



YASH DHINGRA

SCIENTIST 'C'

[incident@cert-in.org.in](mailto:incident@cert-in.org.in)

# Introduction to Mobile Security

# Current Trends

# Current Trends

## Android Malware Campaign Leverages Money-Lending Apps to Blackmail Victims

Dec 15, 2022 Ravi Lakshmanan



Fast Rupee - Online Loan App

1.0.9

Gudang maker

Download APK (15 MB)

[Play On Windows PC](#)

Indian online finance, I wish you a happy life.



### LATEST VERSION

Version  
1.0.9 (4015)

Update  
Aug 9, 2021

Developer  
[Gudang maker](#)

Category

Google Play ID

Installs

Source: Hacker News

# Current Trends



[Home](#) / [Technology](#) / [Tech](#) / India among countries with most Android malware, 'GB WhatsApp' among responsible apps: ESET report

## India among countries with most Android malware, 'GB WhatsApp' among responsible apps: ESET report

As cybersecurity threats around the world decrease post COVID, a new ESET report suggests the situation is still not very good in India, which happens to be one of the largest playgrounds for Android malware.

By: [Tech Desk](#)

Mumbai | October 7, 2022 4:44:51 pm



# Current Trends

## Indian banking customers targeted by SOVA Android Trojan malware: CERT-In

*The Indian Computer Emergency Response Team said that these attack campaigns can jeopardise the privacy and security of sensitive customer data and result in large scale attacks and financial frauds*

**AIHIK SUR** | SEPTEMBER 16, 2022 / 10:12 AM IST

The Indian Computer Emergency Response Team (CERT-In) said that Indian banking customers were being targeted by a new type of mobile banking malware campaign called SOVA Android Trojan.

It has the ability to harvest usernames and passwords via keylogging, stealing cookies and adding false overlays to a range of apps. It also captures the credentials when users log into their net banking apps and access bank accounts.

Source: Money Control

# Current Trends

## TikTok Surreptitiously Collected Android User Data Using Google-Prohibited Tactic

Author:  
Elizabeth Montalbano

August 12, 2020  
/ 8:16 am

App concealed the practice of gathering device unique identifiers using an added layer of encryption.

TikTok has been collecting unique identifiers from millions of Android devices without their users' knowledge using a tactic previously prohibited by Google because it violated people's privacy, new research has found.

The app concealed the practice, which can track users online without their consent, with an added layer of encryption, according to [analysis by and a report in](#) the Wall Street Journal (WSJ). TikTok, owned by Beijing-based parent company ByteDance Ltd., appears to have stopped the practice in November, according to the report.

The identifiers collected by TikTok are called MAC addresses, which are unique to a device and used as its network address in a network segment. They are typically assigned by device manufacturers and aren't usually changed or altered. For this reason, they are valuable to companies and third parties wanting to send targeted advertising to mobile device users, as they provide unique insight into customer behavior.

Source: Threat Post

# Current Trends



**Press Information Bureau**  
Government of India

Ministry of Electronics & IT

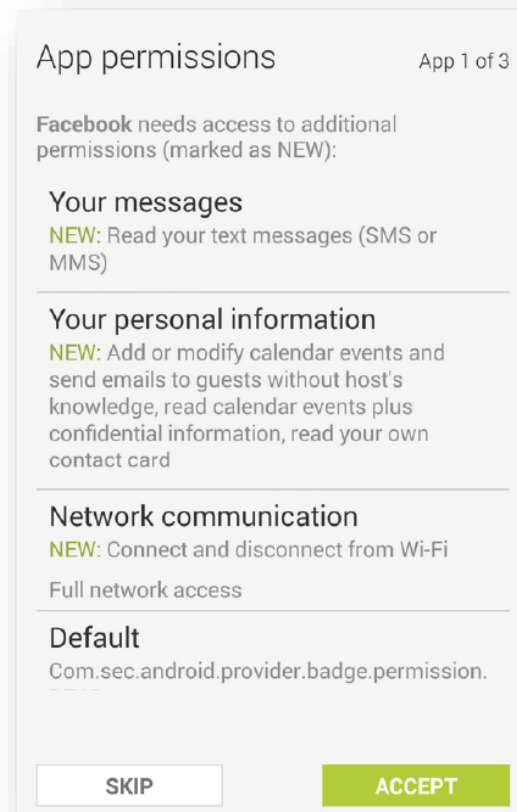
## Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order

