antivirus android tablet free download cnet

DOWNLOAD

Best antivirus software for 2021.

Your Windows PC needs protection against malware -- and free antivirus software may not be enough. Here's the best antivirus protection for Windows 10 and what's worth paying extra for.

Windows users should have an antivirus tool in order to protect personal information. Even if you have a secure browser and other threat detection software, it's just all too easy for an insidious program to wind up on your machine, and that can lead to chaos. The best antivirus software is a program that includes features like malware protection, monitors downloads and observes your system's activity for malicious software and suspicious behavior.

If you're looking for malware protection and antivirus software with the best security features, here's the first thing you need to know: Microsoft Defender Antivirus -- the free antivirus software and virus protection program that comes with Windows 10 -- does a decent job of protecting your PC and offering internet security. (Amazingly, Microsoft provided no built-in protection for Windows back in the days of Windows 98 and XP.) Using Microsoft Defender for threat detection should be your starting point for the best antivirus security on Windows and most people will find they don't need to go any further when it comes to nailing down an antivirus solution.

However, keeping your personal data safe and guarding your privacy extends beyond virus protection, and that's where third-party antivirus software shines. A full protection package can monitor your Windows operating system as well as MacOS, iOS and Android devices and include a password manager, secure online backup, identity theft protection, a VPN, parental control, webcam protection, protection against phishing and malicious websites and more -- all worthwhile security suite tools that can keep your data secure and guard your privacy.

To help you decide, I've put together a list of the best antivirus products for Windows 10, encompassing both free antivirus programs and subscription options. These picks of the best antivirus programs are a combination of recommendations from independent third-party labs AV-Test, AV-Comparatives and SE Labs, as well as our own hands-on testing. This list is updated periodically.

We would also like to note that antivirus software isn't the only security feature you should invest in. A secure VPN to protect your internet traffic, a password manager to keep track of login credentials and an end-to-end encrypted messaging app to stop others from spying on your communications are all essential to protecting your personal information online. Cybercriminals are becoming increasingly more sophisticated and high-profile attacks like the Columbia Pipeline hack are becoming more commonplace, which is concerning.

Our recommendations.

Looking for free antivirus protection, malware protection or virus detection, willing to pay for an antivirus program that offers broad internet security coverage across all your devices, including from ransomware and phishing, or need to remove a computer virus or malware from your PC right now? Here's where to start.

Best free Windows antivirus.

Microsoft Defender.

Free version? Yes, built into Windows 10.

Paid version: Windows Defender Advanced Threat Protection is available to corporate users for a fee.

Honestly, if you practice safe computing -- you keep your software up to date, you use strong passwords (with the help of a password manager), you steer clear of unexpected emails and you don't click suspicious links that may be phishing attempts -- you probably can avoid zero-day attacks and ransomware attacks. And with the free Microsoft Defender Antivirus software running on Windows 10, you have a malware protection safety net if you do let your guard down. (Note that Microsoft changed the name of Windows Defender to Microsoft Defender and has expanded the service to other platforms.) This free antivirus program is built into Windows and it's turned on by default, so just let it do its thing, and this antivirus solution will cover the basics of internet security. Microsoft pushes new updates frequently. Defender also lets you tune the level of protection you want, giving you control over blocking potentially unwanted apps and protecting folders and files from a ransomware attack.

Note that Windows 10 will automatically disable its own Windows Defender antivirus when you install third-party antivirus. If you uninstall the third-party protection, Windows 10 will turn back on its own antivirus.

Best antivirus subscription for Windows.

Norton 360 with LifeLock Select.

Platforms: Windows 10 plus MacOS, Android, iOS.

Cost: $150 per year for five devices, on sale for $100.

For a long time, Norton Security -- now called NortonLifeLock, and no longer part of Symantec -- has earned high marks from AV-Test, AV Comparatives and SE Labs for virus and malware detection. A five-device subscription for Norton 360 with LifeLock Select is normally $150, but you can sign up for $100 for the first year to get coverage across your PCs, Macs, Android devices, iPhones and iPads. (Note, we don't think antivirus protection is terribly useful outside the Windows realm.) In addition to malware and virus protection for your computer and mobile device, this security suite provides 100GB of backup to the cloud, safe-browsing tools, a secure VPN, password manager, parental controls and LifeLock identity theft protection and fraud alert. While not all of those services are necessarily best in their respective class, getting them all in one package is a compelling option.

