PhonePe Users Beware:

Cybercriminals Unleash Fake Reward Scam, Targets UPI Users.
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."
PhonePe Users Beware: Cybercriminals Unleash Fake Reward Scam, Targets UPI Users.

The Research Wing of CyberPeace Foundation recently came across a WhatsApp message containing a link, urging users to claim their PhonePe reward. The link provided was https://pmppxl[](https://pmppx)online/Gift/

**Link**

https://pmppx[](https://pmppxl)online/Gift/

**Case Study**

A joint investigation conducted by the Research Wing of CyberPeace Foundation and Autobot Infosec Private Limited was undertaken to determine the legitimacy of the campaign and identify any signs of online fraud.

Upon visiting the aforementioned link from a mobile device, users are directed to a landing page featuring the PhonePe logo and a message prompting them to "Claim Reward."

To proceed, the user must scratch and reveal the prize. Once completed, the page indicates that the user has won a reward of INR 698.
The subsequent step instructs users to click on a button to transfer the prize reward to their bank account. Upon clicking the “Send Prize Money In Bank” button, the PhonePe application on the device opens and prompts users to enter their UPI pin.

Note: It is important to note that entering the UPI pin is not necessary for receiving money in a bank account. The UPI pin is exclusively used for sending money from the respective bank account. Therefore, if the user enters their UPI pin, an amount of INR 698 will be deducted from their bank account.

Note: It should be noted that if a user attempts to open the link on a desktop or laptop device, they will receive a message stating “We Are Updating.... Comming Soon.....” on the website. This indicates that users are forced to access the URL from their mobile devices.

Technical Analysis

<table>
<thead>
<tr>
<th>Domain</th>
<th>pmppxl[.]online</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>89.117.188.129</td>
</tr>
<tr>
<td>HTTP Source code</td>
<td>200 [OK]</td>
</tr>
<tr>
<td>ISP</td>
<td>SC Lithuanian Radio and TV Center</td>
</tr>
<tr>
<td>ASN</td>
<td>47583</td>
</tr>
<tr>
<td>Country</td>
<td>India</td>
</tr>
<tr>
<td>City</td>
<td>Mumbai, Maharashtra</td>
</tr>
</tbody>
</table>

Domain Name: PMPPXL.ONLINE
Registry Domain ID: D349145022-CNIC
Registrar WHOIS Server: whois.hostinger.com
Registrar URL: https://www.hostinger.com/
Registrar: Hostinger, UAB
Registrar IANA ID: 1636

Updated Date: 2023-02-21T14:42:50.0Z
Creation Date: 2023-02-16T14:28:11.0Z
Registry Expiry Date: 2024-02-16T23:59:59.0Z

Name Server: NS1.DNS-PARKING.COM
Name Server: NS2DNS-PARKING.COM

**Note:** The domain name has been registered very recently.

**HTTP Request Intercepted**

During the backend analysis, it was discovered that an HTTP traffic was being sent to the following URL:

https://super-panel[.]in/V3/api/?token=65794a705a4349364e7a4573496c5a6a6232526c49ba6f7a66513d3d&amount=698&host=pmppxl.online

<table>
<thead>
<tr>
<th>Domain</th>
<th>super-panel[.]in</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>217.21.93.165</td>
</tr>
<tr>
<td>HTTP Source code</td>
<td>200 [OK]</td>
</tr>
<tr>
<td>ISP</td>
<td>Hostinger Hosting</td>
</tr>
<tr>
<td>ASN</td>
<td>47583</td>
</tr>
<tr>
<td>Country</td>
<td>India</td>
</tr>
<tr>
<td>City</td>
<td>Mumbai, Maharashtra</td>
</tr>
</tbody>
</table>

Domain Name: super-panel.in
Registry Domain ID: D46C5882366BB408299BD4E00041A658E-IN
Registrar URL: www.openprovider.com
Registrar: Hosting Concepts B.V. d/b/a Openprovider
Registrar IANA ID: 1647

Updated Date: 2022-12-09T07:06:55Z
Creation Date: 2022-12-04T07:06:54Z
Registry Expiry Date: 2023-12-04T07:06:54Z
Name Server: ns1.dns-parking.com
Name Server: ns2.dns-parking.com

Note: The domain name has been registered very recently.

We have also discovered the payment string that triggers the opening of the PhonePe application:

```
Phonepe://pay?pa=okcredits698@barodampay&pn=YDVXXXXXXX&tn=YDVXXXXXXX&am=698&cu=INR&mode=02&purpse=00&tr=XXXXXXX
```

** Please note that for security reasons, some characters in the string have been replaced with "XX".

Important: the UPI ID to which the amount will be transferred is identified as okcredits698@barodampay.

<table>
<thead>
<tr>
<th>UPI ID</th>
<th>okcredits698@barodampay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>Ok Credits</td>
</tr>
</tbody>
</table>

It appears that the UPI ID is associated with an account at Bank of Baroda. As the UPI id @barodampay is one of the VPA handlers for Bank of Baroda customers who use the BHIM Baroda Pay UPI app.
1. Exercise Caution:
   a. Be cautious when clicking on unfamiliar links received through messaging platforms.
   b. Verify the authenticity of reward schemes before participating.

2. Protect Personal Information:
   a. Avoid sharing sensitive information like UPI pins or banking details with unknown sources.
   b. Only provide personal details to trusted and verified entities.

3. Verify Legitimacy:
   a. Visit official websites or contact legitimate service providers to confirm the authenticity of reward campaigns.
   b. Be skeptical of offers that seem too good to be true.

4. Stay Informed:
   a. Stay updated on the latest Cybersecurity threats and scams through reliable sources.
   b. Follow official announcements from trusted organizations or Cybersecurity authorities.

5. Strengthen Security Measures:
   a. Use strong, unique passwords for all online accounts, including UPI applications.
   b. Enable multi-factor authentication (MFA) for enhanced security.

6. Maintain Security Software:
   a. Install and regularly update antivirus and security software on all devices.
   b. Keep operating systems and applications up to date with the latest patches.

7. Report Suspicious Activities:
   a. Report suspicious messages, links, or scams to the appropriate authorities, such as the Cybercrime Cell or your bank.
   b. Share information about potential scams with family, friends, and colleagues to raise awareness.

Issued by:

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