



A Guide to Mobile Malware:

Protecting Your Device

Protecting Your Device.

As mobile devices have become an integral, almost essential, part of our daily lives, the risk of malware infections has grown, particularly within Android devices.

This guide takes you through the complex world of mobile malware, shedding light on how these infections occur, the potential consequences, and, most importantly, offering advice on protecting yourself from such threats.

While our focus is primarily on Android-based devices due to their higher susceptibility to malware, it's essential to acknowledge that Apple's iOS platform isn't entirely invincible. Despite iOS's robust security

measures making it a more challenging target for cybercriminals, the possibility of compromise exists, albeit small. This guide will also discuss situations and potential vulnerabilities that might put iOS users at risk.

So, whether you're an Android user grappling with the growing threat of malware or an iOS user navigating through a relatively secure environment, this guide provides practical advice and preventive measures to enhance your digital safety. Knowledge and awareness are the cornerstones of cyber security. We're here to help you build that strong foundation.

How does malware get onto your phone?

While our understanding of traditional computer-based malware has grown, navigating the territory of mobile malware presents unique challenges.

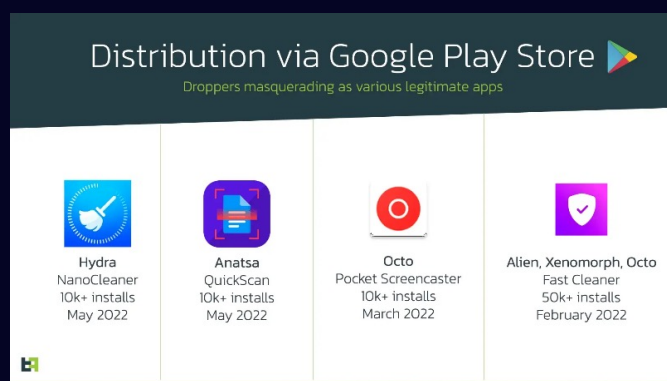


Mobile malware, which operates differently than typical computer-based malware, finds its way into smartphones via less overt means. Instead of relying on phishing emails or dubious network connections, mobile malware often sneaks in through a front door: official app stores, such as Google Play and the Apple App Store.

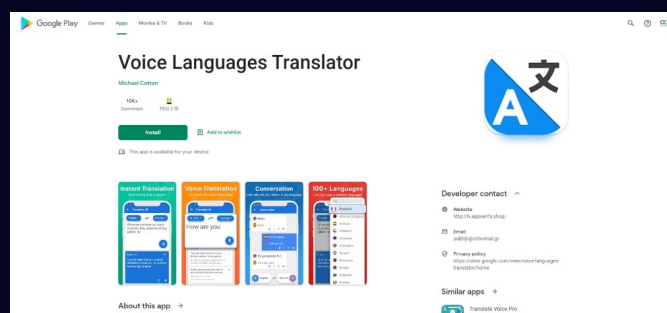
Identifying these malicious apps can be tricky, as they often disguise themselves as legitimate apps. Everything from games, calculators, and file managers to emoji keyboards may not be as benign as they seem. The fact that these apps function as advertised initially makes it even harder to detect any hidden malicious intent.

A more disingenuous tactic observed is that certain apps may not even contain any harmful elements at the outset. This allows them to pass initial security checks and gain popularity among users. Once these apps have established a user base, the creators push updates that carry the hidden malware.

Another significant source of mobile malware comes from the practice known as 'sideloading' apps. Sideloading refers to the installation of apps from sources outside the official app stores, often from websites or third-party app stores. While sideloading can sometimes be used for legitimate purposes, it's frequently exploited to distribute malicious apps. These unofficial sources lack the stringent security checks that official app stores provide, thereby increasing the risk of malware.