Posted On: 29 JUN 2020 8:47PM by PIB Delhi

The Ministry of Information Technology, invoking its power under section 69A of the Information Technology Act read with the relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009 and in view of the emergent nature of threats has decided to block 59 apps ( see Appendix) since in view of information available they are engaged in activities which is prejudicial to sovereignty and integrity of India, defence of India, security of state and public order.

# Android Permission Overview

# Permissions



# Normal Permissions

- Cover areas where an app needs to access data or resources outside the app's sandbox, but where there's very little risk to the user's privacy or the operation of other apps
- Eg: Permission to set the time zone, access internet
- System automatically grants the app that permission at install time
- Cannot be revoked

# Dangerous Permissions

- Cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps
- Eg: Permission to read contacts
- User has to explicitly grant the permission at runtime
- Can be revoked

# Special Permissions

- Cover areas which are particularly sensitive
- Eg: *WRITE\_SETTINGS*
- System responds to the intent by showing a detailed management screen to the user
- Need to be enabled in Settings
- Can be revoked

# Signature Permissions

- System grants these at install time
- Can be used by only those apps are signed by the same certificate as the app that defines the permission

# Permissions

- Always check permissions before installing an app
- If the app asks for further permissions during usage, deny unless absolutely necessary
- Red Flag: Web browser seeking permission to access camera etc.
- Important: Check permissions granted to apps already installed on your phone in Settings

# Things to keep in mind

- Keep OS updated
- Keep applications updated
- Only install what you absolutely need
- Uninstall unused applications
- Avoid applications that claim to be 'Memory cleaners', 'Battery optimisers'

# Things to keep in mind

- Use Anti-Virus
- DO NOT install applications from untrusted sources
- DO NOT click on links in SMS received from unverified sources
- Check which apps have permissions to access location and contacts
- ~~UC Browser, CamScanner~~

# Things to keep in mind

## Researcher: Data Leaked for 300 Million Truecaller Users

But App Company Says Database Was Not Breached

Suparna Goswami ([@gsuparna](#)) • May 24, 2019

A security researcher has reported that the mobile phone numbers, and in some cases, other information, of 300 million Indians that use the Truecaller caller ID app are available for sale on the dark web. But the maker of the app says its database was not breached.

[Rajshekhar Rajaharia](#), an independent researcher, tells Information Security Media Group that the leaked data of 300 million Indians includes mobile phone numbers and, in some cases, email addresses, photos, company names, job titles and more.

The leaked data now available for sale, Rajaharia says, includes:

- 29.9 million Indian's mobile numbers, including those of thousands of celebrities, corporate CEOs and politicians;
- 1.9 million email addresses;
- 1.8 million subscriber photos;
- 20 million Facebook IDs;