Best free antivirus alternative for Windows.

Bitdefender Antivirus Free Edition.

Platforms: Windows 10 plus MacOS, Android, iOS.

Free version? Yes.

Paid version: $40 per year for five PCs.

If you'd like to take a step up in securing your PC without taxing your wallet, it's hard to beat Bitdefender's free antivirus software for Windows 10. The Windows security software offers real-time monitoring for viruses, malware, spyware and ransomware protection. Bitdefender Antivirus Free Edition is easy to set up and stays out of your way until you need it. And the protection this antivirus product offers is solid. Bitdefender antivirus software consistently earns top marks for its antivirus protection and usability from the respected AV-Test independent testing lab. The free antivirus version covers one Windows PC. For broader protection, Bitdefender Total Security 2020 is usually $90 and available at the moment for $40 for the first year. The subscription antivirus suite lets you protect five devices (Windows, MacOS, iOS and Android), set up parental controls on a kid's computer and run a VPN.

Best on-demand Windows malware removal.

Malwarebytes.

Platforms: Windows 10 plus MacOS, Android.

Free version? Yes, after 14-day trial expires.

Paid version: $30 per year for one device, $80 per year for five devices.

Malwarebytes does protect your PC from a virus or malware attack, scoring reasonably well in recent independent testing for guarding against malware threats. But that's not really what Malwarebytes is known for. If you find yourself in trouble, the go-to disinfectant for many is Malwarebytes. You can get protection and disinfection for one device for $30 a year, regularly $40. To cover five devices -- any combination of Windows, MacOS and Android -- it's $80 for a year. To get the free antivirus version, download this trial version, which "downgrades" to a no-fee on-demand cleaner with fewer features that detects and removes viruses and malware when you run an on-demand antivirus scan after 14 days.

Also worth considering.

In addition to the four antivirus apps we recommend above, a handful of other anti-malware tools are worth considering among the best antivirus protection if you find them at a better price or just prefer to use one over our picks above.

Solid subscription antivirus alternative.

McAfee Total Protection.

Platforms: Windows 10 plus MacOS, Android, iOS.

Cost: $100 per year for five devices, on sale for $35.

It feels like McAfee has been around forever, first on its own in the '80s, then as part of Intel starting in 2010, and then again on its own when Intel spun it off in 2017. And it's been around forever because quarter after quarter it creates solid, modern antivirus software that protects your PC. (In recent evaluations by AV-Test, it had high scores on both protection and performance.) McAfee Total Protection guards five devices against viruses and offers ransomware protection, wards off malicious websites and includes a password manager for $35 (usually $100) for the first year. If you agree to auto-renew your security suite subscription, you get access to McAfee ID Theft Protection Essentials, which monitors for ID fraud.

Another good subscription option.

Trend Micro Maximum Security.

Platforms: Windows 10 plus MacOS, Android, iOS.

Cost: $90 per year for 10 devices, on sale for $50.

Maybe not as well known to consumers because of its focus on enterprise security, Trend Micro quietly brings its business expertise to the home with its Trend Micro Maximum Security tools. Trend Micro's software earns high marks from AV-Test -- consistently scoring well for detecting zero-day attacks and widespread viruses and malware. And Trend Micro does a good job of not taxing system resources. Trend Micro's 10-device subscription for computers and mobile devices is $90, but discounted currently at $40.

Worthwhile subscription alternative.

ESET NOD32 Antivirus.

Platform: Windows.

Cost: $80 per year for five PCs.

If you're looking for something easy to set up and use, ESET NOD32 antivirus may meet your needs. It earns high scores for usability and offers solid virus protection. A five-device option is $80 for a year, with a 30-day free trial.

Alternative free Windows antivirus.

Sophos Home.

Platform: Windows plus MacOS.

Free version? Yes.

Paid version: $42 per year for 10 PCs.

The free version of Sophos Home gives you virus protection for three Windows PCs -- using the company's high-scoring anti-malware tool -- plus a 30-day trial of the company's malware-removal tool. With a $45 annual subscription, you can cover 10 PCs.

What about Avast?

