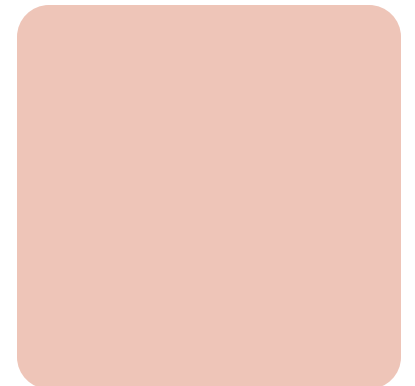


The McAfee Consumer Mobile Threat Report

How cybercriminals are trying harder to appear legitimate and how to protect you and your family from these mobile phone threats



2022



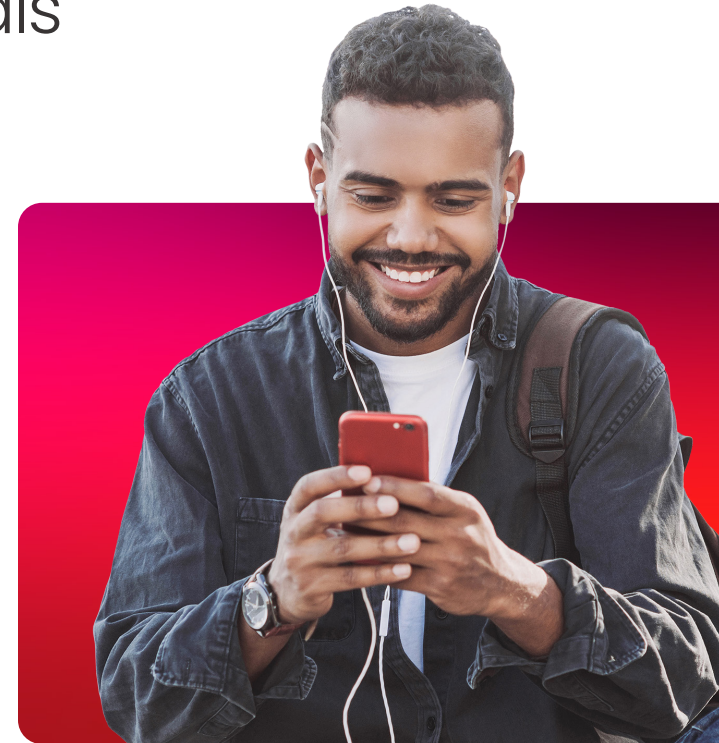
Detect me if you can: How cybercriminals are trying harder to appear legitimate and how to spot them

Cybercriminals are using increasingly sophisticated and personalized attacks to trick you into giving up your personal information or con you into giving them your money. These **criminals are using a wide range of techniques, both technical and social, to try and evade both security scanners and your judgement.** The primary goals of these attacks are to capture personal info to build better databases, more finely target their attacks, and of course make some money.

Whether you are being offered a quick tax refund, an easy way to get a gaming advantage, or a cheaper way to mine cryptocurrency, if a deal is too good to be true, it probably is. Like cheap watches or handbags for sale by a street vendor, you don't have to be a watch or fashion expert to know that the items are fake. The same level of **skepticism and a critical eye are essential tools to protect yourself**, your family, and your growing collection of digital devices. The security defenses for your phone are adapting to these types of threats, adding and enhancing important features such as phishing and

fraud alerts, identity protection, and alerts if personal info is found on the dark web.

In this edition of the McAfee Consumer Mobile Threat Report, we take a closer look at some leading examples of techniques that cybercriminals are using to trick or defraud you via your mobile phone. While they may not be the most common attacks, the number of victims doesn't necessarily represent how sophisticated or dangerous they are. These examples are **some of the more sophisticated attacks, using real logos, quality graphics, and personalized messages.**



We hope this provides a useful resource for protecting your digital life, mobile devices, and personal information, so that you can live your life online with confidence.

Steve Grobman

Senior Vice President &
Chief Technology Officer

Carlos Castillo

Manager, Mobile
Security Research

**Contributions from the Mobile Malware
Research Team**



Look for this sign to get important clues to identify tricks and traps.

Smishing for malware

Criminals are getting more sophisticated and personal in their attempts to spread malicious software and steal information. By building or buying databases of personal information, they send messages to phones that are personally addressed to the individual, making them look legitimate and tricking people into downloading their malware. Learning how to detect these attacks is critical to protecting mobile devices.

McAfee's Mobile Research team has identified several recent mobile malware attacks that **use personalized text messages to appear more credible**. The two examples outlined here are targeting users in India and Japan, but this technique appears to be growing around the world. The messages and malware often include authentic-looking logos, icons, and websites, making them more difficult to distinguish from legitimate communications. However, they often prompt the user to download software directly from their included link, instead of going through Google Play, which should be recognized as an immediate red flag.

