Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

By -R G Singh

Incident Use Cases/Examples

#Incident1 : Phishing Incident

Dear Team,

We would like to inform you that the following phishing page is active impersonating as State Bank of India which is trying to steal the sensitive information.

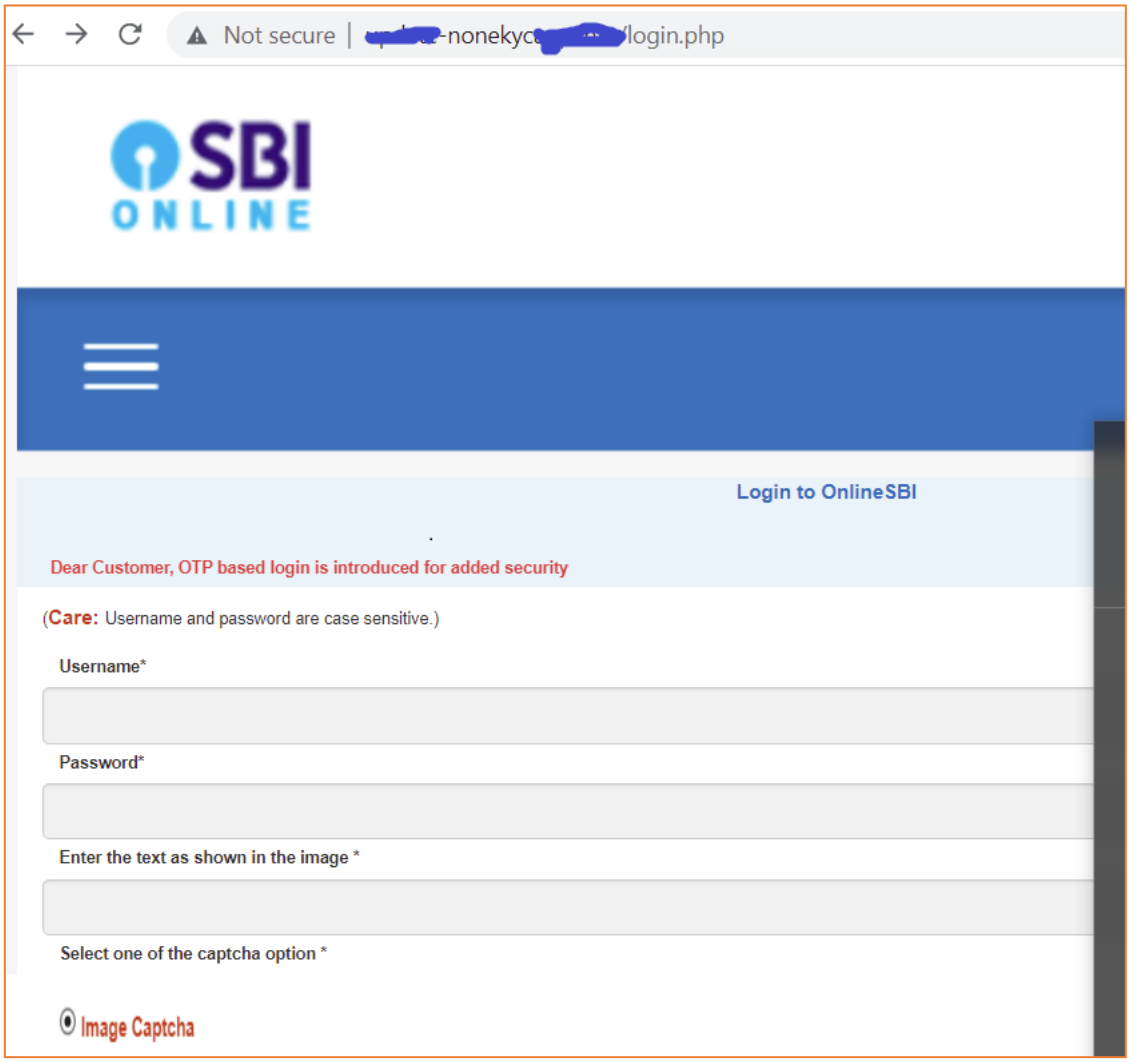


Fig: Screenshot show in phishing page of SBI

Question: To whom you will report????

** In order to report an incident correct portal is always necessary so that the impact of incident can be minimized.

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

By -R G Singh

#Incident2 : Sphere Phishing Incident

Dear Team,

It is observed that a phishing page has been created which appears as the Government offcials Email id “email.gov.in”.