Test after test, Avast's antivirus for Windows performs well for malware detection. And we've included its antivirus in our list of recommended security app options before. But Avast was in the news for several months for its non-antivirus business, so we looked at the company, specifically reports at the end of 2019 that Avast allegedly collected user data with its browser plug-ins and antivirus software and then sold data it collected through its Jumpshot subsidiary in early 2020.

In response to the reports that his company gathered and sold the details of its customers' online activities, Avast's CEO Ondrej Vlcek said in a statement that he understood that his company's actions raised questions of trust in his company. To address that, Avast terminated Jumpshot data collection in January 2020 and closed its operations because the data collection business wasn't in line with Avast's privacy priorities.

These newer reports follow another in 2019 from Avast that its internal network was breached, possibly to insert malware into its CCleaner software, similar to an earlier CCleaner hack that occurred prior to Avast's acquiring the Windows utility.

Avast is now saying the right things about taking its customers' privacy seriously, but it only came to that point after reacting to investigative reporting that revealed the Jumpshot practices. (The CCleaner revelations, while concerning, were self-disclosed, which is important to building user trust.) We hope Avast's more privacy-friendly policies mean that there will be no further Jumpshot-style activities. In the meantime, we'd recommend using one of the many other solid choices in this realm (listed above).

What about Kaspersky?

Because the company has been in the news the past few years, let's talk about Kaspersky Lab -- specifically about the federal ban that blocks US government agencies from using Kaspersky products.

Based in Moscow, Kaspersky Lab has for years produced some of the best antivirus software for business antivirus needs and home customers. But in 2017 the US government prohibited Kaspersky software on federal government computers because of alleged ties between Kaspersky and the Russian government.

Notably, the ban does not apply to its consumer products. But as with China-based Huawei , the question remains: If the federal government doesn't think the products are safe enough for its own devices, should consumers avoid them as well?

In a statement sent to CNET, the company said, "Kaspersky Lab has no ties to any government, and the company has never, nor will ever, engage in cyber offensive activities. Kaspersky Lab maintains that no public evidence of any wrongdoing has been presented by the US government, and that the US government's actions against Kaspersky Lab were unconstitutional."

In Kaspersky's favor, it continues to earn top scores and awards for virus and malware detection and endpoint protection from independent testing labs. And it's reasonably priced .

In the end, even though no one has ever publicly produced a "smoking gun" linking the company to Russian intrigue, we think any of the options listed above are a safer bet. And, if you are a US government employee or work with the federal government, you'll want to steer clear of Kaspersky.

Antivirus basics: What to look for.

Picking the best antivirus software for Windows means finding one that keeps your PC safe, doesn't take up a lot of system resources, is easy to use and stays out of the way till you need it. Here's what to look for.

Effectiveness. Antivirus software runs virus scans for known viruses and malware, of course, and can offer real-time protection. And it watches for shady websites and suspicious links to keep you out of trouble. It can also offer ransomware protection and monitor unexpected behavior that may be a sign of new and not-yet-identified viruses and malware. You want antivirus software that can successfully identify these unknown online threats without flagging too many false positives.

Light on system resources. You don't want antivirus software that taxes your PC's resources. If after you install the program, websites open slowly, apps download or open sluggishly or file copies take longer than expected, you may want to try another service. The good news is, all our picks offer a free trial to let you try out the antivirus program, so if your system feels sluggish after installation, you may want to keep looking.

Cost and discounts. Don't just pay the sticker price for antivirus protection. Before you buy, check for discounts on a company's website. Another way to save: The prices we list above are for 10 devices -- if the company offered that package -- but you can trim your cost with antivirus packages if you need to cover just three or five devices. You may also find discounts on an app's Amazon page.

Privacy. To be effective, antivirus software needs to monitor what's going on with your PC and check in with company servers about unusual behavior. The companies say they anonymize this technical data as much as possible to protect your privacy. But if you want to know more, the security companies on our list post privacy policies on their websites, so read their privacy statements to learn what the companies do with the information you share.

Protection for other platforms. Microsoft is by far the biggest target for viruses and malware. But Android is second, with just under 1% of apps installed on Android devices with Google Play Protect in the potentially harmful app, or PHA, category.

The threat to MacOS and especially iOS is low, in part because of the tight control Apple has over its app stores. While the Mac does come under attack via sideloaded apps, it's rare, and if you download apps only from the Mac and iOS app stores and keep your guard up when clicking links and download files, you should be OK without an antivirus app on Apple devices.

