

Android is the most popular operating system for smartphones, by far, and it's also the most open, in terms of how much you can customize your device – replacing its default keyboard, for example – as well as the approval process for developers to release new apps for it.

This openness is a boon for the tech-savvy Android user, because pretty much anything on their device that they don't like can be swapped out for something better. They also tend to be pretty good at not installing apps that might play fast and loose with personal data. For them, Android doesn't have a security problem.

What about everyone else, though? Android's status as the world's most popular smartphone OS means it has hundreds of millions of users who aren't so clued-in on security. They're not stupid or lazy: they're just normal people. They're the reason so many developers of viruses, other malware and privacy-flouting apps are targeting Android.

Cisco's annual security report claimed in January that 99% of all malware in 2013 targeted Android devices, while security firm Kaspersky Lab suggested a similar figure of 98% in December last year.

"Android ticks all the boxes for cyber criminals – it's a widely used OS that is easy to use for both app developers and malware authors alike," said Kaspersky's senior virus analyst Christian Funk, at a time when his company was detecting 315,000 new malicious files every day.

So, does Android have a big security problem? This is a question that is complicated by the fact that many of the companies warning about Android malware are also selling apps and services that promise to protect against it. They have a good view of what's out there, but also an interest in talking up the risks.

But keeping your data safe on an Android device can be more about taking common-sense steps to minimise your risks, rather than assuming you need to splash out on a monthly security subscription – although there are plenty of choices for the latter if you decide that's the route for you.

With that in mind, here are five tips for ensuring that your Android device is safe:

### 01. Be cautious when installing apps

Using the Google Play Store to download apps (or Amazon's Appstore if you own one of its devices) already makes you among the more secure tiers of Android users – many dodgy apps are distributed through third-party Android app stores rather than the official ones.

Still, it's best to exercise caution, especially when you happen upon what looks like a brand new version of a

popular game. Candy Crush Saga, Angry Birds, Clash of Clans... fake versions of these regularly appear, so if something sets off warning bells (Candy Crush Saga 2, anyone?) it's worth googling its title and checking its developer's website to see if it's a fake.

Also, read the reviews on the Google Play store – a surfeit of one-star reviews is a sign that something's wrong – and check the permissions that an app asks for before you install it. If anything here sets off warning bells – or simply makes you uncomfortable – it's a good prompt to walk away.



### 04. Consider anti-virus software

If you'd still like to take the extra step of installing anti-virus software – or if you're thinking of putting it on the device of someone else (an older parent, for example) – a number of options are available from the big names of the security world.

AVAST Software's Mobile Security & Antivirus, Bitdefender's Mobile Security & Antivirus, Lookout Security & Antivirus, Kaspersky Internet Security, Trend Micro's Mobile Security & Antivirus, Norton Security antivirus and McAfee Antivirus & Security all have

## How Can I Keep My Android Tablet or Smartphone Secure?

Mohammad Javed Morshed Chowdhury

### 02. Watch out for phishing / SMS

Security on Android isn't just about the apps that you install on your phone. As with any device – Android or otherwise – be on your guard for phishing, sites that try to get you to enter personal data and/or credit card details. Text messages and emails can all be phishing methods, and just because you're on your phone doesn't make them less dangerous.

Combating phishing on Android isn't so different from on your computer: useful advice from the Citizens Advice Bureau, Microsoft and Symantec will get you up to speed, while an additional tip is to never tap on a link in a text message from someone you don't know – even if it looks like a company you do business with.

### 03. Lock screen security

Another point that applies to every smartphone OS, not just Android. Have you got your device's lock-screen settings sorted, so that if it gets stolen, the thief can't access your apps and data? Google's default settings will see you fair, but there are some third-party apps that take interesting and unusual spins on unlocking the phone.

Picture Password Lockscreen, for example, gets you to unlock your phone by drawing points, lines and circles on any image you like. ERGO scans your ear and then gets you to unlock the device by holding it up to said lug. Fingerprint Scanner LockScreen is a cheeky Android equivalent of Apple's iPhone 5s' Touch ID – it pretends to scan your fingerprint, but really it's just measuring how long your thumb rests on the screen.


four-star-plus ratings on Google play from thousands of reviewers, with the competitive market meaning they add new features regularly.

Which you choose depends more on which you've used on your computer before, but all offer a good level of security if you're concerned.

### 05. Consider a parental control app

You can follow many of the steps above, but can your children if they're using your device, or have their own Android tablet and/or smartphone? A number of companies are trying to help with this challenge too, with parental control software capable of ensuring children don't install apps that they shouldn't, or compromise data on a shared device.

Kids Place, Famigo, MMGuardian and Norton Family are four of the most popular examples, with varying features to control what apps are installed, what sites are being visited, and to set time limits on usage – and in some cases, add time as a reward for good behaviour.

Alternatively, you could spend a bit of time getting to grips with Android's default features to set up different user profiles on a tablet, and make some of them restricted – found via the users option in your settings menu. But parenting skills are also important here: talking to your children about safe usage of their Android device is as important as trying to lock it down for them. 

*N. B. : Information is collected from different news portals*