# Things to keep in mind

| https://s3-eu-west-1.amazonaws.com/images1.truecaller.com/myview/1/c45b06d4c |                        |         |                                                                            |                             |                 |        |                 |         |      |            |          |           |
|------------------------------------------------------------------------------|------------------------|---------|----------------------------------------------------------------------------|-----------------------------|-----------------|--------|-----------------|---------|------|------------|----------|-----------|
| B                                                                            | C                      | D       | E                                                                          | F                           | G               | H      | K               | L       | M    | N          | O        | P         |
| Carrier                                                                      | Name                   | Gender  | Image                                                                      | Address                     | JobTitle        | Compan | facebook        | Twitter | Tags | Badges     | Score    | SpamCount |
| Vodafone                                                                     | Surander Chhillar      | MALE    | http://images1.truecaller.com/my                                           | New Delhi New Delhi, in     |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Shastri Kumar Singh    |         | http://graph.facebook.com/10000                                            | Delhi                       |                 |        | 100001897730328 |         |      |            | 0.49165  | 0         |
| Vodafone                                                                     | Raj Singh              |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.398076 | 0         |
| Vodafone                                                                     | Manoj Krsoni           | UNKNOWN | https://s3-eu-west-1.amazonaws                                             | Delhi in                    |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Sudha Sama             | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     | S Abbas                | MALE    | https://s3-eu-west-1.amazonaws                                             | New Delhi, India New Delh   | 584249451697870 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Satbir Tanwar          | MALE    | http://images1.truecaller.com/my                                           | Gurgaon gawal phari, 686, t |                 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     | P G                    | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Priyanka Naik          |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.323574 | 0         |
| Vodafone                                                                     | Vikram Tewatia         | MALE    | https://s3-eu-west-1.amazonaws                                             | New Delhi New Delhi, in     | 657951854258487 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     |                        | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Amit Tuteja            | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     | Savita Singh           | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Nishant Agarwal        | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     | Sagar Sehjawas         |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.313462 | 0         |
| Vodafone                                                                     | Kartik Choudhary       | MALE    | https://s3-eu-west-1.amazonaws.com/images1.truecaller.com/e39a925c7ae84f/1 |                             |                 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     | Rajeshdhankar Raje     | UNKNOWN | https://s3-eu-west-1.amazonaws                                             | Delhi in                    |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Yash Jain Axela        |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.383285 | 0         |
| Vodafone                                                                     | Syed Nafees Ahmec      | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Sonia                  |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.371982 | 0         |
| Vodafone                                                                     | 398 2 Renu Pathania Nb |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.31397  | 0         |
| Vodafone                                                                     | Kishniya               |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.313014 | 0         |
| Vodafone                                                                     | Pinak Pal              | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     | Monika Pandita         | UNKNOWN | https://s3-eu-west-1.amazonaws                                             | Delhi in                    |                 |        |                 |         |      | verified,u | 0.9      | 0         |
| Vodafone                                                                     | Pushpa Dawar           |         |                                                                            | Delhi                       |                 |        |                 |         |      |            | 0.330257 | 0         |
| Vodafone                                                                     | Vicky Ninnania         | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | user       | 0.9      | 0         |
| Vodafone                                                                     | Rajesh Sharma          | UNKNOWN |                                                                            | Delhi in                    |                 |        |                 |         |      | verified,u | 0.9      | 0         |

# Things to keep in mind

## 4.75 crore Indian Truecaller data on sale for Rs 75,000? Company responds

As per a report coming from online intelligence firm Cyble, some personal data of 4.75 crore Indians have been put on sale for \$1,000 (that roughly translates to around Rs 75,000) on dark web.