Tax filing in India

This example of a personalized smishing attack pretends to be from the Income Tax Department in India. First noticed in May 2021, **these messages are addressed directly to the phone owner and include the official government logo**. Some variants mention an urgent update about the owner's tax refund, request immediate action, and include a personalized signature from a recognizable name.



Smishing for malware

What's the trick?

- Text pretends to be from legitimate organizations, prompts the user to download "important" software that is really malware.
- Steals personal information, contacts, and SMS messages from the device.
- Adds stolen contacts to their list of people to target to fuel their campaign.

Why it works

- Uses personal information such as full names to appear legitimate.
- Realistic-looking web page seems legit.



SMS + phishing = Smishing

- SMS messages (Short Messaging Service, most common type of phone texting).
- Phishing: fake emails that appear to have been sent by legitimate, trusted organizations.

REPORT

If the user clicks on the included link, they are taken to **a realistic-looking e-filing tax webpage pretending to be from the Indian government**, complete with the user's name and tax-department logos. There are several variants of these webpages that use slightly different wording and next steps. In general, they ask the user to download and install a mobile tax app, grant all requested permissions, register or login with their tax credentials, and then promise to transfer a tax refund easily and instantly to their account.

Of course, there is no tax refund. The installed malware **steals the user's information, including email addresses, phone numbers, address book contents, stored text messages, account information, and other accessible personal or financial details**. Due to poor server security by the cybercriminals, this information was also publicly exposed on the Internet, amplifying the potential threat. Personal data like this can then be used to create other realistic text messages to trick more users into providing account information or downloading malware, providing additional fuel for this and other malware campaigns to appear even more credible.

McAfee was the first to identify this threat called **Android/Elibomi**. The McAfee mobile app will block this malware if it's present on a customer's mobile device and the user will receive an alert.

