Android Vs. IOS: Security Comparison 2022

Android vs. iOS: The threat level

Is it easier to hack an iPhone or Android?

What do iOS and Android security have in common?

iOS vs Android security: The winner is…

How to enhance your smartphone security

App marketplace security

Apple closely inspects every app on its app store, which might reduce the number of apps available, but helps to reduce malware riddled apps.

Android's open Play Store marketplace has far more apps to choose from than on iOS' App Store, but there's a far greater chance that hackers can make it onto the platform to distribute malware apps.

On numerous occasions, highly ranked apps with hundreds of thousands of downloads from the Android app store have been discovered to contain malware.

Android users can also change their settings to allow apps from outside of the Android app store. This provides an even greater selection of apps, but opens users to an even greater risk of malware.

Device manufacturers

iPhone's integrated design makes security vulnerabilities less frequent and harder to find.

Apple's devices and their OS are inseparable, giving them far more control over how they work together. While device features are more restricted than Android phones, the iPhone's integrated design makes security vulnerabilities far less frequent and harder to find.

Android's open nature means it can be installed on a wide range of devices. Depending on the manufacturer and the model, this can be a good thing or a bad thing. Some devices integrate perfectly with Android while others leave significant security vulnerabilities.

Device-based security across Android devices also varies - some offer retinal and fingerprint scanners while others are limited to passwords and patterns.

Updates to patch vulnerabilities

Apple updates are easier to control across devices, promising consistent security.

Constant OS updates are one of the main ways that Apple and Google can keep iOS and Android secure. Because Apple strictly controls the devices in its ecosystem, updates are easier to create and distribute. This also means that Apple can usually keep iOS devices updated for longer, generally withdrawing official support after 5 years.

The number of Android devices Google has to serve makes it virtually impossible to keep all of them updated to the same level of security and for the same amount of time and frequency.

It also makes it harder to roll those updates out, as they have to be distributed across multiple manufacturers and devices. Updates come out less frequently and devices are supported for less time.

In the iOS vs Android competition, there’s one problem that they both face - users who forget to update their phones. In this respect, however, Apple still has an easier time of it. Because everyone’s on a system they control, they can put more pressure on users to update their phones.

Support for third party security apps

Both operating systems support a wide range of third party security apps, including VPNs.

Useful as a device's built-in security features can be, it's also important to be able to integrate third party services like antivirus software and VPN applications into the operating system.

Thankfully, iPhone and Android smartphones both support the most popular and useful security apps, including NordVPN. With the NordVPN app on your device, you can protect your iOS or Android phone against hackers, Wi-Fi snoopers, and data brokers.

Ready to supercharge your security with layers of powerful encryption?

Enhancing your smartphone security is easy.

Stay safe with the world’s leading VPN

OS source code security

Winner: iPhone and Android

Apple closely guards their source code, while Android has made most of their OS open-source.

Apple’s closed source code makes it harder for hackers to find security flaws. While Android’s open-source nature could mean the exact opposite of that, it also makes it more easily accessible to a wide variety of developers, and Google is slowly beginning to use this feature to their advantage.

In addition to its own security research, Google has increased the bounties it’s willing to pay to independent security researchers for reporting new vulnerabilities. At a major annual mobile security event in 2017, mobile security researchers failed to collect a single bounty for finding Android hacks.

Popularity

Winner: iPhone

Less users means less targets, and less motivation for hackers to develop malware for the iPhone.

The smaller number of targets on iOS, as well as its heightened security, make the iPhone a somewhat less attractive target for hackers. As the most used smartphone in the world, Android’s popularity has become it’s weakness; more users means more targets for hackers and more reasons to develop malware for Android (the same goes for the Windows computer OS).

There is a silver lining for Android users. Android’s popularity and open marketplace mean that there’s a far wider range of security apps available. The security of your Android OS and device out of the box may vary, but with the right apps, you can take it to the same level of security as iOS or even further.

Android vs. iOS: The threat level

The threat level depends on things that are out of your control, like inconsistent update releases as well as the ease and rate at which exploits can be developed by hackers.

1. Android makes it easier for hackers to develop exploits, increasing the threat level.

Apple’s closed development operating system makes it more challenging for hackers to gain access to develop exploits. Android is the complete opposite. Anyone (including hackers) can view its source code to develop exploits. ANDROID TECH As the most used mobile in the world, It could be said that Android phones are generally more susceptible to security flaws.

2. Android’s inconsistent update releases, could mean that there are more Android bugs in circulation.

Android and iPhone both receive several updates a year, that also patch dangerous security flaws. Android updates depend on the hardware, manufacturer of your phone, and the

support for your current phone. It’s also easier to push updates back, unlike Apple’s stricter update system.

Is it easier to hack an iPhone or Android?

The likelihood of your phone being hacked partially depends on how you use your device, and what safety precautions you take. At the end of the day, after all, both Android systems and the iPhone can be hacked.

iOS security focuses more on software-based protection, while Android uses a mixture of software and hardware-based protection: the Google Pixel 3 features the ‘Titan M’ chip, and Samsung houses the KNOX hardware chip. Both chips work to isolate, encrypt, and secure your data, and Titan M disables the phone if your passcode is entered incorrectly more than three times. The iPhone also has similar functionality.

Ultimately, a device is only secure up to a point, unless you take your own precautions. To improve security on iOS or Android, you can use the NordVPN app to encrypt your data and secure your smartphone online. A VPN secures your online traffic and app-data, protecting your personal information against any malicious actors.

What do iOS and Android security have in common?

Both iOS and Android have similar built-in security features, including virtual sandboxes that limit the damage that malware apps can do. iOS drive encryption comes standard while Android users must enable this feature.

Both OS fully support VPN encryption, which is especially important for mobile devices (NordVPN provides top-of-the-line security to both iOS and Android devices. Secure yourself today!)

iOS vs Android security: The winner is…

Android has been working hard to clean up their act. David Kleidermacher, the head of security for Android at Google, has even said that Android’s security now equals that of its rival, iOS.

Until we see those changes borne out in the real world, however, we’re going to have to give it to iOS. In 2018, iOS is still the best OS when it comes to smartphone security. But that doesn’t mean it can’t be improved upon.

With Google hot on its heels, Apple hasn’t been sleeping at the wheel. The new iOS 14 is a stampede of security including recording indicators, an ‘approximate location’ option, and password and tracker monitoring in Safari.

How to enhance your smartphone security

Download apps from official stores. Avoid downloading apps from third-party websites, as you can never know if they’re legitimate and safe.

Use strong passwords. A strong password should contain lowercase and uppercase letters, along with special characters and numbers. Make sure to create unique passwords for every account you have.

Avoid logging into apps using Facebook. Many apps and websites allow you to log into their services quickly using your Facebook profile. However, if your Facebook is compromised, hackers can easily access all the other accounts linked to it.

Update your software on time. iOS and Android updates fix bugs and add new security features. It’s tempting to postpone updates for later, but if you do you’re putting yourself at risk.

Use a VPN. A virtual private network hides your IP address and encrypts your traffic, mitigating the risk of getting hacked. If you often connect to public Wi-Fi, having a VPN on your smartphone is a must, as wrongdoers can use fake hotspots to infect your device with malware.NordVPN iOS and Android apps come with the Dark Web Monitor feature, which notifies users if their personal details are ever leaked on the dark web. With one NordVPN account, you can protect up to six different devices: smartphones, laptops, routers, and more.