DENUVO by irdeto

MOBILE GAMES UNDER SIEGE

in-game ads blocking, in-app purchase fraud and GPS spoofing explained

There is a big chance that your game is a target for pirates and cheaters. They do all they can to ruin your intense work and effort, and deprive you of your well-deserved income. They tamper with your title to make it available for free and they cheat to gain an unfair advantage over other players in your multi-player games.

But that is not all.

They also rob you in other ways. They access your premium features or content without spending a penny, they create and use ad blockers and they mess with the GPS to cheat in your location-based games.

From this e-book you'll learn how it all works, how it affects the gaming industry and what you can do about it.

Happy reading!

CONTENTS

IN-GAME AD BLOCKING

Types of mobile in-game ads

Here are some of the most popular in-game ad formats on mobile:

- **Interstitial Ads** – full-screen ads, static or animated, that users can skip after watching them for a certain amount of time.
- **Native Banner Ads** – the ad is placed in a way that makes it look like it's a part of natural game flow. It is relatively unobtrusive and discreet – provided that the right place and timing have been picked for it to appear.
- **Rewarded Video Ads** – the player gets a reward (coins, gems, points, extra lives...) for watching a video ad. Incentivizing viewing ads make them not only a bit less obtrusive, but also "liked" by players.
- **Offerwalls** are similar to rewarded ads – players must complete a task, e.g., fill out a survey, to receive a reward.
- **Playable Ads** blend interactivity and gamification and as such are an alternative to irrelevant and intrusive ads.

How does blocking mobile in-game ads work?

It's easy. Mobile gaming apps have a fail-safe that kicks in if the ad server is not responding. By blocking access to the ad server, players block the ads themselves. In other words, they block web requests that download the ad content into the game.

Some of the popular methods of making that happen include:

- **Changing** the **web request address to a private ad-blocking DNS** provider (no actual blocking app required).
- **Filtering** all **traffic through HTTPS** secure filtering that blocks ads.
- Using a **hosts file to block ad-serving hostnames**. Ad requests that have been sent to known ad-networks are redirected back to user's phone, meaning that requests stay in a loop and no ads are displayed.

- **Establishing** a Virtual Private Network (**VPN**) service and **redirecting DNS** server **traffic to it**. The VPN service intercepts and filters out DNS queries that are on the blocklist while allowing non-blocklisted queries to pass through.
- **Patching the ad code out of the app.** Since displaying the ads is part of the game code, removing this part or breaking it in some way (e.g., by replacing the ad server URL with an invalid one) makes it impossible for the ads to be displayed.

There are a lot of free mobile tools for blocking the in-game ads available – they effectively block ads in every shape and form.

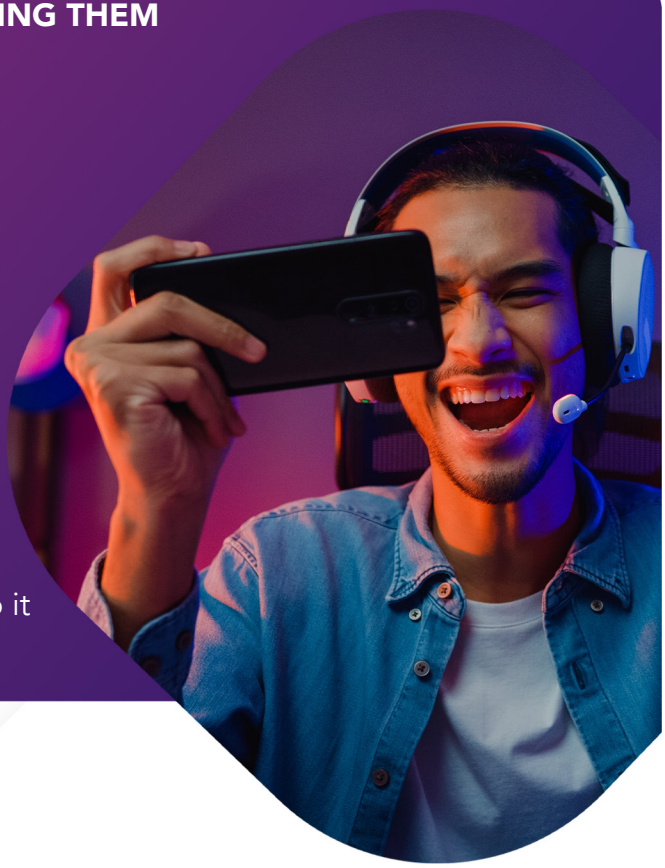
MOBILE IN-GAME ADS AND WAYS OF BLOCKING THEM

Ads

- Interstitial Ads
- Native Banner Ads
- Rewarded Video Ads
- Offerwalls
- Playable Ads

Ways

- Changing web request address to a private ad-blocking DNS
- Filtering traffic through HTTPS secure filtering
- Using hosts file to block ad-serving hostnames
- Establishing VPN and redirecting DNS traffic to it
- Patching the ad code out of the app



MOBILE GAME IN-APP PURCHASES FRAUD

What is an in-app purchase?