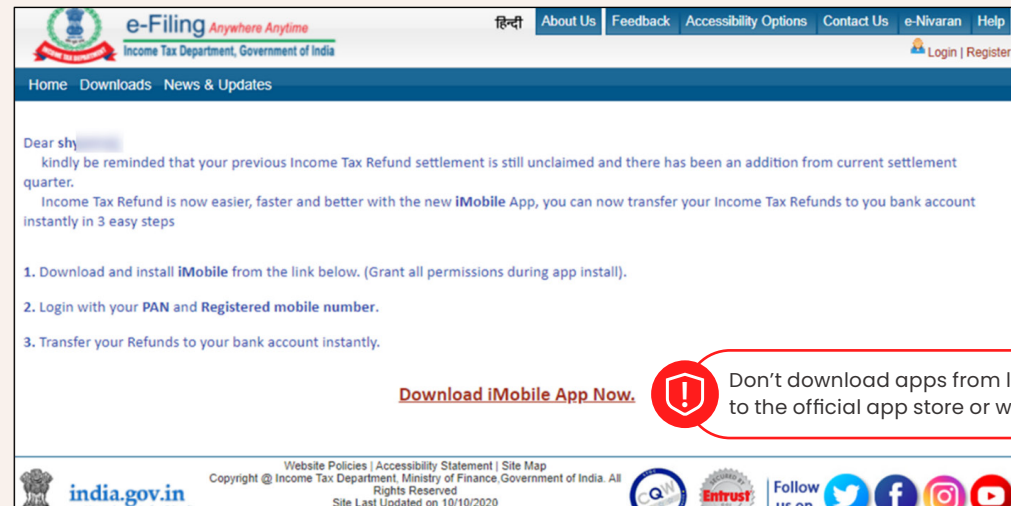


Figure 1. Screenshot of fake tax webpage

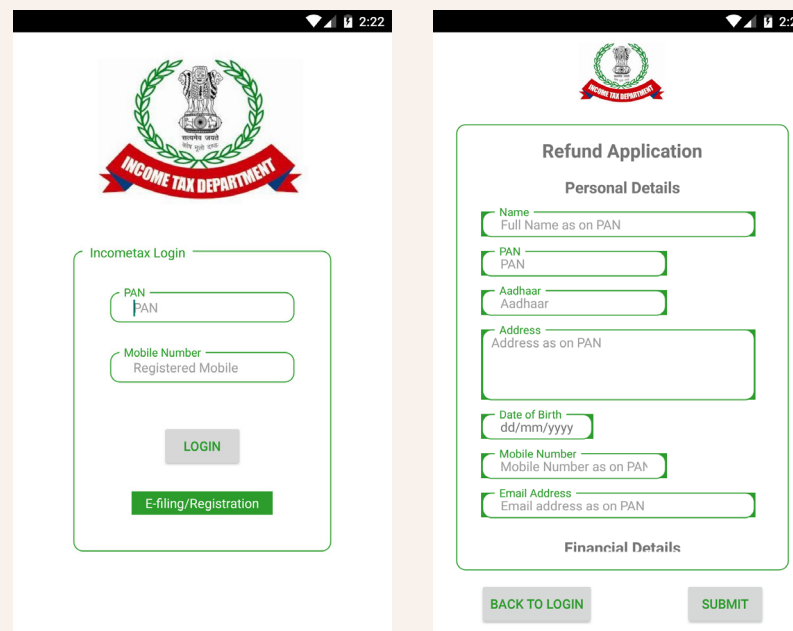


Figure 2. Fake screens designed to capture personal and financial information

SMS spy in Japan

Another smishing example from the malware campaign called Roaming Mantis has been targeting mobile devices in Japan since early 2021. These fraudulent messages pretend to be from a logistics company or a cryptocurrency exchange. For example, **users receive a notification of a missed package delivery or an alert of an abnormal login attempt** to the user's crypto account. Clicking on the included link takes the user to a webpage telling them that they need to update to the latest version of Chrome or Google Play for better security. Both messages are followed by a link to download the fraudulent software.

During installation, the malicious software asks the user to grant the requested permissions, or the app may not work properly. Once installed, **the malware copies and transmits the user's contacts and stored text messages to a command-and-control server** used by the attackers to communicate with their malware. This attack also appears to be capable of sending its own text messages, possibly to spread the infection to other users. At the time of writing, more than 16,000 unique devices have been infected with this malware.

McAfee was the first to detect this new Roaming Mantis malware as **Android/SmsSpy**. When detected, customers with the McAfee mobile app will receive an alert that the threat was blocked, which further protects them from any data loss.

How to not get caught

These are just two examples of the increasing personalization and sophistication of smishing attacks. To avoid getting tricked, mobile device users should be very cautious of links received in text messages, especially if they are from unknown sources. They should use other means to validate the contact info and message content. For software installations, always go to the organization's legitimate website or the Google Play store. Reliable and up-to-date security applications can also help protect against these and many other threats.



TRANSLATION:
Secure internet security.
Your device is protected.
Virus and spyware protection ✓
Anti-phishing protection ✓
Spam mail protection ✓

TRANSLATION:
At first startup, a dialog requesting permissions is displayed. If you do not accept it, the app may not be able to start or its functions may be restricted.

Be suspicious of apps downloaded from untrusted sources urging to grant all permissions as soon as the application is opened.

Chrome

本製品の機能や稼働にアクセスするアプリ / 機能を初めて起動すると、アクセス権限の許可をリクエストする確認画面が表示されます。許可をしないとアプリ / 機能を起動できない場合や、機能の利用が制限される場合があります。

Figure 3. Fake Chrome and Google Play malware screens

Don't get gamed

Gaming hacks and cheat tools that provide players with extra capabilities or shortcuts are very popular. In this case, the mobile game cheaters get cheated by cybercriminals who have added malicious code to an existing open-source game hacking tool. Once this tool is installed, it steals account information such as user ids and passwords for multiple accounts including Facebook, Google, Twitter, and a popular gaming site.

PlayerUnknown's Battlegrounds, known as PUBG, is a very popular battle royale game where multiple players fight until only one remains standing. PUBG quickly rose to the top spot after its initial release in 2017. In this game, a group of players are parachuted onto an island empty handed and must collect weapons and objects with the objective of surviving to the end by killing all other opponents. Like most competitive games, **hacks that help the user win are widely available.**

Hacking royale against PUBG

Cybercriminals took advantage of the open-source development platform known as GitHub to add their own malicious code to an existing gaming hack. This code **targets mobile PUBG players around the world** who join chat channels and social media groups that promise to help them get advantages in the game. Just one of these channels had more than 54,000 subscribers, showing the large reach of this attack.



Game Hacks

Gives players an unfair advantage by granting them capabilities that otherwise would not be available by design, such as seeing other players through walls, automatically hitting weak points without aiming, or exploiting game vulnerabilities to gain in-game currency without earning it through gameplay.



Stealing social media and gaming credentials

What's the trick?

- Malicious code inside a mobile game hacking app being shared via instant messaging and chat tools.
- App requests superuser access to the user's device.
- Steals information on the user's social network and gaming accounts.

Why it works

- Mobile app promises extra info for the player on the screen, such as health of other players or objects they are carrying.

REPORT

McAfee's Mobile Research team has **identified a piece of malware that has been added to an open-source game hacking tool** called "DesiEsp." When a user installs the malicious DesiEsp app, it requests superuser access to the device and warns them that it may not work properly if the access is not granted.

This takes advantage of the fact that most game hacks need this superuser access to work properly, so the request would not be seen as unusual. Once the malware gets superuser access, the entire mobile device is compromised and the criminals can steal account information without any further user actions. Hiding in the background, the malware tries to read the account and application databases on the phone to **get user ids and passwords and other personal or sensitive details**.