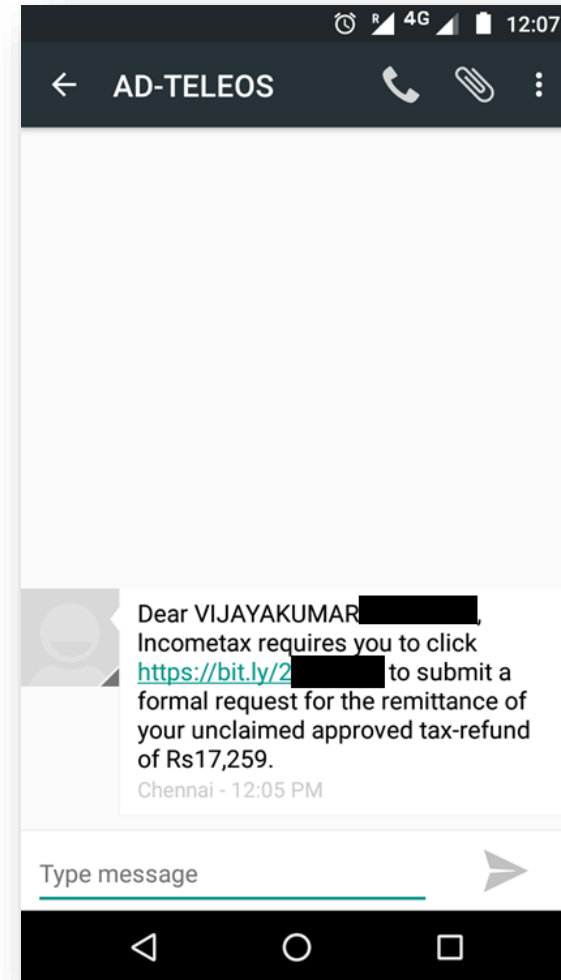
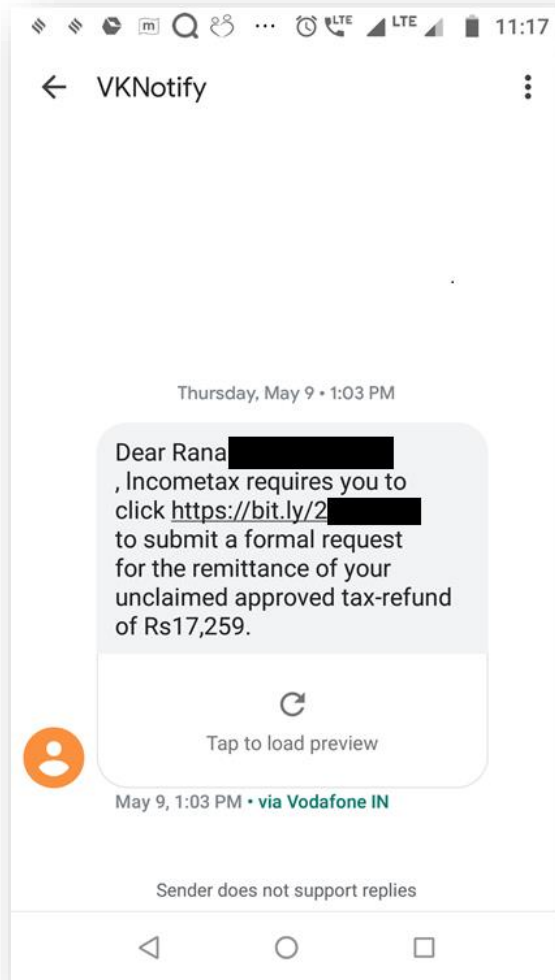
By: **Tech Desk** | New Delhi | Updated: May 27, 2020 3:37:45 pm

4.75 crore Indian truecaller data on sale for Rs 75,000? Truecaller denies report (Image: Truecaller)

As per a report coming from an online intelligence firm, Cyble, suggests that some personal data of 4.75 crore Indians have been put on sale for \$1,000 (that roughly translates to around Rs 75,000) on dark web. The report claims that data has been sourced from Truecaller's database but the company denies the claims. In an email statement, Truecaller said that there has been no breach of its database and all user information is saved securely.

# Case Study 1

# Smishing (SMS Phishing)



# Phishing page

← → ↻ ⓘ Not secure unip[REDACTED].com/369489780/940649167/home.php?id=YWJjQDEyMy5jb20= ☆

Apps Sun™ Convergence VirusTotal ITS 2.0 dawhois Netcraft | Internet Re The Hacker News (@ Login Other bookmarks

Follow us on Twitter ASK 1800 180 1961 / 1961

Skip to main content | Department Use ▾ | Help हिंदी | A+ | A | A- | A

Search...

↓ A to Z Index Search Tips / Advance Search

Home About Us ▾ Citizen's Charter ▾ Forms/Downloads ▾ Taxpayer Services Helplines Feedback

Income Tax Department > Individual

INDIVIDUAL HUF

### Income Tax Refund

Please select your bank and click "PROCEED" to complete Income Tax Refund application

Select your Bank: ----select---- **PROCEED**

taxable income  
exempt  
gains  
assets  
dependants  
write-offs  
deductions  
accruals  
deferrals