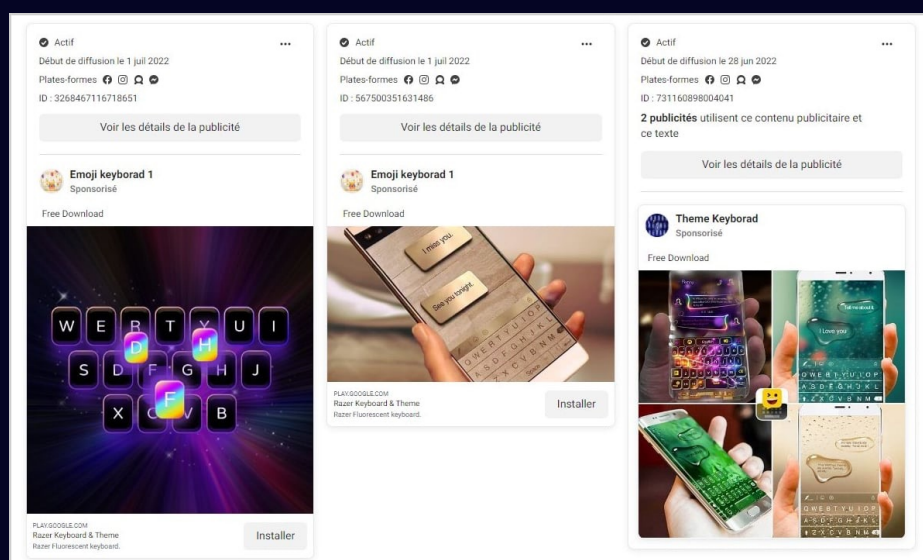
ThreatFabric analysts discover droppers on Google Play having thousands of installations and distributing banking Trojans since the beginning of 2022. Source: <https://www.threatfabric.com/blogs/h1-2022-mobile-threat-landscape>



This language translator was found to be intercepting 2FA codes sent through text. Source: <https://blog.pradeo.com/pradeo-identifies-app-joker-malware-google-play>

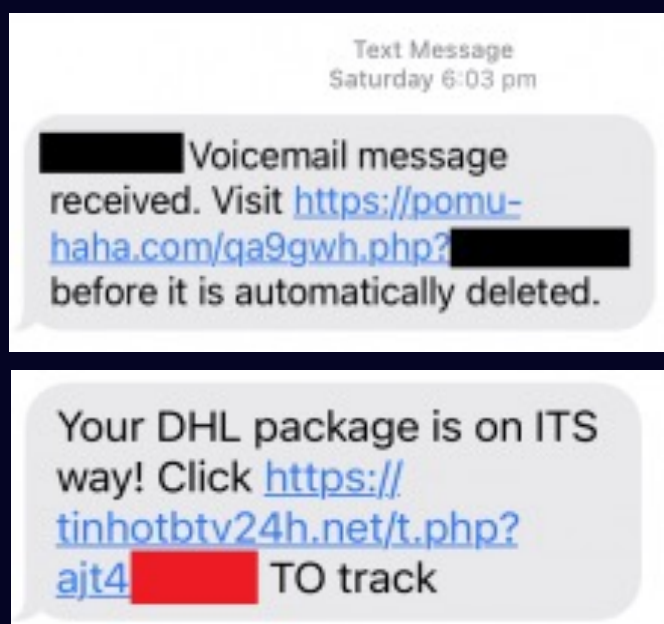
Cybercriminals also use popular social media platforms like Facebook and Instagram to promote their harmful software. With advertisements cleverly disguised to link to legitimate app stores, these covert campaigns often evade detection by the platform's

monitoring systems. As a result, unsuspecting users may unknowingly download malware-infected apps, highlighting the need for constant vigilance when interacting with app store links, even on familiar social media sites.

