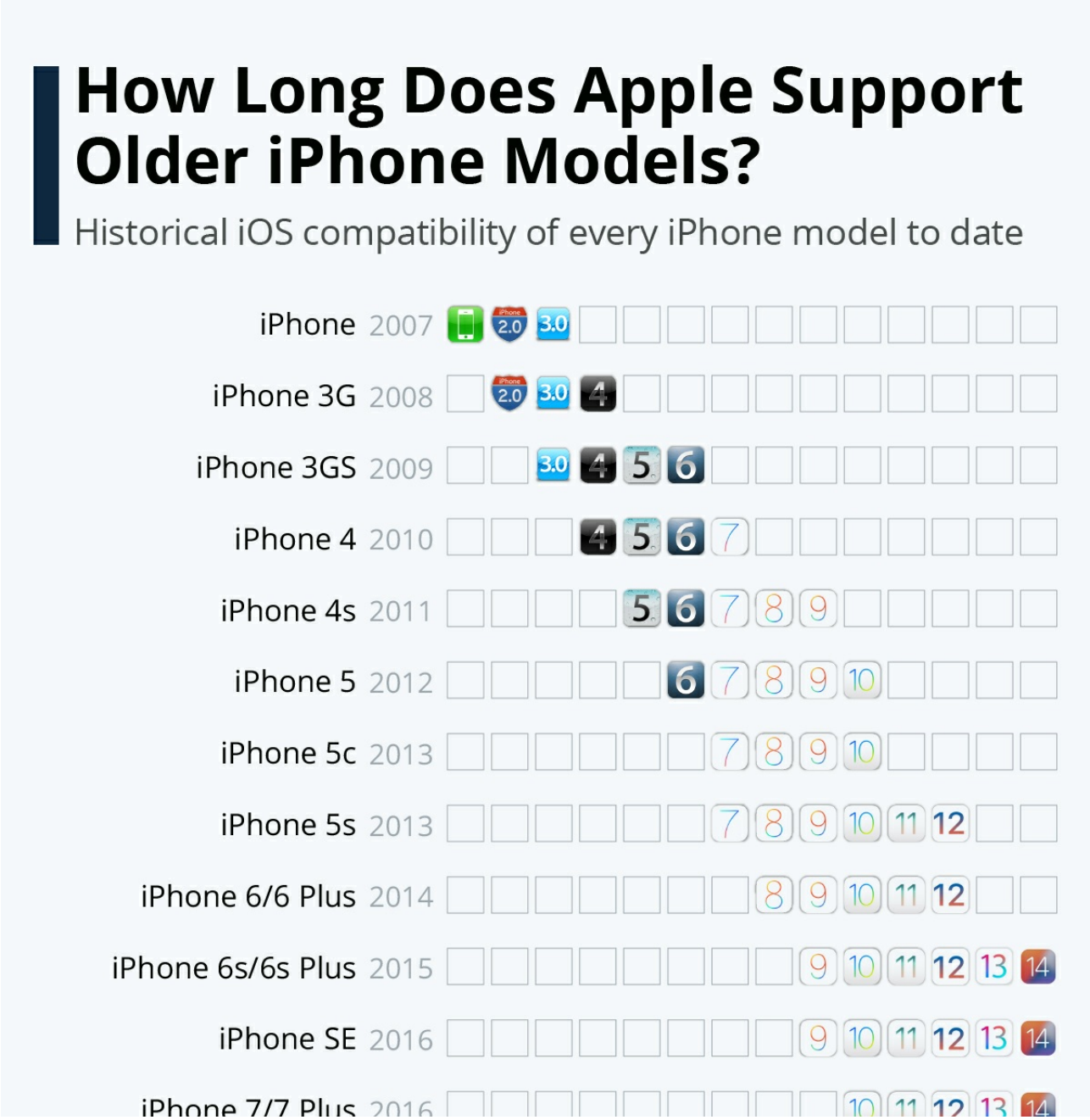
- Pixel or Nexus device users can find out here (https://support.google.com/pixelphone/answer/4457705#when_updates) when updates will become available.
- Owners using other Android devices should contact their device manufacturers to obtain this kind of information.

Older devices might not be compatible with newer Android versions and should no longer be used.

Older iOS versions - End of life

Apple does not provide any timelines for their products' "end of life".

The following graph (Source: Statista (https://www.statista.com/chart/5824/ios-iphone-compatibility/)) shows how long Apple is supporting older iPhone models for.



iPhone models which are no longer compatible with current iOS versions should no longer be used.

Protect your data and all your devices with the help of our "5 steps for your digital security":

Step 1 – Back up (https://www.ebas.ch/en/1-backing-up-data/)
Step 2 – Monitor (https://www.ebas.ch/en/2-monitoring-with-antivirus-software-and-firewall/)
Step 3 – Prevent
Step 4 – Protect (https://www.ebas.ch/en/4-protecting-online-access/)
Step 5 – Exercise Care (https://www.ebas.ch/en/5-exercising-care-and-remaining-alert/)