**tax refund**

**Disclaimer**

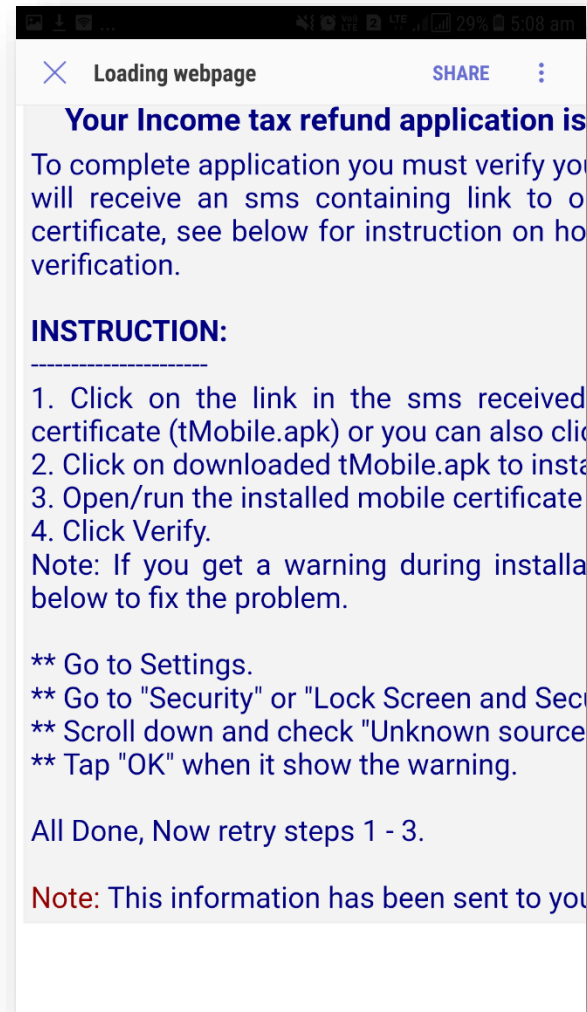
Report Phishing  
RTI  
Ombudsman

Useful Links  
Subscribe  
e-Governance

Sitemap  
Shortcut Keys  
Accessibility Statement

**Contact Us**  
Webmaster # 7008,  
Aayakar Bhawan,  
Vaishali, Ghaziabad. U.P.  
Ph: 0120-2370403, 2370408 / Fax: 0120-2370409

# Android Application



# Android Application Analysis

- Seeks permission to become the default SMS app
- Sent to the user after taking banking details
- Used for snooping OTPs
- Reads all SMS messages and forwards to attacker's number
- The SMS does not show up in the messaging app

# Case Study 3

# Smishing (SMS Phishing)

[Emperor cash] your Rs 130000 low interest loan (vivo) has been approved and is valid for 24 hours. Please click the link for cash: <https://cutt.ly/XfPFJ0M>

4:57 PM

OPPORupee  
bit.ly

[sopposupee]Due to your good reputation, you have successfully obtained a loan of Rs 150,000. Monthly interest of Rs 500, apply now: <https://bit.ly/3f6450b>

