Lures for Money: A First Look into YouTube Videos Promoting Money-Making Apps

Noshaba Nasir*
FAST NUCES Pakistan
noshaba.nasir@nu.edu.pk

Faqia Iqbal
UBC Canada
faqia@cs.ubc.ca

Mahnoor Zaheer
LUMS Pakistan
22100187@lums.edu.pk

Mariam Shahjahan
LUMS Pakistan
22100129@lums.edu.pk

Mobin Javed
LUMS Pakistan
mobin.javed@lums.edu.pk

ABSTRACT

YouTube hosts a wide variety of user-generated videos accessible to a global population of users. The potential of videos to persuade users by engaging them with the experience of the content creator makes them an attractive medium for promoting various kinds of products and services, including apps and websites. The Youtubers promoting these products online may not necessarily be aware of the harms to which they might expose potential users. In fact, they may neither have the incentive nor the technical expertise to look into potential harms.

In this work, we uncover one such ecosystem, where the Youtubers are primarily driven by earning money from their channels, but in doing so expose their audience to fraudulent apps. We collect and analyze a dataset of YouTube videos promoting money making apps. Such videos convince users (primarily in developing regions) that they can make money by downloading and installing the mobile apps being promoted, and performing simple tasks such as watching videos, installing other apps, or playing games. We study the popularity of these videos and apps, as well as illuminate the types of tasks they promote, and whether these apps are potentially malicious.

CCS CONCEPTS

• **Security and privacy**;

KEYWORDS

measurements for fraud, malware, spam

ACM Reference Format:
Noshaba Nasir, Faqia Iqbal, Mahnoor Zaheer, Mariam Shahjahan, and Mobin Javed. 2022. Lures for Money: A First Look into YouTube Videos Promoting Money-Making Apps. In *Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security (ASIA CCS '22), May 30–June 3, 2022, Nagasaki, Japan.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3488932.3517404

*Contact Author.

ASIA CCS '22, May 30–June 3, 2022, Nagasaki, Japan.

ACM ISBN 978-1-4503-9140-5/22/05…$15.00
https://doi.org/10.1145/3488932.3517404

1 INTRODUCTION

While it is widely known that users in developing countries are easy recruits for money making opportunities involving simple online tasks such as clicking and manual CAPTCHA solving [4][10][12][17][18], not much work has focused on how these users are recruited. In this work, we explore YouTube as a channel where such money making opportunities are promoted. The potential to lure users by sharing reviews and experiences in an engaging video format makes Youtube an attractive platform for promoting various kinds of money making opportunities.

A simple search for the keywords *"how to make money online"* returns several hits. While several videos discuss legitimate ways, such as, freelancing tasks, monetizing apps and websites by leveraging Google's advertising platform, and affiliated marketing, our search also revealed several videos that promote *money making apps* (referred to as MMAs from here on), which promise users a monetary commission for completing tasks, such as, clicking on ads, watching videos, and installing other apps. Such apps can involve users in potentially fraudulent or harmful activity, e.g., asking the user to install malicious apps.

In this work, we focus on the following research questions:

- RQ1: Is this ecosystem potentially a fraudulent one?
- RQ2: How do we collect an accurately labeled dataset of such YouTube videos?
- RQ3: How popular are these videos and the apps they promote?
- RQ4: What are the characteristics of the apps (kinds of tasks, level of maliciousness) being promoted in these videos?

We systematically collect a rich dataset of videos that promote MMAs and study the popularity of these videos as well as the apps they promote. Collecting this dataset poses the challenge of being able to accurately identify these videos. We start by identifying a set of search queries that real users would use to arrive at these videos. We then use the YouTube search API to collect a dataset of ≈20K videos from these queries and extract the links to apps they promote, as well as meta-data corresponding to the apps. This search gives us a wider dataset containing videos other than those strictly promoting MMAs. We design regex based filtering approaches to identify MMAs based on the presence of certain keywords (such as, *"make money", "earn cash"*) in descriptions and names of the apps being promoted.

We then filter our dataset to retain the videos in which we find evidence that MMAs are being promoted, arriving at a rich seed

set of ≈2.2K videos, belonging to 1.1K channels, that promote ≈562 MMAs promising real-world money to users. We analyze the meta-data of these videos and channels finding they are quite popular, aggregating ≈90M views in total. In addition to being popular, user feedback metrics, such as app ratings and video likes indicate that users perceive such apps and videos positively. We also find that the majority of the channels promoting these apps are from users in developing countries (India, Pakistan, and Bangladesh). We then extend our dataset by crawling the entire channels of the videos in our seed sets, as well as running search queries on the Google Play Store, collecting an additional set of ≈311K videos and ≈1.5K apps. In aggregate, we collected ≈1.9K unique apps, which gather a total of ≈720M installs. We also investigate the apps being promoted for malicious behavior. A subset of the apps in our dataset were detected as malicious by at least five Anti Virus engines on Virus Total [21]. These apps have ≈5.7M installs and ≈1M views on videos showing these apps, indicating the large scale at which these videos expose users to harmful content.

To gather further insights into this ecosystem, we interviewed a sample of channel owners, inquiring them about their motivations, their methods for discovering such apps, as well as the amount of money they make by running these channels. We find that although these channel owners spend some time vetting the apps they promote, they themselves do not use these apps to earn money due to the low payouts. They instead make money through their YouTube channel, as well as through sponsorships from the app owners, thereby serving as *advertising channels* for these apps. In essence, they cash out the "earn easy money" idea by luring naive users into an ecosystem that asks them to generate inorganic clicks, likes, views, and installs.

The rest of the paper is organized as follows: § 2 provides details of our dataset collection. § 3 outlines data filtering. In § 4 and § 5, we provide an analysis of the MMAs and the videos that promote such apps respectively. § 6 discusses how we expand our dataset by collecting MMAs from Play Store and YouTube channels. § 7 provides insights into the motivations and earnings of these YouTube channel owners. Related work is discussed in § 8. We provide pointers for future work in § 9 and conclude in § 10.

2 DATA COLLECTION

Figure 1 shows the workflow of our data collection and data filtering methodology. We explain these steps in detail below:

(i) Collecting trending search queries: First, we used Google Trends to get search queries that users typically use to arrive at videos of our interest. We started by searching four seed queries: *make money online*, *earn money online*, *make money mobile*, and *earn money mobile*, and obtained trending queries related to these. This resulted in 421 queries trending across 73 countries. We then searched these again on Google Trends to get related queries in respective countries. The two levels of searching resulted in 1,777 ⟨query, country⟩ combinations. We then filtered this set to retain only the ones with the word *"app"*, giving us a final set of 35 queries. [1] Some example queries in our final set are: *online earning app, best app to earn paytm cash*, and *spin to earn money app*.

[1]Some of the non-app trending queries were: *make money on paytm, earn money at home, earn money online without investment.*

Table 1: Dataset Characteristics

Characteristic	Total	Unique
Search queries	-	35
Total videos (first 5 pages of result)	52,363	20,203
Channels	-	8,557
Videos with ≥ one URL	-	17,881
URLs in video descriptions	118,274	57,093
Domains in landing URLs	-	5,820
Play Store URLs	8,416	2,817
Downloaded Play Store APKs	-	2,472

(ii) Collecting YouTube videos, channels, and meta-data: We used the YouTube API to obtain videos corresponding to the 35 queries. We varied the *video published* year from 2015 to 2020, and obtained the first 250 video IDs for each ⟨query, year⟩ combination.[2] This gave us ≈52K videos, out of which ≈20K were unique. Since the 35 query terms are highly related, this reduction in unique videos is expected. We then obtained video and channel meta-data containing *title, description, view count, like and dislike count, and channel id* fields for the videos, and *country, video count, view count, and subscriber count* for the channels. The videos correspond to ≈8.5K unique channels. Table 1 summarizes our dataset.

