

The 2023 McAfee Consumer Mobile Threat Report

**Digital everything:
Our phones help make it
possible. We'll tell you
how to reduce the risks.**

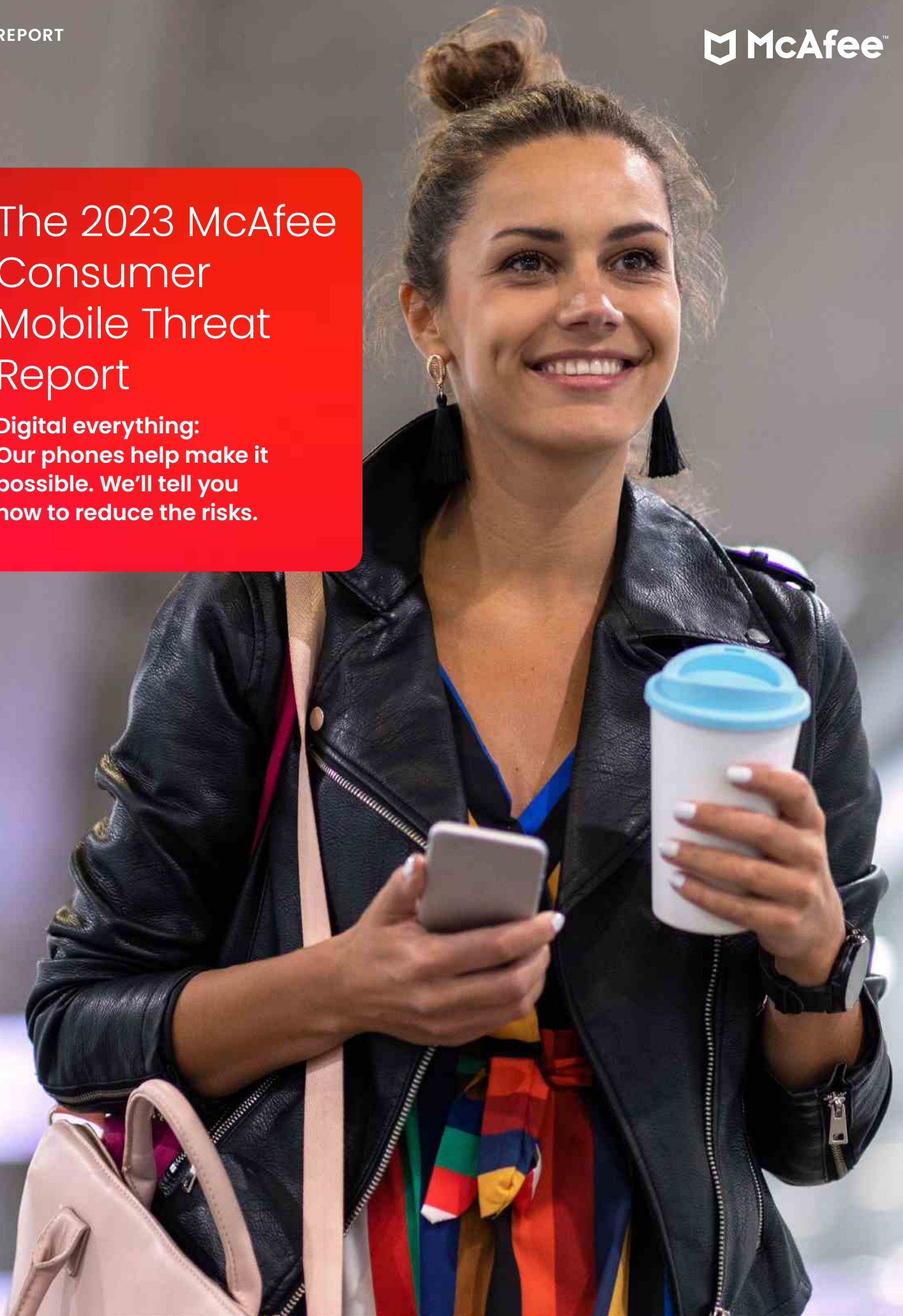


Table of Contents



Threat: Trusting apps because they look legit **5**

What types of apps? 5

How do they get into the store? 6

What bad things do these apps do? 6

Tips to protect yourself from fraudulent apps 8



Threat: Scammers sliding into your DMs **10**

What types of messages? 10

Have you heard about “pig butchering”? 12

Do you know about the risks of QR codes? 12

Tips to protect yourself from direct messaging scams 13



Threat: Using your personal phone for work **15**

Risk assessment: Mixing work and personal tasks 15

Tips to keep work and personal devices safe from each other 16



Challenge: Modern parenting of teens and tweens with phones **18**

More than just malicious apps 18

Influencers, challenges, and bullying 19

Tips on keeping your children safe on their phones 21



Top 10 malware families **23**

2023 Threat predictions **29**

New applications will impact the threat landscape 29

Misinformation and deepfakes 29

Investment scams 29

Fake loans 30

Metaverse 30

Social engineering 30

Future-proofing your mobile device 31

The 2023 McAfee Consumer Mobile Threat Report

Digital everything: Our phones help make it possible. We'll tell you how to reduce the risks.

When was the last time you looked at your phone? Research suggests that many of us spend approximately one-third of our day on mobile devices.¹ This shouldn't come as a surprise since our phones and other mobile devices are how we stay connected, pay bills, play games and keep our lives in order.

The end of 2022 saw the release of some game-changing applications such as OpenAI's ChatGPT chatbot and DALL-E 2 image generator. These tools have provided powerful artificial intelligence to the masses. While this creates exciting opportunities for innovation and productivity, it also provides those same opportunities to cybercriminals.

McAfee's Threat Research Team has the benefit of getting an inside look at today's mobile threats. Using this insight, we have created this report to help you better understand the risks and how to protect against them, so you can get all the freedom, control, access, and fun that our phones provide, while avoiding the potential pitfalls that cybercriminals throw your way.

We hope this provides a useful resource for protecting your digital life, mobile devices, and your family, so you can safely live your online life.

Steve Grobman

Senior Vice President & Chief Technology Officer, McAfee

Fernando Ruiz

Senior Security Researcher, McAfee Mobile Threat Research Team

Four broader topics presented themselves through this report, with each topic presenting several follow-on findings:

- **Topic One**—Threat: Trusting apps because they look legit
- **Topic Two**—Threat: Scammers sliding into your DMs
- **Topic Three**—Threat: Using your personal phone for work
- **Topic Four**—Challenge: Modern parenting of teens and tweens with phones
- **Top 10 malware families**
- **2023 Threat predictions**

Topic One: Threat



Trusting apps because they
look legit



Threat: Trusting apps because they look legit

Mobile apps are a big part of our lives, and they help us do so many things—getting from point A to point B, sharing content on social media, or managing budgets. But how do you know which ones to trust? Relying on the store’s security review processes to catch and delete malicious apps before you download one is not enough. The bad guys are getting cleverer at sneaking their apps into the stores, so a few more steps are necessary to keep your device and your data safe.

What types of apps?