Stay current on the latest Microsoft news, plus reviews and advice on Windows PCs.

AVG AntiVirus for Android Mobile security for your photos, messages, & memories.

Ours was the first antivirus app on Google Play to break 100 million downloads, and is used today to secure phones and tablets across the globe.

Once installed, it runs silently to protect you from the latest viruses, malware, spyware, unsafe apps and settings, unwanted callers, and other nasty threats.

Anti-Theft Phone Tracker.

Lost it? Remotely find & lock it.

Just visit our Anti-Theft website from another device to locate and track your lost phone or tablet on Google Maps. You can even remotely lock it and blast an alarm at full volume.

Best of all, if you think your mobile is gone for good, you can remotely wipe it to prevent your private data from falling into the wrong hands.

App Lock.

Lock down your privacy with a PIN code.

Prevent others from snooping on your private photos, messages, and documents by locking any of your apps with a unique PIN code. App Lock will also offer to lock potentially sensitive apps (e.g., Facebook, Instagram, WhatsApp, etc.) when you install them.

Camera Trap.

See who's got your phone or tablet.

Now you'll know if an annoying brother—or master thief—tries snooping on your phone or tablet. When anyone fails 3 times to unlock your device, Camera Trap will take a secret photo of them and then email that photo to you with the time and location of the incident.

AVG AntiVirus for Android.

Mobile security for your photos, messages, & memories.

Clean up your Android.

More space, speed, & battery life.

Get AVG Cleaner for Android.

Protect all your devices.

Unlimited devices, remote actions.

Get AVG Internet Security.

Protect & Clean all your devices.

Unlimited devices, remote actions.

Get AVG Ultimate.

Frequently Asked Questions.

Why does AVG offer one of the best Android antivirus solutions?

AVG AntiVirus for Android is one of the best free antivirus apps for Android because our powerful security app has been specially designed with Android devices in mind. With a cutting-edge antivirus engine, you'll be protected against the wide range of Android malware, which includes ransomware, spyware, adware, and more. Should your Android device get stolen or lost, we'll lock it up and help you track it down with the built-in Anti-Theft Phone Tracker.

Upgrade to PRO to automatically lock your device if a thief swaps out your SIM, secretly capture the thief's identity with the Camera Trap, and place a fingerprint or PIN lock on any apps you choose. This comprehensive feature set and world-class anti-malware protection are just two of the reasons why AVG AntiVirus for Android has earned a 4.7 rating on Google Play. We're also proud to be one of PCMag's best Android antivirus apps in 2021.

Why do Android phones and tablets need antivirus protection?

Like computers, Android devices are vulnerable to malware and other security threats. And especially in recent years, Android malware has only grown more common. AVG AntiVirus for Android is a powerful cybersecurity tool that can defend your Android device against a wide range of threats, absolutely free. Not only can AVG AntiVirus for Android remove Android spyware and other malware, but it also defends against unsafe Android apps, and helps you track down your phone in case it gets lost or stolen.

What kinds of malware do Android devices get?

Hackers have created a wide range of malware for Android devices, including spyware, Android ransomware and adware. You're also just as vulnerable to phishing attacks on your smartphone as you would be on your computer. A trustworthy Android security app like AVG AntiVirus for Android is your strongest ally in the fight against Android threats, whether you're removing adware or tracking down a stolen phone.

How can I check my Android phone and tablet for viruses?

Once you learn the common signs that your phone has been hacked or infected with malware, it's easy to figure out when something is wrong. Here's how to spot malware on your Android phone:

Your phone suddenly runs a lot slower. The battery drains faster than usual. Your phone bill is unusually high. Ads pop up where they shouldn't. You see apps you don't remember installing.

If you experience any of these problems, your Android might be infected with malware. AVG AntiVirus for Android will monitor your phone or tablet in real time to detect and remove malware from your Android device.

How do I get an antivirus app on my Android phone or tablet?

To download AVG AntiVirus Free for Android, all you need to do is go to the Google Play Store and search for AVG. You'll find our antivirus among our other mobile offerings, which you can then install with the tap of a finger.

Antivirus Free for Android.