In-app purchases – or IAPs – are optional fees charged to game users in exchange for additional features. They are also often referred to as microtransactions and can be, e.g., in-game currency, extra lives, bonus health, new levels, cosmetics or power-ups. In-app purchases can cost as little as $0.99, but sometimes they are quite expensive – which is an incentive for fraudsters.

How can in-app purchases be circumvented?

Cheaters circumvent in-app purchases in three main ways:

1. By **modifying the app**, so that the premium content is unlocked without any actual in-app purchase involved.
2. By **faking the payment** for the purchase using **tools such as Lucky Patcher**.
3. By **voiding it** – through cancelling, revoking or charging it back. (Some even go as far as using stolen credit card data to pay for IAPs…).

IN-APP PURCHASE EXAMPLES AND WAYS OF CIRCUMVENTING THEM

Examples

- In-game currency
- Extra lives
- Bonus health
- New levels
- Cosmetic items
- Power-ups

Ways

- Modifying the app
- Faking payments using rooted devices
- Voiding payments

GPS SPOOFING

What is GPS spoofing in mobile gaming apps?

In short, GPS spoofing is when the positional information of a specific device is altered. This is achieved by using tools that pretend to be a GPS receiver. They output location data that looks like real GPS coordinates but are not produced by decoding an actual GPS signal; they are produced by clicking somewhere on the map. When somebody spoofs GPS, their location shows as if they were somewhere else. In video games, it broadly means the location of the player is changed to anywhere in the world.

Cheaters use the falsified location or time zone for cheating purposes: they sabotage a game mission or cheat their way through a game. A common scenario is to fake one's location in order to, e.g., win perks, just like what happened in the popular mobile game Pokémon Go (see below).

How does GPS spoofing in mobile gaming apps work?

GPS spoofing starts with an external app that overrides GPS signals on a particular device. That means **replacing a trusted source of information with their own source and convincing the network that they are trusted instead**. This is possible because the signal is not encrypted, meaning it requires no verification for transmission.

There are a multitude of applications available that override GPS signals, they are free to download and use, and work across all mobile devices. They manipulate the data of the original coordinates on the device, enabling a variety of options for cheating.

WHAT IMPACT DOES IT ALL HAVE ON YOUR BUSINESS?

You know this already, but let's stress it anyway: **the more in-game ads your players display or the more in-app purchases your players make, the more revenue they generate for your business**. So, stopping players from blocking or defrauding that source of revenue should be a no-brainer for you. It will protect your revenue stream and increase the overall profitability of your mobile gaming app.

As for **GPS spoofing**, it unfairly allows location-based rewards as players can easily fake their location to anywhere on the globe. It creates noticeable inconsistencies in the quality of the game, **frustrating honest players**, discouraging them from continuing their playthrough, which results in a **shrinking player base**.

Leaving the above threats unaddressed greatly reduces your revenue – if you offer free-to-play titles, this is your source of income. Also, it can give an undeserved advantage to cheaters over honest players who can then become frustrated at having to pay for your extra offerings. It may also inspire other players to use this method to also avoid paying for extras.

POKÉMON GO – a mobile gaming app GPS spoofing case study

Pokémon Go – a game that was downloaded over 500 million times – is a prime example of a game where location spoofing happened daily. In the game, players must walk around in different locations or pay money to unlock a new Pokémon, which later earns them further rewards.

Where did it go wrong? The game uses technologies to block mock-locations, enough players were able to find an alternative way to 'catch 'em all' without physically going to places. Not only did they use GPS spoofing apps, but also some other location faking techniques, e.g., bots, PokeDrones and Wi-Fi spoofing. Researchers examining this phenomenon concluded that location spoofing in Pokémon Go happened for trivial reasons – the players did not want to spend money or travel for their rewards.

Eventually, the location spoofing ruined some players' overall experience which called for testing out actions against spoofers.

HOW CAN YOU PROTECT YOUR GAME FROM THESE THREATS?

Surprisingly, you can prevent all that from happening.