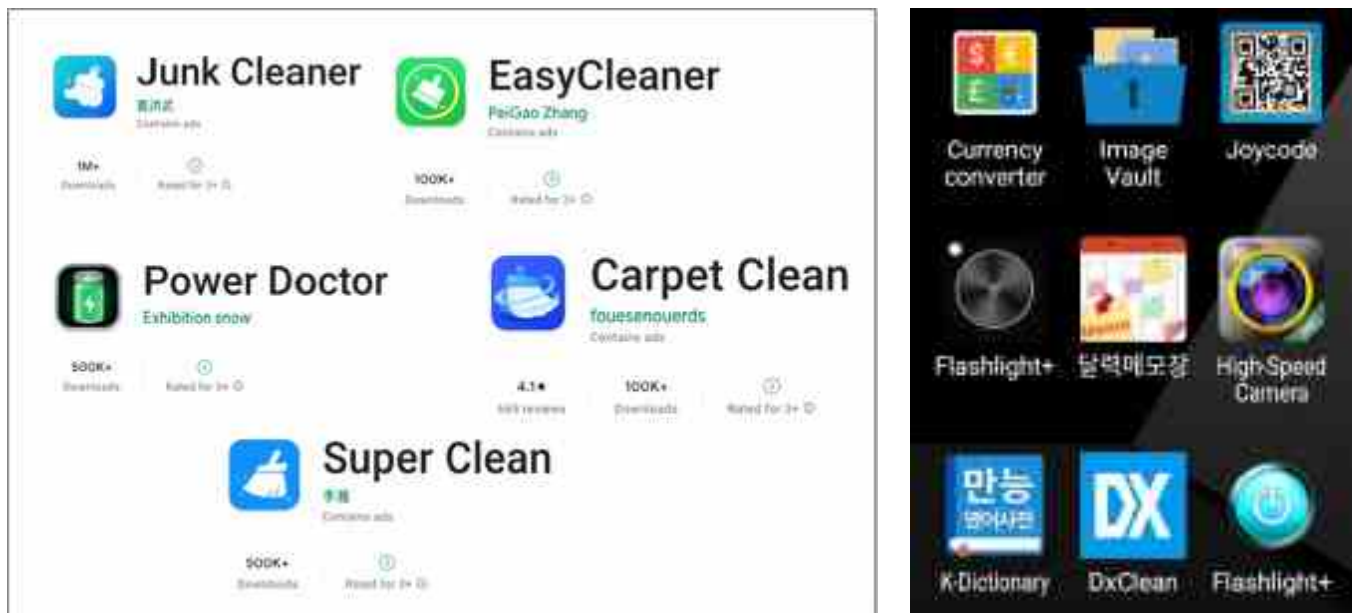


Figure 1. A variety of mobile apps that have been identified by McAfee as malicious. (Apps shown have been removed from Google Play.)

Malicious apps tend to fall into a few categories—things that are popular, easy to use, and seem outwardly harmless. Yes, this covers a lot of the apps that you are interested in—that’s kind of the point. So be extra careful when downloading apps, especially:

- Image editors and photography filters
- Business and phone utilities
- Gaming tips and cheats
- Social media tools

How do they get into the store?

Without getting into technical details and coding techniques, scammers tend to use a few tricks to get their malicious code past the inspectors. Knowing about these tricks can help you avoid bad apps or spot one quickly after you've installed it.

First, many malicious apps actually deliver some legitimate functionality. Just because the free photo editor or social media tracker you downloaded works, doesn't mean that it's not hiding something. Criminals often use encryption to hide their malicious code from reviewers, or they build in a delay, so the bad stuff doesn't show up until it has passed the tests. Another trick is to check the device's location and only behave badly in certain countries. Others download additional code to themselves after installation, keeping reviewers from ever seeing the malicious bits. Finally, sometimes criminals manage to infect legitimate apps by putting their code in a third-party code library that gets automatically included in the next software update.

What all of this means is that almost any app you come across could be malicious, so you need to take some extra steps to protect your phone, tablet, and digital life from the bad guys.

What bad things do these apps do?

Scammers are generally after money, or data that they can turn into money. Clicking on or creating fraudulent advertising and stealing user credentials are some of the most common swindles that these apps try. Much of this can happen in the background, so you may not even be aware of it.

If any of these things occur while you are downloading, installing, or using an app, stop the installation, or locate and delete the app immediately:

- The app asks for unnecessary permissions
- After installation, the app icon disappears from the menu
- You get advertising out of the context of an app, such as on the home screen or lock screen
- The web browser redirects you to an unrecognized website
- Your phone does unexpected things, such as turning on the camera, microphone, or location services
- Settings are changed, such as your default homepage or search engine





How AI is helping scammers

At the end of last year, OpenAI made news headlines with the launch of their AI image generator, DALL-E 2. This release ushered in a wave of AI-based mobile applications that could create artistic images based on photos. While some of these apps, like Lensa, are legitimate, [others may be malicious apps looking to capitalize on recent AI advancements.](#)

The subsequent release of ChatGPT poses its own concerns. ChatGPT is an AI program that can converse and write text much the same way humans can and could be helping scammers improve their spelling and grammar.

Other signs that malware may be running on your phone include:

- Higher mobile data consumption than you expect
- Shortened battery life or device overheating, especially when it's not in use
- Unrecognized social media activity, login locations, post, likes, etc.
- Unrecognized new contacts or calendar events
- New apps installed without your consent or new icons in the home screen
- Premium SMS messages that you don't remember sending
- Subscriptions to carrier paid services that you didn't sign up for

If you think your phone is infected, here are some steps you can take:

- Put your phone in safe mode (Android phones only)
- Run a virus scan with a trusted security app—don't just download something you've never heard of because it's cheap or free
- Update your operating system if it is not current
- Restart your device
- Delete any suspicious apps
- Finally, if none of these worked, you may need to reset your phone to factory settings, which should clear any remaining issues

Tips to protect yourself from fraudulent apps

McAfee and other members of the [App Defense Alliance](#) are working together to help prevent malicious applications from making it to the official app stores, but there are actions that consumers should also take:



Do some research

Does the application come from a trusted source? Check out other apps from the same developer. If it's a banking or other financial app, check the company's website to ensure you're downloading the official app from the official developer account.



Check the reviews

Read a selection of negative or 1-star reviews. Scammers often post a lot of short, generic 4-star and 5-star reviews such as "Good app", and then generate a flood of fake votes to move these reviews to the top of the list.



Is it too good to be true?

There's a theme throughout much of cybersecurity—if it's too good to be true, it probably is. If the app promises a higher-than-normal return on investment or to exponentially grow your social media following at no charge, chances are you'll be paying the price behind the scenes.



Pay attention to permissions.

Does a flashlight app really need to record audio or have access to your contacts? On Android phones you can click on "Settings" then "Apps," click on the app, then click "Permissions." On iPhone, click on "Settings" and then "Privacy & Security." You should be able to select what permissions you're willing to grant to the app and which ones you want to block. And don't forget to ask yourself why it even needs some of these permissions in the first place.



