

# Online training on Internet of Things (IoT) and Mobile Security

Organized by CIET-NCERT in collaboration with I4C, MHA



7 Sep, 2023



4:00 pm-5:00 pm

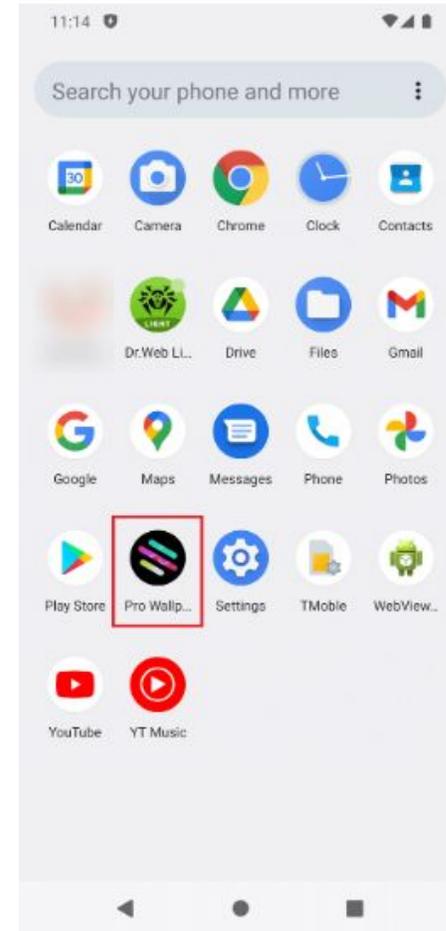


**Day 4: Mobile: Security, Threats and Safety Measures**

**Dr. Deepak Kumar**  
Sr. Cyber Intelligence and Digital  
Forensic Professional  
I4C, MHA

**Mr. Shinku Saran Singh**  
Deputy Commandant  
I4C, MHA

# Shifted from vishing to mobile app



# MOBILE THREATS

Threat actors are using newly **discovered** “**SandStrike spyware**” and delivered via a malicious VPN application to target Android users

<https://www.bleepingcomputer.com/news/security/new-sandstrike-spyware-infected-android-devices-via-malicious-vpn-app/> Nov 2022

New **ERMAC 2.0 banking** Android Trojan malware steals accounts, wallets from 467 apps to steal account credentials and crypto wallets.

<https://www.bleepingcomputer.com/news/security/new-ermac-20-android-malware-steals-accounts-wallets-from-467-apps/> May 2022

Meta uncovers **400 malicious apps** on Android and iOS apps, Fraudsters are stealing Facebook users' information through malicious apps downloaded from Apple and Google's software stores

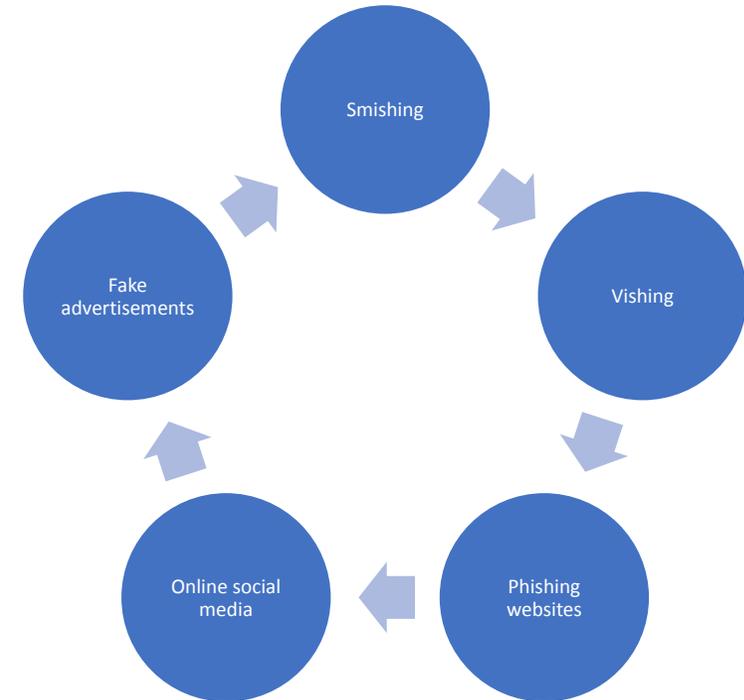
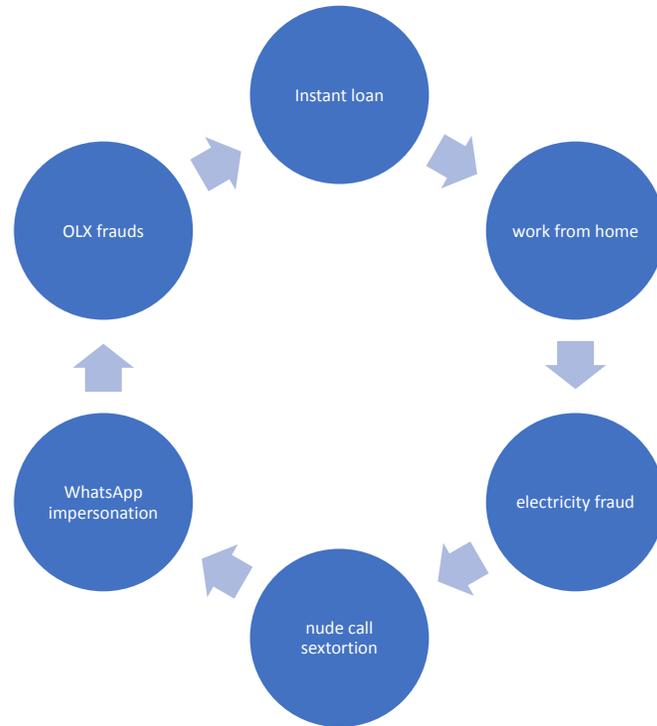
<https://www.scmagazine.com/analysis/application-security/meta-uncovers-400-malicious-apps-on-android-and-ios-apps> Oct 2022

Experts Uncover 85 Apps with 13 Million Downloads Involved in **Ad Fraud Scheme**

<https://thehackernews.com/2022/09/experts-uncover-85-apps-with-13-million.html?m=1>

Sep 2022

# RED FLAGS



- The first stage of gathering contacts could be followed by **mass-phishing** via text messages.
- Fake e-commerce websites, phishing campaigns, **data & credential harvesting**
- Fake **SMS Headers** & Bombers contains short links of WhatsApp example: wa.me/919560348xxx
- Domains mimicking (look alike, name and logo) popular Android app and services, brands

# METHODOLOGY



- Furnished in many folds **Instant loan, work from home, electricity fraud, nude call sextortion, WhatsApp impersonation, etc.**
- Propagating through **Smishing, Vishing, Phishing of online social media websites and Luring by fake advertisements**
- The first stage of gathering contacts could be followed by spear phishing via text messages.
- URL shared through telegram channels, groups, referral
- If they download the app, they are met with a permission request that demands complete control of their device.
- Designed to **run silently in the background**, constantly spying on its victims without raising suspicion