Bitdefender Antivirus Free utilizes high-detection engines, coupled with in-the-cloud scanning capabilities, to keep Android devices safe from attack - with minimal impact on resources.

Malware Protection Cloud Scanning Low Battery Impact.

Get it now.

*No credit card required. It's Free :)

*Available in English.

Bitdefender Antivirus Free for Android.

Bitdefender Antivirus Free is a free and powerful solution that utilizes in-the-cloud scanning technology to arm your Android device with the very latest industry leading virus detection, without interfering with your mobile experience or draining your battery.

Unparalleled Detection.

Bitdefender Antivirus Free uses the same scanning engines as Bitdefender Mobile Security - our flagship application that has been independently certified to catch more than 99% of all viruses targeted at Android devices.

Feather-Light Performance.

Instead of downloading and storing virus signatures directly to Android devices, Bitdefender Antivirus Free uses in-the-cloud services to check online for the latest safeguards to outbreaks.

Full Speed & Low Battery Impact.

Thanks to its cloud-based threat detection and top-of-the-line security services, Bitdefender Antivirus Free for Android prevents installation of malicious applications with virtually no battery life impact.

What Else You Get.

On-install Scanning.

Bitdefender Antivirus Free ensures Android device stay clean by automatically scanning any application immediately after its install. This also helps users stay informed and protected whenever they try a new application.

On-Demand Scanning.

On-demand scans may be run at any time, to make sure that all the applications that are installed and kept in the device’s storage are legitimate and safe.

Zero Configurations.

Bitdefender Antivirus Free offers you essential antivirus protection against all Android threats. It is ready to go right after installation, acting as an effective guardian against mobile malware. Moreover, the Autopilot automatically scans any new apps you install.

The best Android antivirus app of 2021.

Having the best Android antivirus app installed on your smartphone or tablet is essential. After all, Android is the most widely-used operating system in the world, and that means it can be a big target for malicious users.

We do so much with our Android devices - such as mobile banking and shopping - that getting malware on your smartphone or tablet could be incredibly serious indeed, which is why it's vital to install one of the best Android antivirus apps you'll find on this page.

In this article, we’re going to highlight 10 of the best Android antivirus apps in 2020 - a few of which are completely FREE apps to download.

Many of them do much more than run automatic scans, and they’ll actively try to prevent malicious web pages and files from being opened or downloaded in the first place. The easy way to protect your Android phone or tablet.

Check out the best Android VPN for another great way to stay safe online.

The best Android antivirus in 2021 is:

1. Bitdefender Mobile Security.

Well-featured with tight security - the best Android antivirus app.

Specifications.

Reasons to buy.

Reasons to avoid.

Bitdefender Mobile Security offers excellent protection for your Android device, with a raft of features including anti-theft, and top-notch antivirus capabilities. In fact, this android antivirus mobile app got full marks in the latest AV-Test roundup, and AV-Comparatives (the other major independent antivirus test lab) observed a protection rate of 99.9%. That’s impressive indeed.

Mobile Security gives you real-time protection for Google’s Chrome browser, and an autopilot feature that claims to be capable of making intelligent recommendations for security actions depending on your system and typical usage pattern.

There’s also a nifty privacy advisor tool that adds a layer of security to your smartwatch via its WearOn technology, which alerts you if you accidentally leave your phone behind - clever stuff.

Another interesting extra is a bundled VPN, although don’t get too excited. The provided version is restricted to extremely light use at just 200MB daily, but still, that could be useful in a pinch.

As mentioned, there are anti-theft capabilities here, and Bitdefender Mobile Security allows you to remotely locate and lock your device, or send a message to the phone or tablet (which could be very useful if you’ve lost it). It’s also possible to completely wipe the device remotely if you so choose.

There are a lot of features on offer here, then, and the asking price is more than reasonable to cover a single Android device for a year (plus if you want to give the app a spin before you buy, there’s a 14-day free trial available).

2. Norton Mobile Security.

Provides innovative mobile defenses on the app checking front.

Specifications.

Reasons to buy.

Reasons to avoid.

Norton Mobile Security for Android offers a wealth of features, including an App Advisor which is powered by Norton Mobile Insight, and vets apps for any possible privacy risks, or other unwanted behavior like being overly taxing on your battery (you can even get these evaluations before you install an application, which is very handy).