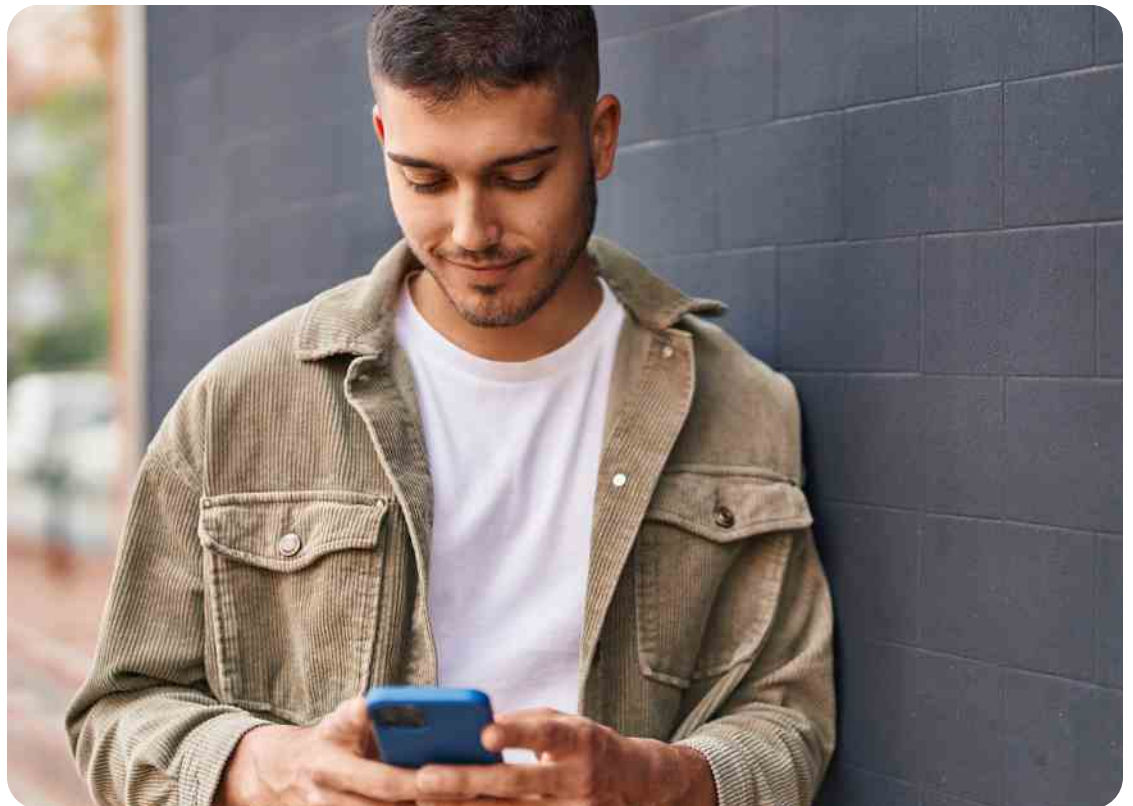
Stick to the verified stores

While any app store is susceptible to hosting malicious applications, official platforms like Google Play and the Apple App Store have rigorous processes in place to both examine apps before they are released and to identify and remove malicious apps that are discovered after release. Third-party app stores do not necessarily observe these processes, and some are even designed to intentionally distribute malware to mobile users.

Topic Two: Threat



Scammers sliding into
your DMs



Threat: Scammers sliding into your DMs

Direct messages, or DMs, are a popular way for people to have private conversations that aren't visible to their friends and followers. Whether these are basic text or SMS messages, messaging apps like iMessage and WhatsApp, or add-ons to a social media platform, they are being used by criminals to send malicious links or groom people for larger frauds. Messages can be secured or encrypted and still have a scammer at the other end!

What types of messages?

Your Netflix account has been suspended, because we're having some trouble with your current account information.

Recovery your Netflix account immediately by click link below:

[Redacted Link]

Please take action on your account within 48 hours to avoid permanent suspension.

Best regard,
Netflix, Inc.

Venmo,

Your Venmo account has been suspended, because we're having some trouble with your current account information.

Validate your account information by click link below:

[Redacted Link]

Please take action on your account within 24 hours to avoid permanent suspension.

Best regards,
Venmo. Inc

Reminder: Take action on your PayPal account

Your PayPal account is currently limited, We noticed that you've been using your PayPal account in a questionable manner. To understand this better, we need more information from you.

To help keep your account secure, immediately by click link below and perform the required tasks.

[Redacted Link]

Please take action on your account within 24 hours to avoid permanent suspension.

Best regards,
PayPal Pte. Ltd.

FBsej1

Amazon :

Your account has been locked due suspicious activity.

All of your last orders and subsription has been on hold until this issues fixed.


Click link below to unlock your account :

[Redacted Link]

If you do not complete the verification process before 24 hours, your Amazon account will be terminated.

Sincerely,
Amazon Team

While most messages are safe, it's important to take a few seconds before clicking on a link or responding to a DM to make sure that it's genuine. Scammers will use fraudulent messages to trick you into clicking on a malicious link, trying to get you to enter your login credentials or account numbers, or share personal information. These messages sometimes, but not always, contain spelling or grammar errors or use odd phrasing.



AI is helping the scammers:

With the emergence of artificial intelligence tools like ChatGPT, scammers can clean up their spelling and grammar mistakes, making it tougher to identify scam messages by mistakes in the content.

Some other warning signs or red flags to look out for are:

- Unexpected contact from an unknown number or a number that claims to be from a legitimate organization
- Urgent or threatening language, such as a warning that your account will be closed if you don't provide your personal information
- Asking you to click on a link to update your personal information or log in to your account
- Offering a bonus, reward, or refund
- Asking for a processing or administrative fee in advance

Typical examples include:

Urgent! We have detected unusual activity on your account. Please click this link to login and verify your information or reset your password.

Dear [name], we apologize for [company's] recent service issues. Your loyalty is important to us. Receive your refund/credit at: [redacted]

You have won a free gift! Click here to claim your prize!

The malware family known as MoqHao is one of the most prevalent mobile threats and is distributed mainly by SMS messages. MoqHao infected over 573,000 devices worldwide in 2022, with targeted victims found primarily in Japan, France, South Korea, Spain, Turkey, and the United States. However, there are MoqHao infections all around the world.

Six point two percent of threats that McAfee identified on Google Play during 2022 were in the “Communication” category, mainly fake SMS Messaging applications. Joker malware is the most prevalent family within fake SMS apps. This malware sends SMS messages and makes calls to premium numbers without the phone owner’s knowledge, running up the phone bill and giving the criminals a cut. The practice is often referred to as “toll fraud.”

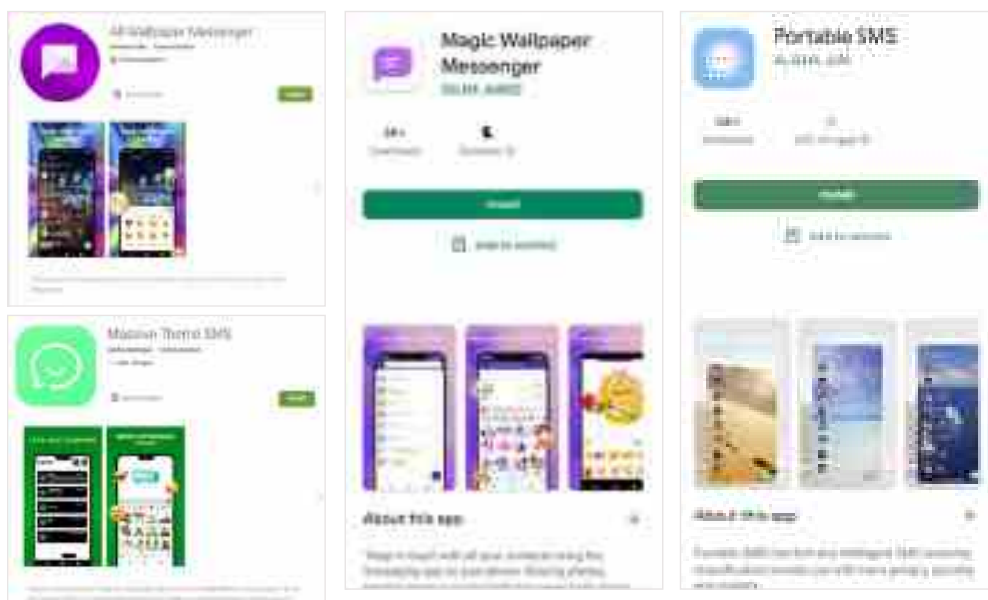


Figure 2. Examples of malicious communication apps that McAfee identified in 2022. Best to stick with tried-and-true apps. (Apps shown have been removed from Google Play.)

Have you heard about “pig butchering”?