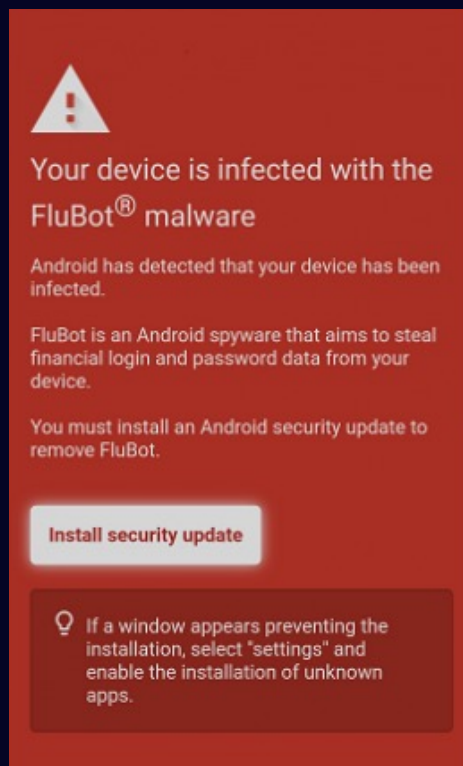


These Facebook ads were found promoting apps that were designed to secretly read users' text messages. Source: <https://www.bleepingcomputer.com/news/security/new-android-malware-on-google-play-installed-3-million-times/>

Mobile malware can infiltrate your device through seemingly innocent text messages, a common phishing technique cybercriminals employ. As highlighted by organisations like Australia's ScamWatch, malicious campaigns often utilise persuasive text messages to distribute harmful software. Although the websites linked in these deceptive messages may vary across different campaigns, their ultimate objective remains consistent: persuading users to download an app to solve a problem outlined in the original text message. This underlines the necessity of maintaining high caution when receiving such messages and abstaining from downloading apps suggested by unfamiliar sources.



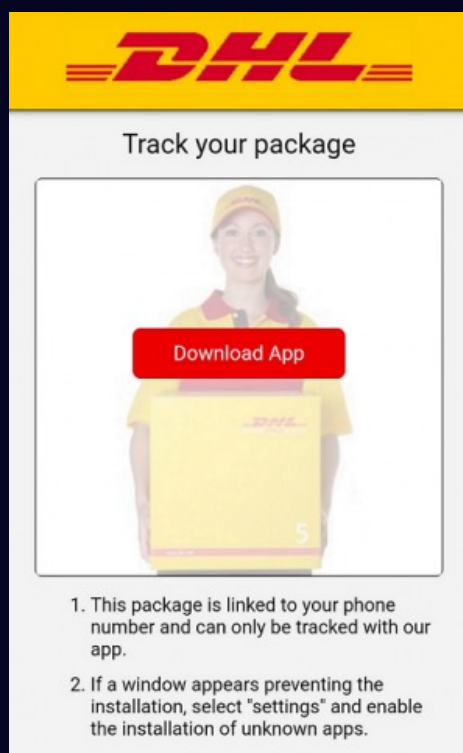
An example of phishing messages used to spread mobile malware. Source: <https://www.scamwatch.gov.au/news-alerts/missed-delivery-call-or-voicemail-flubot-scams>



Clicking on the links within the above text messages took users to sites like these, pushing them to download an app or install a "security update". Source: <https://www.scamwatch.gov.au/news-alerts/missed-delivery-call-or-voicemail-flubot-scams>

In addition to the recognised delivery mechanisms for malware, such as social media, phishing, and 'smishing' (SMS-based phishing), a vast landscape of unofficial Android app stores exists. These stores offer many applications for download and, unfortunately, serve as popular playgrounds for threat actors.

Within this landscape, many malware versions cleverly masquerade as premium apps ordinarily chargeable on Google's official platform. Lured by the appeal of a freebie, users may unknowingly download these infected versions from third-party stores, mistakenly believing them to be their genuine, cost-free counterparts.



While most Android devices are designed to alert users against such risky downloads, a potential loophole exists. Users can turn off the security feature that prevents installations from unknown sources within their Android settings. While providing flexibility, this freedom also allows malicious apps to access devices.

Navigating these less-regulated app sites calls for increased caution and awareness. Understanding that free versions of typically paid apps might come with unwelcome add-ons, such as malware, is essential to securing your mobile device.

What does mobile malware do?

Despite a varied range of operation methods, both traditional and mobile malware share a common objective: financial gain. However, that's where the similarities cease, and mobile malware carves out its unique path of malice.

Unlike ransomware, which tends to hold entire systems hostage in computer malware, mobile malware often adopts a subtler approach. It prefers to linger inconspicuously on the device, making minor alterations without raising the user's suspicion. Let's explore some of the different types of mobile malware:

✦ **Banking Trojans:** focus on stealing banking and financial credentials. In addition, they may provide attackers with backdoor access to the device. A 'backdoor' in cyber security refers to bypassing standard authentication or encryption in a system, a product, an embedded device, etc. Attackers exploit these backdoors to access the device without the user's knowledge, allowing them to control the device or extract sensitive information remotely. The increasing prevalence of these Banking Trojans is a rising concern in the mobile world.