(iii) Collecting app URLs: We first extracted all URLs given in the descriptions of these videos, and their corresponding landing pages.[3] ≈89% of videos contained at least one URL, giving us a total of ≈57K unique URLs. We then identified the app-hosting domains and found apps to be hosted on several platforms such as Play Store, fistapk.com, and even shared via Google Drive (see Appendix for details). However, Play Store apps made the major portion of the shared apps. For this work, we focus on the Play Store apps since we were able to obtain their meta-data whereas we lacked the information (such as installs, description) for apps on other platforms.

(iv) Downloading APKs and meta-data of apps: To download APKs of the apps shared via Play Store URLs, we extracted the app *package ids* from URLs and downloaded them from popular websites that host Play Store APKs.[4] In total, we were able to collect APKs of 2,472 apps. The rest were either not available on these websites or had restrictions on downloading them. Out of 2,472, only 927 apps were still present on the Play Store. The rest may have been removed by the Play Store or by the developers themselves. We scraped the meta-data of these 927 apps, including *name, description, installs, ratings, and reviews* from Play Store. We were able to get the *name* and *description* of the remaining 1,545 apps from the same website from which the app was downloaded. *Ratings and reviews* for 1,545 apps were not available on any website. We were able to get *installs* of 2,434 apps from *apkcombo.com*.

3 DATA FILTERING

Despite our search queries on YouTube being highly targeted towards MMAs, our dataset expectedly contains some unrelated

[2]We limited to 250 to retain the most relevant videos.

[3]We follow redirections until we reach the landing page.

[4]We collected APKs from the following five websites: apkcombo.com, apkmonk.com, apkplz.com, apkcloud.com, apkpure.com.

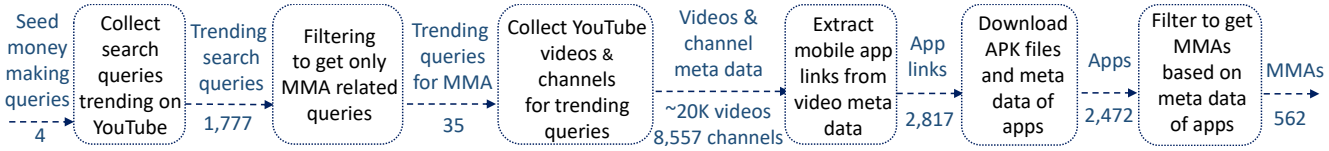

Figure 1: Our data collection and data filtering pipeline. MMA stands for Money Making Apps.

videos due to the way the YouTube search engine determines relevance. For example, the video that receives the highest number of views in our dataset is *"Taylor Swift - Bad Blood ft. Kendrick Lamar"*. The lyrics of the song containing the term *money* and the popularity of the song, likely made it appear in our search results. Similarly, the linked apps might not all be related to real world money. For example, a video titled *"Moy 5 - Virtual Pet Game"* with 15M views contains a link for a game app ***com.frojo.moy5***. The descriptions of the video and the app says *"Play one of the 45 mini-games and earn money!"* but the money is equivalent to game points, and can only be used to play the game.

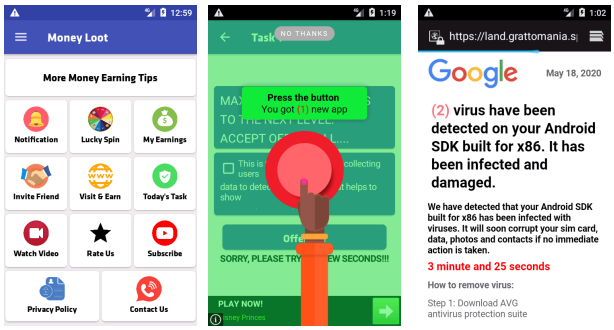

Figure 2: *com.moneyloot.day* screenshots. (Left) Shows the offered tasks. (Middle) Full screen pop up asking user to install apps. Such a pop up appears after every activity. (Right) Landing page after the install app pop up is clicked.

Manual Analysis. Since the focus of our work is to study apps that promise real-world money and the videos that promote such apps, we needed to filter our dataset to remove any videos that do not fall in our category of interest. For this, we first manually analyzed a sample of videos as well as 20 apps by looking at their Play Store app descriptions and interacting with them after installing them on an Android emulator. Our goal in doing so was to identify the attributes of apps that appear to offer real-world money.

We observed that most of these apps give users some tasks to perform, such as *watch videos*, *play games*, or *watch ads*, and award points for completing these tasks. Points are then converted to money, which can be redeemed through some payment methods. We observed `Paytm` (a popular payment gateway in India) to be the most common payment method. Other methods also include `Paypal`, bank transfer, and gift cards. As an example, Figure 2 shows screens of **com.moneyloot.day**, an app that offers users several tasks such as, watch videos, invite friends, and lucky spin. A pop-up opens to install other apps after every action in this app. The pop-ups lead to suspicious pages. The app offers payment via `Paytm` and

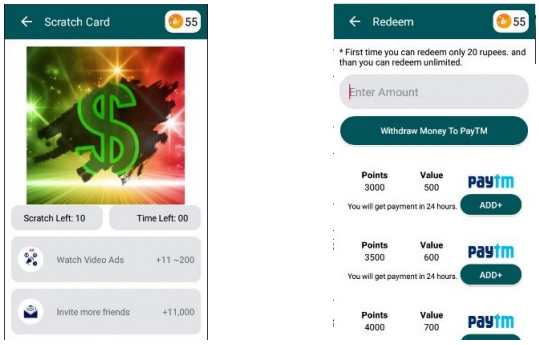

Figure 3: *dailyemoney.watch.video.statusapp* app screenshots. (Left) Shows that it offers scratch cards, watch video ads, and invite friends tasks. (Right) Shows the payment screen listing the conversion rate of points to cash.

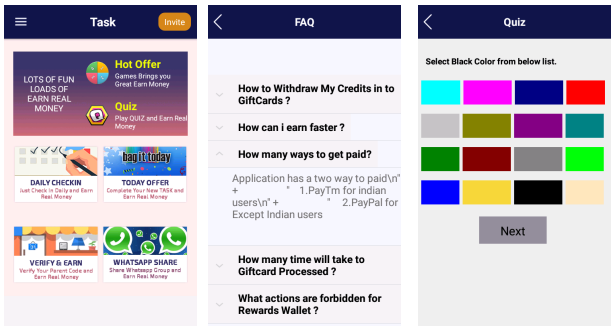

Figure 4: *com.eccflowers.ccehdwallpapers* screenshots. (Left) Shows the offered tasks. (Middle) FAQs on payment. (Right) A question from the quiz task.

the minimum withdrawal is 100INR (USD 1.35). Figure 3 shows the **dailyemoney.watch.video.statusapp** app. It gives the user the option to choose from several tasks such as watch videos, watch ads, lucky spin wheel, and scratch cards. Paytm is the payment method. Figure 4 shows examples of **com.eccflowers.ccehdwallpapers**. Its homepage showed options for multiple tasks. However, we were unable to open any task other than the quiz. The Payment method listed in FAQs is Paytm and PayPal.

These apps, and most of the others we inspected, specify how the app works and the tasks to perform to earn money in the app description.

Regex-Based Filtering. Based on the above manual analysis, we designed regexes to identify MMAs based on the package name, title, and description meta-data. The first regex matches phrases such

as *"earn cash"* or *"make money"*. The second regex matches payment or cashout methods. The third filters false positive apps. For example, games that only pay virtual currency, and buying/(re)selling apps. We arrived at these regexes iteratively, at each step prioritizing reduction in false positives over reducing false negatives. The regexes are listed in Table 8 in the Appendix.