The malware also uses Android's accessibility services to watch for login screens and capture info as the user types, as an alternative in case superuser access is not granted, because the malware itself does not have the ability to take control of the device. Common account targets include social media apps like Facebook, Google, and Twitter, and the account details for PUBG itself. The stolen credentials are typically used to try to break into other accounts, build fake accounts to damage reputations, post fake reviews, or even post fraudulent articles for sale.

Sending hacks by Telegram

Another attack campaign is targeting users of PUBG through chats and messages related to the game on the popular messaging platform Telegram. Criminals take advantage of apps like Telegram to **reach more users and hide within a legitimate online app**. Since apps on Google Play are typically scanned by Google for potential malware, cybercriminals include links to their own website for users to download the hacked gaming app so they don't get caught.

The McAfee Mobile Security app identifies this threat as **Android/Stealer** and alerts the mobile user that the malware was blocked on their device. However, the malware authors are producing variants that try to avoid detection with various techniques, such as encrypting or otherwise disguising their code. Gamers should **be very careful about downloading and installing game hacking tools**, especially if the tools request superuser permissions or access to accessibility services. Reliable and up-to-date security applications can help protect against this and many other threats.



Figure 4. Mobile game hacks in action

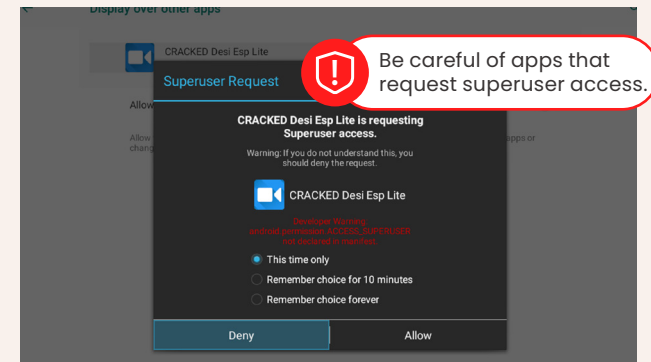


Figure 5. Screenshot of a malicious app message asking for superuser access

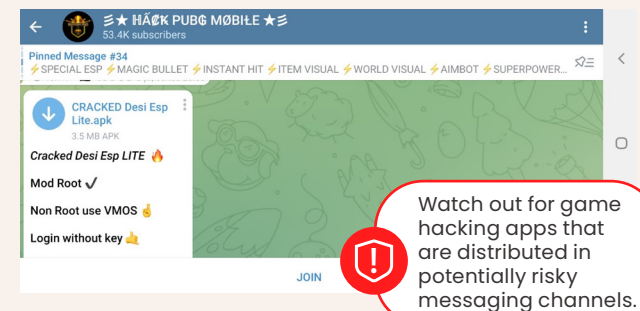


Figure 6. Repackaged game hacking tool distributed via Telegram

Mining for nothing

The growing popularity of cryptocurrency is providing criminals with new attack opportunities. Some malicious apps and webpages target mobile devices to hijack the device's processor for "mining" or creating new coins for the criminals. This new attack uses a fake app that promises to mine cryptocurrency for the user with cloud-based services for a small fee. But it just takes the user's money and does nothing.

Cryptocurrency mining is the process of using a computer to solve complex puzzles that, when completed, result in the creation of a new coin that has monetary value. The dramatic rise in value and popularity of cryptocurrencies over the past few years has **caught the attention of cybercriminals**. This recent **scam uses a variety of fake apps that promise to use the cloud to mine different currencies**, for a small fee. The catch is that they take the user's money but don't actually do any mining or increase the value of the wallet.

Selling nothing for something

Selling nothing for something has long been a favorite ploy of hucksters, cheats, and con artists. In this scam, criminals have constructed almost 200 very realistic-looking apps that promise the user a cheap way to get in on the cryptocurrency action. This global campaign, with heavier concentrations in United States, Brazil, and Turkey, claims to mine in the cloud for the user's benefit. Mining in the cloud instead of using the resources of a mobile device would save the user from potential overheating



Fake cryptocurrency mining (aka cryptomining) service

What's the trick?

- Fraudulent app and subscription service promises to mine cryptocurrency in the cloud for a small fee. But the user's cash value never goes above zero.

Why it works

- Fake app promises to "earn money by just having a phone in your pocket."
- Available for multiple cryptocurrencies, including Bitcoin, Dogecoin, Ethereum, and Litecoin.
- Charges user monthly until explicitly cancelled.



Cryptomining

- Cryptocurrency mining is the process of using a computer to solve complex puzzles.
- Completed puzzles result in the creation of a new coin that has monetary value.