This mobile security suite also gets top marks for the protection its antivirus engine delivers going by AV-Test’s findings (the other main test lab didn’t evaluate Norton recently).

Other features include call blocking to protect against spam phone calls, Wi-Fi security that alerts you when you connect to an insecure wireless network, plus anti-theft features that allow you to remotely lock a stolen (or lost) device, or wipe all your data.

All this adds up to an impressive level of protection for your Android device – but are there any downsides here? Well, the app is pricey, or at least the recommended asking price is, but given the discount on offer at the time of writing, it’s actually the same price as Bitdefender above (making it an excellent buy currently, given that you get coverage for three Android devices, not just one).

3. Avast Mobile Security.

A great free Android antivirus offering, but it does show adverts.

Specifications.

Reasons to buy.

Reasons to avoid.

Antivirus giant Avast has produced another quality app which goes above and beyond being a mundane scanner, although that said, it does virus scanning very well, and is highly rated by the independent test labs.

Avast Mobile Security’s nifty features include an anti-theft system allowing you to track and remotely lock (or wipe) your Android device if it’s stolen, or if you lose it. There are also some interesting performance enhancing features including a junk cleaner to free up storage space, and a ‘RAM boost’ which aims to speed up your device.

The app used to be paid but is now free, albeit supported by ads. You can pay a small monthly or yearly premium to remove the adverts if they annoy you, though. Another very useful premium feature is ‘in-app locking’ whereby your device will ask for a PIN before opening certain apps. This prevents malware from launching apps such as internet banking automatically.

4. AVG AntiVirus Free.

Hugely popular Android antivirus app.

Specifications.

Reasons to buy.

Reasons to avoid.

AVG AntiVirus Free is another high-quality app for securing your Android device, and it delivers an impressive level of protection at no cost whatsoever. In fact, it uses the same well-liked antivirus engine as Avast above (remember that Avast bought up AVG back in 2016).

This isn’t the same product, though, and it doesn’t have some of the features you’ll find in Avast’s freebie offering. It is, however, still built around very robust core antivirus protection, plus anti-theft features which allow you to locate, lock or wipe a stolen (or lost) phone. Also like Avast, this app is ad-supported, but by upgrading to the premium version you can get rid of those adverts.

The paid Pro version of AVG comes with a whole load of extra features, including extended anti-theft capabilities (such as the device locking itself if the SIM card is replaced, and sounding an alarm), a Photo Vault to secure your photos, an app lock, Wi-Fi security scanner, and additional privacy settings, such as for blocking callers.

There are also a host of other features such as performance enhancement measures, which aim to kill unnecessary processes, turn off battery-draining settings, as well as deleting junk files such as those commonly found in temp and cache folders.

Note that you can try out all these Pro features for free, at least for the first two weeks when using AVG AntiVirus Free; but after that, you have to pay.

With so many features bundled in the Pro version, it’s no wonder this app is the most popular antivirus when you search for one in the Google Play store, with more than 100 million downloads, over 6.5 million reviews and an average score of over 4.5.

Android malware tries to trick you. Here's how to spot it.

Malicious apps are common, and they can drive you nuts with ads or steal your personal information.

Malware on Android phones can make you miserable. Here's how to prevent it or deal with a malicious app.

Omar Marques/SOPA Images/LightRocket via Getty Images.

Android malware is often deceptive. A mobile app called Ads Blocker, for example, promised to remove pesky ads from your phone, which sometimes pop up to cover your screen just when you're about to access something important. But people quickly found the app was nothing less than malware that served up more ads, according to security researchers.

It's just one example of malware that can frustrate Android phone users, plaguing them with ads that the creators get paid to display, even when they're looking at unrelated apps. Malware often also harvests fake clicks on the ads, doubling up on the value for the makers.

"They're making money," said Nathan Collier, a researcher at internet security company Malwarebytes who helped identify the bogus ad blocker in November, "And that's the name of the game."

Discover the latest news and best reviews in smartphones and carriers from CNET's mobile experts.

Researchers say adware like Ads Blocker is the most common type of malware on Android devices. An adware infection can make your phone so frustrating to use that you want to Hulk out and crush it, but Android malware can do worse things -- like stealing personal information from your phone.

Malware can be disorienting, getting in the way of how you normally use your phone and making you feel uneasy even if you aren't sure what's causing the problem. It's also common. Malwarebytes says it found close to 200,000 total instances of malware on its customers' devices in May and then again in June.