“Pig butchering” is a term used for messaging scams where criminals “fatten up” the victim before stealing their money. These schemes often start with a simple “Hi” or “it was fun hanging out last week” message that triggers a “sorry, wrong number” response. The scammer then acts as if they have found a new friend and starts a conversation to build trust with the target. They may reveal that they are a successful trader and start talking about how much money they are making with some special investments, such as cryptocurrency. The goal is to get the victim to download a fake investment app or open a legitimate-looking investment account and transfer some funds.

These apps or websites are quite sophisticated, and scammers sometimes host a video call about the investment opportunity or allow the victim to withdraw a small amount of their fake gains to make them feel more comfortable. Then they solicit more and more funds, even encouraging victims to borrow money for these investments, until the criminals have stolen everything they can. Behind the scenes are detailed scripts and playbooks that make it easy for crime syndicates to run these on a large scale, often exploiting forced labor or human trafficking victims.

The best advice to stay clear of these scams is to be very skeptical about any get-rich-quick schemes or unsolicited investment opportunities. If things sound too good to be true, they usually are!

Do you know about the risks of QR codes?

QR codes, those square boxes of black and white pixels, are “quick response” barcodes that mobile devices can read with a camera and translate into a message or action. They became popular during the pandemic as a method of sharing information without having to touch something, like a restaurant menu.

Since each QR code can hold more than 4,000 characters of data, they can be used to open a web page, send a message, link to an app download, and many other actions. This technology has a lot of flexibility and potential uses, such as:

- More than just menus, including restaurant ordering and payments
- Easy access to shared Wi-Fi
- Product packaging contents and info
- Social media links
- Museum and art gallery exhibit info
- Event info, transit timetables
- Mobile payments

But, like many other digital tools, they are also being used for criminal or malicious purposes. Scammers promote their QR codes via websites, social media, text messages, or even put stickers over the original QR codes.

The resulting links can:

- Direct users to fraudulent sites designed to steal personal information
- Download malware
- Connect to a compromised Wi-Fi network
- Phish for banking credentials or other valuable personal info



How can you protect yourself? Tips to avoid malicious ones:

- Be cautious when scanning a QR code you didn't expect to receive
- Check the URL of the website the QR code is directing you to
- Use a reputable QR code reader app from a trusted source and check the reviews before downloading it
- Protect your personal information—be careful about where and to whom you provide it
- Don't download apps directly from QR codes—authentic ones should direct you to the official app store

Tips to protect yourself from direct messaging scams

In summary, here are some tips that will help you protect your money and personal info from direct messaging scams.



Know the red flags of fraudulent DMs

Be skeptical about messages from unknown senders, urgent warnings, refund offers, or requests to log into your account. Look carefully at any links in the message before clicking on them. Go directly to the company's website instead of clicking on an embedded link.



Watch out for mods

There are many "mods", or application modifiers, available that have extra features for direct messaging apps, or offer ways to bypass communication blocks in some countries. These mods are a frequent target for malware or spyware.



Be aware of "pig butchering"

Don't let yourself get fattened up by criminals looking to steal your life savings. Be careful who you transfer money to and investigate any investment proposals that you did not initiate. Legitimate investment companies will be registered with state or national authorities and cannot promise or guarantee high returns.



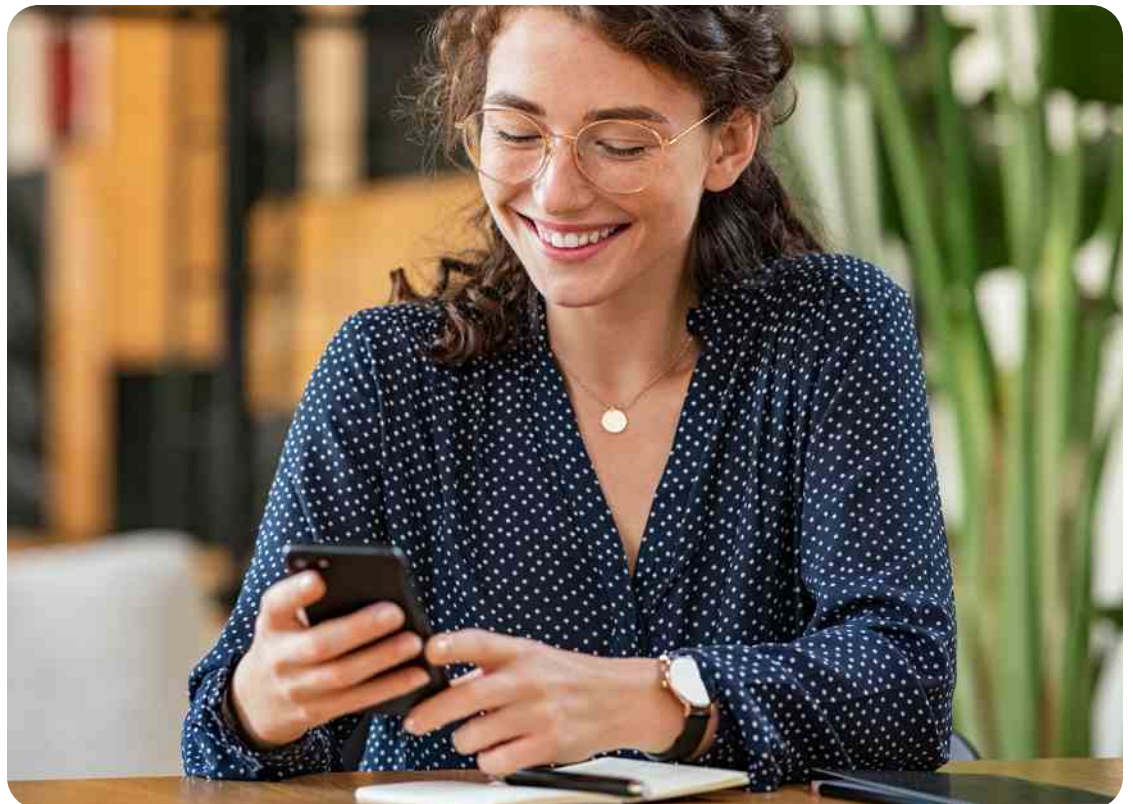
Be careful with QR codes

Take a good look at the website address that any QR code links to, and make sure that it's authentic. Use a reputable QR code reader, such as the one that comes from the developer of your phone's hardware or software or is built into your phone's camera. Be extra cautious when giving out personal info.

Topic Three: Threat



Using your personal phone
for work



Threat: Using your personal phone for work

Many of us have felt that moment of panic of being without a phone when you're waiting on an important call or email from work. Our work and personal lives have become electronically intertwined via mobile devices, as we check email from the car, from soccer practice and even from bed.

Mobile phones are a powerful work tool, giving people access to productivity apps, communication tools, and freedom from their desk. But how are we putting our companies at risk with this behavior?

According to recent studies, most of us are using mobile devices for both work and personal tasks—whether that be checking your personal email on a work device or checking your work email on a personal device. And while work devices are theoretically managed by employers, with IT departments to patch vulnerabilities and update applications, do you know how secure your work device is? Does your employer manage how secure your personal device is? Or are you putting each other at risk to some degree?

Risk assessment: Mixing work and personal tasks

For many people, there is no distinction between personal and work devices. Larger companies may give you a device or have a Bring Your Own Device (BYOD) policy that encourages you to use your personal phone or tablet at work. Smaller businesses, entrepreneurs, or “gig workers” like rideshare drivers or dog walkers rely heavily on their personal mobile device.