Filtered Dataset. The regex matching resulted in 562 MMAs. We then filtered the videos to retain only the ones having these apps. Our filtered dataset contains 562 MMA apps appearing in 2,256 videos from 1,100 channels. For Section 4 and 5, we only focus on this filtered dataset. We note that although the filtered dataset potentially misses some MMAs and related interesting videos, our goal in this paper is to develop a view into the popularity of these apps and videos based on an accurately labeled set.

4 ANALYSIS OF MONEY MAKING APPS

In this section, we characterize the set of 562 apps, both in terms of the tasks they ask users to perform and the popularity of these apps.

4.1 Types of Tasks in Money Making Apps

MMAs can be categorized based on the task they assign users to earn money. After manually looking at the descriptions of a sample of 50 apps, we identified nine major categories of tasks in MMAs that users need to perform to earn money, as described below:

(i) Install other apps. The apps with this task pay users to install and use other apps. This model is called pay per install (PPI). Apps to be installed can be potentially harmful to the users as shown by prior work [9][20].

(ii) Play games. These apps pay users to play games either in the app, or ask users to install other game apps on their phones to earn money.

(iii) Watch ads. These apps ask users to watch ads to get paid. This task can result in potentially fraudulent activity for ad networks.

(iv) Watch videos. These apps pay users to watch videos or video ads. This task can also result in potential fraud with ad and video networks, as many ad network policies state that users cannot be incentivized with money to watch ads or videos.

(v) Spin wheel. Some apps have a roulette wheel that spins when tapped. The user accumulates points depending on the number where the roulette stops. Points convert to money. This task usually appears with other tasks, such as watching ads or videos or installing apps to get spin chances. The earnings from just spinning the wheel are extremely low, and users have to do other tasks to earn enough to cash out.

(vi) Fill surveys. These apps ask users to fill surveys or give reviews to get money. There are many good paid survey platforms. However, according to a study by Kharraz et al. potentially malicious platforms also exist which ask users to provide sensitive information and redirect them to malicious pages [11].

(vii) Scratch Card. This is similar to the *Spin a wheel* category. The user swipes the phone screen to reveal points that are initially covered. Here again, point to cash conversion is very low and these apps come with other potentially fraudulent and harmful tasks, such as watch ads and install apps.

(viii) Refer. These apps pay users a small amount for inviting more people to the app.

(ix) Miscellaneous tasks. We observed many apps that give users non-challenging tasks. Examples include, take a simple quiz, tap on the screen to break an egg shown on the screen, and click a specific color on the screen. These apps are more likely interested in getting click impressions.

We also installed some of these money making apps on an emulator to study if the description is consistent with the behavior of the apps. We found that description can be a good indicator of tasks given in the app. After that, we looked for keywords in the description of apps, such as *spin to win, refer to friend, install games/apps, watch/click ads, fill survey and scratch and win*, using regular expressions, to identify the tasks in all the apps. Figure 5a shows the number of apps for each category of tasks. Referring other users, watching videos, and playing games are the most popular tasks. Figure 5b shows the number tasks per app. 102 apps that have zero tasks either do not mention the tasks in the description or the tasks are of some other categories.

It is interesting to see how some apps do not state the tasks the user has to perform to earn. Specifically, *watching ads* task is not highlighted in the description. However, when we emulated the apps, most pay for watching ads. Apps that have simple tasks such as, spin wheel, scratch card, and simple quiz pair these with watching ads or videos or installing other apps. For example, **com.bdearners** and **com.flashcash.earnmoney** only say *"earn money and redeem via Paytm"* without stating the task to be performed. However, **com.bdearners** only has *watch ads* task and gets fake click impressions from users. It instructs users to watch an ad for 30 sec and only allows a certain number of ads per day to avoid fraud detection by ad networks. **com.flashcash.earnmoney** asked users to watch videos, with additional ads being played during videos that user has to watch to earn points. Figure 3 shows another app, **dailyemoney.watch.video.statusapp**, in which user has to watch video ads to earn, but this is not stated in the app description. Forcing users to watch ads or paying to watch ads is against the policy of many ad networks and offerwalls. We give more details on this in § 9 discussion.

4.2 App Analysis

(i) Domains Analysis. Given that our initial manual and task analysis showed that MMAs use ad networks and offerwalls to generate revenue, and a part of that revenue is likely promised to the users, we used MobSF, a static/dynamic mobile app analysis tool, to extract and study the domains that were contacted by these apps [16]. We then categorized these domains using McAfee's domain categorization service [15].

Ad networks/ Offerwalls: 320 of 562 MMAs contacted at least one ad network domain. The top three ad networks in these apps were *applovin, moatads, and vungle. Applovin* and *vungle* advertise games and show ads. Both pay publishers if the user installs the app/game, or watches a complete or partial video ad showing apps. Both specify for publishers that users can be incentivized for watching ads or installing apps in the form of in-app benefits but not in form of real money. On investigating *moatads*, we found online anectodal evidence that it is a malware domain that shows unwanted, cling ads in the form of popups containing harmful content [7].

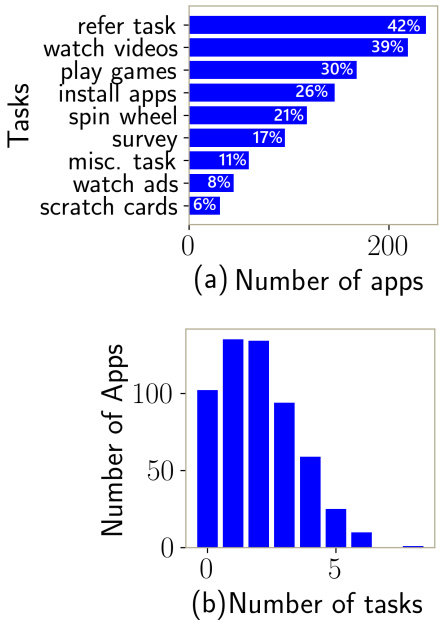

Figure 5: (a) Number of apps for each task. (b) Histogram of number of tasks per app.

Payment Methods: Although 86% of the apps in our dataset mention a payment method in the app description, our domains analysis revealed only 38 out of 562 MMA used a banking or financing domain. The most common finance domains were PayTM, PayPal, and RazorPay. Such a small number of APKs that use a payment method can be due to the limitation of our method. It is also possible that some of the apps do not have an in-built cash-out method, as we observed a few apps where the user had to request payment via a Google Form or email. We also attempted to use Libradar to detect libraries in APKs as done in [9]. However, we found that the pre-trained version of Libradar was unable to detect many payment libraries.

(ii) Malicious Apps. We used Virus total to test the apps for maliciousness. 93 apps were labeled as malicious by one or more Anti Virus engines. 30 were labeled malicious by 5 or more AV engines. These 30 apps accumulated a total of ≈5.7M installs and appeared in 71 videos. Two of the apps **com.app.cash.panda** and **com.ygy.earndayandday** were labeled malicious by 14 AV engines. Each has 100+ installs (max of 999) and each appeared in 1 video.[5] Upon looking at the update history of **com.app.cash.panda** on apkmonk.com, we noted that it was on Play Store from May 2017 to at least Oct 2017. Despite being highly malicious, it managed to live on Play Store for 6 months and gathered these many installs. **com.ygy.earndayandday** was also on Play Store for at least 3 months and managed 100 to 999 installs during this time. We observed that out of the 562 apps, only 170 were left on Google Play Store. It is possible that the apps were taken down by Google Play Store due to maliciousness. Out of 93 apps that were identified as malicious, 4 are still on Google Play Store, while others have been removed. These four were labeled as malicious by one AV engine on VirusTotal.