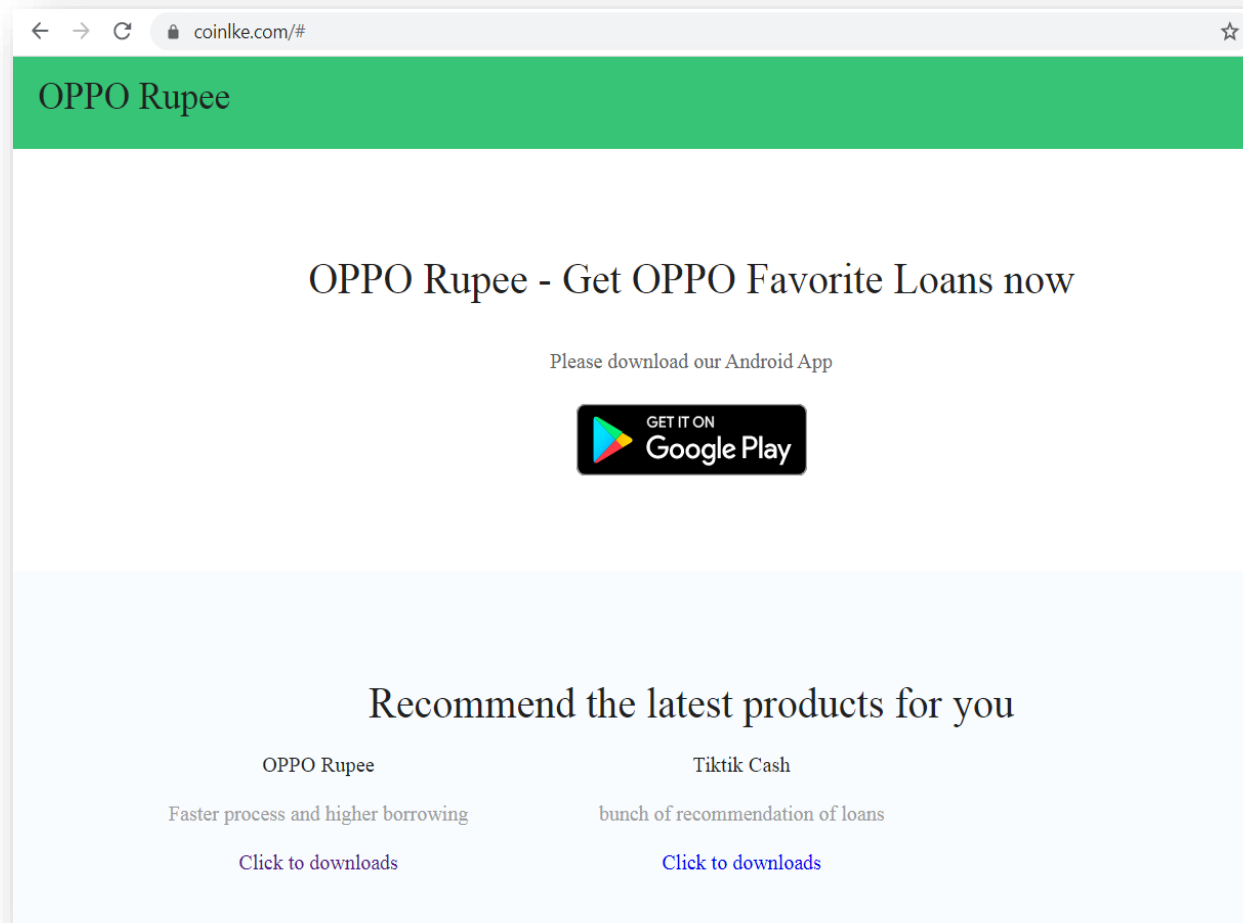
5:33 PM

Emperor Cash  
cutt.ly

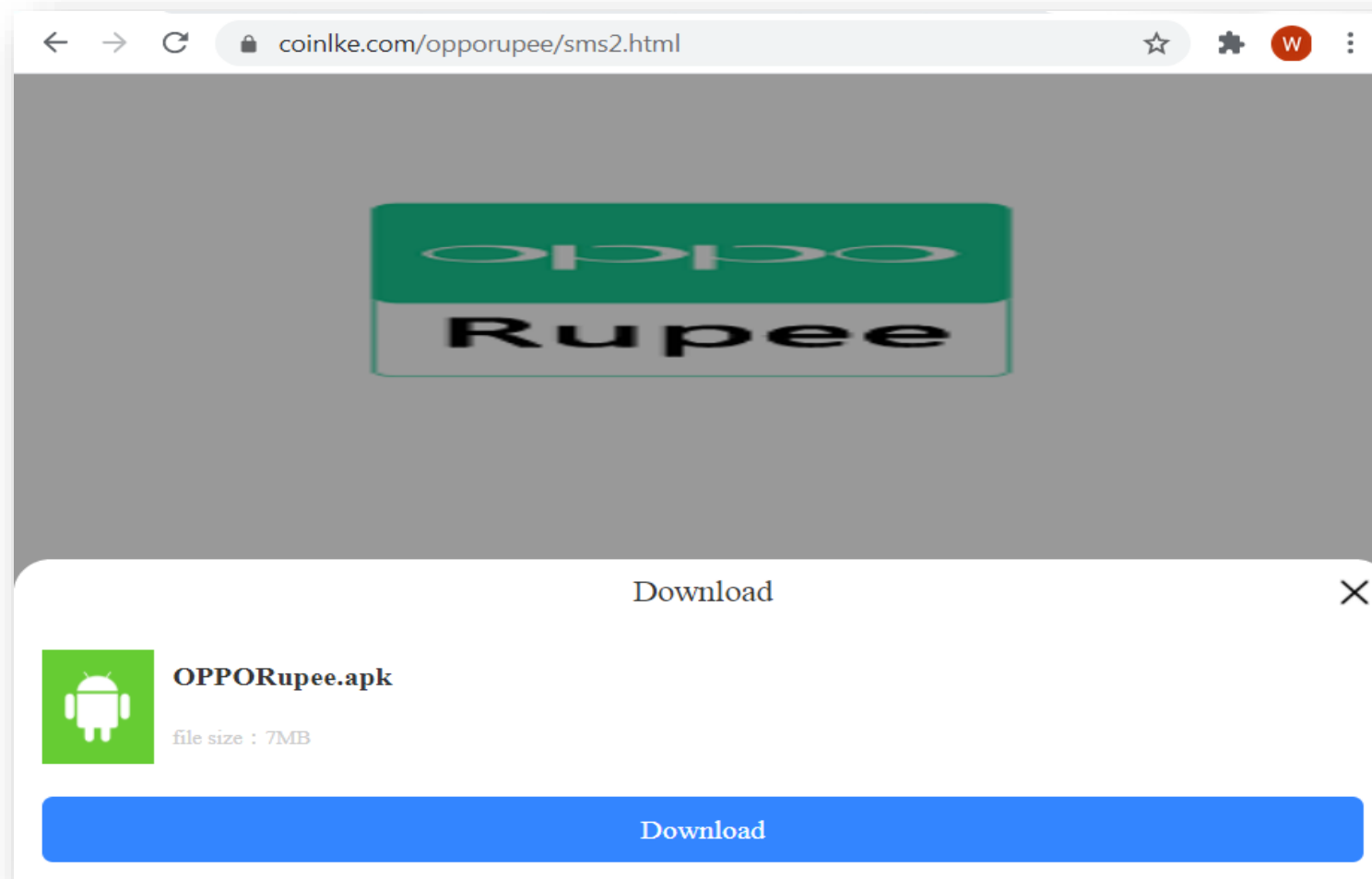
[Emperor cash] Dear user, due to your good reputation, vivo approved your low interest loan of Rs 200,000, please click to get cash <https://cutt.ly/zfWe26U>