Whichever group you fit into, mobile threats, such as the direct messaging scams or app store security issues discussed in this report, apply just as much at work as at home. Is that message really from the boss, asking you to buy gift cards or transfer company funds for an urgent project? Is the app you've downloaded to help you manage your various tasks legitimate and secure? Are you logging into work apps or databases securely so that you don't open your company up to security threats and scams?

Work-related apps for mobile devices can be great productivity boosters—categories like PDF editors, VPNs, messaging managers, document scanners, battery boosters, and memory cleaners. These types of apps are targeted for malware because of their typical access profile. Asking for permissions to storage, messaging, calendars, contacts, location, and even system settings is not unusual and enables the scammers to retrieve all sorts of work-related information.

Technology has enabled us to work more flexibly, but that flexibility comes with responsibility—ensuring the security of not just our personal digital lives, but also our professional digital lives.

Twenty-three percent of threats that McAfee identified on Google Play during 2022 were in the “Tools” app category, the highest percentage among all the app categories, including Entertainment, Communication, and Personalization Apps.

Social engineering and scams

Technical Support scams have been around for years, but a shift to more remote working has caused a spike in these offenses as cybercriminals leverage the increased use of phone support vs. in-person support. These scams often begin with the caller offering tech help for a problem you weren't aware of. While many of them may offer to help fix your personal computer, you should also beware of your company helpdesk reaching out to you for information. Find out how these scams work and what to do [here](#).

Tips to keep work and personal devices safe from each other

Actions you can take on your personal device

- Ensure your phone requires a passcode to unlock it and set a reasonable auto-lock time.
- Consider using different apps for work and personal tasks, or devoting a folder or screen on your mobile device to “work only” applications, to reduce the potential for accidental disclosures.
- Keep your apps and mobile OS updated to the latest version available to reduce risks from known security issues and vulnerabilities .
- Install and use a VPN if you’re connecting to public or unknown Wi-Fi networks.
- Be cautious when installing new apps on your device.

Things to stay vigilant about

- Watch for fraudulent or phishing messages and which account they come to. Did you share your personal email address with coworkers? If not, how did they get it?
- Take the time to verify the sender’s identity and if it makes sense for them to be contacting you through your personal email or via SMS.
- Use multi-factor authentication whenever possible and be aware of potential scams—criminals are sending formal-looking text messages that request verification with an authentication code, which they can then use to try and break into your account.

Things to verify with work

- Check to see if your organization has a BYOD policy and make sure that you are following the security requirements.
- Install and use the company-approved VPN when you are connecting to work apps or databases, or using public or unknown Wi-Fi networks.

Topic Four: Challenge



Modern parenting of teens and
tweens with phones



Challenge: Modern parenting of teens and tweens with phones

Parenting in the digital age comes with a distinct set of challenges. While mobile phones are great for helping parents and kids stay in touch, these devices can also be a source of potential dangers. Parental controls certainly help protect kids' digital lives. But keeping them fully safe online requires a combination of technology, in-person monitoring, and education—of both kids and their parents.

More than just malicious apps

Malicious apps often target things that children and teens like, such as gaming, making videos, and managing social media. We covered the threat from apps earlier in the report, but it's important to make sure that kids' phones are either restricted from downloading new apps, or that they're informed and capable of questioning suspicious apps and identifying fraudulent ones. Nine percent of threats that McAfee identified on Google Play during 2022 were Games from app categories such as Casual, Arcade and Action.

Bad apps and aggressive advertising malware or adware are promoted on social media popular with kids and teens, such as TikTok, Instagram, and YouTube. They target channels for games like Minecraft and Roblox. Malicious games and gaming mods even sometimes show up in official app stores. The security process often catches these apps and removes them, but this doesn't necessarily delete the app from phones they've already been downloaded to. Which is why it's important to have security protection on your kids' devices that can promptly identify and flag harmful apps, and even uninstall them.



Figure 3. This is an example of a game that was also a social network password stealer—once installed it suggests authenticating with Facebook to capture the account credentials. (App shown has been removed from Google Play.)

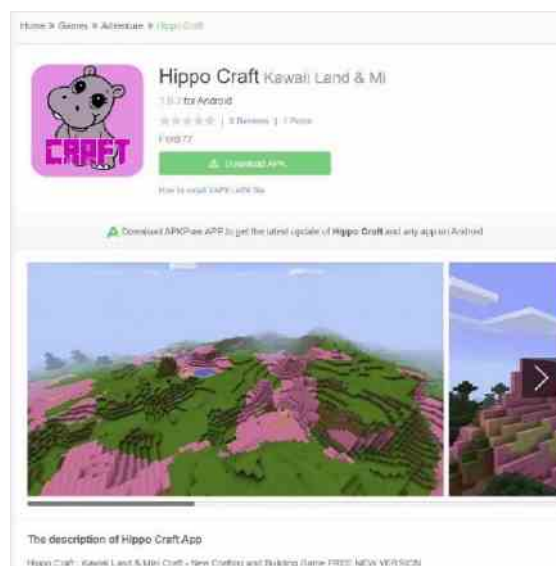


Figure 4. This is an example of the HiddenAds malware category, which was distributed as a block crafting game mod. (A mod can modify the original game to make it more interesting, easier, or more challenging for players.) This app was removed from Google Play but still available in third party markets.

The most common types of threats detected within the gaming category in 2022 were aggressive adware—apps that display excessive advertisements while using the app and even when you're not using it. These can affect the phone's performance and make using the phone very frustrating. A leading example of adware is the [HiddenAds Trojan](#), which displays advertising and collects user data for marketing. Adware may also collect personal data and track the child's activity, especially interactions with friends that may lead to additional infections.

But bad apps and malware aren't the only thing that kids and their parents must navigate in the digital world. Social media creates a host of new things to be aware of, such as influencer culture, dangerous or illegal fad "challenges", and cyberbullying. And since many of these apps and channels are supported by advertising revenue, children and teens are exposed to a high volume of targeted advertising and subtle or undeclared product sponsorships.

Influencers, challenges, and bullying

Social media plays a big part in the lives of many children and teens and comes with a wide range of pluses and minuses. There's no question that these tools can help nurture relationships with family and friends, connect social circles, and expose people to new concepts and cultures. But they have also become target-rich environments for cyberbullying, peer pressure, and bad actors preying on uninformed followers.

Influencers and self-image

Children of all ages look to role models for inspiration and motivation. But today's popularity measurements of likes, follows, and shares can quickly turn from motivational to toxic. Talking with your children about influencers can be challenging—we recommend asking children about who they follow, what they admire about the person, and how they might act if they were in a similar situation. And focus on exploring values and goals, not directly criticizing the influencer.²

Dangerous or illegal "challenges"

TikTok has been in the news a lot recently about potential privacy violations. But one of the biggest threats to children on this and other apps are the "challenges" that go viral—and which can be dangerous or illegal. Recent examples include eating a large amount of cinnamon, taking Benadryl to the point of hallucination, or hotwiring a car (and stealing it) with a USB plug. TikTok's safety centre recommends helping teens develop a four-step critical thinking process—Stop, Think, Decide, and only then, Act.³



Popularity measurements of likes, follows, and shares can quickly turn from motivational to toxic.

Subscriptions and mobile payments

One way that bad actors take advantage of children and teens is through unclear or deceptive in-app purchases and subscriptions. Kids may not understand or care about the terms and conditions or exactly what they're agreeing to, resulting in outrageously high payments far beyond the value of the application.