REPORT

issues or even damage to the device. With **popular coins worth hundreds or thousands of dollars each, the small monthly fee of about five dollars appears extremely attractive.** Like anything that seems too good to be true, this one certainly is, charging the user every month but doing no actual mining.

These fake apps usually **have high positive customer ratings that have been artificially inflated by malware.** Typical signs of fake reviews include vague and repeated phrases, and a mix of mostly one-star and five-star ratings. Also, the descriptions on these apps often do not match the title or other info. For example, in the screenshot above, the title is “Bitcoin Miner,” but the application developer name mentions “Video Player.”

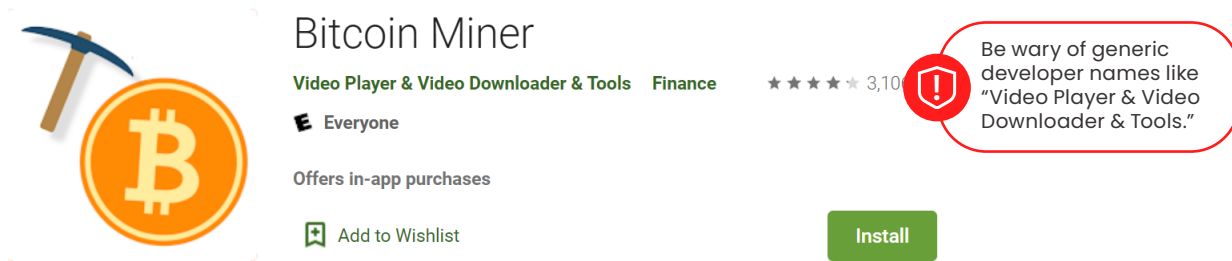
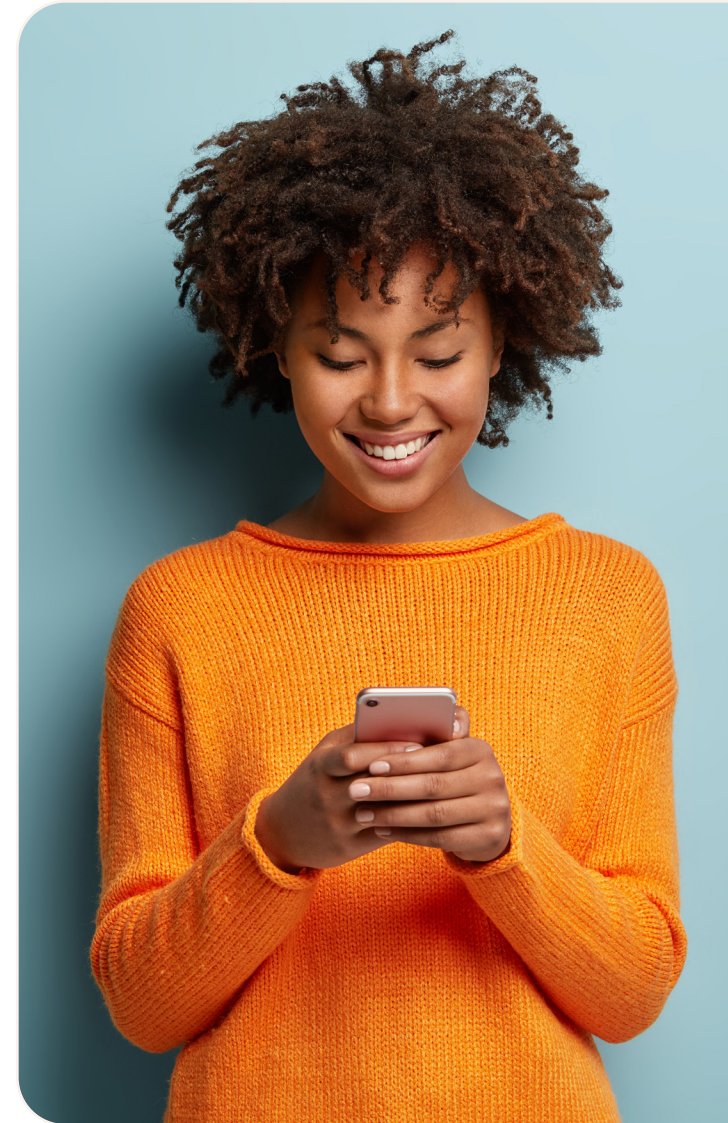


Figure 7. Example of a fake Bitcoin mining app

Building mines in the cloud

In this example, the initial app screen claims that a fee is paid just once at the beginning of the contract. However, **details on a later screen show that this is in fact a subscription with automatic payments every four weeks.** In addition to the performance level, subscribers are presented with the option of setting a target value or minimum payout, at which point the subscription is supposed to stop. After analyzing the code and running a few experiments, McAfee found that no actual cryptomining is done, the value of the user’s wallet never increases, and the subscription continues until it is canceled by the user.