**Loan App**

**Dating App**

**Gaming App**

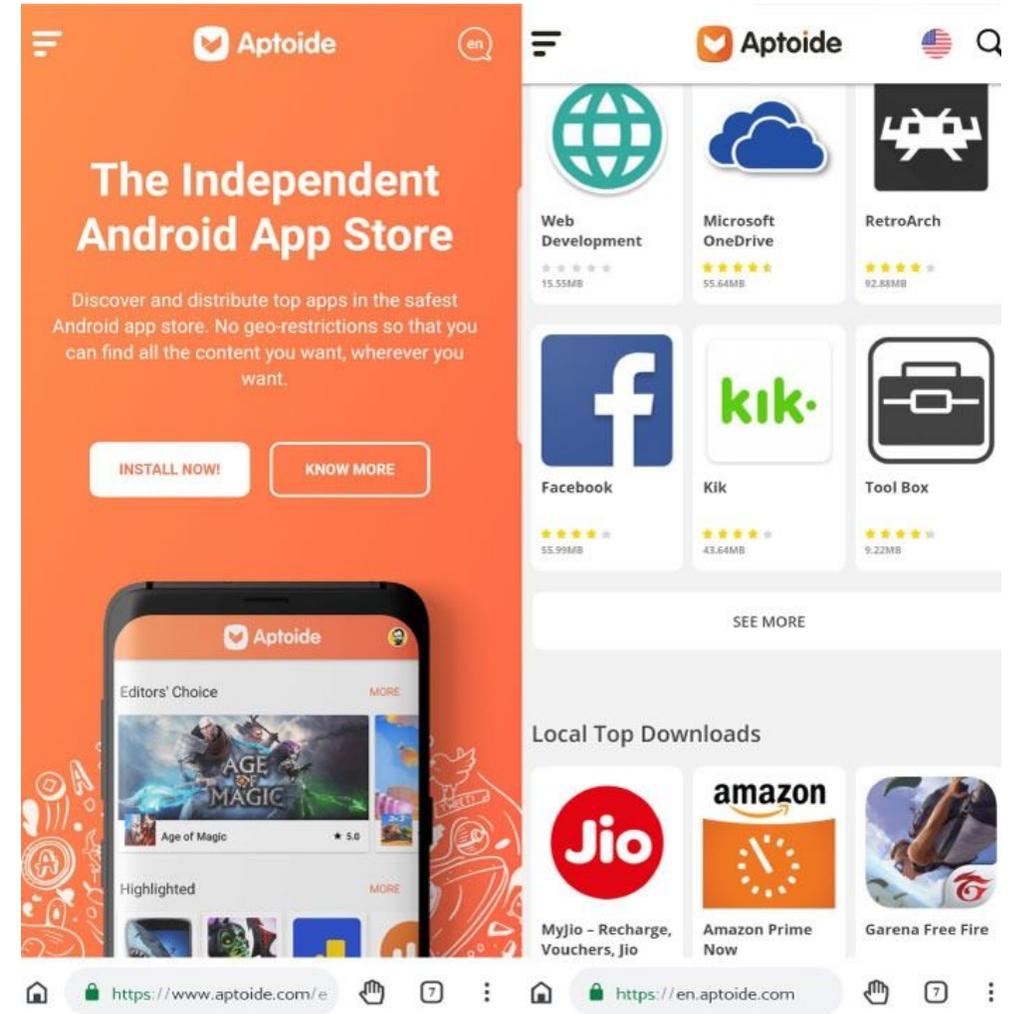
**Screen Sharing / Remote Access Apps**

**Covid-19 Apps**

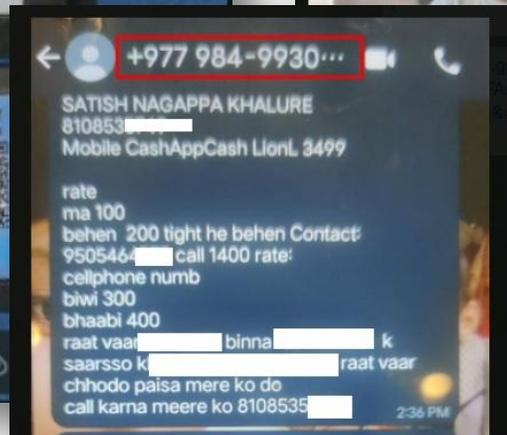
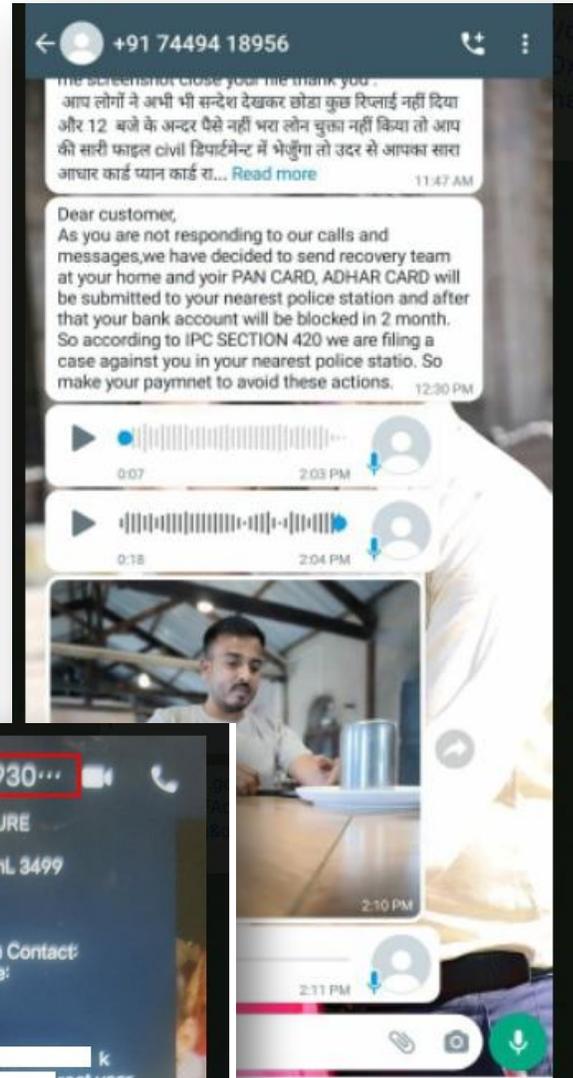
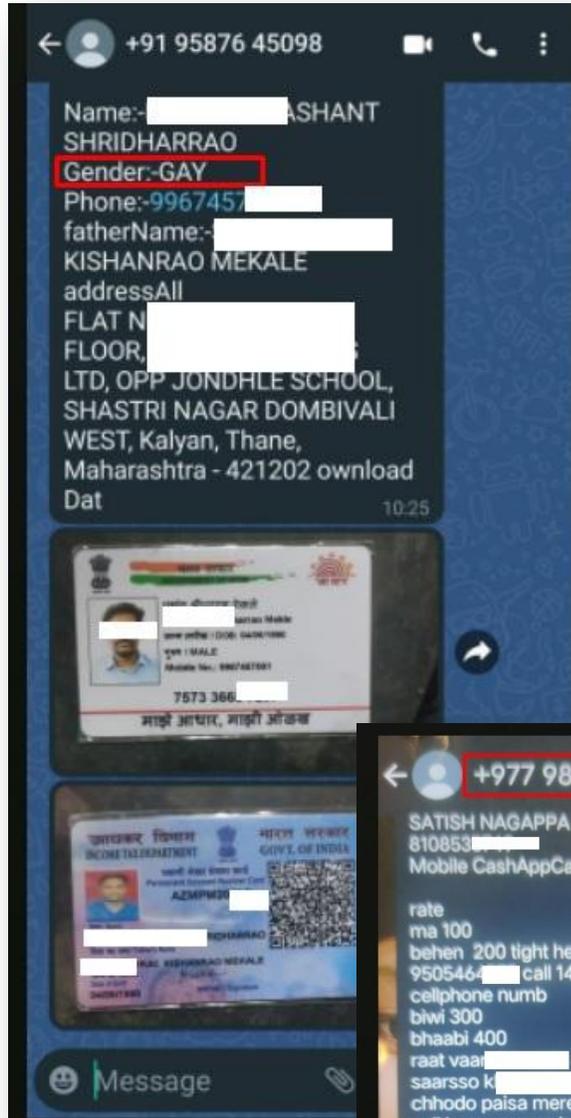
**E-Shopping Apps**

**Social Media Apps**

**Unknown / Unverified (Fake) Apps**



# Loan App Frauds



apkso.com/app/com.loans.cash.cal

## Cash Loans 1.0.9 APK

Version: 1.0.9  
File size: 5.59MB  
Requires: Android 5.0+  
Package Name: com.loans.cash.cal  
Developer: Cash Loans ps  
Updated: May 11, 2022  
Price: Free  
Rate 3.30 stars – based on 20126 reviews

[Download APK \(5.59MB\)](#)

Contact Us:  
Address: Banglow No D 10, Pandav Nagar, Delhi  
Email: linlinyizhou1117@gmail.com

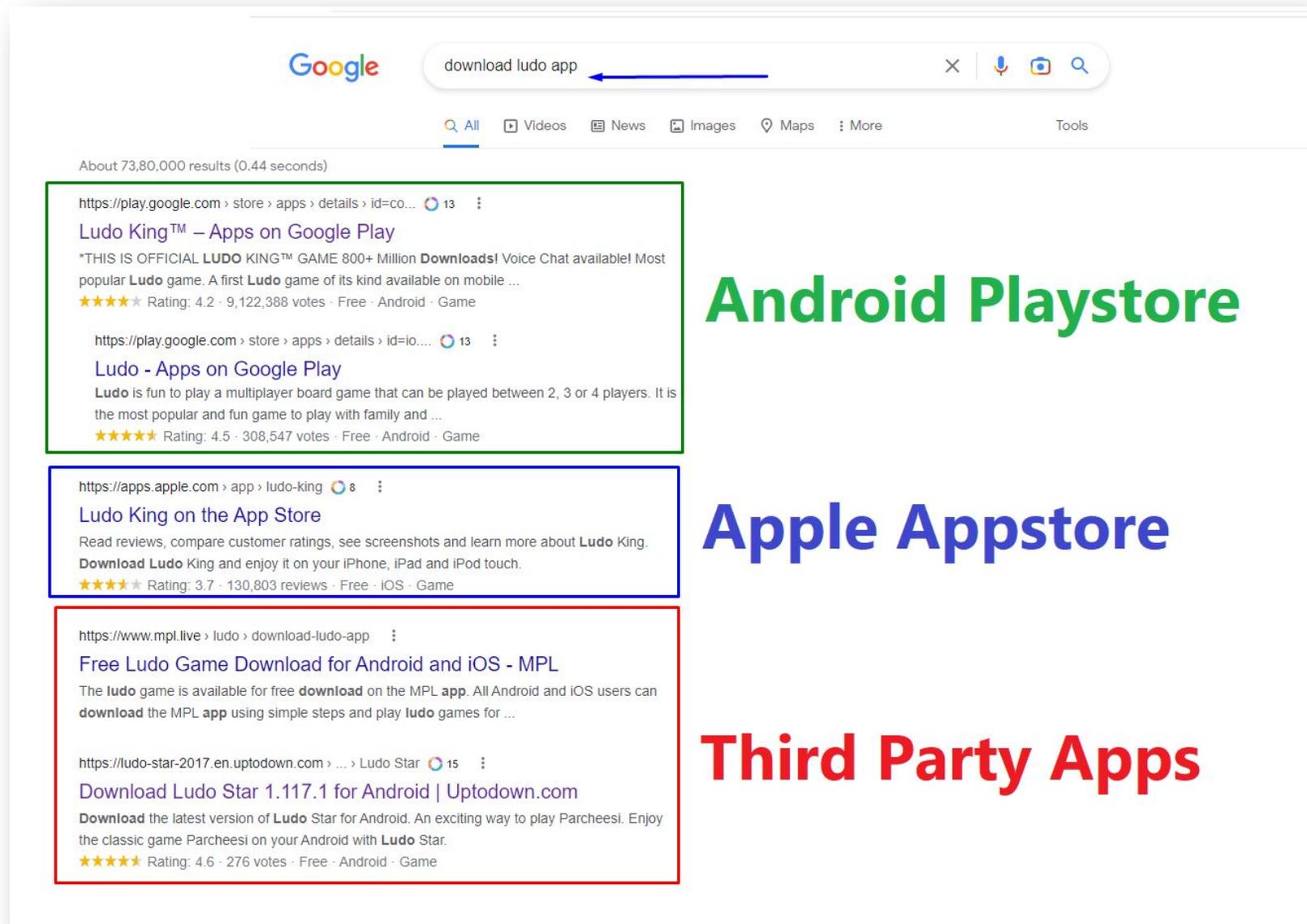
★★★★★ 11937  
★★★★★ 0  
★★★★★ 0  
★★★★★ 0  
★★★★★ 8953

### Ratings

3.6 out of 5 - 8,745 reviews

5★	4,657
4★	1,100
3★	189
2★	151
1★	2,646

# MOBILE APPLICATIONS



Google search results for "download ludo app".

Results include:

- Ludo King™ – Apps on Google Play**  
\*THIS IS OFFICIAL LUDO KING™ GAME 800+ Million Downloads! Voice Chat available! Most popular Ludo game. A first Ludo game of its kind available on mobile ...  
★★★★★ Rating: 4.2 · 9,122,388 votes · Free · Android · Game
- Ludo - Apps on Google Play**  
Ludo is fun to play a multiplayer board game that can be played between 2, 3 or 4 players. It is the most popular and fun game to play with family and ...  
★★★★★ Rating: 4.5 · 308,547 votes · Free · Android · Game
- Ludo King on the App Store**  
Read reviews, compare customer ratings, see screenshots and learn more about Ludo King.  
Download Ludo King and enjoy it on your iPhone, iPad and iPod touch.  
★★★★★ Rating: 3.7 · 130,803 reviews · Free · iOS · Game
- Free Ludo Game Download for Android and iOS - MPL**  
The ludo game is available for free download on the MPL app. All Android and iOS users can download the MPL app using simple steps and play ludo games for ...
- Download Ludo Star 1.117.1 for Android | Uptodown.com**  
Download the latest version of Ludo Star for Android. An exciting way to play Parcheesi. Enjoy the classic game Parcheesi on your Android with Ludo Star.  
★★★★★ Rating: 4.6 · 276 votes · Free · Android · Game

Android Playstore

Apple Appstore

Third Party Apps

# Third Party Apps

https://apkcombo.com/wallet-pro.com.apkbuilder.emranbd744.Wallet/

APKCombo Search APK Search APKFLASH APK DC

**Opera Browser** Ad  
Opera Browser with integrated WhatsApp & FB Messenger. Keep chatting while you browse **DOWNLOAD**

APKCombo > Apps > Entertainment > Wallet Pro

**Wallet Pro**  
1.0.1.1  
**Smart Pro**

**Download APK (6 MB)**  
[Play On Windows PC](#)

A very good app.

Entry Options Gear Up Instruction Love It

# Third Party Apps

APKCombo > Smart Pro

DEVELOPER: SMART PRO

	<b>BD Spin</b> Smart Pro · Entertainment ↓ 10 K+ 3.8 ★ 8 MB		<b>Team Pay</b> Smart Pro · Entertainment ↓ 1 K+ 3.8 ★ 6 MB
	<b>Team Pro</b> Smart Pro · Entertainment ↓ 1 K+ 4.1 ★ 6 MB		<b>Wallet Pro</b> Smart Pro · Entertainment ↓ 50+ 5.0 ★ 6 MB
	<b>Dcash Beta</b> Smart Pro · Entertainment ↓ 0+ N/A ★ 6 MB		<b>Yolo Cash</b> Smart Pro · Entertainment ↓ N/A N/A ★ 6 MB
	<b>Smart Cash</b> Smart Pro · Social ↓ N/A N/A ★ 5 MB		<b>Star Cash</b> Smart Pro · Entertainment ↓ N/A N/A ★ 6 MB

# EXAMPLE 1

# Understand the mobile app

The screenshot shows the Google Play Store interface with a search for 'ludo'. The search bar at the top contains the text 'ludo'. Below the search bar, there are two tabs: 'Apps and games' (selected) and 'Device'. The search results are displayed in a grid of 12 app cards. Each card features a colorful app icon, the app name, the developer's name, and the user rating. The apps listed are: Ludo King™ (Gametion, 4.2★), Ludo Club - Fun Dice Game (Moonfrog, 4.3★), Ludo (Yarsa Games, 4.5★), Ludo SuperStar (BlackLight Studio Games, 4.5★), Yalla Ludo - Ludo&Domino (Aviva Sun, 4.1★), Ludo Star: Online Ludo Gaming (Gameberry Labs, 4.1★), Parchisi STAR Online (Gameberry Labs, 4.4★), and Ludo Titan (Gameberry Labs, 4.1★).