We also identified that at least 30% of the apps ask users to install other apps/games (Figure 5a), which can potentially expose them to harmful apps. Figure 2 (right) shows an example of how one such app tricks the user to perform an installation by redirecting them to a page which is designed to look like it belongs to Google.

We were unable to perform automated mass dynamic analysis as most apps do not work on emulators. In addition, almost all the apps required signing up using a phone number and email address. Automating this process was out of scope for this work.

4.3 App Popularity

(i) Number of videos sharing the app. Figure 6a shows more than 45% of the apps appeared in two or more video's description. The top two MMAs that appeared in most videos are: *com.databuddy.app*, which offers users shop and cashback option, and appeared in 372 videos, and *videos.share.rozdan*, a content sharing app, which appeared in 100 videos. Both of these are Indian apps.

(ii) Agg views on videos. Figure 6b shows the CDF of aggregated views on videos sharing MMAs. More than 75% of apps had at least 1K aggregate views. Top two apps with the highest aggregated video views are *com.databuddy.app* and *best.game.bulbsmash*. Data Buddy is discussed above. Bulb Smash pays for referring friends and playing games.

(iii) Installs. Figure 6e shows the histogram of number of installs for each app. 40% of the apps have ≈100 installs, and around 60% have more than 100 installs. *com.whaff.whaffapp* and *videos.share.rozdhan* are two apps with the highest number of installs (10M). The former pays for installing other apps/games, and the latter for playing games, watching videos, and sharing content.

(iv) Ratings on Play Store. Figure 6c shows the CDF of app ratings. This plot is only for apps that were still on Play Store at the time of data collection (174/562). 93% have a score of 3 or more and 50% have a score of 4 or more. These high ratings can be due to two reasons: either only good quality apps are still on Play Store, or the ratings are potentially fake [19]. Table 2 shows the two highest rated apps (*com.tvtwo..free.income* and *proxima.makemoney.android*). Both give users a variety of tasks such as install apps, play games, surveys, and watching videos.

(v) Reviews on Play Store. Figure 6d shows the CDF of the number of reviews on apps. Around 60% of apps have more than 100 reviews. The two apps with the highest number of reviews (given in Table 2) offer the tasks of survey, watch videos, play games, and scratch card. This graph is also only for apps that were still on Play Store.

(vi) Release year on Play Store. Figure 6f shows the number of apps released each year. This data is also only for 174/562 apps. The number of MMAs released each year has consistently increased over time.

More examples of apps according to popularity in each category along with the tasks, payment methods, and minimum cash-out value are given in Table 2.

[5]Installs on Play Store are given in ranges; 100+ = [100 - 999].

Table 2: Examples of Google Play Store Money Making Apps having High(H), Medium(M), and Low(L) popularity in each category

Metric	Pop.	Package name of app	Installs	Reviews	Ratings	Videos	Agg. views	Task [+]	Payment methods [++]	Min. withdraw
Installs	H	com.whaff.whaffapp	10M	-	-	60	1.7M	IA,PG	PT,PP	$10
	H	videos.share.rozdhan	10M	72K	3.94	100	6.8M	PG,VW,SH	PT	200 INR
	M	com.mydeals.myAds	50K	1	3.6	2	16K	WA,QU	MR	19 INR
	M	com.dmgame.waffelraffel	10K	6K	4.19	1	140	WA	PP	$10
	L	com.appybuilder.mukeshlab00.FireMoney	100	-	-	1	13K	-	PT	
	L	makemoney.earnmoney.moneymachine	100	-	-	3	55K	IA,WV	PP	$1
Aggr. views	H	com.databuddy.app	10M	32K	3.57	372	29M	CB	PT,AZ	50 INR
	H	best.game.bulbsmash	5M	-	-	79	8.6M	RF, PG	PT,PP	100 INR
	L	com.wonder.adharloan	50K	-	-	1	8	WV,WA,SW	PT	100 INR
	L	com.gerry.bestrewardzall	100	-	-	1	9	PG	PP,AZ	
Videos	H	com.databuddy.app	10M	32K	3.57	372	29M	CB	RT,AZ	50 INR
	H	videos.share.rozdhan	10M	72K	3.95	100	6.8M	PG,VW,SH	PT	200 INR
	L	gameshow.realmoney.quiz.game.app	100K	-	-	1	5K	QU	PT	200 INR
	L	com.appybuilder...trendwallet *	100	-	-	1	400K	WV	PT	
Reviews	H	proxima.makemoney.android	5M	300K	4.64	16	300K	WV,SU,PG	PP	$5
	H	com.luckyday.app	10M	400K	4.33	10	200K	JP,SC	AZ,PP	$10
	L	app.plticl.nwspolict	1K	0	0	5	9K	RN,QU	PT	2 INR
	L	com.wheathr.news	1K	0	0	1	2K	RN,WA,QU	PT	2 INR
Ratings	H	com.tvtwo...free.income**	1M	99k	4.72	2	367	SU,PG,RN	PP	$5
	H	proxima.makemoney.android	5M	300K	4.64	16	300K	IA,SU,WV	PP	$5
	M	com.innovativehall.ghc	100K	2K	2.46	1	46K	WV,WA,IA	PP	$5
	M	de.mobileheroes.realmoneyminer	500K	3.5K	2.80	1	2K	WA,PG	PP	$5
	L	com.digibrain.earnmoney	1K	5	3.1	1	372	WA,SW	PT	10 INR
	L	com.wheathr.news	1K	0	0	1	2K	RN,WA,QU	PT	2 INR
	L	com.nws.redr	1K	0	0	4	11K	RN,WA,IA,QU	PT	2 INR

*com.appybuilder.trendwallet8090.trendwallet, **com.tvtwo.highest.paying.cash.app.make.money.surveys.rewards.free.income

[+]Key for tasks given in app: **IA**= install apps, **PG**= play or install games, **VW**= visit websites, **SH**= share content, **WA**= watch ads, **QU**= quiz, **WV**= watch videos, **CB**= cashback, **RF**= refer friends, **SW**= spin wheel game, **SU**= survey, **JP**= jackpot, **SC**= scratch card, **RN**= read news.

[++]Key for Payment methods used in app: **PT**= Paytm, **PP**= Paypal, **AZ**= Amazon, **MR**= mobile recharge

5 VIDEO AND CHANNEL ANALYSIS

The 562 MMAs trace back to 2.2K unique YouTube videos and 1.1K unique channels. In this section, we analyze the videos and channels from the perspective of user engagement and the channel owners commitment to producing content. Attributes such as views, subscriber count, and likes are an indicator of user engagement and channel popularity, whereas the number of videos and years active are indicators of the channel owner's commitment to producing such content.

(i) Apps per video. We would expect that a video would lead us to one APK, however, we can see from Figure 7a that this is not the case. While more than 1,000 videos led us to only one APK each, the remaining videos led to more than one APK, and the highest count of APKs per video was 22.

(ii) Video views. Figure 7b shows view count for MMA videos range from 5 to 3.85M. ≈50% videos have more than 5K views, indicating a good fraction have a large audience. The top 5 videos with the highest views, shown in Table 4, are examples of videos promoting MMAs with the largest audience. These 5 videos are all from different channels and promote one APK each. All 5 channels are of Indian Youtubers and all 5 videos are of short duration. The two videos that gave the link of **com.databuddy.app** in the description were in fact promoting something else in the videos. The first video focused on teaching the viewer to create their app to make money, while the second video taught the viewers how to go about making money from a site called *pay-box.in*. One video shows how to use **best.game.bulbsmash** app and another shows how to use **videos.share.rozdhan** app to make money. The video showing **in.coupondunia.androidapp** app was hosted on the official channel of this app.