To prevent players from blocking your in-game ads…

…stick to the rules below (when done right, in-game ads can be engaging and useful):

1. **Keep the ads short**. When adverts are between 5 and 15 seconds, players are less likely to divert away as it doesn't take up too much of their time. Ads that last for over 30 to 60 seconds frustrate the players, particularly if they are unskippable.
2. **Make your in-game ads nice**. If they're visually pleasing and adding to the game experience, players will get less distracted and annoyed by them. As a result, they will be more likely to watch them.
3. **Make your in-game ads relevant for your players**. Even if they are relatively bothersome, relevance of their message will sweeten the experience and lower the chance of frustrating your players.
4. **Make your in-game ads relevant to your game**. If your ad is somehow related to the story of your game, it's more likely to catch players' attention and spark their interest, rather than cause their annoyance.
5. **Keep the number of ads sparse**. Players who engage with your game for a longer duration typically will not complain if ads are present, however when they feel they are watching more ads than time spent playing, they will not hesitate to uninstall.
6. **Tie your in-game ads to a reward in the game**. Players don't have to watch the ad but make it clear to them that it will mean no reward.
7. **Offer a purchase option**. Ultimately, players don't want ads, they want products and services, so give them a way out.

For specific ad formats, you can also do the following:

8. **For Interstitial Ads, pick their timing carefully**. If you don't interrupt players in the middle of their game, they will not get annoyed as easily. A good practice would be to display an ad when the game naturally pauses or transitions, e.g., after a completed level.
9. **For Native Banner Ads**, make sure you pick both the right place and timing for them to appear. If it's discreet enough, players will not get annoyed.
10. **Use Rewarded Video Ads**, Playable Ads and Offerwalls more often. Blending interactivity and gamification, as well as incentivizing viewing ads, will make them not only a bit less obtrusive, but also more "likeable" by players.

To protect your in-app purchases…

…take the following steps early in the development process:

- **Do server-side purchase verification**. In-app purchases are best validated on a server and content should only be handed out by the server if verification succeeded. Never validate the purchase directly in your app, as some players will be able to simulate it and get access for free.
- **Monitor suspicious transactions**. Make sure you detect void purchases quickly by subscribing to the "server-to-server notifications" services offered by mobile game stores. You will know instantly that the status of a purchase has been changed and you'll be able to, e.g., revoke the entitlement or perform a clawback. In case of re-offenders, you'll be able to disable purchasing option for them or ever completely block them from accessing your mobile gaming app.
- **Keep game logic at the backend**. As a rule of thumb, always move game logic and sensitive data to the backend, so in case of bugs or security issues it will be much more difficult for players to access it for free. Never bundle the unlocked content in your app but retrieve it from your server instead. Also, be sure to encrypt premium content and use a device-specific encryption key to decrypt it.
- **Use anti-tamper solutions**. Most of the time, hackers need to modify the app in some way, so make it harder for them by tamper-proofing your game. How? By using a service such as Denuvo by Irdeto.

PROTECTING IN-APP PURCHASES

- Do server-side purchase verification
- Monitor suspicious transactions
- Keep game logic at the backend
- Use anti-tamper solutions

To protect your mobile gaming app from GPS spoofing…

…ask yourself, **is your game** location-based with rewards **associated with specific locations**, and can it draw cheaters to exploit them?

If the answer is yes, it is your task to **make it difficult for cheaters to fake locations** in your mobile gaming apps. How? By applying protective solutions available. Denuvo's Mobile Protection SDK, for example, **detects GPS spoofing** and provides **protection against this threat**.

What other software-based measures can you take to protect your mobile games?

Taking protective measures into account early in the game development phase is one of your options. You can also strengthen the defense of your mobile gaming app using any of the available plug-ins:

- **Integrity verification** checks for modifications of the app on the file system and in the code in memory.
- **Anti-debugging** detects ptrace- as well as jdwp-debuggers in real-time to learn if hackers have been working on figuring out your game mechanics.
- **Hook detection** detects different rooting frameworks to learn in real time if your game has been hooked.
- **Jailbreak/Root detection** detects all common rooting frameworks and root cloaking apps to spot cheating attempt early.
- **Emulators detection** detects the most common Android emulators.

HOW DO YOU GET STARTED PROTECTING YOUR MOBILE GAMES?

It's simple, reach out to us and tell us more about your next mobile game! We offer a one-stop service for developers big and small, with a suite of cybersecurity solutions that includes over 20 mobile game security plug-ins to meet your particular needs.

Irdeto is the world leader in digital platform security, protecting platforms and applications for video entertainment, video games, connected transport, connected health and IoT connected industries. The **Denuvo** team at Irdeto is the world leader in gaming security, protecting games on desktop, mobile, console and VR devices. We provide core technology and services for game publishers/platforms, independent software vendors, e-publishers and video publishers across the globe. Denuvo technology enables binary protection for games and enterprise applications across multiple platforms, including desktops (Windows), consoles, VR devices and mobile gaming. Denuvo's gaming security technology prevents revenue loss for game publishers and disruptive, undesirable cheating in the gaming environment.