Google Play

ludo

Apps and games Device

**Ludo King™**  
Gametion  
4.2 ★

**Ludo Club - Fun Dice Game**  
Moonfrog  
4.3 ★

**Ludo**  
Yarsa Games  
4.5 ★

**Ludo SuperStar**  
BlackLight Studio Games  
4.5 ★

**Yalla Ludo - Ludo&Domino**  
Aviva Sun  
4.1 ★

**Ludo Star: Online Ludo Gaming**  
Gameberry Labs  
4.1 ★

**Parchisi STAR Online**  
Gameberry Labs  
4.4 ★

**Ludo Titan**  
Gameberry Labs  
4.1 ★

# Scenario 1

← → ↻ [https://play.google.com/store/apps/details?id=com.ludo.king&hl=en\\_IN&gl=US](https://play.google.com/store/apps/details?id=com.ludo.king&hl=en_IN&gl=US) 🔍 📄 ☆ 📄 📄 📄 📄 📄 📄 📄 📄

Google Play Games Apps Movies & TV Books Children

# Ludo King™

Gametion  
Contains ads · In-app purchases

 4.2★ 91.2L reviews 50Cr+ Downloads Everyone

Install on more devices

📱 This app is available for all of your devices

▶ Trailer



Real Time Voice Chat

### Developer contact

- Website: <https://www.gametion.com/>
- Email: [support@ludoking.com](mailto:support@ludoking.com)
- Address: Mumbai, India
- Privacy policy: <https://www.gametion.com/privacypolicy.htm>

# Scenario 2

← → [https://play.google.com/store/apps/details?id=com.ludo.ludoapp&hl=en\\_IN&gl=US](https://play.google.com/store/apps/details?id=com.ludo.ludoapp&hl=en_IN&gl=US)

Google Play Games Apps Movies & TV Books Children

## Yal3ab Ludo

pirateking  
Contains ads · In-app purchases

50T+ Downloads | Teen

Install Add to wishlist

This app is available for all of your devices



### Developer contact

- Email: [bloodforest9@gmail.com](mailto:bloodforest9@gmail.com)
- Address: BEIJING SHI CHAO YANG QU BEI TU CHENG DONG LU 1 HAO LOU 2 CENG 3003 SHI
- Privacy policy: [https://dl.pokersky.net/yal3ab\\_ludo/privacy\\_policy.html](https://dl.pokersky.net/yal3ab_ludo/privacy_policy.html)

# Observation

play.google.com/store/apps/details?id=com.sports.insider&hl=en\_IN&gl=US → 1: Application URL Playstore

OSINT Stack DEMO Email SM TAU TI Cyber Feeds Intel Tools Fake News Mobile VA Dark Web Learning Fake Mail Torrent Forensic Malware & URL

Google Play Games Apps Movies & TV Books Children

**SI - Betting tips** → 2: Application name

IMA CORPORATION LTD  
In-app purchases → 3: Developer Name

4.1★ 5L+  
2.13T reviews Downloads Everyone

Install Add to wishlist

This app is not available for any of your devices

PREDICTIONS FROM THE EXPERTS TRY 3 DAYS FREE  
PASSABILITY IS OVER 75%  
HIGH ODDS FOR LIVE MATCHES  
IN-DEPTH SPORTS ANALYTICS  
FOLLOW ALL SPORTS IN ONE PLACE

Developer contact ^

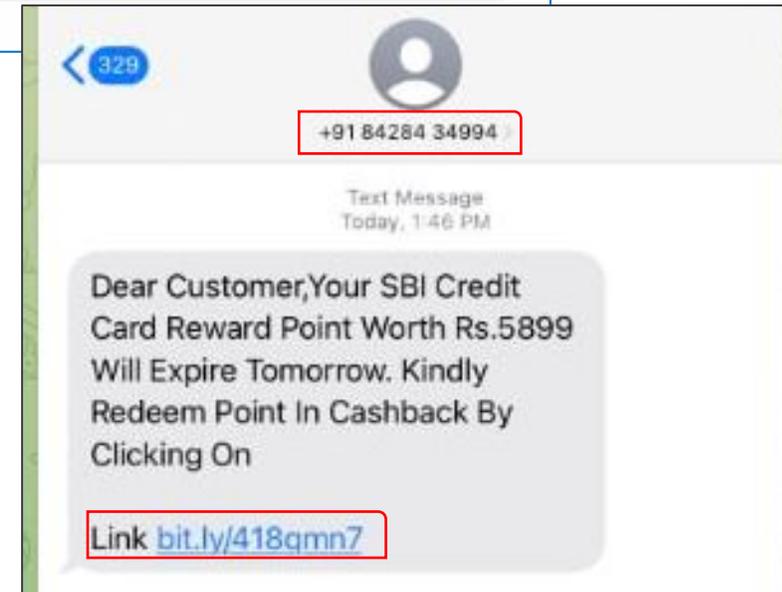
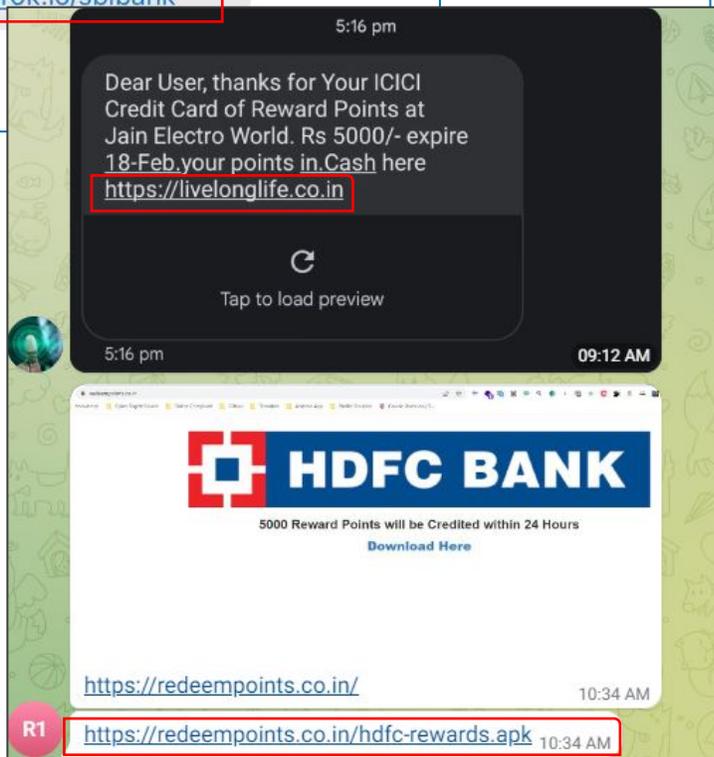
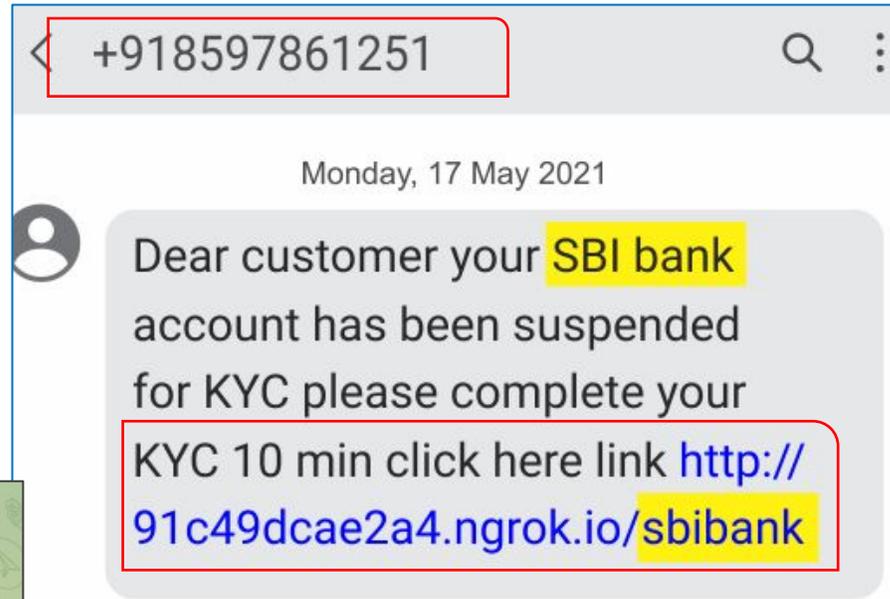
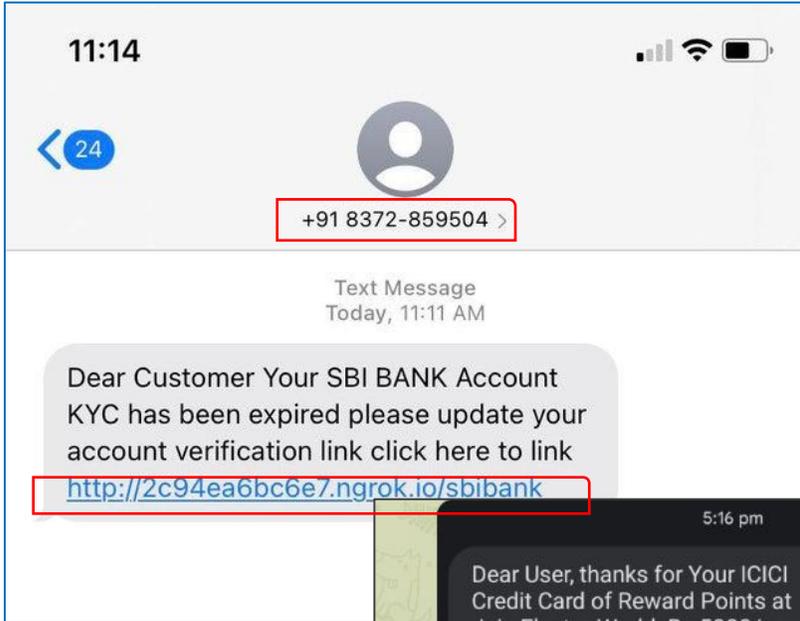
Email → 4: Email  
probettapp@gmail.com

Address → 5: Address  
Suite 10319 45 Salisbury Road, Cardiff, Wales, CF24 4AB

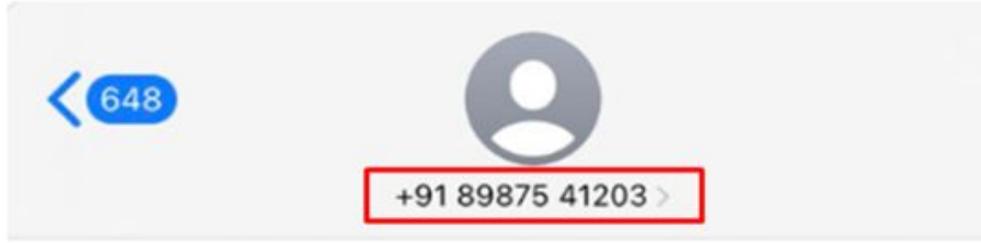
Privacy policy → 6: Privacy URL  
https://docs.google.com/document/d/1oOgxqjYIFUAKaVjxOWxZpvYumZFPjUnlr8B\_\_neJBFw/edit?usp=sharing