(iii) Video likes/ dislikes. Figure 7c shows that more than 50% of the videos have ≈8 times the number of likes to dislikes, and 20% have more than 10 times the number of likes to dislikes, indicating a positive user feedback image being maintained by these videos.

(iv) Channel video count. Figure 7d shows more than 50% of the channels have 150 video uploads or more. The highest video count is ≈5K. The top 5 channels with the highest video count (out of 2.2K videos in our dataset) are shown in Table 5. These top channels had a minimum view count of 1.3M, and a minimum subscriber

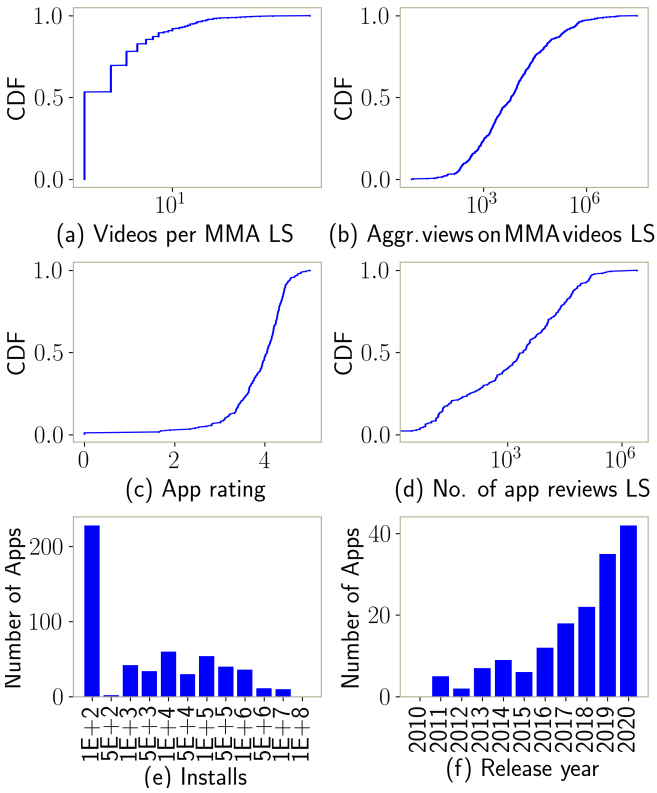

Figure 6: Plots showing popularity metrics of Money Making Apps (MMAs). LS= log scale, CDF= Cumulative distribution function.

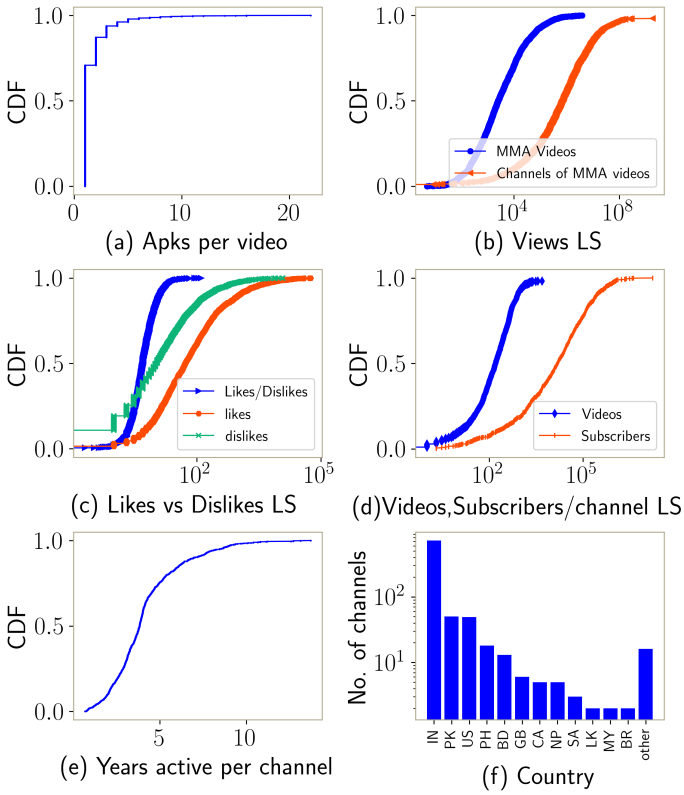

Figure 7: Plots showing various metrics of videos and channels promoting money making apps. LS= log scale, CDF= Cumulative distribution function.

count of ≈13K. The number of distinct MMAs we have in our data set from these channels is also high. All 5 channels are from India promoting dedicated content on money making apps. They use flashy thumbnails promising money making apps. Figure 8 shows two sample thumbnails of videos from ***My Advice*** channel. The accounts behind two of the top 5 popular channels, ***Teach Me*** and ***Tamil Snekithi*** have been terminated by YouTube at the time of this writing, and the following text appears when trying to reach these channels on YouTube:

> "This account has been terminated due to multiple or severe violations of YouTube's policy against spam, deceptive practices, and misleading content or other Terms of Service violations."

(v) Channel years active. Figure 7e shows that 50% of the channels have been active for less than 3.5 years, while the oldest channel is a little over 13 years old. Table 3 shows the 5 oldest active channels. The first and third channel have been inactive for many of the years between the time they were first published to date. Initially, their content was music videos or videos of nature, and recently they added a very small number of videos related to money making. The fourth channel seems to have mixed content, with news about cricket and packages offered by phone companies. The second and fifth channels, with the highest number of videos from these 5, seem to be dedicated to content related to making money from

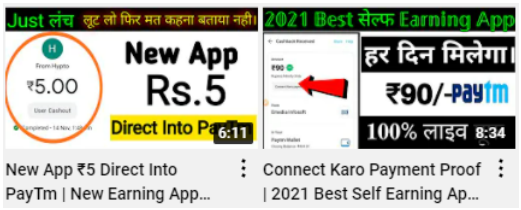

Figure 8: Thumbnails of two videos showing money making apps from *"My Advice"* channel.

home.

(vi) Channel subscribers. More than 50% of channels had over 10K subscribers as shown in Figure 7d. High subscriber count is predictive of high view counts. Figure 7b shows that ≈50% of channels have more than 0.1M views. The highest view count across all videos for a channel was 1.8B. The highest number of subscribers for a channel was 21M.

(vii) Channel countries. Figure 7f shows that a major fraction (71%) of these channels are from the developing countries (India, Pakistan, and Bangladesh). From non-developing countries, the US had 49 channels. Distinct apps from channels from the top three countries in our dataset were, IN: 386, PK: 67, and US: 57.

Table 3: Top five channels by duration active

Title	Active Since	Country	Views	Subscribers	Videos
GrafLubber	2007	-	2.8K	245	20
Mani Karthik	2009	IN	1.1M	4.8K	119
SileNiM	2008	US	2.8K	262	17
Technical Baroli G	2008	IN	357K	2.5K	51
Entertaining tv	2008	US	13M	91200	710

(viii) Malicious apps. 30 of 562 apps that were labeled as malicious by 5 or more AV engines on VirusTotal, appeared in 71 videos and accumulate a massive ≈1M views in total. These videos were from 40 channels and these channels have ≈2 M subscribers in total.