✦ **Adware:** Adware capitalises on serving unwanted advertisements, often in places on your phone typically free from ads, like your home screen or web browser. Some newer variants run ads invisibly in the background, making their activity even less discernible.

✦ **Spyware/Stalkerware:** this steals a wide range of information from your device, including text messages, location, login details, photos, and emails. Though typically deployed by threat actors to acquire login credentials, spyware has also been misused by stalkers and domestic abusers. Avast reported a 300% increase in stalkerware use in the UK over the past three years.

✦ **SMS Trojans:** these manipulate a phone's SMS functions, aiding threat actors in creating new accounts. SMS Trojans exploit the compromised phone as a "virtual number" to receive one-time codes and two-factor authentication codes, unbeknown to the owner.

✦ **Fleeceware or Subscription Malware:** This type of malware enrolls the victim's devices in unwanted services, with charges applied directly to the mobile carrier, making detection more challenging. Some versions offer a deceptive "free" trial, which can be difficult to discontinue. While Google and Apple have taken measures against these, they remain an issue, notably affecting Apple iOS devices.

✦ **Cryptomining Malware:** While not as prevalent as in previous years, cryptomining malware uses the phone's processing power to solve complex mathematical problems required for mining cryptocurrencies, potentially causing severe damage to a victim's device.

Awareness of these types of mobile malware and their tactics underlines the importance of vigilance in protecting our mobile devices. As the mobile malware landscape evolves, so too must our defences.

Building Defences – Preventing Mobile Malware

Fortunately, the threat of mobile malware need not be a cause for alarm. With modern smartphones offering built-in protections and a measure of discretion on the user's part, warding off these digital nuisances can be remarkably straightforward. Here are some practical steps to enhance your device's security:

- ✦ **Utilise inbuilt security features:** Make the most of your device's native protective measures, such as Google's Play Protect. These security tools, generally activated by default, serve as an antivirus shield for your phone. They conduct regular sweeps for malicious apps and prevent malware operations. It's crucial to keep these safeguards activated, despite having the option to disable them.
- ✦ **Inspect apps before installation:** Always review the ratings, reviews, and download count of an app before installing it, especially if it originates from an unknown developer. Beware that cybercriminals may fabricate reviews and download numbers to give an illusion of legitimacy. Fake reviews often repeat the exact phrases, so thorough scrutiny of the reviews can save you from falling into a trap.
- ✦ **Exercise caution with permissions:** Today's smartphones require apps to ask for consent before accessing specific features or data on your device. Be wary of apps that request permissions beyond what seems necessary for their functionality.
- ✦ **Recognise phishing attacks:** Develop an understanding of phishing tactics and avoid downloading apps suggested by unfamiliar websites. Phishing schemes often exploit high-stress scenarios to trick users into downloading harmful apps. Being aware of these tricks can fortify your defences significantly.
- ✦ **Stay updated:** Keeping your device updated with the latest software is a crucial defence against potential attacks. Each software update typically includes fixes for known bugs or vulnerabilities that threat actors might exploit. Ensuring your device is updated can help prevent you from becoming an easy target.
- ✦ **Take advantage of free premium antivirus software:** If available from your bank or employer, consider using complimentary premium antivirus software. These security applications are highly efficient at detecting malicious activities and often include additional protective features like secure browsing and scam call protection.

Implementing these simple yet effective measures can provide peace of mind, safeguarding your device and the personal data it holds, and making your devices safer and more secure.

This guide was created in collaboration with the Cyber and Fraud Centre's financial and banking partners.



📍 Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

☎ 01786 447 441

✉ enquiries@cyberfraudcentre.com

🏠 www.cyberfraudcentre.com

🐦 [@cyberfraudcen](https://twitter.com/cyberfraudcen)

🌐 [cyber-and-fraud-centre](https://www.linkedin.com/company/cyber-and-fraud-centre)