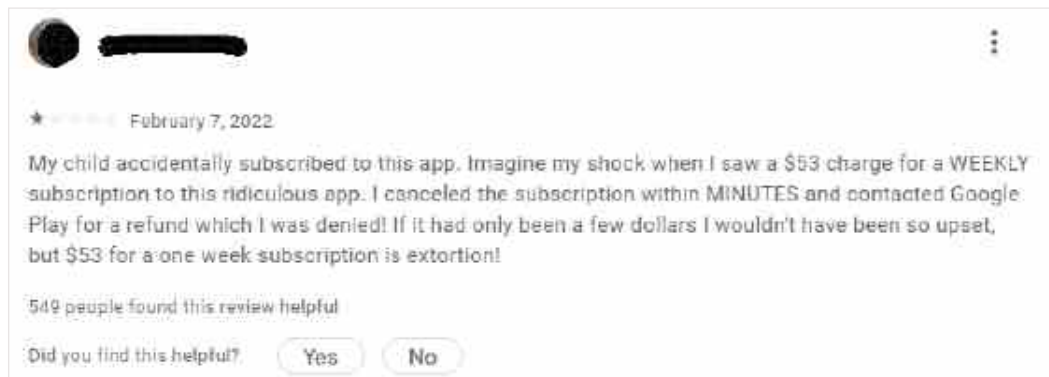


Figure 5. Screenshot of a user's comment on Google Play.

Cyberbullying

A recent [McAfee Connected Family Report](#) found that 60% of children said they were more worried about cyberbullying this year than last year. The report found that more than one in four children worldwide have been victims of racially motivated cyberbullying, one in eight have been cyberbullied in the form of physical threats, and one in six have received sexually explicit messages or images.⁴

Cyberbullying is persistent. Giving kids a safe place to talk about these topics and develop solutions is one of the most important aspects to keeping them safe in a digitally connected world.

Targeted advertising and sponsored content

Social media is free because companies collect all sorts of personal data. Marketers leverage that data to target specific audiences, making users the product. Personalized ads, sponsorships, and product placement, while sometimes helpful, can be misleading and, in some cases, foster a sense of being left out or negative self-image if you don't purchase or subscribe.

Talking to your children about product placement and sponsorship related to the influencers they follow is important. After all, these are individuals they look up to and may even want to emulate. It's important for kids to understand that social media influencers sometimes use or promote products because they are being paid to do so, and while they should provide adequate disclosure around this, not everyone does.

Finally, if your child is on the other side of the camera, it's worth having a conversation about the responsibilities that come with including sponsored products or services on their own posts. The U.S. Federal Trade Commission (FTC) has a useful guide on when and how to make disclosures about any brand sponsorships or financial relationships.

Tips on keeping your children safe on their phones

Here are some key tips that will help you protect your child's privacy and online activity.⁵



Monitor activity

No kid wants to have their digital life examined by their parents or guardians. However, there is no substitute for the occasional check-in on what they're doing online, new applications they're interested in, or the latest social media trends. What are they watching on YouTube, what's happening on TikTok, or getting posted on Instagram?



Educate your kids and yourselves

Similarly, ensure that you and your kids know how to adjust their privacy settings. And that they're aware of the impact of the personal information they may be inadvertently or intentionally sharing. This not only helps everyone make safer, more informed decisions in the present, but has future benefits when applying for college, jobs, or even just meeting new people. Social media searches are a common practice for potential employers, college applications, or even new friends and colleagues.



Use the available technology tools

There are some good tools available to parents, such as screen time limiters, website blocking, and download restrictions on devices. While these won't solve all digital parenting challenges, they can certainly help by keeping track of activity and blocking access to known malicious sites. Security software adds another layer of protection, with real-time threat detection, identity monitoring, and privacy guards.



Talk to your kids about the issues

Finally, try to talk about the issues often and listen to your kids' point of view. Model and encourage open and honest dialogue. Check out the apps yourself. The more you know about what they're doing online, the easier it'll be to have an informed conversation. Encourage them to do their own research and come to you with comments and questions. Keep in mind that it's not just malicious apps that you and they need to watch for, but malicious people and harmful behavior, which can happen on otherwise harmless apps.



Top 10 malware families



Top 10 malware families

McAfee researchers spend a lot of time hunting down and protecting customers from malware. But what is malware? Turns out it's not just a single thing, but rather ANY software or code designed to harm or exploit a computer system, network or user data.

The damage caused by malware can range from simply causing minor inconvenience, like leeching energy from your computer to carry out crypto-mining, all the way to theft of sensitive information or even holding accounts for ransom.

Researchers group these threats into "families" or types. Below is a list of the top mobile malware families McAfee identified in 2022.



1 Dropper

A dropper is a type of malware that is used to deliver and install malicious software to a victim's device, and as it has been for years, the most prevalent. It's usually used in the initial stage of an attack and is designed to evade security systems in order to install the primary "payload" or the malicious code that will actually execute the malware that can be anything from a virus to spyware to ransomware.



2 HiddenAds

HiddenAds, as the name implies, runs ads in the background of a user's device without their knowledge or consent (hence the word Hidden in the name). This malware fraudulently accesses advertisements that can cause a variety of headaches from slowing down your device to tracking your online activity and personal information with the intent of monetize from third-party advertisers.

Ad fraud consequences are not limited to users that installed HiddenAds malware. The whole app ecosystem that depends on ads to finance their functionality is impacted due to fake ad impressions that are a waste of advertising dollars for companies and publishers.



3 FakeApp

FakeApps are malicious applications that pretend to have a functionality that they actually don't. Once they're downloaded, they deliver adware or exhibit malicious behavior.

In the "Trusting Apps" article in this report we talked about an example of this type of malware related to the recent rise of AI and ChatGPT. Many malicious FakeApps claim to be based on the same generative AI as ChatGPT in order to get users to download them, however, they actually turn out to be simply traditional photo filters.

4

HiddenApp

HiddenApp usually hides their icon after installation to persist in the system without the user's knowledge. Some HiddenApps have an invisible or harmless-looking icon to try to avoid being visually detected by the user while it performs a malicious activity on the background. Users might think it is a system utility app, software update or something that should be there or just not notice it at all.

This is why it's essential that you download applications from official app stores like Google Play or the Apple Store. Ideally, if you're sharing personal information, it's best to click on the link for the app on the official website of the service you're accessing.

5

MoqHao

MoqHao is a server-side polymorphic banking trojan, primarily distributed via [smishing](#) in Asia and Europe. If you're thinking "I know all of those words, but don't understand what you just said," you are not alone. Let's break it down:

Server-side polymorphic malware is simply malware that is programmed in such a way that it "mutates" or changes over time, but still maintains its original malicious function. These changes make it difficult for traditional security measures to detect since they rely on the code or "signature" remaining the same. MoqHao is server-side polymorphism due to the mutations that occurred at the download time from the server that hosts the malware.

A **Banking Trojan** is a program or application that pretends to have a legitimate set of useful features that might be related to your financial institution. In reality, it contains a malicious "payload" whose goal is to steal your banking credentials or gain access to your financial information.

So, MoqHao is a "server-side polymorphic banking trojan"....makes sense? Think of it this way—it's like trying to catch a bank robber based on what they were wearing. Police may be looking for a suspect in a blue suit and tie, but the suspect changed clothes before leaving the premises, and is now outside in a t-shirt and jeans, thereby evading arrest. In this case, MoqHao is stealing your credentials or banking information and attempting to evade security solutions by "changing clothes."





Syringe

Syringe malware injects malicious code into running processes on Android systems. Usually, it comes in applications that are repackaged and distributed in third party markets (not from the main app stores) and it is used to steal sensitive information or to install other malware and is usually financially motivated.

Process injection is a method that allows attackers to execute their malicious instructions into other programs (usually system services) that can perform tasks that the attackers originally cannot achieve. Android does not provide a legitimate way to perform process injection, so the only viable way is getting administrator-level access to the phone or exploiting other vulnerabilities.

