Research Report on

Cybercriminals lure internet users with fake Credit offers and malicious application in the name of ICICI Bank.
Disclaimer

"This report is purely based on technical findings made by the research team during an investigation. It does not intend to malign or in any way target any country, actor or person. All the information provided in this report has been extracted during the investigation and information might be changed after generating the reports."
Research Report on Cybercriminals lure internet users with fake Credit offers and malicious application in the name of ICICI Bank

The Research wing of CyberPeace Foundation has received a WhatsApp message containing a link asking users to redeem their ICICI credit points worth INR 5000 before it expires.

Case Study

The Research wing of CyberPeace Foundation and Autobot Infosec Private Limited have looked into this matter to conclude whether the campaign is legitimate and launched by ICICI Bank or is an online fraud.

When any individual visits the link https://climreward.co.in/, the landing page appears to be a web page having ICICI Bank's Logo and asks users to download an application in order to avail 5000 reward points.
On clicking the “Download Here” link, it starts downloading the application offer.apk

Domain Whois Lookup:

**Domain Name:** climreward.co.in  
**Registry Domain ID:** D842134176B8C48EF80F82C140C9DC71E-IN  
**Registrar URL:** www.godaddy.com  
**Registrar:** GoDaddy.com, LLC  
**Registrar IANA ID:** 146  
**Updated Date:** 2022-12-15T22:01:03Z  
**Creation Date:** 2022-12-05T10:24:31Z  
**Registry Expiry Date:** 2023-12-05T10:24:31Z  

**Registrant State/Province:** Delhi  
**Registrant Country:** IN  

**Name Server:** ns08.domaincontrol.com  
ns07.domaincontrol.com

Source Code Analysis

- The title of the landing page is “Offer”.
Application Analysis

Once the user installs the offer.apk application on an android device, as usual, the app asks the user to give the following permission.

- Access of send and view SMS
The application opens with a ‘Lets Get Started!’ message and asks users to submit confidential information viz. Name, Mobile Number, Email Id, Date of Birth, Credit Card Limit, Card Holder Name, Card Number, Expiry Date, CVV.

After filling all the details it shows a congratulatory message.

“Congratulations
Available Redeemable 5000 Points

Your Redeem Points Successfully Processed it will be reflect with in 24 hrs.”

**Note:** The congratulatory message contains several Grammatical mistakes.

Application Icon
## Application Details

<table>
<thead>
<tr>
<th>App name</th>
<th>ICICI Rewards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package name</td>
<td>com.md_2.newcopyappreward</td>
</tr>
<tr>
<td>App Security Score</td>
<td>53/100</td>
</tr>
<tr>
<td>Main Activity</td>
<td>com.md_2.newcopyappreward.SplashActivity</td>
</tr>
<tr>
<td>Target SDK</td>
<td>33</td>
</tr>
</tbody>
</table>

## Hash Details

<table>
<thead>
<tr>
<th>MD5</th>
<th>07a1eba61f42e9841fcc508de7295038</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA1</td>
<td>96596d59534ba4a5c28dfc844ca07a34a8e3d18b</td>
</tr>
<tr>
<td>SHA256</td>
<td>e098d8b63a7fac3a2a029ef08770d772004415c7e3c4c647d9d723107cfe0654</td>
</tr>
</tbody>
</table>

## Application Certificate Details

<table>
<thead>
<tr>
<th>Issuer:</th>
<th>C=debugging</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid From:</td>
<td>2016-09-23 11:57:06+00:00</td>
</tr>
<tr>
<td>Valid To:</td>
<td>3015-01-25 11:57:06+00:00</td>
</tr>
<tr>
<td>Serial Number</td>
<td>333a0b9b</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>SHA256</td>
</tr>
<tr>
<td>PublicKey Algorithm</td>
<td>RSA</td>
</tr>
</tbody>
</table>
## Application Permissions Details

```xml
<uses-sdk android:minSdkVersion="23" android:targetSdkVersion="33" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.INSTANT_APP_FOREGROUND_SERVICE" />
<uses-permission android:name="android.permission.START_FOREGROUND_SERVICES_FROM_BACKGROUND" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.SEND_SMS" />
<application android:theme="@style/Theme.Newax" android:label="@string/app_name" android:icon="0" />
```

