UltimaSMS: A widespread premium SMS scam on the Google Play Store

JAKUB VÁVRA 25 OCT 2021

A fake photo editor, camera filter, games and other apps promoted via Instagram and TikTok channels

Last week, I reported 80 apps belonging to a premium SMS scam campaign, which signs victims up for expensive premium SMS services that earn a bad actor or actors money while ultimately leaving victims completely empty-handed, to Google's Security Team. This led to their swift removal from the Google Play Store. The apps that I discovered are part of the UltimaSMS campaign, consisting of 151 apps that at one point or another had been available for download on the Google Play Store. These apps have been downloaded more than 10.5 million times, and are nearly identical in structure and functionality; essentially copies of the same fake app used to spread the premium SMS scam campaign. This leads me to believe that one bad actor or group is behind the entire campaign. I have dubbed the campaign "UltimaSMS", because one of the first apps I discovered was called *Ultima Keyboard 3D Pro*.

The fake apps I found feature a wide range of categories such as custom keyboards, QR code scanners, video and photo editors, spam call blockers, camera filters, and games, among others. UltimaSMS appears to be a global campaign, as according to insights from Sensor Tower, a mobile apps marketing intelligence and insights company, the apps have been downloaded by users from over 80 countries. The apps have been most

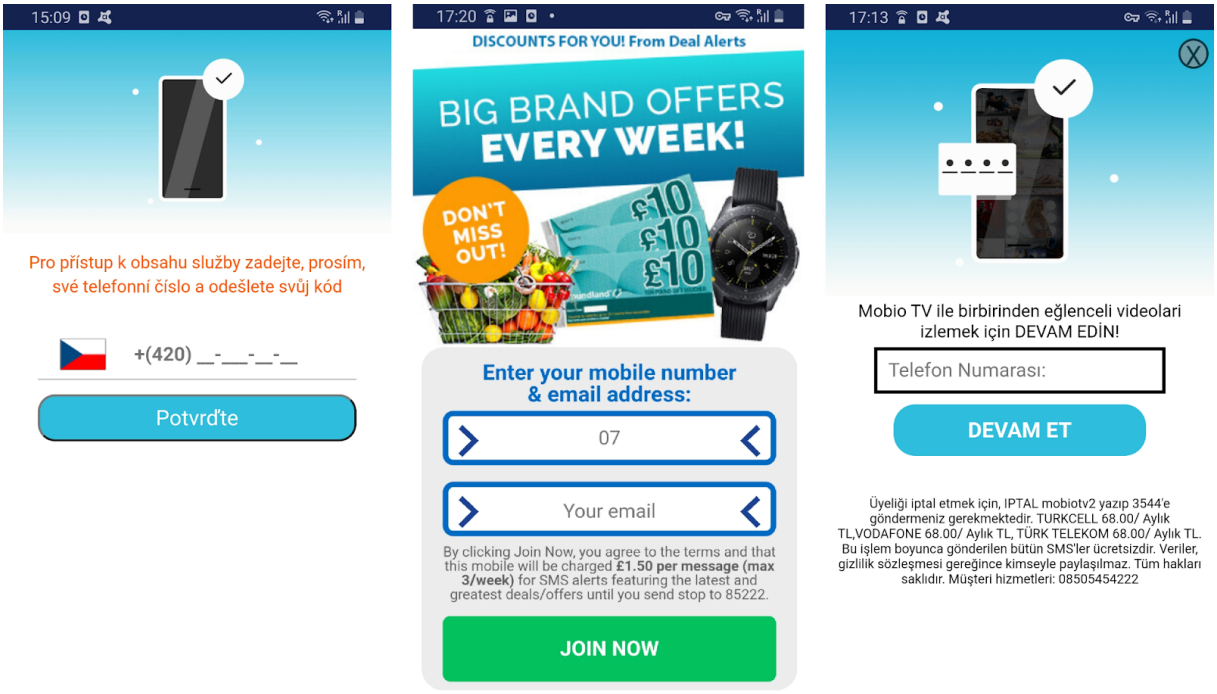
downloaded by users in the Middle East, such as Egypt, Saudi Arabia, Pakistan, followed by users in the US and Poland. Avast has traced the earliest UltimaSMS samples to May 2021 and new samples from the campaign were released earlier this month, meaning that the scam is still ongoing.