Imagine process injectors are criminals that provide the instruction and command “to rob a bank” to a bank employee that already has access to the vault.



Banker

This family of malware is a banking Trojan that has the mission of stealing your credentials or personal information.

Mobile banking Trojans are constantly evolving to try to steal your money and break the security policies and limitations that new versions of Android put in place to limit this malware’s capabilities, especially the measures to limit overlay attacks (more on what this is below) and abuse the Accessibility services on your phone.

Google Play limited which apps can access powerful permissions such as Accessibility because it is widely abused by banking Trojans, therefore finding banking Trojans on Google Play is rare. Usually, they’re distributed by [smishing](#) or malicious third-party sources such as phishing banking sites.

An overlay attack is a technique used by malicious apps that consists of layers of invisible elements that can track what you’re typing when logging on to your bank app or superimposing a malicious app over the legitimate one without notice.

Accessibility services are designed to help users with disabilities like visual, motor or hearing; therefore, accessibility services (AS) can control the user interface and simulate actions of the screen. These capabilities can be used to bypass security measures and steal second authentication factors, login credentials and sensitive data and might be used to drain your wallet.

To prevent this abuse, it’s important to only grant access to this powerful Accessibility access permission to apps that absolutely need it.



SpyAgent

SpyAgent is spyware, or malicious software that gathers information about a user's location, contacts, messages, or personal data and passes it on to third parties – all without the device user's knowledge. These third parties include hackers, stalkers or scammers that exploit this information to their advantage. Spyware, in simpler words, is a type of software that “spies” on you.

There is widespread spyware that attempts to collect enormous amounts of sensitive data from any individual that might be used by the attackers to try to exploit it. (And the servers that hold that personal info are unsecured, and many have been hacked, leaking the data.) However, the most common usage of this type of malware is targeted attacks and the use of stalkerware (which is a type of malware found in the SpyAgent malware family) which involves the use of commercial spyware software to spy on a person.



Clicker

Clicker is one of the families that you might not be immediately alerted to, or even consider yourself a victim of. Instead, it's almost like you are an unknowing accessory to the crime.

In 2022 clicker malware was mainly distributed in malicious apps that were posing as system [tools](#) like flashlights and task managers, but aren't limited to any app category, this malware is usually found in third party markets (not in the main app stores) but sometimes crooks made their way into Google Play.

Once it's installed, the clicker malware runs in the background and repeatedly clicks on ads (hidden banners, popups, videos) or links that generate revenue for the attacker. Meanwhile, you, the owner of the device, may only notice a small change in how your phone functions or its battery life.



FaceStealer

Do you have a friend whose social media account was taken over and posted about “How to become rich with crypto”? Maybe your friend was infected by FaceStealer, a type of malware that can steal your social media account, targeting the Meta platforms Facebook, Instagram and WhatsApp. Once accounts are compromised, they might be used to commit other types of scams such as impersonation to ask your contacts for money, to follow other accounts, and to distribute (mal)advertising campaigns.

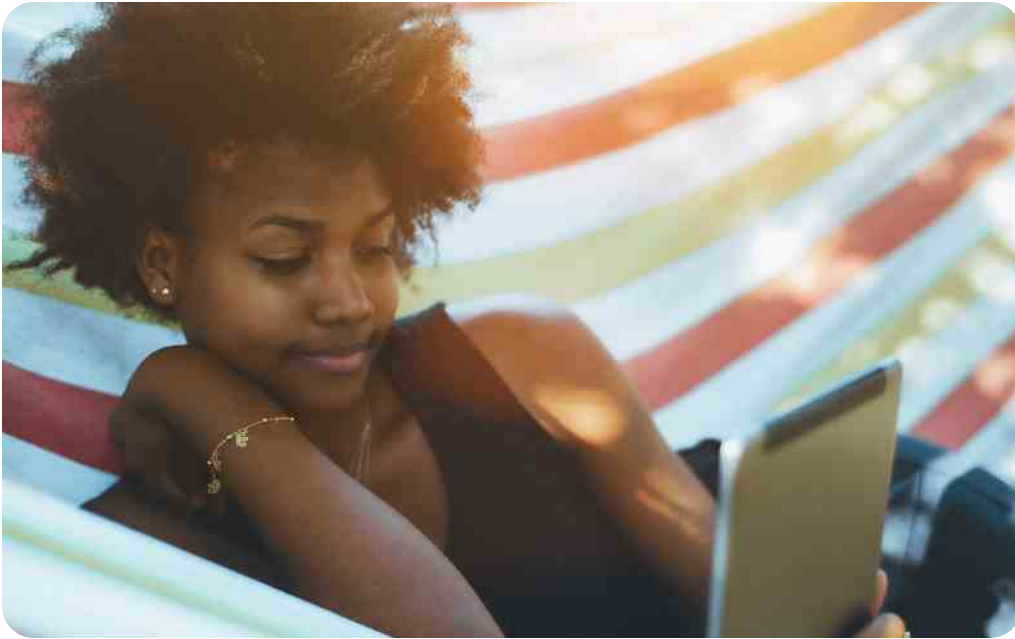
In 2022 we blogged about two campaigns distributing [Face Stealer as a “Mod”](#) app that were stealing Instagram accounts. McAfee detected about 20,000 unique samples (or versions) of FaceStealers, affecting over 110,000 devices around the world.



How do I protect myself and my family?

We've covered a LOT of different variations of malware here, but our advice to stay safe applies to most of them. Ultimately, your first and best line of defense is YOU and a healthy dose of skepticism. Any time an app or website asks for credentials or information, just review the tips below. The more you examine apps and ask questions, the easier these will come to you:

- **Question, question, question.** Do I know this sender? Was I expecting this message or link? Is this someone I would normally give money or information to?
- **Who's this?** How many times have you received a text message from an unknown number that seemed to know who you are? What if that unknown number was pretending to be the CEO of your company? Be aware of social engineering tactics, and don't be afraid to ask who is on the other end of the line. Worst case scenario? It's actually the CEO and he appreciates your due diligence.
- **Is this request legit?** Take a second and ask yourself if the request makes sense. Don't underestimate your gut feelings. Also remember that most organizations that ask for your personal information are bound by regulations and have an official site and an actual person you can call. For example, your bank will NEVER reach out to you and ask for your username and password.
- **Become an anti-scammer!** Familiarize yourself with known scams that are out in the wild. Learn how to spot them, avoid them and how to keep an eye out for new and emerging scam vectors.
- **Know your permissions!** Some permissions can be managed centrally on your phone (messages and location for example), but it's a great idea to look at apps individually and evaluate what information they're tracking and if they REALLY need to be watching you that closely.
- **Slow DOWN!** This is the most important piece of advice we can give. Attackers are targeting that sense of urgency and counting on it to cloud your judgement. Take a beat to assess and apply the above.



2023 Threat predictions



2023 Threat predictions

What does the future hold? No one can know for sure, but McAfee's Mobile Research Team has made some educated guesses.

The end of 2022 saw some amazing advancements in access to technologies that had previously required a fuller understanding of artificial intelligence as well as a significant amount of funding. Now, with applications like OpenAI's ChatGPT AI chatbot and DALL-E 2 AI image generator, anyone with access to the internet can leverage the power of AI. While this is an exciting technological development, it also changes the threat landscape. This, combined with an uncertain global economy, creates a target-rich environment for scammers.

Below are our research teams predictions for 2023, and some ways that you can safeguard yourself and your family.