6 COLLECTING MORE MMAS

The previous sections established the popularity of apps and videos using a small set of MMAs. To expand our dataset and collect more MMAs, we used the following two approaches:

Directly collecting apps from Play Store. Using the following search terms, we directly searched Play Store to see if we can collect more MMAs. We selected these search terms after observing common keywords used in the meta-data of the 562 MMAs we collected from YouTube. *Terms: make money, earn money, spin and win cash, spin and earn, watch videos earn money, earn money surveys, watch ads earn money, free money, scratch and win, earn paisa.*

For each query, Play Store results in 250 apps at maximum. This gave us 984 unique apps out of which 381 were identified as MMAs after matching with our MMA regexes outlined in § 3. We believe the number of MMAs to be higher than 381, since our regexes are designed to reduce false positives and therefore result in false negatives. For example, **com.dailyearningsonline.thequizmoney** was not identified as MMA, as it does not specify any payment means in the description. From these 381 apps, 41 were also in 562 MMAs that were collected from YouTube videos. 340 new apps from Play Store and 521 apps that were only found from YouTube shows that both sources (direct search from Play Store and search from YouTube) are valuable for collecting MMAs.

From YouTube channels. The viewers of videos promoting MMAs are likely to watch other videos on the same channel. Therefore, we identified if channels of videos, that gave 562 MMAs, promote similar apps in their other videos that did not appear in our initial YouTube search. To do so, we collected all the videos of 1.1K channels. This gave us ≈311K videos. These videos contained ≈20K unique Play Store links in the description. We followed the same process to obtain Play Store apps as given in § 2 and collected ≈17K apps. 1,126 of 17K apps were identified as MMAs by regex matching. 73 of the 1,126 were also present in the direct Play Store search.

1,053 unique MMAs from exploring YouTube channels indicate that there can be more MMA promoting videos on YouTube by the same channels. These videos did not appear in our initial query based search but it is natural for users to see these videos while exploring the channel.

7 INTERVIEWS WITH CHANNEL OWNERS

To gain insight into the ecosystem, we interviewed a sample of channel owners. The study was approved by the IRB of the authors' institution (LUMS). We searched for email addresses of the channel owners in the description of their channels. In total, we found contact information for 130 channels. Before beginning the interviews, we informed the interviewees about the purpose of our research, and that their names and channel information will not be disclosed in any published research. We compensated the participants at $10 per 30 minutes of their time. We were able to get responses from 13 of channel owners, but eventually only 4 appeared in interviews. The others either stopped responding or were unavailable during our study period.

Table 6 shows the demographics of the four channel owners we interviewed. Two of the owners belonged to Pakistan, one to India, and one to Bangladesh. Three of the channels have been active since 2017, while one has been active since 2013. The total number of videos on their channels ranged between 79 to 445, and the channel subscriber count ranged between 4.4K and 547K. All channels had descriptions in English, however the language in the videos was either Urdu, Hindi, or Bengali depending upon the country of the channel owner. Three channels had major content on money making apps and websites, and one had content on a variety of topics (still ≈1/3 on MMAs).

While the interviews were semi-structured, we sought to gather insights to the following main questions: (i) how did they learn about and get interested in this ecosystem?, (ii) how much money do these money making apps offer per hour?, (iii) how much earnings do they make from their YouTube channel and at what level of time investment?, (iv) what platform do they use to learn about new apps and whether the app owners offer any incentives / sponsorships for promoting apps on their channel?, (v) are they aware that some of these apps might be fraudulent and expose users to harm? If yes, what vetting procedures do they use to prevent their channel's audience from fraud?, and (vi) what strategies (if any) do they use to retain and increase their audience and channel earnings?

We now discuss our findings on each of the above questions.

(i) How did they learn about and get interested in this ecosystem? Most of the interviewees learned about this ecosystem through friends who were earning money online in various ways (freelancing, Forex, money making apps). In particular, one interviewee mentioned they had a friend who used to earn 3,000 Indian Rupees (USD 40) per download using the app *mCent*, which got him interested.

(ii) How much money do these money making apps offer and who is their target audience? All Youtubers mentioned that earnings from task-based money making apps is very low – on the order of 100-200 Indian Rupees (USD 1.35- USD 1.7) per 2-3 hours of time investment. In fact, they mentioned that one of the reasons for starting these channels is that the earnings from these apps were not enough. For example, the apps that require referrals for earning money were not very fruitful for them without the channels, because they were only able to generate 5-6 referrals (mostly friends). With YouTube, they have a bigger audience through which they can earn money from referral link apps and also teach their audience about it.

Table 4: Top five videos by viewcount [these titles have been translated from Hindi*]**

Title	Views	Apk(s)	Country
EARN Rs. 350/- PAYTM CASH DAILY with this trick	3.85M	best.game.bulbsmash	IN
Earn millions by creating your own app [only 5 mins]*	3.02M	com.databuddy.app	IN
Meet Coupon Kumar - The Crazy Coupon Guy | CouponDunia	2.95M	in.coupondunia.androidap	IN
Best Earning App 2019 For Android | Earn Money From Smartphone	2.45M	videos.share.rozdhan	IN
1 Gmail->100 Rupees!! 10Gmail->1000 Rupees!! Free Paytm Cash!! Man earned 12000 rupees*	2.08M	com.databuddy.app	IN

Table 5: Top five channels by videocount (out of 2,256 videos)

Title	Videos (out of 2,256)	Distinct MMAs shown in videos	Active since	Country	Viewcount	Subscribers	Total Videos
Tech And Free Cash	26	10	2017	IN	3.4M	36K	1446
My Advice	25	24	2018	IN	1.3M	17K	790
NK Technical Guru	25	3	2012	IN	4.5M	67K	976
Teach Me	23	21	2016	IN	1.6M	13K	871
Tamil Snekithi	23	21	2016	IN	3.2M	60K	1362

Table 6: Interviewee demographics and channel characteristics

Interviewee #	1	2	3	4
Country	PK	PK	IN	BD
Subscribers	4.4K	547K	268K	8.41K
Videos	445	427	234	79
Language (videos)	Ur	Ur	Hi	Be
Language (description)	En	En	Hi En	En
Major content on MMAs?	Yes	Yes	Yes	No^{+}
Active since	2013	2017	2017	2017
Views range	43-42K	1K-130K	1K-300K*	43-999K

Interviewee names and channels have been anonymized
Be=Bengali, En=English, Hi=Hindi, Ur=Urdu
$^{+}$ ≈1/3 videos were on MMAs.
* Interviewee mentioned that some views are fake.

Target Audience: Most interviewees mentioned their target audience are young people (for example, high school kids) looking to earn pocket money. One interviewee commented: "I prefer young people because I myself acknowledge the fact that these apps are not the main source of income and even YT is not reliable, and I fear that any small mistake might lead to the closure of my channel and hence, hinder my earning." Upon asking whether they think if their videos enable people to make decent money, one interviewee said no, indicating that YouTubers are inclined to make videos on money making apps and online earning due to their popularity among users even if those people do not use them in the longer term.

(iii) How much earnings do they make from YouTube channels? One of the interviewees who owns eight channels mentioned that he earns 25K-30K Indian Rupees (USD 336- USD 400) per month per channel, and spends approximately 20 minutes per video. The number of videos he makes per month depends on the number of sponsors. A second interviewee disclosed he has earned 60K, 41K, and 100K Pakistani Rupees (USD 342, USD 234, and USD 571) respectively in the last three months, and dedicates around 15-20 hours per month to producing content for his channel. While the majority of the earnings come from YouTube monetization, some fraction of these earnings are also through app sponsors, who pay to have their apps featured on these channels.

The interviewees added that one can earn a good amount of money once their channel gets established, however, establishing a channel takes a lot of time and patience. Some Youtubers mentioned that they could not spend much time when they made the channel because some of them were studying or doing other things at that time. This is why it took them quite long to reach to a point where they are earning handsome amount of money from YouTube. Over time, their channels grew, and now they are doing it as a side business and still cannot allocate their whole time to the channel. One of the Youtubers mentioned, "I cannot devote much time to the channel because I am studying along with managing two businesses". They also emphasized on the fact that one should not rely completely on YouTube's earning because "it takes a second to get your channel suspended or terminated without any warning."