Country	Downloads
Egypt	2,600,000
Saudi Arabia	2,400,000
Pakistan	2,000,000
United Arab Emirates	1,000,000
Turkey	790,000
Oman	400,000
Qatar	450,000
Kuwait	200,000
US	170,000
Poland	170,000

The above table shows the top 10 countries where the apps have been downloaded, according to Sensor Tower

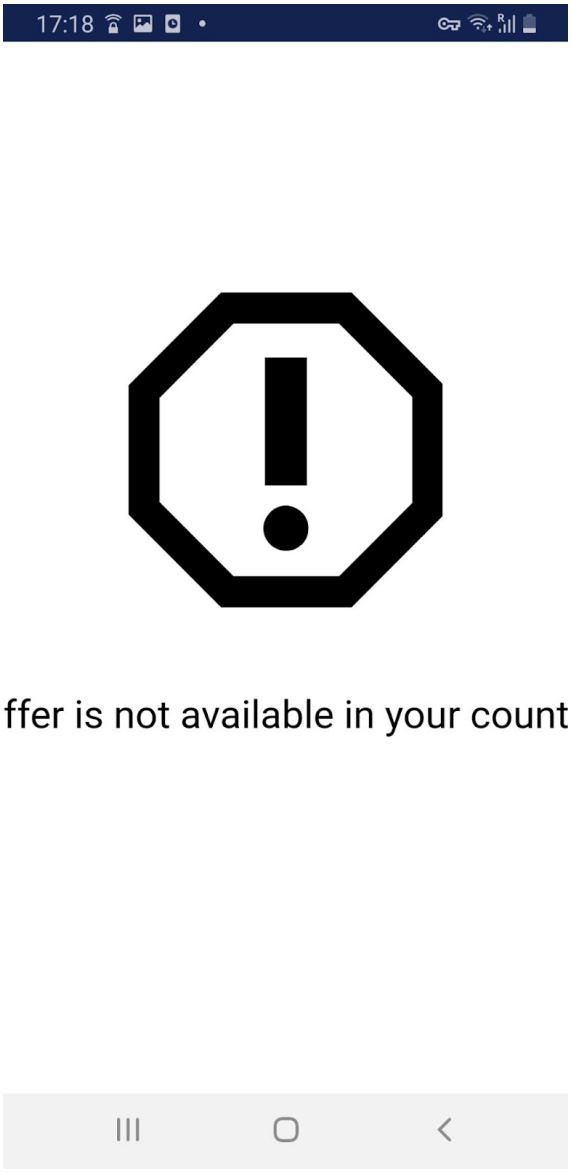
How UltimaSMS scams users

When a user installs one of the apps, the app checks their location, International Mobile Equipment Identity (IMEI), and phone number to determine which country area code and language to use for the scam. Once the user opens the app, a screen, localized in the language their device is set to, prompts them to enter their phone number, and in some cases, email address to gain access to the app's advertised purpose.



Some of the many prompts that users can encounter upon opening the apps. They differ based on the country and are localized. Not all of them include fine print warning users' of the potential charges.

Upon entering the requested details, the user is subscribed to premium SMS services that can charge upwards of $40 per month depending on the country and mobile carrier. Instead of unlocking the apps' advertised features, which users might assume should happen, the apps will either display further SMS subscriptions options or stop working altogether. The sole purpose of the fake apps is to deceive users into signing up for premium SMS subscriptions. While some of the apps include fine print describing this to users, not all of them do, meaning many people who submitted their phone numbers into the apps might not even realize the extra charges to their phone bill are connected to the apps.



After entering a phone number and/or email address, the apps will continue to display further SMS subscriptions or stop working altogether

Once subscribed, the premium SMS are charged weekly and, from what I can tell, appear to be the maximum possible amount that can be charged in the country the user is from. Many countries limit the amount of premium SMS charges that can occur within a week. The user may be notified by their carrier of the excessive charges, but they could also go unnoticed for weeks or months. Affected users may dismiss the apps as nonfunctional and uninstall them, however, the SMS charges will continue and could amount up to an unpleasant sum.