New applications will impact the threat landscape

One of the immediate implications of these new AI applications is that they make traditional phishing harder to spot. One of the hallmarks of a traditional phishing campaign—meaning one that spread a wide net to collect multiple victims—was basic misspellings and grammar errors. With the introduction of ChatGPT, the authors of those phishing emails no longer have to worry about correct grammar and spelling, ChatGPT can easily write a grammatically correct email for you. Bad actors need only to enter a message, translate and wait for the program to create a message.

Misinformation and deepfakes

Misinformation and fake images have been concerns in both government and cybersecurity circles since elections have been held. Staged photos and false info have been standard practice for nations that rely on propaganda.

Today, we now have what are called deepfakes, which use a form of artificial intelligence called deep learning to make falsified images and videos. Just like ChatGPT, applications are being introduced that make this even easier, elevating some cybersecurity concerns. For example, emerging technologies like DALL-E 2 (an AI system that creates images based on text prompts) can be used to make crypto scams more believable. The double your money cryptocurrency scam, for example, used an old Elon Musk video as a lure. We expect such scams to evolve in 2023 and make use of deep fake videos, as well as audio, to trick victims into parting ways with their hard-earned money.

Investment scams

The financial outlook of 2023 remains uncertain for many people. During these times, people often look for ways to make some extra money, and this can leave them vulnerable to social media messages and online ads that offer huge financial gains for little investment.

According to the FBI Internet Crime Complaint Center's [2021](#) report, the losses for investment scams increased from \$336,469,000 in 2020 to \$1,455,943,193 in 2021. This shows that this type of scam is growing by an enormous amount, and we expect it to continue.

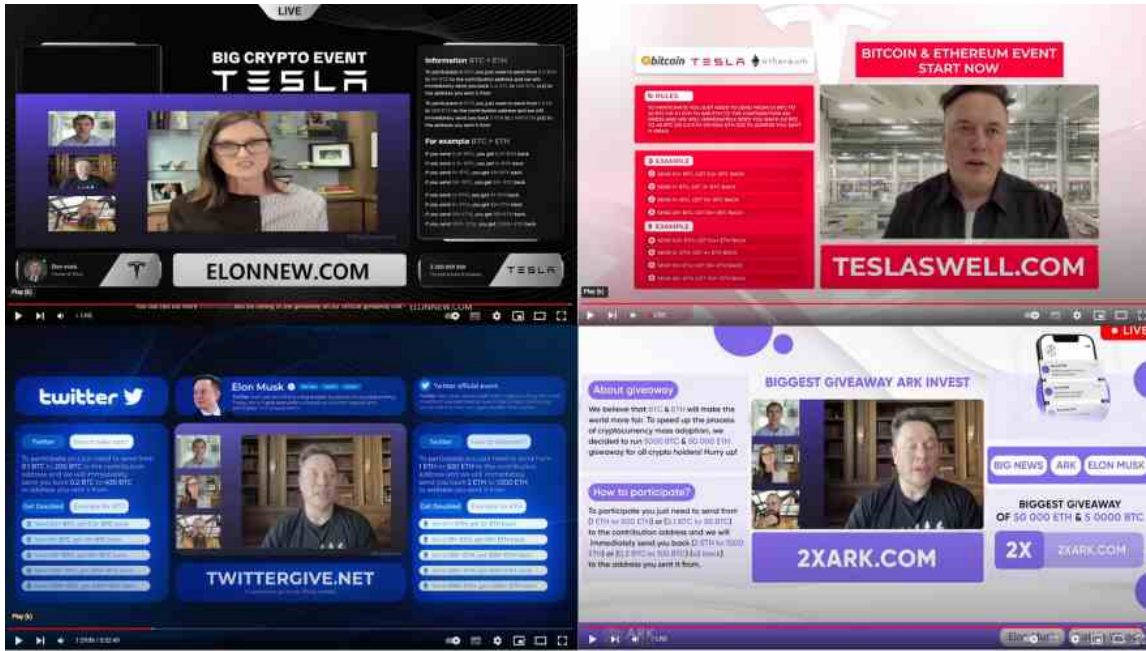


Figure 6. Images of YouTube deepfake cryptocurrency scams.

Fake loans

Unfortunately, scammers will often target the most vulnerable people. Fake loan scams are one such scam where the criminals know that the victims are desperate for the loan and therefore are less likely to react to warning signs such as asking for an upfront fee. We predict that there will be a large increase in these types of scams in 2023. When looking for a loan, always use a trusted provider and be careful of clicking on online ads.

Metaverse

Metaverses such as Facebook’s Horizon enable their users to explore an online world that was previously unimaginable. When these platforms are in the early stages, malicious actors will usually attempt to exploit the lack of understanding of how they work and use this to scam people. We have observed phishing campaigns targeting users of these platforms in 2022 and we expect this to increase dramatically in 2023 as more and more users sign up for the platforms.

Social engineering

Hacking into your phone happens but it requires criminals’ time and effort. There’s an exponentially higher chance of you being the target of a widespread attack that uses social engineering. These attacks can be sent quickly and easily, increasingly through texts and will continue to proliferate, like pretending to be your bank, PayPal or Venmo, tricking you into giving up your personal data, like account logins.

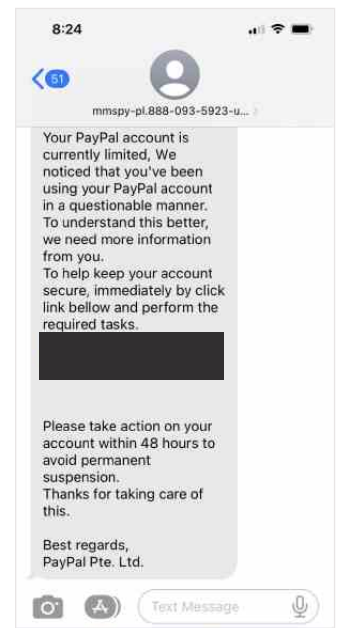


Figure 7. Images of Youtube deepfake cryptocurrency scams.

Future-proofing your mobile device

The technology and applications used by cybercriminals is constantly evolving and has been for decades. We've shared ways to keep yourself and your family safe throughout this report, and those still apply to these future threats.

- Be suspicious of unsolicited emails, texts, or direct messages and think twice before you click on any links.
- Remember that most of these scams work because the scammer creates a false sense of urgency or preys on a heightened emotional state. Pause before you rush to interact with any message that is threatening or urgent, especially if it is from an unknown or unlikely sender.
- If it's too good to be true, it probably is.
- Ensure that your mobile device is protected with software that includes features to monitor and block potentially malicious links and malware like the [McAfee Security app](#).

As always, criminals will continue to get smarter and more creative and the tools for their misdeeds continue to advance. So, we as technology users will continue to get smarter as well.



Want to read more about our 2023 threat predictions?
www.mcafee.com/blogs/security-news/mcafee-2023-threat-predictions-evolution-and-exploitation/



Protect your phone and the life you live on it
Scan this QR code to download the McAfee Security mobile app directly to your phone or tablet from the Apple or Google Play app store.

1. <https://www.data.ai/en/go/state-of-mobile-2023/>
2. <https://www.mcafee.com/blogs/family-safety/helping-kids-think-critically-about-influencers-they-follow-online/>
3. <https://www.mcafee.com/blogs/family-safety/tiktok-update-dangerous-viral-challenges-age-restrictions/>
4. <https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-cyberbullying-in-plain-sight-2022-global.pdf>
5. <https://www.mcafee.com/blogs/family-safety/getting-your-kids-ready-for-school-and-their-smartphones-too/>
<https://www.mcafee.com/blogs/family-safety/does-your-child-have-an-unhealthy-relationship-with-social-media/>