9:53 AM

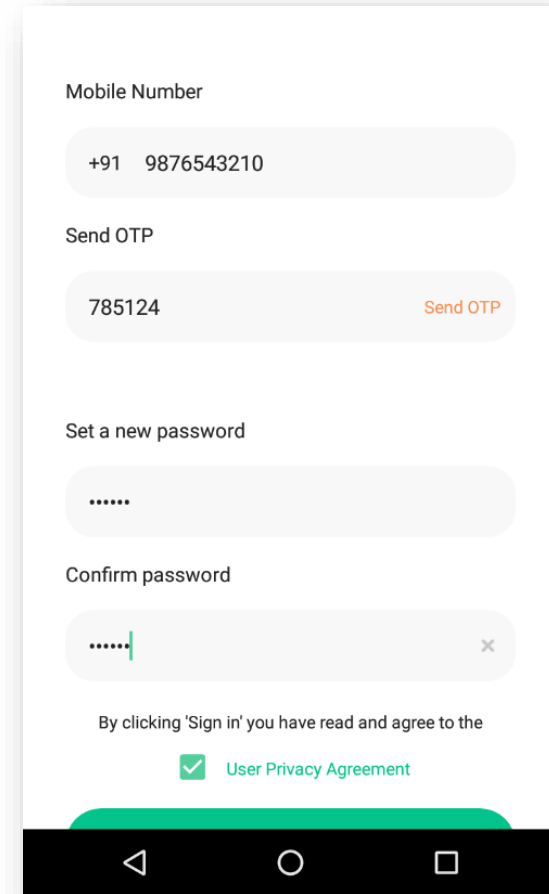
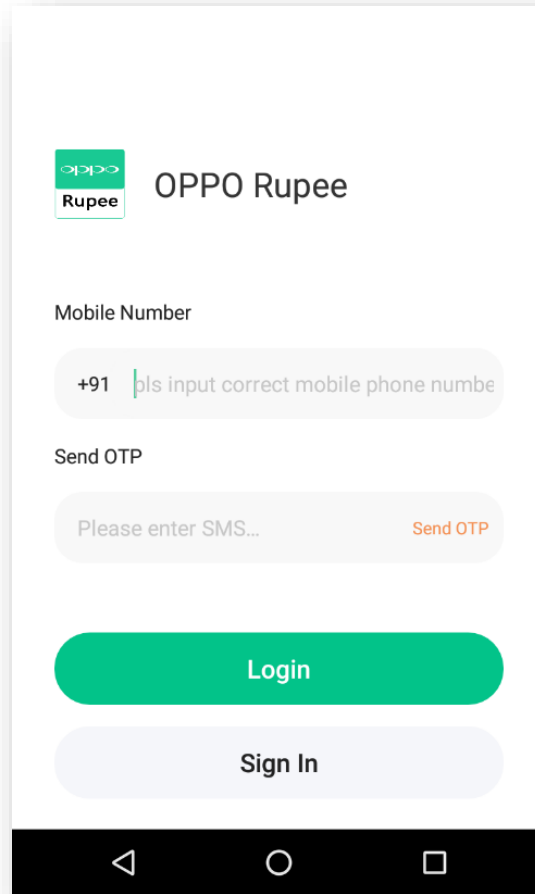
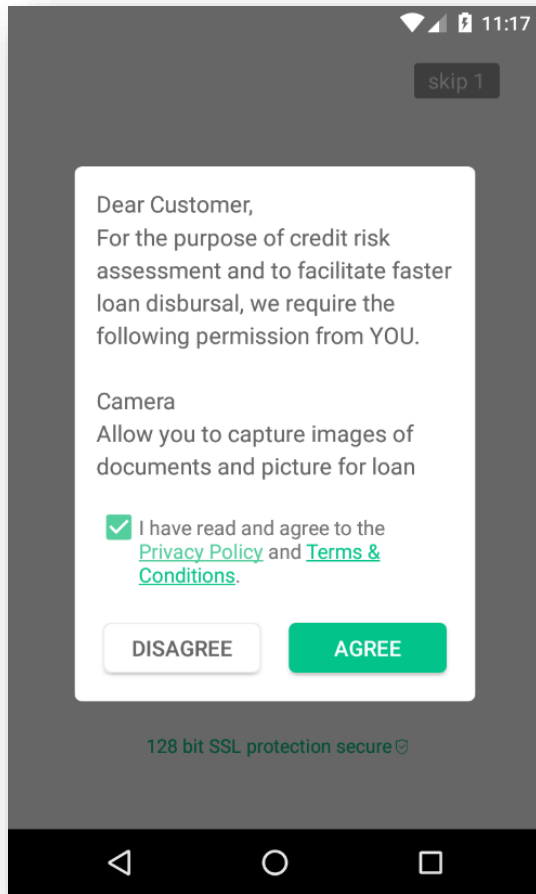
# Website



# Website



# Android Apps



# Android App Permissions

|                                              |                                           |
|----------------------------------------------|-------------------------------------------|
| android.permission.ACCESS_FINE_LOCATION      | android.permission.READ_CONTACTS          |
| android.permission.BLUETOOTH                 | android.permission.READ_EXTERNAL_STORAGE  |
| android.permission.CALL_PHONE                | android.permission.READ_LOGS              |
| android.permission.CAMERA                    | android.permission.READ_PHONE_STATE       |
| android.permission.CHANGE_WIFI_STATE         | android.permission.RECEIVE_USER_PRESENT   |
| android.permission.GET_TASKS                 | android.permission.WAKE_LOCK              |
| android.permission.INTERNET                  | android.permission.WRITE_EXTERNAL_STORAGE |
| android.permission.MOUNT_UNMOUNT_FILESYSTEMS | android.permission.WRITE_SETTINGS         |

# Thank You

Email: [incident@cert-in.org.in](mailto:incident@cert-in.org.in)