# EXAMPLE 2

# ATTACK METHOD



# SMS Phishing link URL redirected to **Malicious APK**

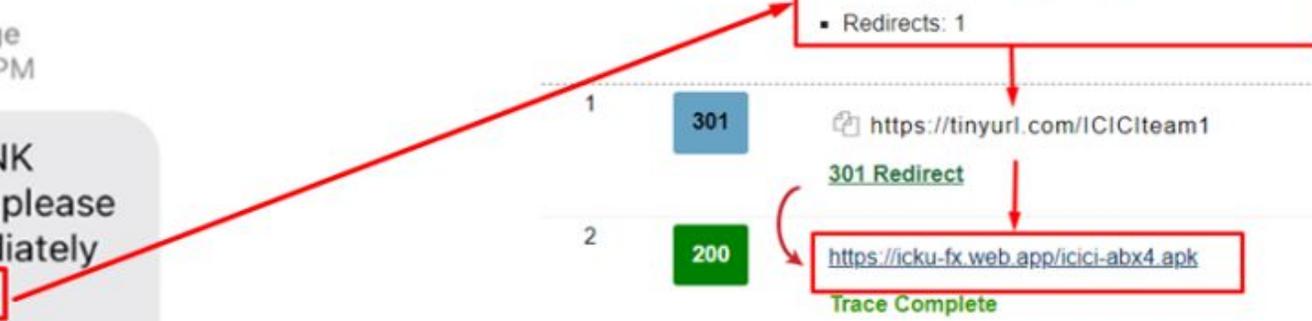


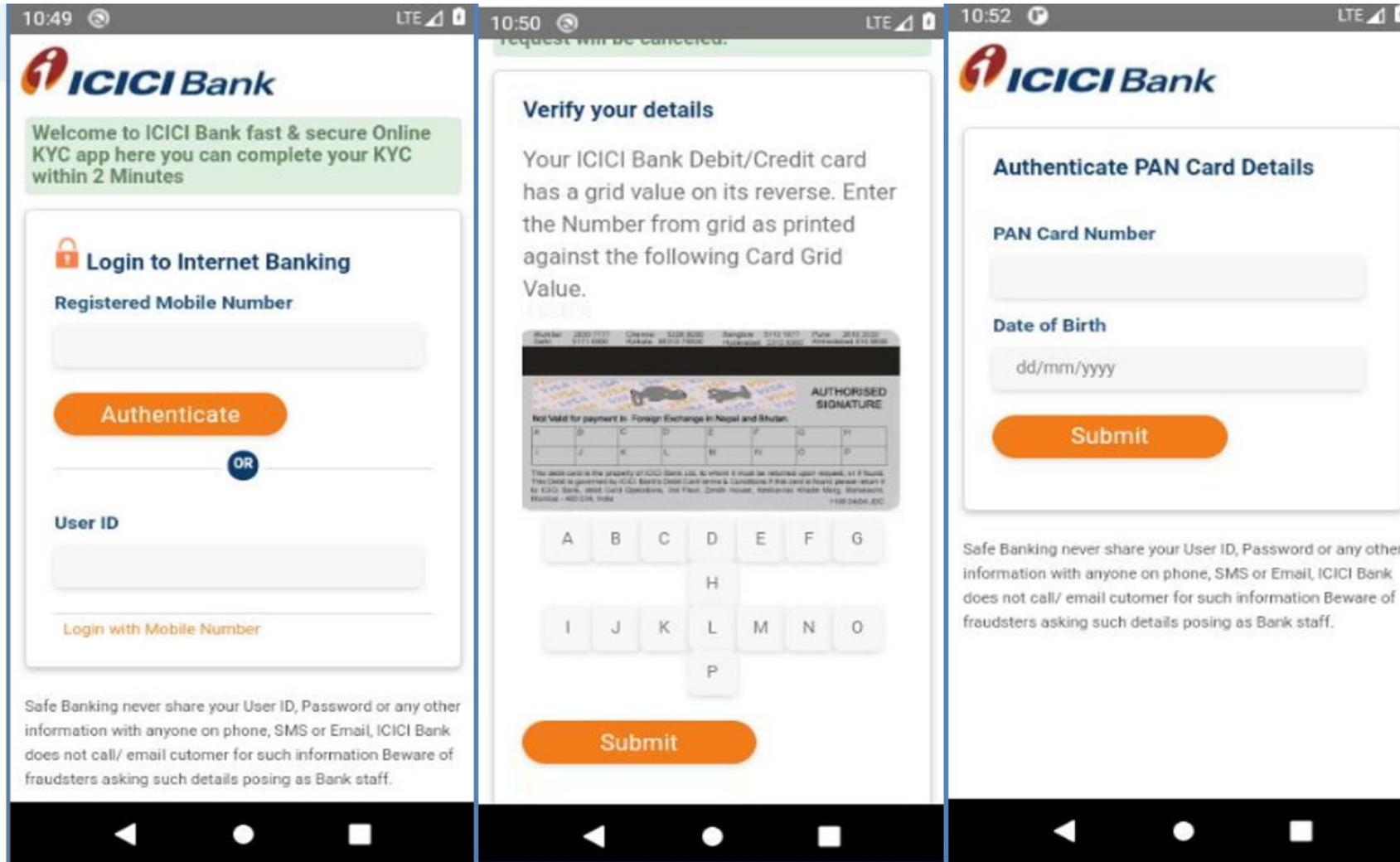
Text Message  
Today, 10:11 PM

Dear Customer, your ICICI BANK Account will be blocked today please update your PAN CARD immediately Click here <https://tinyurl.com/ICICItteam1>

User Agent: Wheregoes.com Redirect Checker/1.0

#	Code	Requested URL
√	301	<a href="https://tinyurl.com/ICICItteam1">https://tinyurl.com/ICICItteam1</a> ▪ Redirects: 1
1	301	<a href="https://tinyurl.com/ICICItteam1">https://tinyurl.com/ICICItteam1</a> 301 Redirect
2	200	<a href="https://icku-fx.web.app/icici-abx4.apk">https://icku-fx.web.app/icici-abx4.apk</a> Trace Complete





The image displays three sequential screenshots of the ICICI Bank mobile application interface during a KYC process.

**Screenshot 1 (10:49):** Shows the "Login to Internet Banking" screen. It features a green banner with the text "Welcome to ICICI Bank fast & secure Online KYC app here you can complete your KYC within 2 Minutes". Below this, there is a "Registered Mobile Number" input field, an "Authenticate" button, and a "User ID" input field. A small "OR" button is positioned between the "Authenticate" and "User ID" sections. At the bottom, there is a "Login with Mobile Number" link and a security warning: "Safe Banking never share your User ID, Password or any other information with anyone on phone, SMS or Email, ICICI Bank does not call/ email customer for such information Beware of fraudsters asking such details posing as Bank staff."

**Screenshot 2 (10:50):** Shows the "Verify your details" screen. It instructs the user: "Your ICICI Bank Debit/Credit card has a grid value on its reverse. Enter the Number from grid as printed against the following Card Grid Value." Below the text is an image of a credit card's reverse side showing a grid of numbers. The grid is as follows:

1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4	5	6	7	8	9	0
1	2	3	4	5	6	7	8
9	0	1	2	3	4	5	6
7	8	9	0	1	2	3	4
5	6	7	8	9	0	1	2
3	4						

# Malicious Payload hosted on 'web.app' : <https://icku-fx.web.app/icici-abx4.apk>

**Names** ⓘ

icici-abx4.apk

MD5 c2be5de66405d65b3fd23caec90b92cd

SHA-1 f631b05fe231f58ea8054d23c4023e9c48409616

**summary**

Android Type	APK
Package Name	com.ikycappi.cxzx4
Main Activity	com.ikycapp.android.MainActivity
Internal Version	1
Displayed Version	1.0
Minimum SDK Version	22
Target SDK Version	32

**Certificate Attributes**

Valid From	2008-04-15 22:40:50
Valid To	2035-09-01 22:40:50
Serial Number	b3998086d056cffa
Thumbprint	27196e386b875e76adf700e7ea84e4c6eee33dfa

**Certificate Subject**

Distinguished Name	C:US, CN:Android, L:Mountain View, O:Android, ST:California, OU:Android, email:android@android.com
Email	android@android.com
Common Name	Android
Organization	Android
Organizational Unit	Android
Country Code	US
State	California
Locality	Mountain View

## Permissions

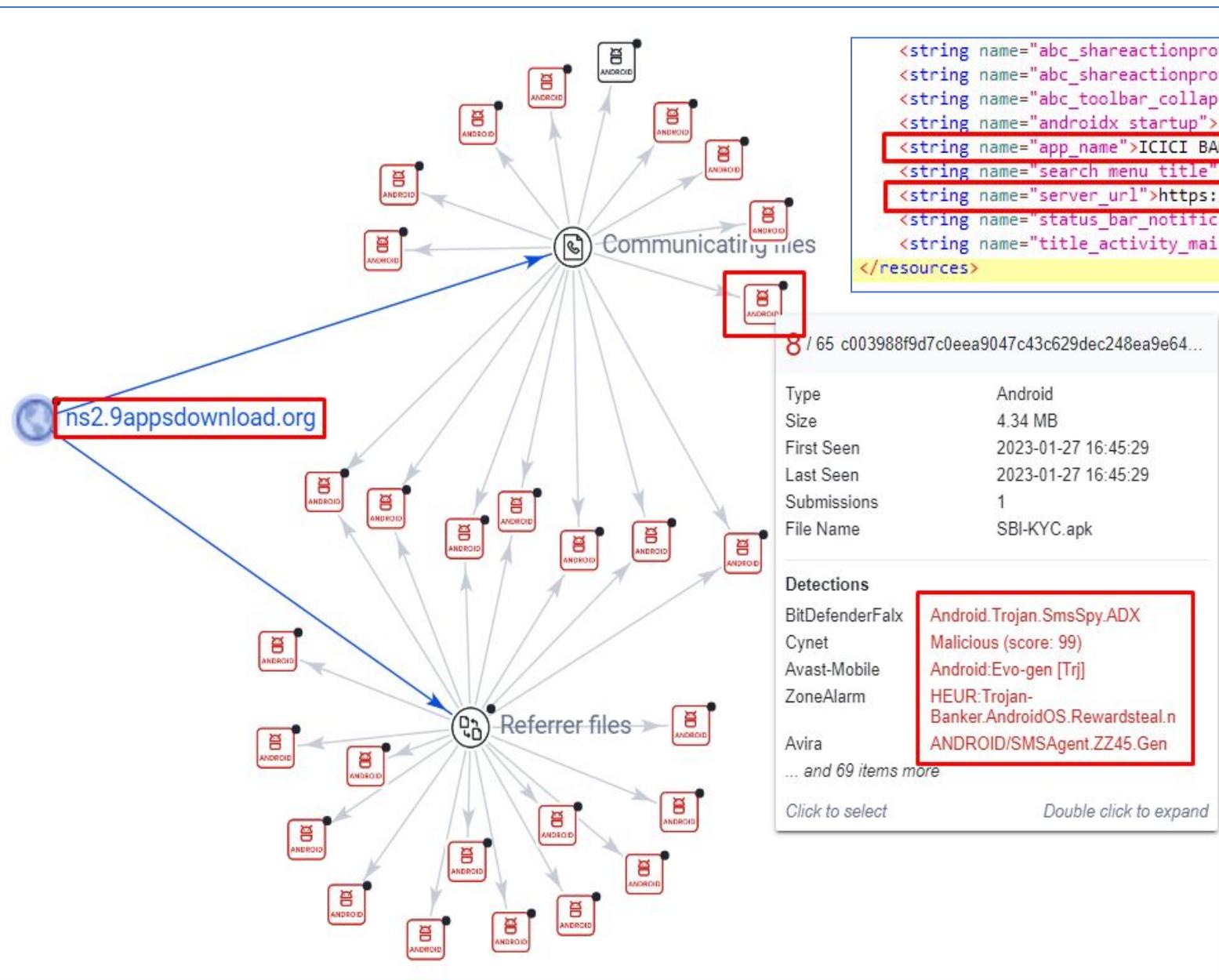
- ⚠ android.permission.RECEIVE\_SMS
- ⚠ android.permission.READ\_SMS

Gallery

Unable to open **Gallery**. Go to Settings > Permissions, then allow the following permissions and try again:

- 👤 Contacts
- 📅 Calendar
- 📍 Location

**CANCEL** **SETTINGS**



```

<string name="abc_shareactionprovider_share_with">Share with</string>
<string name="abc_shareactionprovider_share_with_application">Share with %s</string>
<string name="abc_toolbar_collapse_description">Collapse</string>
<string name="androidx_startup">androidx.startup</string>
<string name="app_name">ICICI BANK KYC</string>
<string name="search_menu_title">Search</string>
<string name="server_url">https://ns2.9appsdownload.org/app.php</string>
<string name="status_bar_notification_info_overflow">999+</string>
<string name="title_activity_main">ICICI BANK KYC</string>
</resources>

```

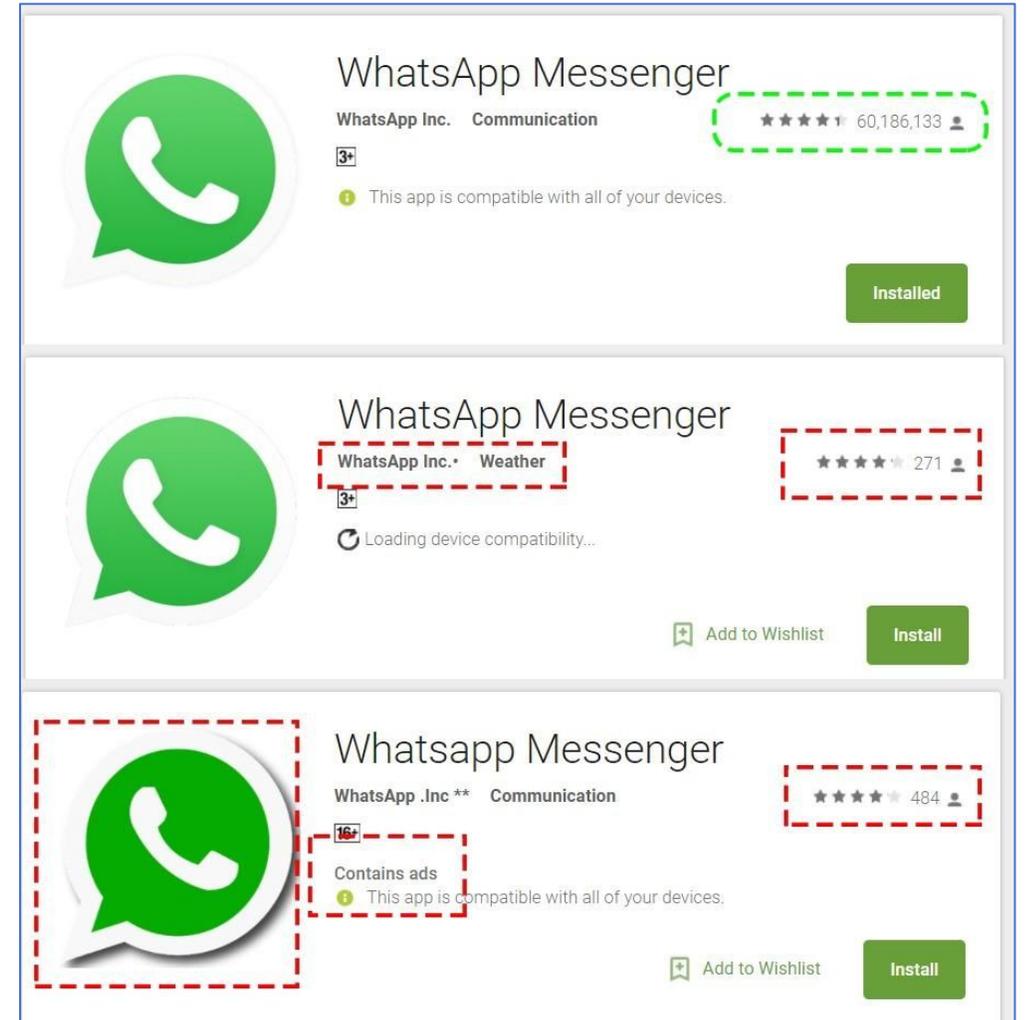
8 / 65 c003988f9d7c0eea9047c43c629dec248ea9e64...

Type	Android
Size	4.34 MB
First Seen	2023-01-27 16:45:29
Last Seen	2023-01-27 16:45:29
Submissions	1
File Name	SBI-KYC.apk
<b>Detections</b>	
BitDefenderFalx	Android.Trojan.SmsSpy.ADX
Cynet	Malicious (score: 99)
Avast-Mobile	Android:Evo-gen [Trj]
ZoneAlarm	HEUR:Trojan-Banker.AndroidOS.Rewardsteal.n
Avira	ANDROID/SMSAgent.ZZ45.Gen
... and 69 items more	
Click to select      Double click to expand	

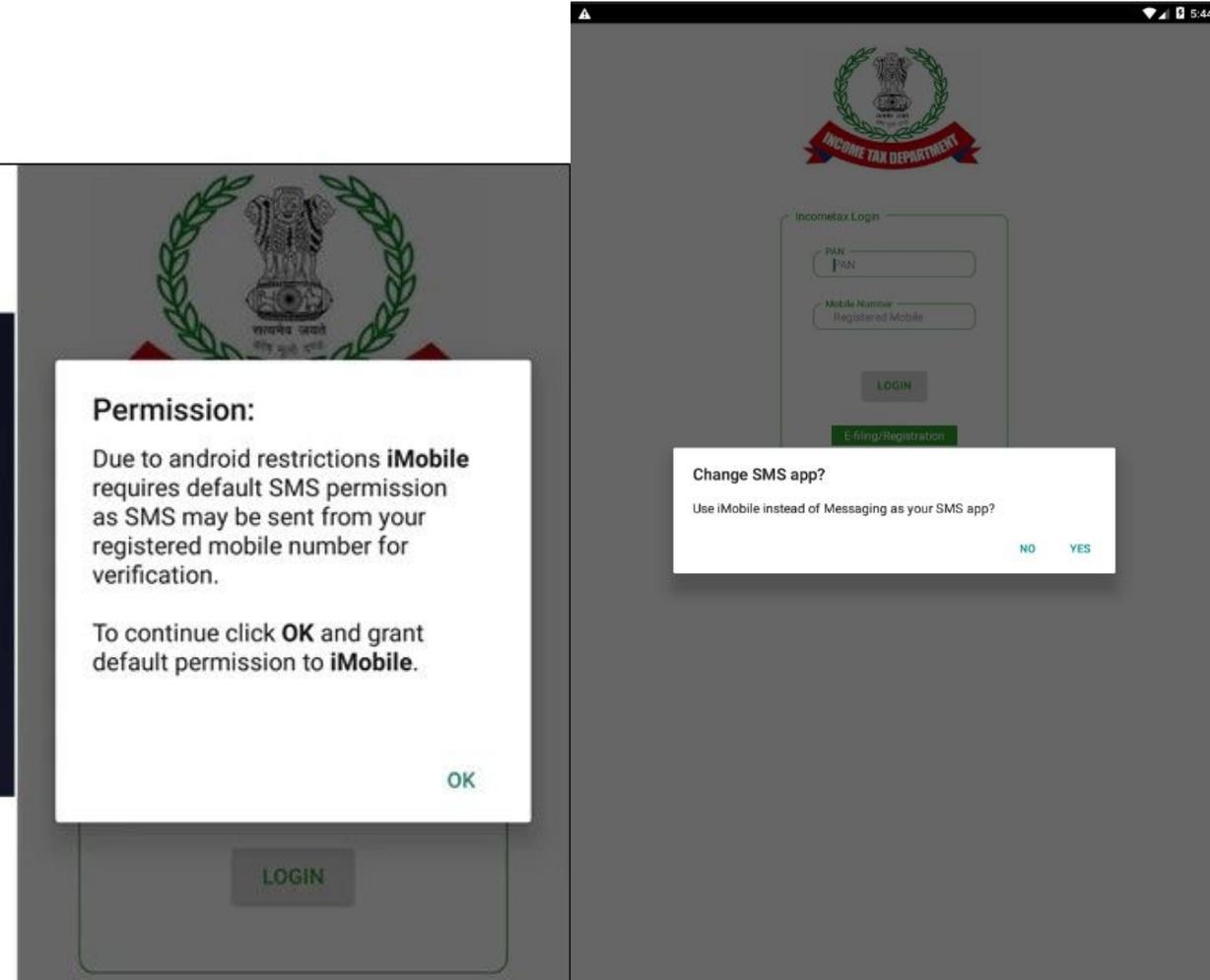
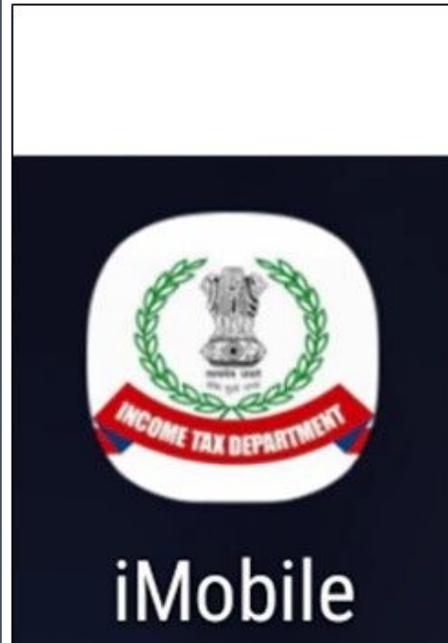
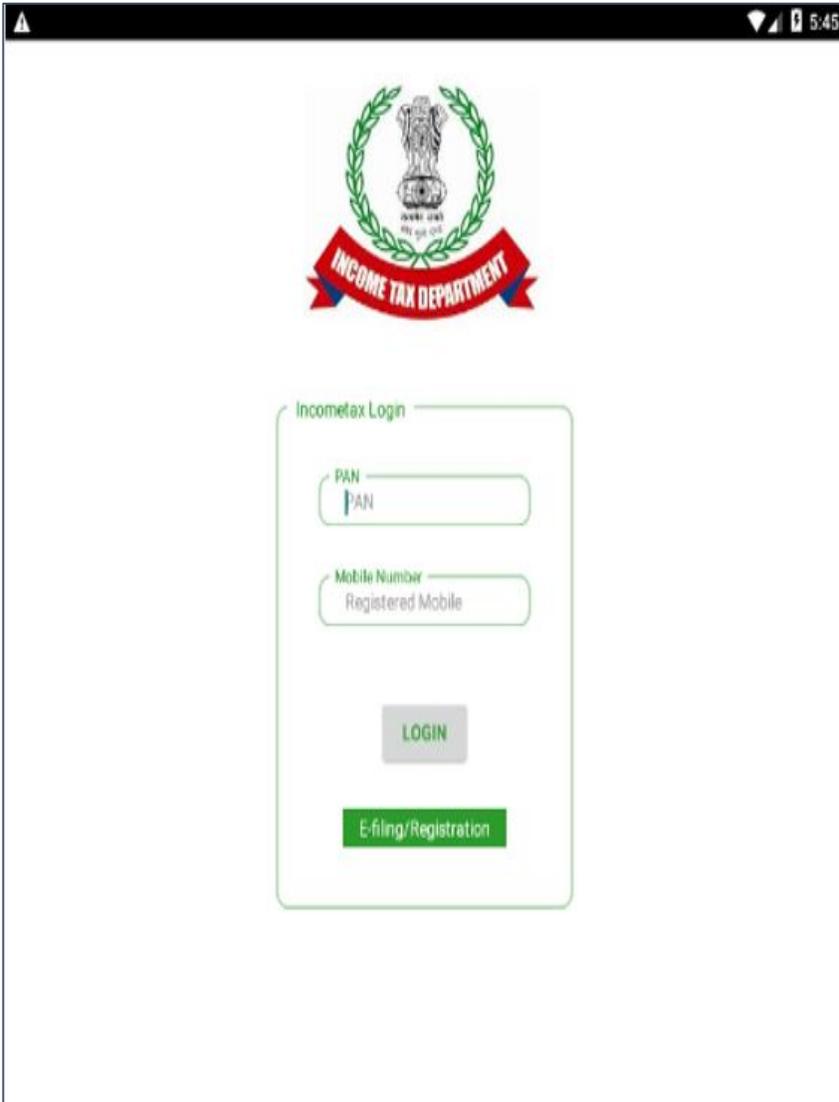
Hosting templates on phishing Server/Domains