## Application Permissions

<table>
<thead>
<tr>
<th>PERMISSION</th>
<th>STATUS</th>
<th>INFO</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>android.permission.ACCESS_NETWORK_STATE</td>
<td>normal</td>
<td>view network status</td>
<td>Allows an application to view the status of all networks.</td>
</tr>
<tr>
<td>android.permission.ACCESS_WIFI_STATE</td>
<td>normal</td>
<td>view Wi-Fi status</td>
<td>Allows an application to view the information about the status of Wi-Fi.</td>
</tr>
<tr>
<td>android.permission.CHANGE_NETWORK_STATE</td>
<td>normal</td>
<td>change network connectivity</td>
<td>Allows an application to change network connectivity state.</td>
</tr>
<tr>
<td>android.permission.CHANGE_WIFI_STATE</td>
<td>normal</td>
<td>change Wi-Fi status</td>
<td>Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.</td>
</tr>
<tr>
<td>android.permission.FOREGROUND_SERVICE</td>
<td>normal</td>
<td></td>
<td>Allows a regular application to use Service.startForeground.</td>
</tr>
<tr>
<td>android.permission.INSTANT_APP_FOREGROUND_SERVICE</td>
<td>Signature OrSystem</td>
<td></td>
<td>Allows an instant app to create foreground services.</td>
</tr>
<tr>
<td>android.permissionINTERNET</td>
<td>normal</td>
<td>full Internet access</td>
<td>Allows an application to create network sockets.</td>
</tr>
<tr>
<td>PERMISSION</td>
<td>STATUS</td>
<td>INFO</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>android.permission.READ_SMS</td>
<td><strong>dangerous</strong></td>
<td>read SMS or MMS</td>
<td>Allows an application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.</td>
</tr>
<tr>
<td>android.permission.RECEIVE_SMS</td>
<td><strong>dangerous</strong></td>
<td>receive SMS</td>
<td>Allows an application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.</td>
</tr>
<tr>
<td>android.permission.SEND_SMS</td>
<td><strong>dangerous</strong></td>
<td>send SMS messages</td>
<td>Allows an application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.</td>
</tr>
</tbody>
</table>

**Domain Connected**

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>GEOLOCATION</th>
</tr>
</thead>
</table>
| connectivitycheck.gstatic.com | IP: 142.250.182.195  
Country: United States of America  
Region: California  
City: Mountain View  
Latitude: 37.405991  
Longitude: -122.078514 |
| www.google.com | IP: 142.251.42.100  
Country: United States of America  
Region: California  
City: Mountain View  
Latitude: 37.405991  
Longitude: -122.078514 |

**Interesting Strings**

The application is flagged as malicious by 25 Security Vendors on Virustotal.

Reference: Virustotal
Conclusive Summary

- The campaign appears to be an offer from ICICI Bank, however, it is hosted on a third-party domain instead of the official ICICI Bank website, raising suspicion.

- The application asks several access permissions of the device. Allowing such access permissions could result in a complete compromise of the system, including access to sensitive information such as microphone recordings, camera footage, text messages, contacts, pictures, videos, and even banking applications.

- Cybercriminals used the lookalike icon of the ICICI Bank while creating the malicious application in order to lure the users.

- The application collects the user's personal and banking information. Getting into this type of trap could lead users to face massive financial losses.

- The application is flagged as malicious by several Security Vendors.

- Customers who desire to avail credit rewards from the respective bank, download relevant apps, believing that the chosen app will assist them. However, they are not always aware that the app may be fraudulent.
CyberPeace Advisory

! CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms. One must always think before clicking on such links, or downloading any attachments from unauthorised sources.

! Downloading any application from any third party sources instead of the official app store should be avoided. This will greatly reduce the risk of downloading a malicious app, as official app stores have strict guidelines for app developers and review each app before it gets published on the store.

! Even if you download the application from an authorised source, check the app's permissions before you install it. Some malicious apps may request access to sensitive information or resources on your device. If an app is asking for too many permissions, it's best to avoid it.

! Keep your device and the app-store app up to date. This will ensure that you have the latest security updates and bug fixes.

! Do not share confidential details like credentials, banking information with such types of Phishing scams.

! Never share or forward fake messages containing links with any social platform without proper verification.

Issued by

Research Wing, CyberPeace Foundation.
Research Wing, Autobot Infosec Private Ltd.