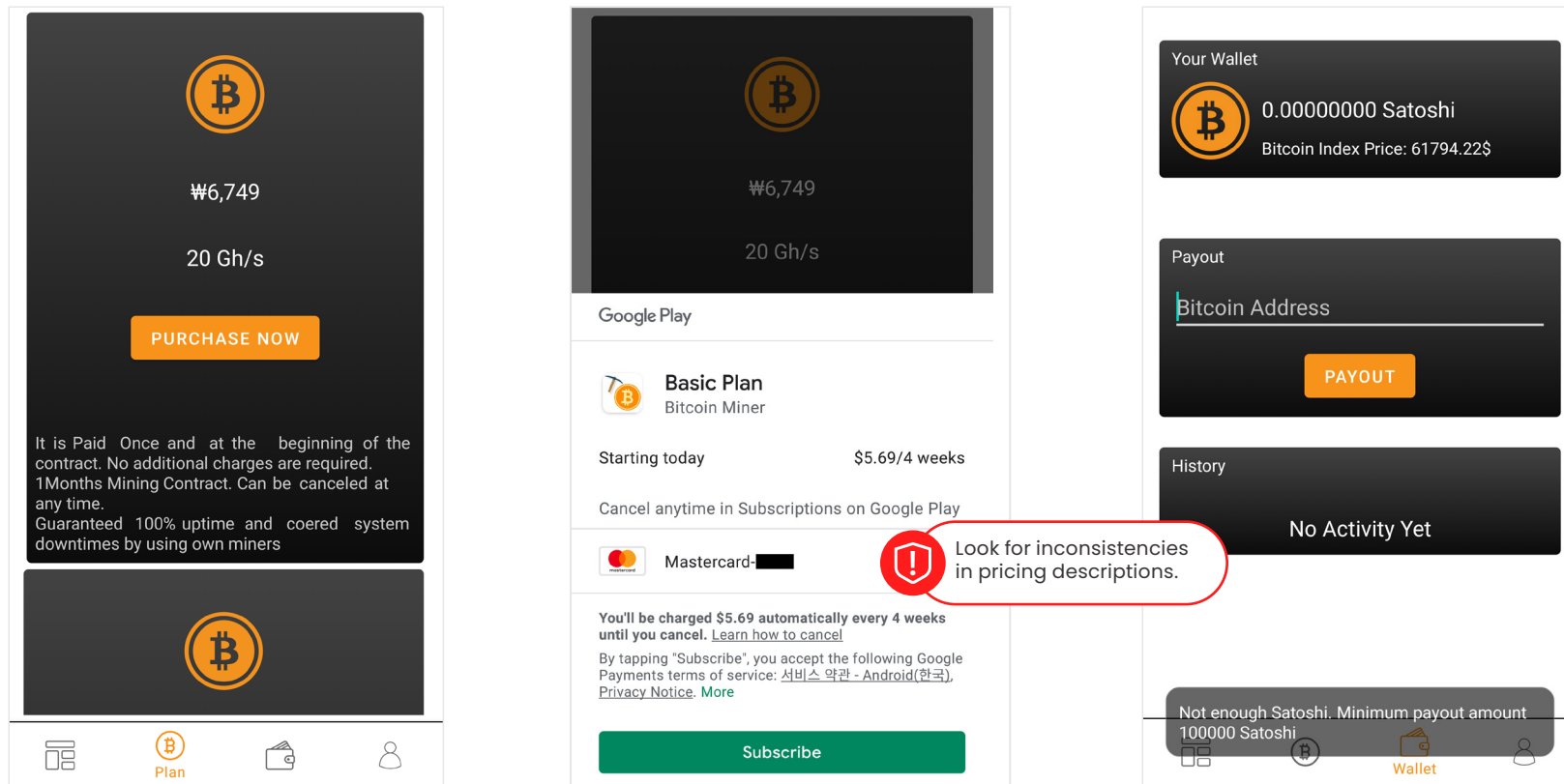


Figure 8. Fake app promising one charge but subscribing the user to monthly payments and never reaching the minimum payout amount.

The McAfee Mobile Security app identifies this threat as **Android/FakeApp** and will alert mobile users when the malware is blocked on their device. Following standard disclosure practice, McAfee reported these apps to Google and at the time of writing they are no longer available in Google Play.

These fake mining apps can be difficult to detect, as the code does not actually include any malicious features—it just doesn't do what it promises. Criminals are producing many variants of this app, targeting different countries and cryptocurrencies, and scamming almost 100,000 people and counting. Since it currently

costs thousands of dollars to mine one Bitcoin, depending on the cost of electricity, **offering to mine for five dollars a month is unrealistic.** Be wary! Offers that are too good to be true usually are. Reliable and up-to-date security applications can help protect against this and many other threats.