# EXAMPLE 3

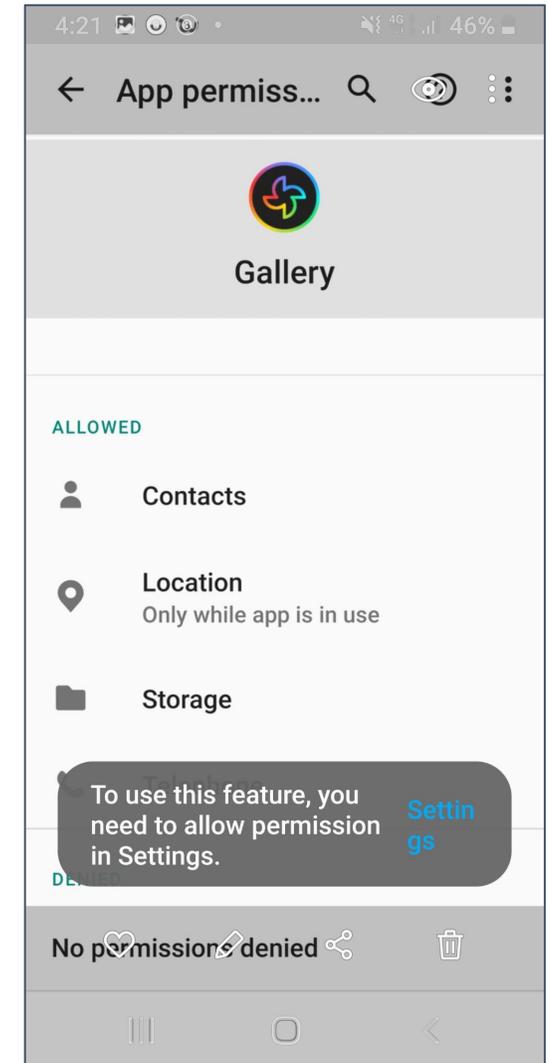
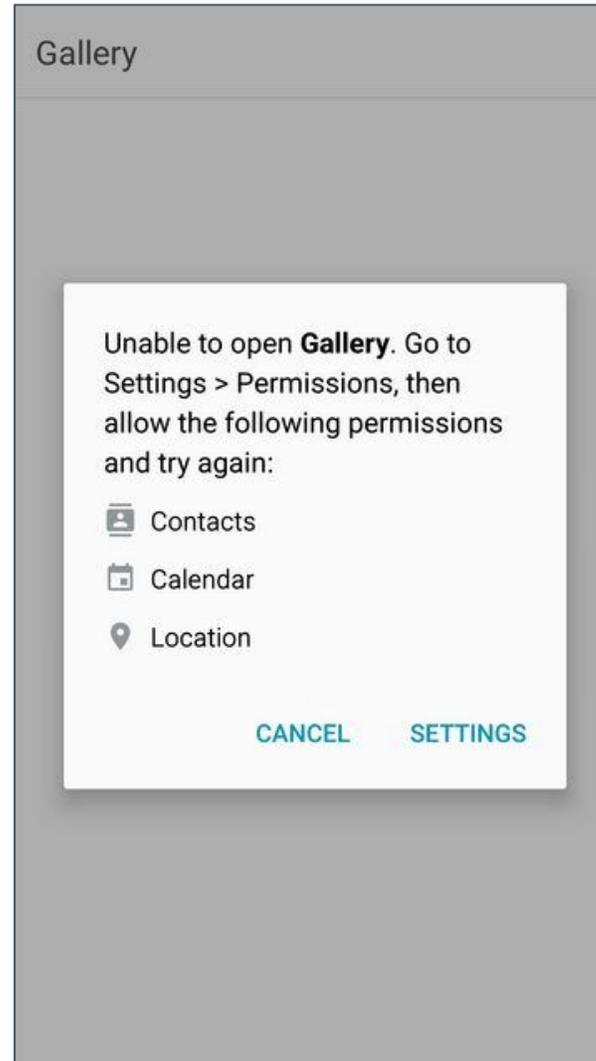
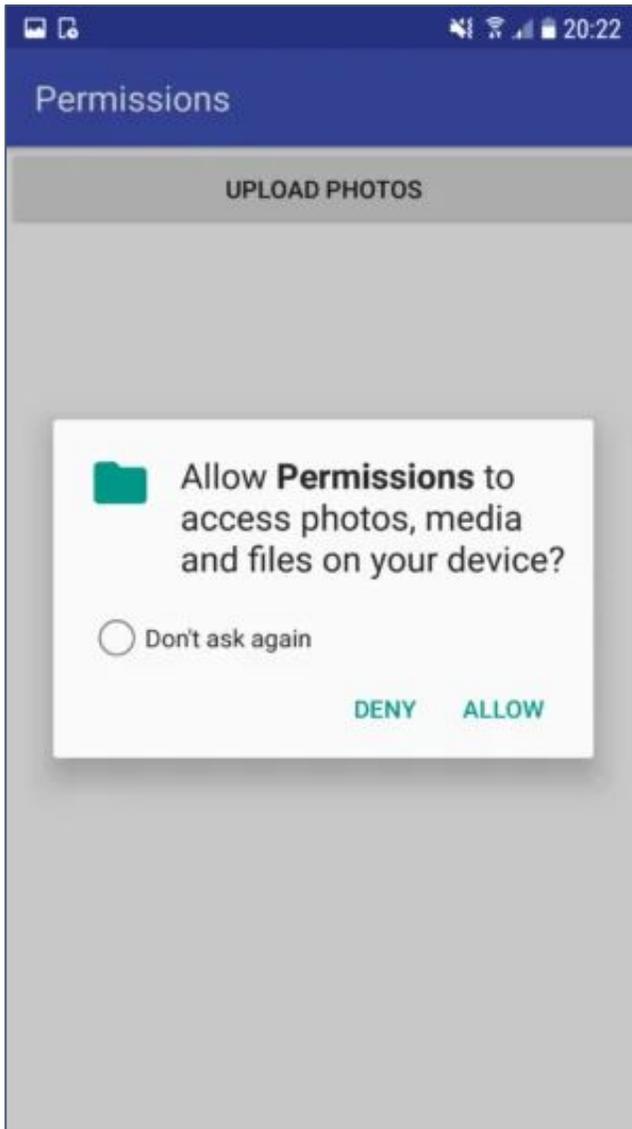
# Example



# SMS PERMISSION

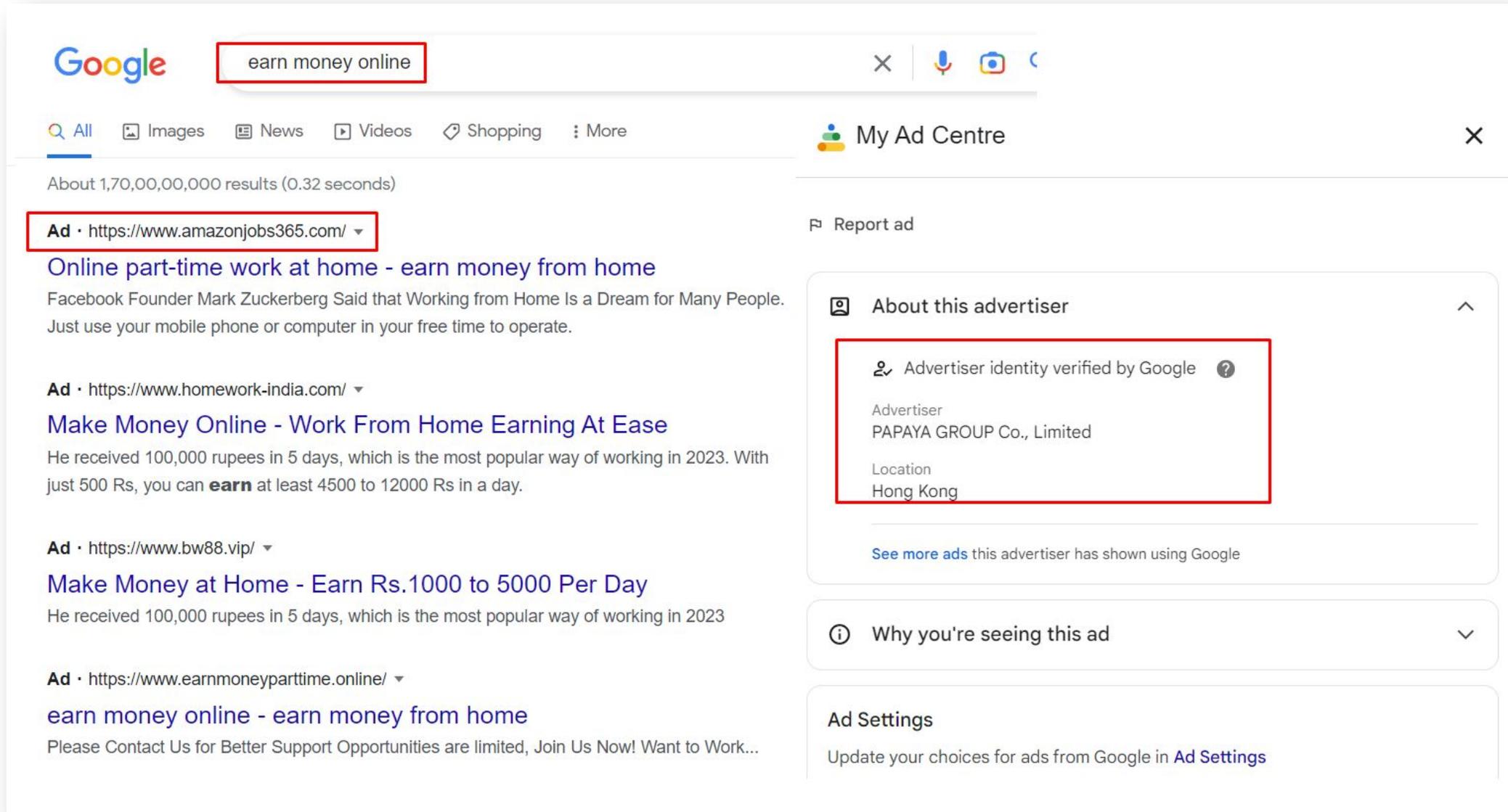


# Permissions



# EXAMPLE 4

# Search Engine



Google

All Images News Videos Shopping More

About 1,70,00,00,000 results (0.32 seconds)

**Ad** • <https://www.amazonjobs365.com/>

**Online part-time work at home - earn money from home**

Facebook Founder Mark Zuckerberg Said that Working from Home Is a Dream for Many People. Just use your mobile phone or computer in your free time to operate.

**Ad** • <https://www.homework-india.com/>

**Make Money Online - Work From Home Earning At Ease**

He received 100,000 rupees in 5 days, which is the most popular way of working in 2023. With just 500 Rs, you can **earn** at least 4500 to 12000 Rs in a day.

**Ad** • <https://www.bw88.vip/>

**Make Money at Home - Earn Rs.1000 to 5000 Per Day**

He received 100,000 rupees in 5 days, which is the most popular way of working in 2023

**Ad** • <https://www.earnmoneyparttime.online/>

**earn money online - earn money from home**

Please Contact Us for Better Support Opportunities are limited, Join Us Now! Want to Work...