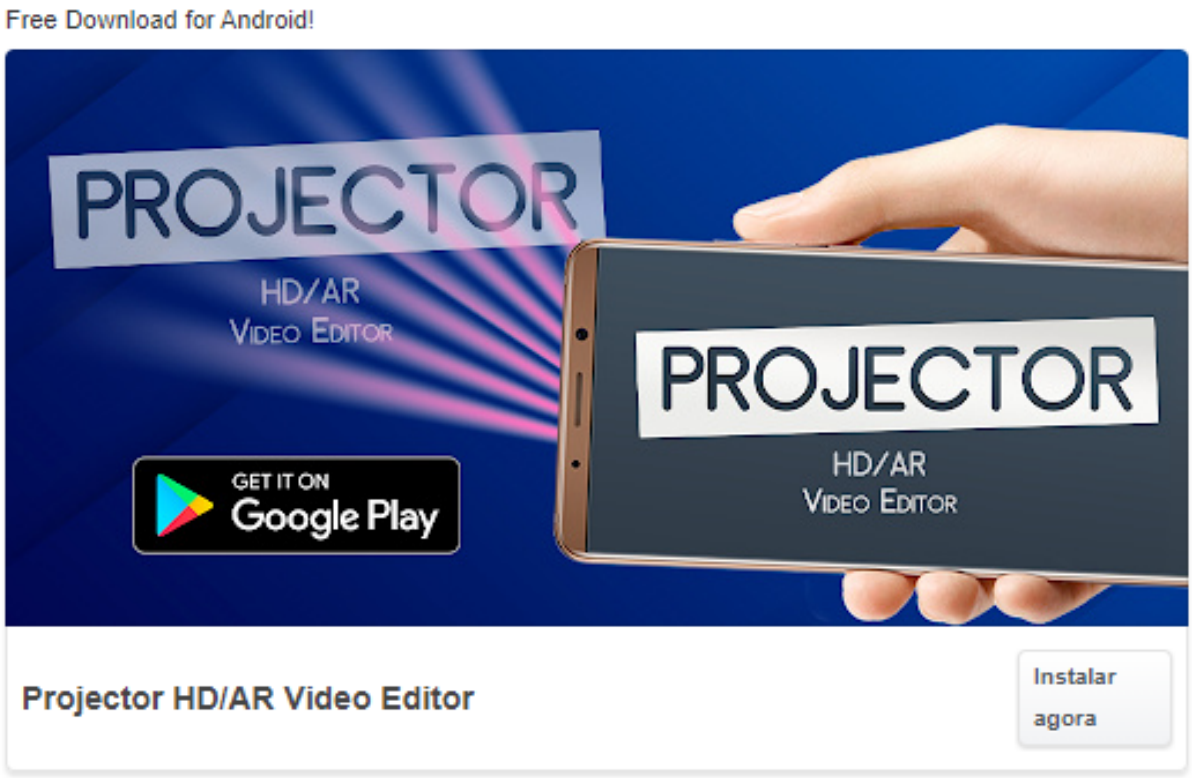
UltimaSMS on the Play Store

The apps discovered are essentially identical in structure, meaning the same base app structure is repurposed numerous times. These copies are disguised as genuine apps through well constructed app profiles on the Play Store. The profiles feature catchy photos and enticing app descriptions alongside often high review averages. However, upon closer inspection, they have generic privacy policy statements and feature basic developer profiles including generic email addresses. They also tend to have numerous negative reviews from users that correctly identified the apps as scams or have fallen for the scam.

Users often correctly recognize the scam apps in reviews

UltimaSMS has been propagated through advertising channels on popular social media sites such as Facebook, Instagram and TikTok, as seen with other recent scams and cases of adware. There are numerous catchy video advertisements targeting users on these social media platforms. It speaks to the size and impact of this particular strain of scam apps, as the malicious actors are spending funds to boost downloads. Premium SMS

scams are increasingly prevalent as evidenced by Zimperium's reporting of GriftHorse, for example. In fact, these types of scams are not new at all, they appear to just be making a comeback. Years ago there were malware families that would secretly use dial-up modems to dial-up premium services, racking up thousands of dollars in charges.



Advert shown on Facebook for the Projector HD/AR Video Editor app

How to avoid UltimaSMS and similar scams

-
  - **Remain vigilant** when downloading new apps, especially apps advertised in short and catchy videos. Children may be particularly vulnerable to this type of scam.
  - **Disable premium SMS option with your carrier.** While there are legitimate uses for premium SMS, such as donating to charities, it is an easy avenue for malicious actors to abuse. Disabling this option will nullify the UltimaSMS scam. Based on some of the user accounts that left negative reviews, it looks like children are among the victims, making this step especially important on

children's phones, as they may be more susceptible to this type of scam.

- **Carefully check reviews.** Scam apps often have boosted review averages, but written reviews may reveal the true purpose of an app. Checking the developer's history and profile may also be useful.
- **Don't enter a phone number unless you trust the app.** Being careful with personal details, including phone number and email, goes a long way to avoiding similar scams.
- **Read the fine print before entering details.** Legitimate apps will have Terms of Service and a Privacy policy alongside a statement of how they intend to use your data and entered details.
- **Stick to official app stores** when downloading apps. Although these apps were available on the Google Play Store, they have been removed by Google's security team, but they are still available for download elsewhere on the internet.

To explore the list of UltimaSMS IOCs, check out the dedicated page on GitHub.