RESEARCH REPORT ON PHISHING CAMPAIGN

REPLICATING STATE BANK OF INDIA
INTERNET BANKING WEBSITE
The Research Wing at CyberPeace Foundation has received an SMS asking users to update their KYC details for the SBI bank account by clicking on the respective link.

Link: [http://8ef628b4602c.ngrok[.]io/sbibank](http://8ef628b4602c.ngrok[.]io/sbibank)
The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited have looked into this matter to reach a conclusion that the website is either legitimate or an online fraud.

On the landing page a page appeared which was mostly similar to the official SBI Online page [https://retail.onlinesbi.com/retail/login.htm](https://retail.onlinesbi.com/retail/login.htm).

On clicking the “CONTINUE TO LOGIN” button it redirected us to [http://8ef628b4602c.ngrok[.]io/sbibank/full-kyc.php](http://8ef628b4602c.ngrok[.]io/sbibank/full-kyc.php) page where it asked users for confidential information like Username, Password and a Captcha in order to login to the online banking.

(CARE: Username and password are case sensitive.)
After submitting some dummy data we were redirected to [http://8ef628b4602c.ngrok[]/sbibank/otp.php](http://8ef628b4602c.ngrok[]/sbibank/otp.php) which asked for a OTP.

![SBI Online OTP Entry Form](image1)

After entering a random OTP it redirected us to [http://8ef628b4602c.ngrok[]/sbibank/acholder.php](http://8ef628b4602c.ngrok[]/sbibank/acholder.php) page which asked users to enter again some confidential information like Account Holder Name, Mobile Number, Date of birth.

![SBI Online Account Holder Form](image2)

After providing the dummy data we reached to [http://8ef628b4602c.ngrok[]/sbibank/last-otp.php](http://8ef628b4602c.ngrok[]/sbibank/last-otp.php) where it again asked for OTP.
After clicking on the Confirm button it redirected us to the same page again.

**Key Points**

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>8ef628b4602c.ngrok[.]io</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 [ Active ]</td>
</tr>
<tr>
<td>IP Address</td>
<td>3.17.7.232</td>
</tr>
<tr>
<td>ISP</td>
<td>Amazon.com</td>
</tr>
<tr>
<td>ASN</td>
<td>16509</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>
"ngrok is a cross-platform application that enables developers to expose a local development server to the Internet with minimal effort. The software makes your locally-hosted web server appear to be hosted on a subdomain of ngrok.com, meaning that no public IP or domain name on the local machine is needed. .........................

ngrok is able to bypass NAT Mapping and firewall restrictions by creating a long-lived TCP tunnel from a randomly generated subdomain on ngrok.com (e.g. 3gf892ks.ngrok.com) to the local machine.”

https://www.pubnub.com/learn/glossary/what-is-ngrok/
→ Title of the site “SBI Online”.

→ Some of the Images used in the site:

http://8ef628b4602c.ngrok[.]io/sbibank/first.jpg
http://8ef628b4602c.ngrok[.]io/sbibank/otp-footer.jpg
http://8ef628b4602c.ngrok[.]io/sbibank/footer.jpg

→ Captcha that appeared in the login section was static which remains the same every time users load the site.

→ We noticed that on clicking anywhere in the landing page it redirects to the */full-kyc.php* page whereas users should be redirected only if they click on the “CONTINUE TO LOGIN” button. It means users are deliberately forced to reach to the */full-kyc.php* and provide the confidential information.
By URL manipulation we found that the webserver has directory listing enabled and found other links visible in the screenshot below.

On visiting each link we came to a conclusion that not only the SBI users, IDFC, PNB, Indusland, Kotak bank users are also targeted by the same type of Phishing scam.
Conclusive Summary

The campaign is pretended to be launched from State Bank of India but hosted on the third party domain instead of the official website https://www.onlinesbi.com/ which makes it more suspicious.

Overall layout of the web page used in the campaign is kept similar to the official SBI net banking site to lure laymen.

The campaign is collecting banking information like Username, Password, Account Holder Name, Mobile Number, Date of birth from the user. Getting into this type of trap could lead the users to face a massive financial loss.

The whole campaign uses plain http protocol instead of the secure https. This means anyone on the network or internet can intercept the traffic and get the confidential information in plain text to misuse against the victim.

Cybercriminals used ngrok technology to hide the real IP address of the hosting site to be anonymous.

CyberPeace Advisory

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

Falling for this trap could lead to whole system compromisation (Access to microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications etc.) as well as financial loss for the users. One must always think before clicking on such links, or downloading any attachments from unauthorized sources.

Do not share confidential details like login credentials, banking information with such a type of scam.

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