My Ad Centre

Report ad

About this advertiser

Advertiser identity verified by Google

Advertiser  
PAPAYA GROUP Co., Limited

Location  
Hong Kong

See more ads this advertiser has shown using Google

Why you're seeing this ad

Ad Settings

Update your choices for ads from Google in [Ad Settings](#)

PAPAYA GROUP Co., Limited

Any time **Shown in India** All formats

**PAPAYA GROUP Co., Limited**

Legal name: PAPAYA GROUP Co., Limited

Verified as based in Hong Kong

[https://adstransparency.google.com/advertiser/AR02376743917019201537?region=IN&sig=AC0UafwAAAAAY\\_SStOYJNjGv1ZoM2GNP5w79Taw&hl=en\\_IN](https://adstransparency.google.com/advertiser/AR02376743917019201537?region=IN&sig=AC0UafwAAAAAY_SStOYJNjGv1ZoM2GNP5w79Taw&hl=en_IN)

**Sponsored**  
gadgetslaboratory.com  
www.gadgetslaboratory.com/  
**#1 Lightbulb Security Camera - 360° Front Door Security Cam**  
Best Light Bulb Security Cameras That Give You Perfect Peace of Mind & 24/7 Protection.

**Phone Security, Virus Cleaner**  
Phone Cleaner  
Google Play  
Install

**Tap Coin**  
Only for Malaysia  
Google Play  
Install

**Balls Bricks Breaker 2**  
Casual arcade game.  
Google Play  
Install

**Word Search Puzzle**  
Word Search 2021.  
Google Play  
Install

**FTL VPN**  
The Best Free VPN Free Forever  
Google Play  
Install

**Sponsored**  
www.piaproxy.com/  
**proxy pass ip address list**  
PIA proxy The best IP conversion software on the market, 200+ countries around the world

Ad · www.heyfriday.ai/  
**Ultimate AI Writer**  
Generate an article in 4-clicks: 500-word article in 5 minutes. Start Now.

**Tap Coin**  
वर्ल्ड कप की 10 हाइलाइट्स  
Google Play  
इंस्टॉल

**Sponsored**  
mobitracker.org  
www.mobitracker.org/  
**Find Mobile Device Location - Just Need Phone Number**  
The best phone tracker 2022 - search phone number and get location, for all carriers

**WeLive**  
obrolan video langsung  
Google Play  
Instal

**Sponsored**  
News Break  
www.newsbreak.com/  
**Savannah Local Newsletter**  
Stay up to date with what's happening in Savannah

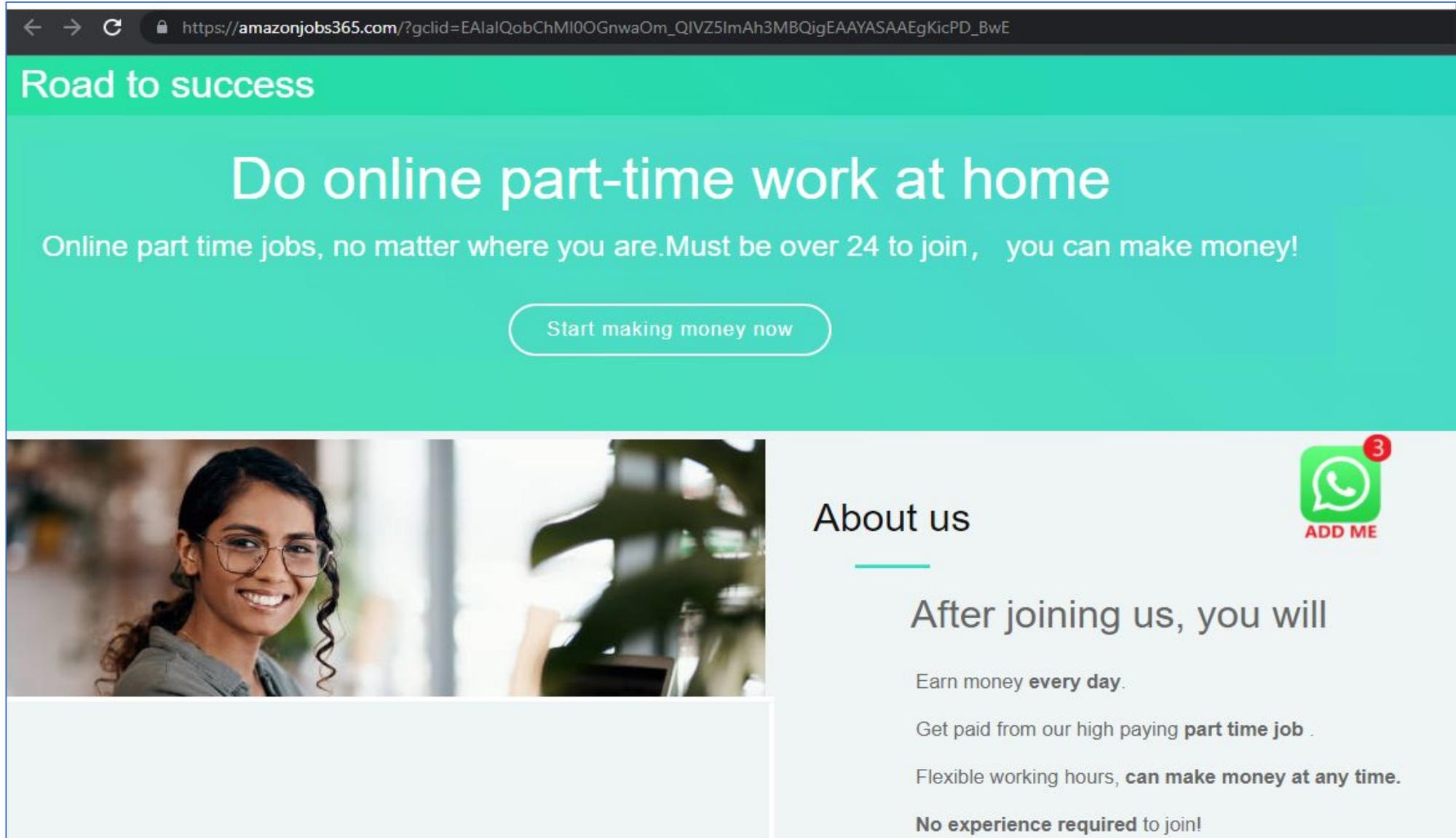
**Sponsored**  
www.pyproxy.com/  
**Rotating Residential Proxies**  
High Quality Proxy Service, Unlimited Concurrent Sessions & Domains, As Low as \$0.7/GB

**Sponsored**  
my.octafx.com/  
**OctaFx Platform - OctaFx Sign up now**  
OctaFX Trading App is the official trading tool for both deposit and withdrawal. Join with Octafx. Free comission. Octafx is the best.

**Sponsored**  
track.deriv.com/  
**Deriv.com - Deriv - Deriv**  
Highlights: DERIV Help Center, Security expertise, Free Demo Account - Get Started Easily  
Rating for deriv.com  
4.5 ★★★★★ (877)  
Deriv  
Deriv MT5  
Sign up for a free demo  
Contact Us

**Tap Coin**  
इंग्लैंड बनाम ईरान  
Google Play  
इंस्टॉल

# Redirection



← → ↻ [https://amazonjobs365.com/?gclid=EAIaIQobChMI0OGnwaOm\\_QIVZ5ImAh3MBOQigEAAAYASAAEgKicPD\\_BwE](https://amazonjobs365.com/?gclid=EAIaIQobChMI0OGnwaOm_QIVZ5ImAh3MBOQigEAAAYASAAEgKicPD_BwE)

## Road to success

# Do online part-time work at home

Online part time jobs, no matter where you are. Must be over 24 to join, you can make money!

Start making money now



### About us



#### After joining us, you will

- Earn money **every day**.
- Get paid from our high paying **part time job**.
- Flexible working hours, **can make money at any time**.
- No experience required** to join!

# Attack medium

← → ↻ [https://api.whatsapp.com](https://api.whatsapp.com/send?phone=27847563213&text=Hello,%20can%20you%20tell%20me%20about%20the%20process%20of%20this%20part-time%20job?) send?phone=27847563213&text=Hello,%20can%20you%20tell%20me%20about%20the%20process%20of%20this%20part-time%20job?



Open WhatsApp?

https://api.whatsapp.com wants to open this application.

Always allow api.whatsapp.com to open links of this type in the associated app

Open WhatsApp

Cancel

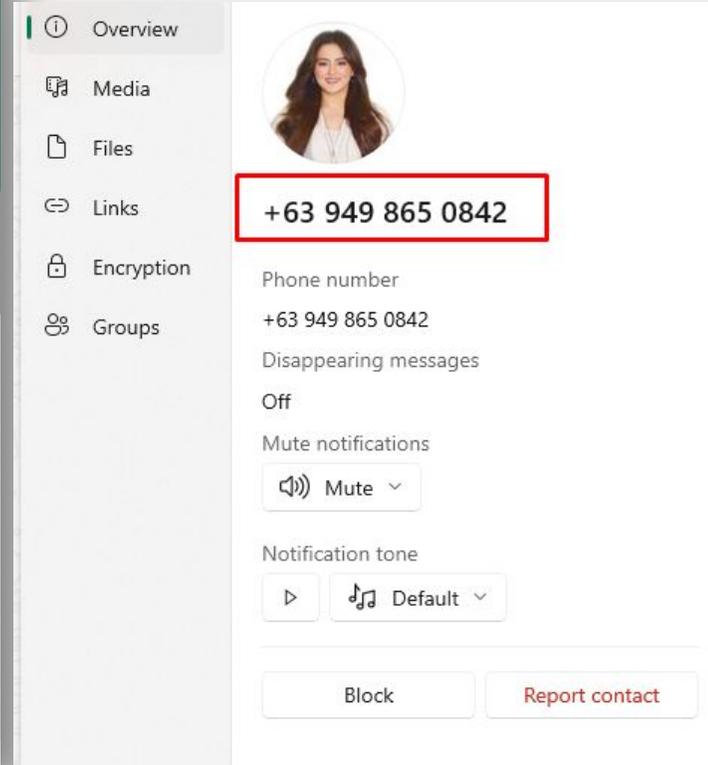
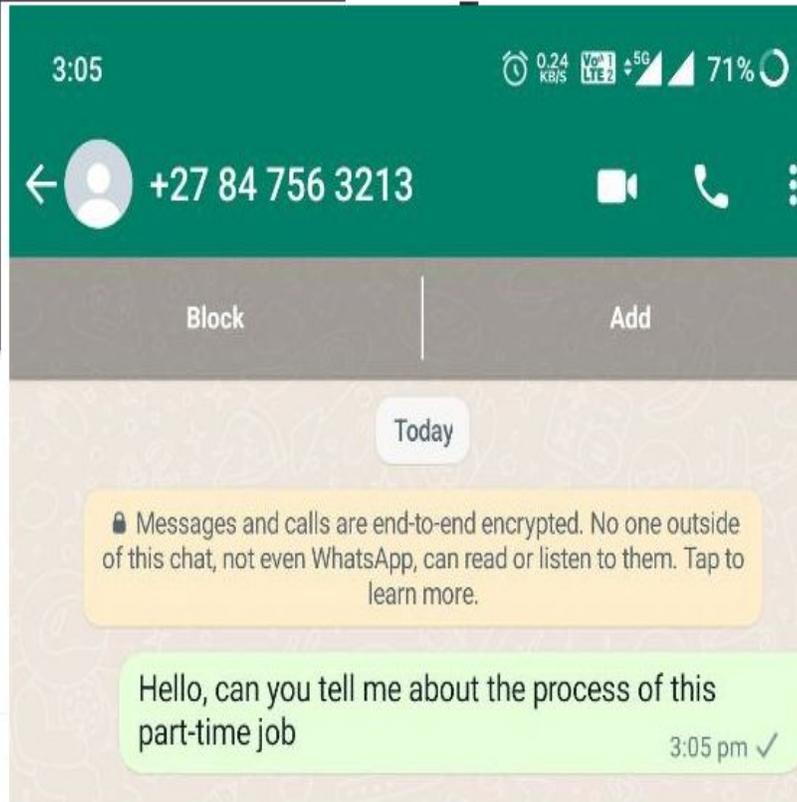
Nicola Honey Nahum

Continue to Chat

Hello, can you tell me about the process of this part-time job?