(iv) What platforms do they use to learn about new apps? The interviewees mentioned a number of sources including searching for apps and websites themselves, videos of other Youtubers, Play Store, Facebook groups, and app developers approaching them for sponsorship on their channels.

We probed further about sponsors, and found sponsors reach out to those channels which have a high number of subscribers and views. One of the YouTubers mentioned that it took them almost 7-8 years to get their first sponsor, while for another, they got the first sponsor in 4 years. One interviewee also mentioned that due to the difficulty of obtaining real subscribers and views on their

channels, they have used fake subscribers and views to build the reputation of their channel.

(v) Are they aware that some of these apps might be fraudulent and expose users to harm? If yes, what vetting procedures do they use to prevent their channel's audience from fraud?

While in general, the channel owners did not seem to be aware about participation in fraud resulting from the nature of tasks (clicks and installs) or that the apps could result in malware installation, they did seem knowledgeable about scams and incorporated various strategies to prevent users from scams. Two of the interviewees stated that they feel a moral responsibility towards their audience, and take steps to prevent users from negative experiences.

One of them mentioned that he checks whether the apps have completely free earning mechanisms. He doesn't promote any apps if there is any investment involved stating "due to increased fraud nowadays, I can't risk people losing money as in turn, it is my loss too". He also mentioned that he does not promote any apps that require users to enter credit card information.

Similarly regarding app sponsorships, we probed them further to inquire if they have any set criteria for accepting the apps for promotion on their channels, since it appears there is a tension between obtaining money from sponsorships and protecting their audience from fraudulent apps and negative experiences. We obtained the following responses:

> "Not really but I let the users know that they are not very reliable (by adding the tag of "Paid Content")."

> "Yes, I accept all offers because my rate is fixed. I don't accept sponsors with less than my rate but the apps themselves should be of average quality too. Because some apps look like that they are definitely fake, so I don't promote those. Rest I accept."

We also found that there is a community of these Youtubers connected via Whatsapp groups where they share information with each other about apps that scam users. They have exposed such apps in the past by creating videos about them and uploading on their channels.

(vi) What strategies (if any) do they use to retain and increase their audience and channel earnings? One interviewee mentioned they used fake reviews and likes to increase the channel's reputation. Others were either vague, mentioning they use 'some techniques', without elaborating further, or did not disclose any methods.

8 RELATED WORK

The work closest to ours is [9]. Yangyu Hu *et al.* identified 1,377 MMAs out of 2.5M apps from Chinese app distributors and Play Store, by matching meta-data of apps with a manually created list of words in MMAs and identifying payment Libraries using Libradar. They found the tasks given to the users to be harmful, such as asking users to share inappropriate content or to install malicious apps. In addition, they analyzed comments on the apps and found several user complaints. 26% of their apps were detected as malicious by one or more AV engines in Virus Total. Their 1,377 apps had 1M total installs and 90% had 5-star ratings.

Many activities that we identified in MMAs have been investigated by the research community for their fraudulent behavior. Paying real money to users for watching ads is against the policy of many ad networks (e.g Google Admob [1]) and offerwalls (e.g Applovin [2]). A lot of work has been done to identify violations of these policies and detect click fraud [3][6][5]. Harms of PPI have also been explored in prior work, revealing prevalence of malicious products and Potentially unwanted programs (PUP) in PPI [13][20]. Authors in [8] specifically study PPI in Android apps. By using a Honey Mobile app and other apps that use the PPI services, they showed harms such as inflating app's ranking on app stores and potential fraud with advertisers. Buying views to inflate video viewership (in watch videos task) is against the policy of many video sharing platforms, such as YouTube. Marciel *et al.* studied how it disrupts the monetization system in YouTube, DailyMotion, and Vimeo [14]. Kharraz *et al.* showed that a large number of survey gateways require user's sensitive information and redirect users to pages hosting PUP, malware, and adult content [11].

The works mentioned above focused on studying different kinds of fraud. To the best of our knowledge, we did not find any work studying how users are lured in for participation. Our study focuses on identifying the role of YouTube in promoting MMAs, and our results illuminate its role in luring people to these apps in hope of earning cash without realizing the potential harms.

9 DISCUSSION AND FUTURE WORK

We presented the first study of the role of YouTube videos in convincing users to install money making apps. Our work shows that these videos and the apps they promote are quite popular. Aggregated views of such videos reached ≈90M, aggregated installs on these MMAs reached ≈720M, and aggregate subscribers of these channels are ≈111M, indicating their popularity. By looking at the channels of videos we observed that these videos and apps are most popular in developing countries, and offer cash out in local currencies and payment systems (for example Paytm).

Our preliminary investigation of maliciousness of the promoted apps flags 93 out of 539 apps as malicious. We also observed malpractices with ad networks, where users were tricked or forced to watch ads while performing other tasks to gain points. We also found apps to be violating *Rewarded Ads* offered by mobile ad networks, by offering cash in return for these ads, when the ad network policy strictly prohibits this. For example, according to one of the popular ad networks, Vungle's policy:

> "Rewarded ads deliver a great user experience by offering users something of value in exchange for watching or engaging with an ad. This exchange is typically a reward within your app, such as extra lives in a game, virtual currency, or a hint in a puzzle" – Vungle [22]

Vungle restricts publishers from invalid impressions , which they define as:

> "Invalid Impressions are caused by: ... using offers of cash, prizes, incentives, gift cards, vouchers or anything of value, including cryptocurrency" – Vungle [23]

Our interviews with a sample of four channel owners showed that the Youtubers are more interested in creating YouTube content and getting views on their videos, so that they can make money from YouTube and sponsorships. They are not necessarily aware of the fraud and harm facilitated by the tasks in such apps. While they

often check for potential scams, they lack the technical knowledge to check these apps for other types of fraud and maliciousness.

Future work. Our app identification method was primarily based on regexes, and the regexes were chosen conservatively to avoid false positives. Future efforts can focus on robust methods for automated detection of MMAs based on behavioral analysis of apps. Our initial analysis reveals that one challenge in doing this at scale is that the apps require accounts, and typically use strategies to detect when they are being run on emulators (by checking for cellular network connectivity). Similarly, our identification of the videos that promote MMAs relied on the presence of a MMA link in the description. Future efforts can focus on automated detection of videos promoting such content, perhaps by leveraging video thumbnails, content, or meta-data.

While our work sheds light on the motivations of the Youtubers, understanding the ecosystem behind the apps is also an interesting direction for future work. Who are the developers behind these apps and what fraction of these apps abuse Rewarded Video Ads offered by mobile ad networks? Do the users of these apps actually earn any money or are these mostly scams that lure users in, and the users eventually give up? An NLP-based analysis of the comments on the Play Store as well as YouTube videos can help answer some of these questions.

10 CONCLUSION

In this work, we examined the role of YouTube in promoting money making apps. We found that the majority of these videos are made by and for people in developing countries. These videos gathered huge audiences indicated by the number of views and likes on the videos. Apps promoted in these videos also gain a massive number of users, as indicated by the number of installs of the apps. Our analysis also sheds light on potential harms and malpractices of the promoted apps. In conclusion, we find YouTube videos to be a potential driver of luring users to install these apps with promises of earning money without realizing the harms.

ACKNOWLEDGEMENTS

This research was funded by the Ministry of Planning, Development, and Special Initiatives through the Higher Education Comission (HEC) of Pakistan under the National Center for Cyber Security (NCCS). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.