Apps that charge you to do nothing

Malware that subscribes unsuspecting users to premium text messaging services has been around for a while but is experiencing a new wave of popularity. These apps often have detailed descriptions of their features, slick graphics, promotional videos, and lots of reviews. However, they don't include any of the functionality described. They just prompt the user for a phone number and use it to subscribe to paid text messaging services that funnel money to the cybercriminals.

Premium text messaging services are an easy way for legitimate service providers to charge for information, contests, and other services. The messages often use short, 3-7 digit "speed dial" numbers and provide one-time, recurring, or on-demand services, such as flight info, sports results, or a daily joke. Messaging rates charged by *criminals* using this scheme can be 10s of dollars per message, and **recurring charges across multiple messaging services can quickly add a substantial amount to the user's phone bill** before the fraud is detected.

After installation, the fake app asks for a phone number and the criminals attempt to subscribe the user to one or more premium

text services. The user is also asked to confirm the subscription by entering a PIN number sent via text into a web page. Since the charges for these are included in the monthly phone bill, **it can take a while for users to realize that they have been defrauded** which makes it difficult to link the fraud to a specific app. Sometimes the fine print includes details about the premium subscription charges and how to cancel, possibly to satisfy legal requirements of the service provider. However, cancelling is usually quite difficult. Because the subscription service is linked directly to the phone number, uninstalling the app has no effect on the charges.



Fake apps and premium subscriptions

What's the trick?

- Multiple types of fake apps that claim to offer a variety of functions. Subscribes the user to premium messaging services unrelated to the promised app functionality. Does not include any legitimate capabilities.

Why it works

- Variety of fake apps with a wide range of popular functions, such as a photo editor, mobile game, or fitness planner.
- Asks for the user's phone number during installation.
- Uses phone number to subscribe the user to paid services and asks for a PIN or code sent via SMS to confirm the subscription.
- Details on how to unsubscribe are buried in the terms and conditions.

REPORT

Faking it repeatedly

McAfee and other security researchers have detected hundreds of these fake apps on Google Play over the past year, some of them with downloads measured in the hundreds of thousands. Many of these apps have a mix of one-star and five-star reviews. The five-star reviews often have similar wording, providing clues that the reviews may not be legitimate. The **one-star reviews give a more accurate representation**, mentioning that the app is fake, may ask for a payment after downloading, and generally complain that the app is a scam because they cannot access the promised functionality.

Paying a premium for nothing

In **last year's report**, we examined billing fraud malware in apps that had real functionality, as well as hidden capabilities that subscribed users to premium services. These new text messaging fraud examples are easier to create and get published on Google Play, because they don't have any real (or hidden) functionality. Instead, they just link to a webpage controlled by the criminals that asks the user for their phone number to unlock the promised features. This technique of **hiding malicious activity in a web browser instead of in the mobile app makes it easier to evade malware scanners**, as the criminals can change the link at any



FlowFX Photo Editor

Dovkar83 Photography

Everyone

★★★★★ 242

Add to Wishlist

Install



Always read the reviews to look for signs that the high reviews may not be legitimate.



City Bus

Fan For Fan Entertainment

Everyone

★★★★★ 617

Add to Wishlist

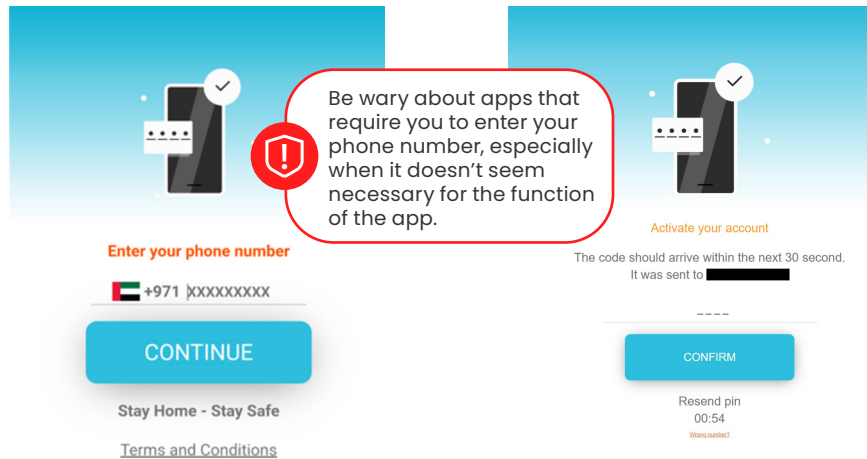
Install

Figure 9. Two examples of fake apps that are part of this campaign

REPORT

time. While criminals wait for the app to be approved by the app store, they can link to a legitimate website to bypass the automated malware analyzers.