Don't have WhatsApp yet?

Download



# Malware

people tend to trust text messages more than emails

shifting from text to SMS to internet based messaging platforms

Malware is short for "malicious software"

cyber incidents. Also Push Pull agent facility through app

as call forwarding

services such as 'BOMBitUP', 'Blast', 'Bomber', etc

made to fake cell numbers,

## Some of the malwares are:

Virus

Worm

Trojan horse

Spyware

Ransomware

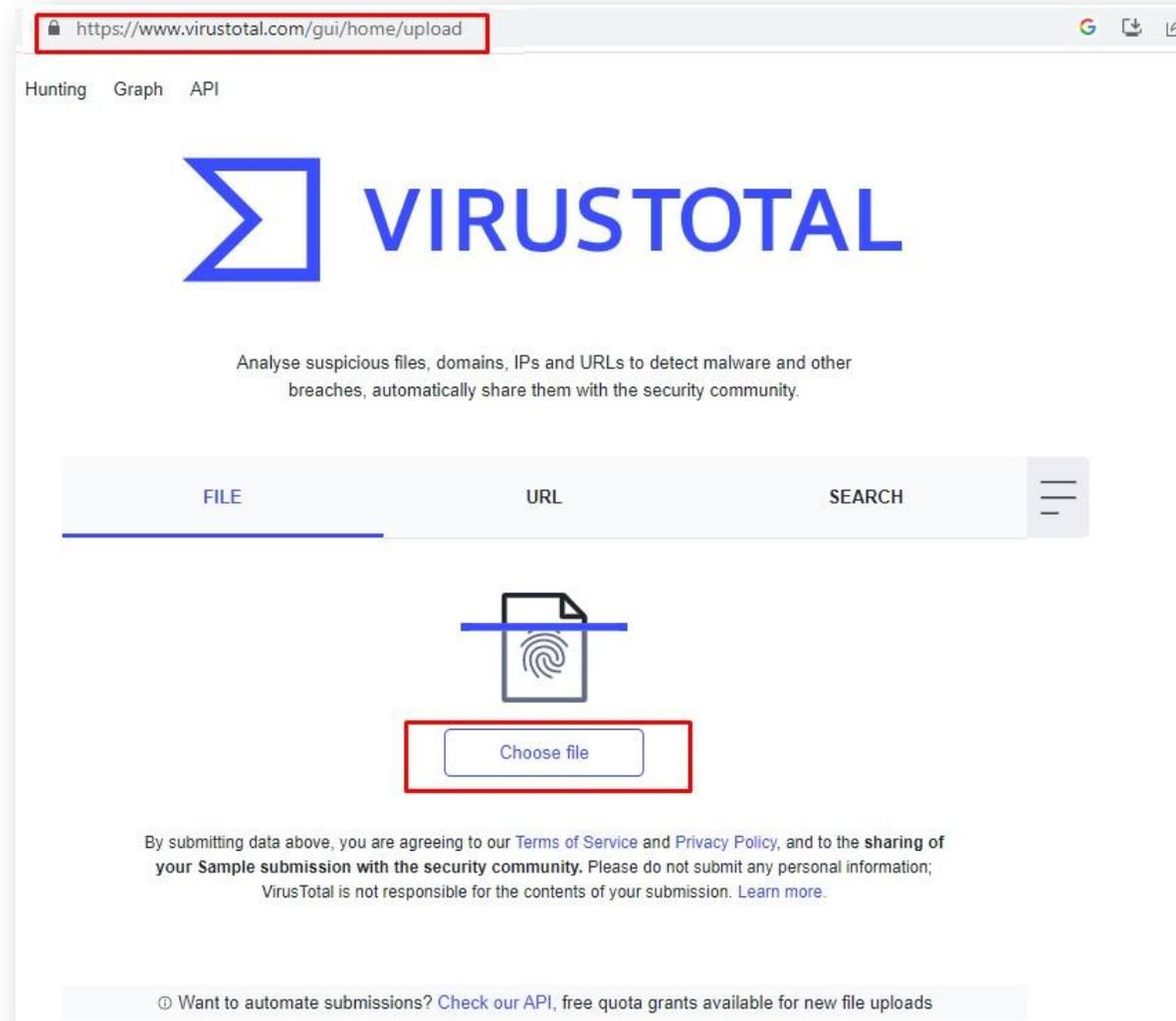
Rootkit

Adware

Keyloggers

Backdoor virus or remote access Trojan (RAT)

# COUNTERMEASURE



The screenshot shows the VirusTotal upload interface. The browser address bar is highlighted with a red box, containing the URL <https://www.virustotal.com/gui/home/upload>. The page features the VirusTotal logo and a navigation menu with 'Hunting', 'Graph', and 'API'. Below the logo, a description states: 'Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.' A navigation bar includes 'FILE', 'URL', and 'SEARCH' tabs, with 'FILE' selected. A central area contains a document icon with a fingerprint and a 'Choose file' button, which is also highlighted with a red box. At the bottom, a disclaimer reads: 'By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.' A footer link says: 'Want to automate submissions? Check our API, free quota grants available for new file uploads.'

<https://www.virustotal.com>

m

# COUNTERMEASURE

34 / 64

34 security vendors and 1 sandbox flagged this file as malicious

5a12974cddc7006bbc65daed16cb05ea7cd8713ef69dcb4110149a823689d92e  
com.c101421042723.apk

282.32 KB Size | 2022-06-02 01:54:01 UTC 1 month ago

android apk contains-elf dyn-calls reflection runtime-modules sends-sms telephony

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 9

Security Vendors' Analysis

AhnLab-V3	Trojan.Android.Agent.56488	Alibaba	TrojanDropper.Android/Feejar.bf88b6ed
Avast	Android.Feejar-BP [Trj]	Avast-Mobile	Android.Feejar-BQ [Trj]
AVG	Android.Feejar-BP [Trj]	Avira (no cloud)	ANDROID/TrojanDrop.FNB.Gen
BitDefenderFalx	Android.Trojan.SMSSend.TY	Comodo	Malware@#rurfodrl38o
Cynet	Malicious (score: 99)	Cyren	AndroidOS/Agent.LG
DrWeb	Android.SmsSend.1565.origin	ESET-NOD32	A Variant Of Android/TrojanSMS.Feejar.I
F-Secure	Trojan.Android/SmsSend.XH	Fortinet	Android/Generic.Z.2E1AAC!tr
Ikarus	Trojan-SMS.AndroidOS.Feejar	K7GW	Trojan ( 004c330a1 )

Virustotal will give the Output (Whether the APK is Malicious or Not)

# COUNTERMEASURE

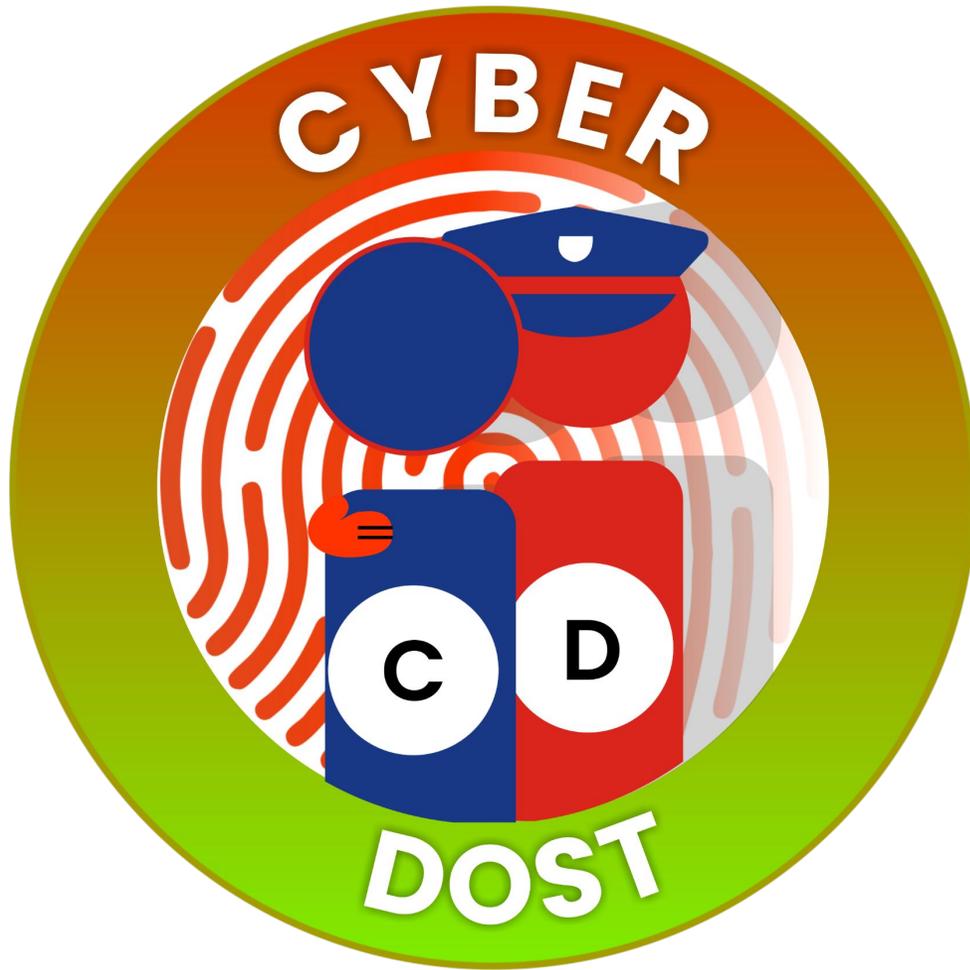
URL to scan

Public Scan Options

Recent scans Updates every 10s - Last update: 14:51:29

URL	Age	Size	IPs	
<a href="https://www.akademiefuersicherheit.de/">www.akademiefuersicherheit.de/</a>	13 seconds	2 MB	138	24 3
<a href="https://www.ovamba.com/">www.ovamba.com/</a>	13 seconds	2 MB	120	10 3
<a href="https://gpi.explainsafe.nl/nl/login">gpi.explainsafe.nl/nl/login</a>	18 seconds	4 MB	88	21 5
<a href="https://imfdb.org/wiki/Main_Page">imfdb.org/wiki/Main_Page</a>	20 seconds	922 KB	59	16 3
<a href="https://postindex.pp.ua/">postindex.pp.ua/</a>	23 seconds	2 MB	179	35 8
<a href="https://techplanet.today/post/megapelis-after-amor-infnito-2022-pelicula-c-o-m-p-l-e-t...">techplanet.today/post/megapelis-after-amor-infnito-2022-pelicula-c-o-m-p-l-e-t...</a>	24 seconds	1 MB	38	16 2
<a href="https://community.windy.com/user/montoyamcdermott35">community.windy.com/user/montoyamcdermott35</a>	24 seconds	2 MB	50	10 2
<a href="https://www.ivtinternational.com/">www.ivtinternational.com/</a>	24 seconds	4 MB	113	8 3
<a href="https://training.lucid.co/page/live-training-labs?utm_medium=email&amp;utm_source=marketo&amp;u...">training.lucid.co/page/live-training-labs?utm_medium=email&amp;utm_source=marketo&amp;u...</a>	24 seconds	2 MB	48	10 3
<a href="https://www.bbc.com/">www.bbc.com/</a>	25 seconds	6 MB	165	16 2

<https://urlscan.io/>



## Follow *CyberDost* on social media

- Get the latest Cyber Safety Tips
- Learn about various types of Scam Alerts
- Get updates on National and International Cyber news
- Learn about the achievements in the attempt to make the nation cyber safe
- Become a Cyber Volunteer and share the CyberDost content with your community
- Do your bit to stay vigilant and stay cyber safe!



@cyberdosti4c



@CyberDosti4c



@cyberdosti4c



@cyberdost



@cyberdosti4c



@cyberdost.i4c



@cyberdosti4c



@cyberdost



@cyberdost