REFERENCES

[1] AdSense. 2022. Rewarded inventory policy. Retrieved March 3, 2022 from https://support.google.com/adsense/answer/9121589
[2] Applovin. 2022. Terms of Use Agreement. Retrieved March 3, 2022 from https://www.applovin.com/terms/
[3] Geumhwan Cho, Junsung Cho, Youngbae Song, and Hyoungshick Kim. 2015. An empirical study of click fraud in mobile advertising networks. In *Proceedings of the 10th IEEE International Conference on Availability, Reliability and Security*. 382–388.
[4] Dancho Danchev. 2008. Inside India's CAPTCHA solving economy. https://www.zdnet.com/article/inside-indias-captcha-solving-economy/
[5] Feng Dong, Haoyu Wang, Li Li, Yao Guo, Tegawendé F Bissyandé, Tianming Liu, Guoai Xu, and Jacques Klein. 2018. Frauddroid: Automated ad fraud detection for android apps. In *Proceedings of the 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 257–268.
[6] Feng Dong, Haoyu Wang, Li Li, Yao Guo, Guoai Xu, and Shaodong Zhang. 2018. How do mobile apps violate the behavioral policy of advertisement libraries?. In *Proceedings of the 19th International Workshop on Mobile Computing Systems & Applications*. 75–80.
[7] EngimaSoft. 2020. Z.moatads.com. Retrieved March 3, 2022 from https://www.enigmasoftware.com/zmoatadscom-removal/
[8] Shehroze Farooqi, Álvaro Feal, Tobias Lauinger, Damon McCoy, Zubair Shafiq, and Narseo Vallina-Rodriguez. 2020. Understanding Incentivized Mobile App Installs on Google Play Store. In *Proceedings of the 20th ACM Internet Measurement Conference*. 696–709.
[9] Yangyu Hu, Haoyu Wang, Li Li, Yao Guo, Guoai Xu, and Ren He. 2019. Want to earn a few extra bucks? a first look at money-making apps. In *Proceeding of the 26th IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*. 332–343.
[10] Mobin Javed, Cormac Herley, Marcus Peinado, and Vern Paxson. 2015. Measurement and analysis of traffic exchange services. In *Proceedings of the 15th ACM Internet Measurement Conference*. 1–12.
[11] Amin Kharraz, William Robertson, and Engin Kirda. 2018. Surveylance: automatically detecting online survey scams. In *Proceedings of the 29th IEEE Symposium on Security and Privacy (SP)*. 70–86.
[12] Do-kyum Kim, Marti Motoyama, Geoffrey M Voelker, and Lawrence K Saul. 2011. Topic modeling of freelance job postings to monitor web service abuse. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence*. 11–20.
[13] Platon Kotzias, Leyla Bilge, and Juan Caballero. 2016. Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services. In *Proceedings of the 25th USENIX Security Symposium*. 739–756.
[14] Miriam Marciel, Rubén Cuevas, Albert Banchs, Roberto González, Stefano Traverso, Mohamed Ahmed, and Arturo Azcorra. 2016. Understanding the detection of view fraud in video content portals. In *Proceedings of the 25th International Conference on World Wide Web*. 357–368.
[15] McAfee. 2020. https://www.trustedsource.org/.
[16] MobSF. 2020. https://github.com/MobSF/Mobile-Security-Framework-MobSF.
[17] Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. 2010. Re: CAPTCHAs—Understanding CAPTCHA-Solving Services in an Economic Context. In *Proceedings of the 19th USENIX Security Symposium*. 28–28.
[18] Oli. 2021. Click Farms: What Are They and What Are They For. Retrieved March 3, 2022 from https://www.clickcease.com/blog/click-farms-what-are-they-what-are-they-for/
[19] Mizanur Rahman, Nestor Hernandez, Ruben Recabarren, Syed Ishtiaque Ahmed, and Bogdan Carbunar. 2019. The Art and Craft of Fraudulent App Promotion in Google Play. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 2437–2454.
[20] Kurt Thomas, Juan A Elices Crespo, Ryan Rasti, Jean-Michel Picod, Cait Phillips, Marc-Andr'e Decoste, Chris Sharp, Fabio Tirelo, Ali Tofigh, Marc-Antoine Courteau, et al. 2016. Investigating commercial pay-per-install and the distribution of unwanted software. In *Proceedings of 25th USENIX Security Symposium*. 721–739.
[21] VirusTotal. 2020. https://www.virustotal.com/
[22] Vungle. 2020. Vungle-Integrate Interstitial and Rewarded Ads. Retrieved March 3, 2022 from https://support.vungle.com/hc/en-us/articles/360047788532-Integrate-Interstitial-and-Rewarded-Ads
[23] Vungle. 2020. Vungle SDK License and Publisher Terms. Retrieved March 3, 2022 from https://publisher.vungle.com/LICENSE.html

A APPENDIX

Collecting app URLs. Other than URLs belonging to app stores, we looked at the most frequent domains across the videos (excluding social media domains) and identified the popular domains that can potentially host apps for downloading. We did so using a combination of manual inspection and identifying domains that contained the keyword "app" or "apk". Table 7 shows the number of URLs of these domains. Note that some domains host only one app, but had several different links due to the referral parameter.

Explanation of Regex used for app filtering: Table 8 gives the regexes used for identifying MMAs. The first regular expression catches the most common keywords in MMA app descriptions, however, on its own, it results in false positives as well. The most common false positives that matched regex 1 but were not MMA were of games with virtual money (such as *com.skgames.trafficracer* and *com.fro*

Table 7: Popular app hosting domains in our dataset

Type	Domain	URLs
App store	play.google.com	2,817
	apps.apple.com	257
Non app store (Hosts one app, but different links due to referral parameter)	winzogames.com	665
	m.videobuddy.com	115
	m.helo-app.com	217
	flipkart.com	74
	getmpl.com	187
	cash.app	96
	draw.4fun.mobi	161
Non app store (Hosts multiple apps)	drive.google.com	274
	fistapk.com	91
	r.appvirality.com	69

Table 8: Regexes for identifying money making apps

No.	Regex
1	(\bearn|\bmake\b|\bwin|\bmaking|\bfree|\bredeem |\bearning)(?:\W+\w+){0,5}\W+(\bmoney\b|\bcash \b|\bpaisa\b|\bpaise\b|\bpaisy\b)|(\bspin)(?:\W+\w+) {0,5}\W+(\bwin|.)(?:\W+\w+){0,5}\W+(\bcash\b| \bmoney\b)|(\bearn|\bwin)(?:\W+\w+){0,5}\W+ (\bmoney\b|\bcash\b)(?:\W+\w+){0,5}\W+(\bspin)|(\bearn)(?:\W+\w+){0,5}\W+([$]|rupees|dollar|rs.)
2	(\bv wallet\b|(win|earn) real (money|cash)|cash prize(|s)|\bbtc\b|\bbitcoin(|s)\b|\bcashout\b| \bpaypal\b|\beasypaisa\b|\bjazzcash\b|\bwithdraw \b|\bpaytm\b|\brazorpay\b|\balipay\b|\bgiftcard(|s)\b)
3	(does not offer (.|)real money|\bbuy(|ing) (&|and)(sell|resell)(|ing)\b|\bresell(|ing)\b)

jo.moy5) and gambling apps with a disclaimer in the description "no real money is paid" (such as *com.zynga.hititrich* and *com.teenpatti.hd.gold)*. Other false positives included payment apps (such as *net.one97.paytm*, offical app of `Paytm`, *com.paypal.android.p2pmobile*, `Paypal's` mobile app), buying/(re)selling apps (such as *com.snapdeal.main*), and online shopping apps (such as *com.localqueen*, *com.balancehero.truebalance*, *com.meesho.supply* and *com.shpock.android*). To avoid these false positives, regex 3 was added. Any app that matched the third regex was not considered as an MMA. Regex 2 was added to keep only those apps that specify payment methods in the description.