The McAfee Mobile Security app identifies this threat as **Android/FakeApp** and blocks it on the customer's device. It can be difficult for a mobile user to identify these apps as fake without an up-to-date security application, as the malware code does not actually try to exploit a vulnerability or steal personal info—it just doesn't do what it promises and charges users for app functionality that doesn't exist. Criminals are actively producing hundreds of these fake apps using the same underlying code and disguising them with different names and graphics. Users should be skeptical about apps they download, **checking the positive reviews for repetitive wording and paying closer attention to the statements in negative reviews.** They should also be careful when providing their phone number to an app and any PIN or code after the phone number is provided. Reliable and up-to-date security applications can help protect against this and many other threats.



Gamezine is a subscription service that will automatically renew for 2.00 AED / 1 Day(s) for etisalat subscribers. You can unsubscribe from the service at anytime, by sending Stop 825 to 1741 for etisalat subscribers. To make use of this service, you must be 18 or more unless you have received permission from your parents or the person who is authorized to pay your bill.

Fake apps often include small, lengthy legal text to look legitimate, knowing the user isn't likely to read it.

Figure 10. Example of a fake installation step that requests the user's phone number

Figure 11. Example of a fake installation step that requests the PIN to confirm the subscription

One variant included code that first checked the device's battery level and loaded google.com if the battery was at 100 percent. Since the devices used in labs are always plugged in, this is a quick test to avoid easy detection.

Summary

Cybercriminals are upping their game, **using personal information and high-quality graphics to make their malware look like legitimate apps** or official messages. Because these attacks are successful at defrauding significant numbers of mobile users out of their money and information, more criminals will jump on this approach or expand their malicious campaigns. Security and mobile device providers are responding with broader protections and malware screening to safeguard online privacy, personal identity, and device security.

Smishing



Mobile smishing attacks are using personalized greetings in text messages that pretend to be from legitimate organizations to appear more credible. These messages often link to websites with authentic logos, icons, and other graphics, **prompting the user to enter personal information or download an app**. Users should be extra careful about text messages from unknown sources and should go directly to the organization's website to validate requests.

Gaming hacks



Cheat codes and hacking apps are popular ways to get extra capabilities in mobile games. Criminals are **exploiting this by adding malicious code apps** and promoting them on legitimate messaging channels. If installed, the malware steals account credentials for social media and gaming accounts. Gamers should use caution when installing game hacks, especially if they request superuser permissions.

Cryptomining



Cryptocurrencies are providing new opportunities for mobile device attacks. The latest ploy is phony apps that promise to mine coins in the cloud for a monthly fee. **Fake reviews and a low cost make them sound too good to be true—and they are.** These apps just take the money without doing any coin mining. With no actual malicious code, these apps are hard to detect, so users should be suspicious of being promised hundreds or thousands of dollars of crypto coins for just a few dollars a month.

Fake messaging apps



Another attack uses a variety of fake apps with slick graphics to trick users into premium subscriptions. Hundreds of these apps promise features such as mobile games or photo editing and are **supported by plenty of fake five-star reviews**. When installed, the apps ask for the user's phone number and verification PIN and use them to sign up for premium text services that direct payments to the criminals. Users should read reviews looking for vague statements, repetitive wording, and a mix of five-star and one-star ratings.

How to protect yourself

While threat tactics continue to change as criminals adapt and respond to detection and enforcement techniques, there are a few steps users should take to limit their exposure and risk.

Stay on the app stores

While some malicious apps do make it through the app store screening process, most of the attack downloads appear to be coming from social media, fake ads, and other unofficial app sources. Before downloading something to your phone, do some quick research about the source and developer. Many of these scams have been flagged by other people.

Watch requests for settings and permissions

Many malicious apps get the access they need by asking the user to grant them permission to use unrelated privileges and settings. When installing a new app, take a few moments to read these requests and deny any that seem unnecessary, especially for superuser access and accessibility services.

Update software

Developers are actively working to identify and address security issues. Both operating systems and apps should be frequently updated so that they have the latest fixes and security protections.

Be wary of too many five-star reviews

Cybercriminals often flood their Google Play apps with fake five-star reviews. Many fake or malicious apps only have a mix of five-star and one-star reviews. The five-star ones typically have vague statements and repetitive wording, giving clues that they are submitted by bots. Compare them to the one-star reviews for insight on the app's real capabilities.

Pay attention if your phone is acting funny

Devices that are behaving unusually may just have a basic tech issue but it can also be a sign of being hacked. Follow up when something is not quite right, check recent changes, or contact tech support from the mobile device vendor or security software provider.

Use security software

Comprehensive security software across all devices, whether they are computers, tablets, or smartphones, continues to be a strong defensive measure to protect your data and privacy from cyberthreats.

We hope this report helps you stay on the lookout for these and other mobile threats so you can safely and confidently enjoy your life online.



6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2022 McAfee, LLC. FEBRUARY 2022