So how do you know if you have malware on your phone, and how can you stop it? Here are some takeaways from mobile malware experts on what you can do.

How malware on your phone works.

Mobile malware typically takes one of two approaches, said Adam Bauer, a security researcher for mobile security company Lookout. The first type of malware tricks you into granting permissions that let it access sensitive information.

Keep your Android phone safe from hackers with regular software updates.

That's where the Ads Blocker app fits in, and many of the permissions it requested sound like something a real ad blocker would have needed. But they also let the app run constantly in the background and show users ads even when they were using unrelated apps.

The second type of malware exploits vulnerabilities in phones, gaining access to sensitive information by giving itself administrator privileges. That reduces the need to get users to click "OK" on permissions requests, making it easier for malware to run without users noticing its presence on the device.

Signs of malware on your Android phone.

If you notice these things happening, your phone might be infected:

You're seeing ads constantly, regardless of which app you're using. You install an app, and then the icon immediately disappears. Your battery is draining much faster than usual. You see apps you don't recognize on your phone.

These are all worrying signs that mean you should investigate further.

Ransomware on Android phones.

Another type of malware is ransomware. Victims typically see their files locked away where you can't use them. Typically, a pop-up demands payment in Bitcoin to get them back. Most Android ransomware can only lock up files on external storage, such as photos, Bauer said.

What mobile malware can do to your phone.

Besides making you miserable with constant ads, mobile malware can access private information. Common targets include:

Your banking credentials Your device information Your phone number or email address Your contact lists.

Android phones infected with the Anubis banking trojan can invisibly log passwords entered by users.

Courtesy of Lookout.

Hackers can use this information for a variety of malevolent tasks. They can commit identity theft with your banking credentials. The Anubis banking Trojan, for example, accomplishes this by tricking users into granting it the access to an Android phone's accessibility features. This, in turn, allows the malware to log every app that you launch and the text you enter, including passwords. After you grant the permission one time, the malware's activity is completely invisible on screen, with no sign anything malevolent is happening as you log into your accounts.

Hackers can also use malware to collect and sell your device and contact information, until you're flooded with robocalls, texts and, oh yeah, more ads; and they can send links for more malware to everyone on your contacts list.

If you suspect your information has already been caught up in the robocall machine, you can see what your phone carrier offers to help keep the annoying phone calls to a minimum. For example, customers of T-Mobile, Sprint and MetroPCS will have access to Scam Shield , a free app announced in July.

How to stop malware on your Android phone.

Whether you think you already have malware on your Android device or you just want to protect yourself, there are clear steps you can take.

First, keep your phone's software updated. Security experts consistently rank a current OS and updated apps as one of the most important steps users can take to protect their devices and accounts. If you already have malware running on your phone, software updates from your phone-maker -- say Android 10 or the upcoming Android 11 -- can patch vulnerabilities and cut off the access the malicious software enjoyed. Updates can also keep malware from working in the first place.

Next, review what permissions your apps have. Does a game have the ability to send SMS messages? That's probably unnecessary and could be a red flag, Bauer said. Keep this in mind when installing apps in the future, too.

Removing apps you think are malicious can be tricky. At times you can just remove the app's permissions, delete the app and be done with it. Other malicious apps will give themselves administrator privileges, so they can't just be deleted without extra steps. If you have trouble removing a specific app, you can try looking it up online to find what has worked for other people.

You can also consider installing antivirus apps. These services can sometimes slow your phone, and they do have heightened access to your phone in order to spot malicious behavior, so you have to choose one you trust. And you're likely to want to choose the paid option if you can, both to unlock all the best features and to avoid seeing even more ads.

Still, the apps can warn you about malware on your phone and offer you customer service when you need to deal with something nasty. At the very least, you can use a well-known program like Malwarebytes, Norton, Lookout or Bitdefender to scan your device if you think you already have malware installed.

Finally, you can get rid of or avoid Android apps downloaded from third-party app stores. These apps don't go through review by Google and can more easily sneak malicious software onto your phone. Google doesn't catch everything before it gets on your phone, as reports about malicious Android apps being removed show, but sticking to the official Google Play Store -- and having a direct outlet to report problems you encounter -- is a further line of defense.