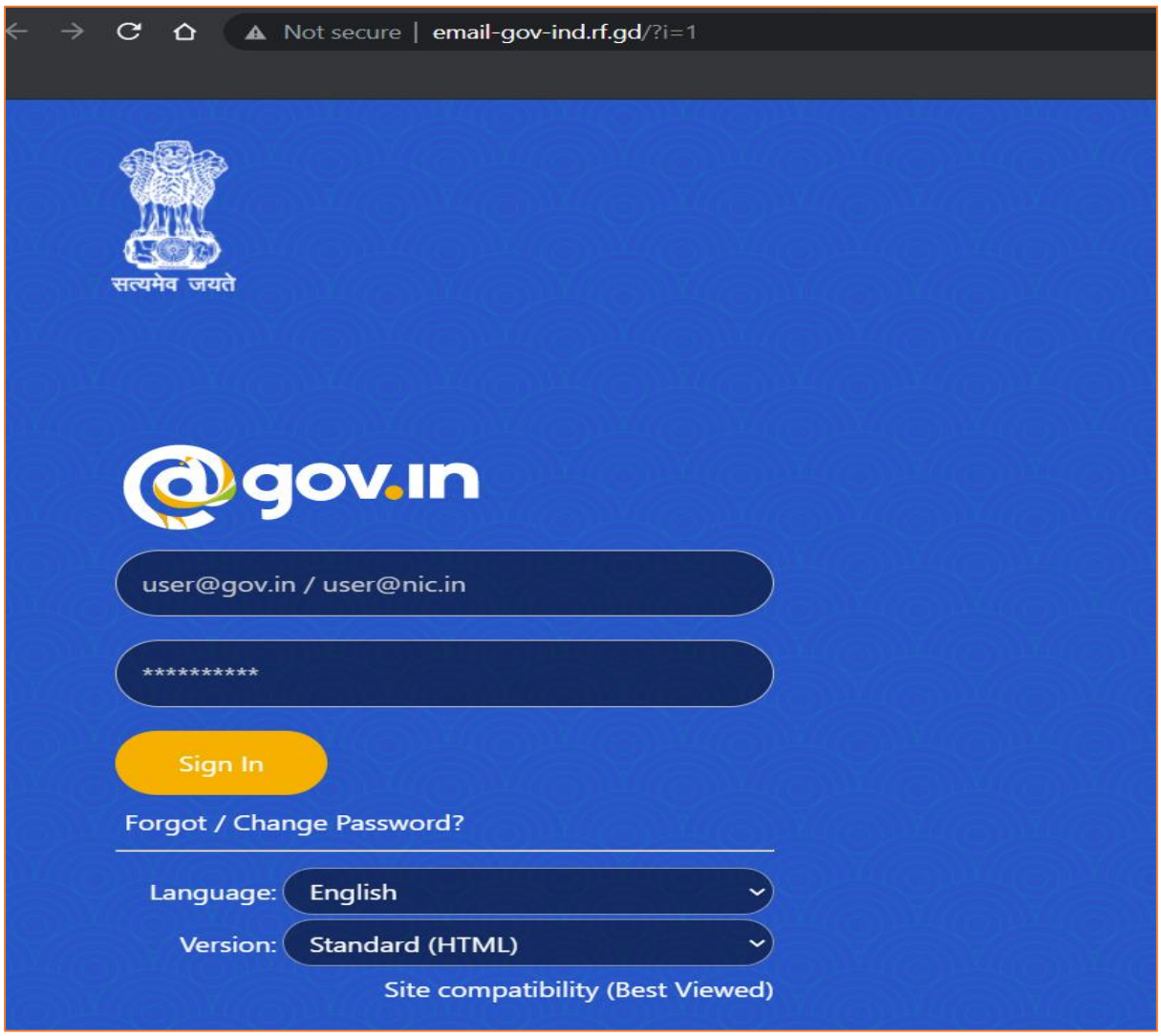


Fig: A phishing page impersonating as Govt official email page

Questions2: If you have received such phishing email (you may consider it as an incident). What will be your action plan?
Question 3: To whom you will contact?
Question 4: Are you able to analyze and evaluate whether this is a phishing email **(Email Header analysis)**?

Question 5: What if this email is clicked by few of the user's within your organization?
Question 6: What will be your action plan?
Question 7: Whether this sphere phishing email is dropping any file?

#Incident3 : Websites with intention of Financial Fraud

A website is created which is offering the Flipkart offers and giving product at very cheap rate.

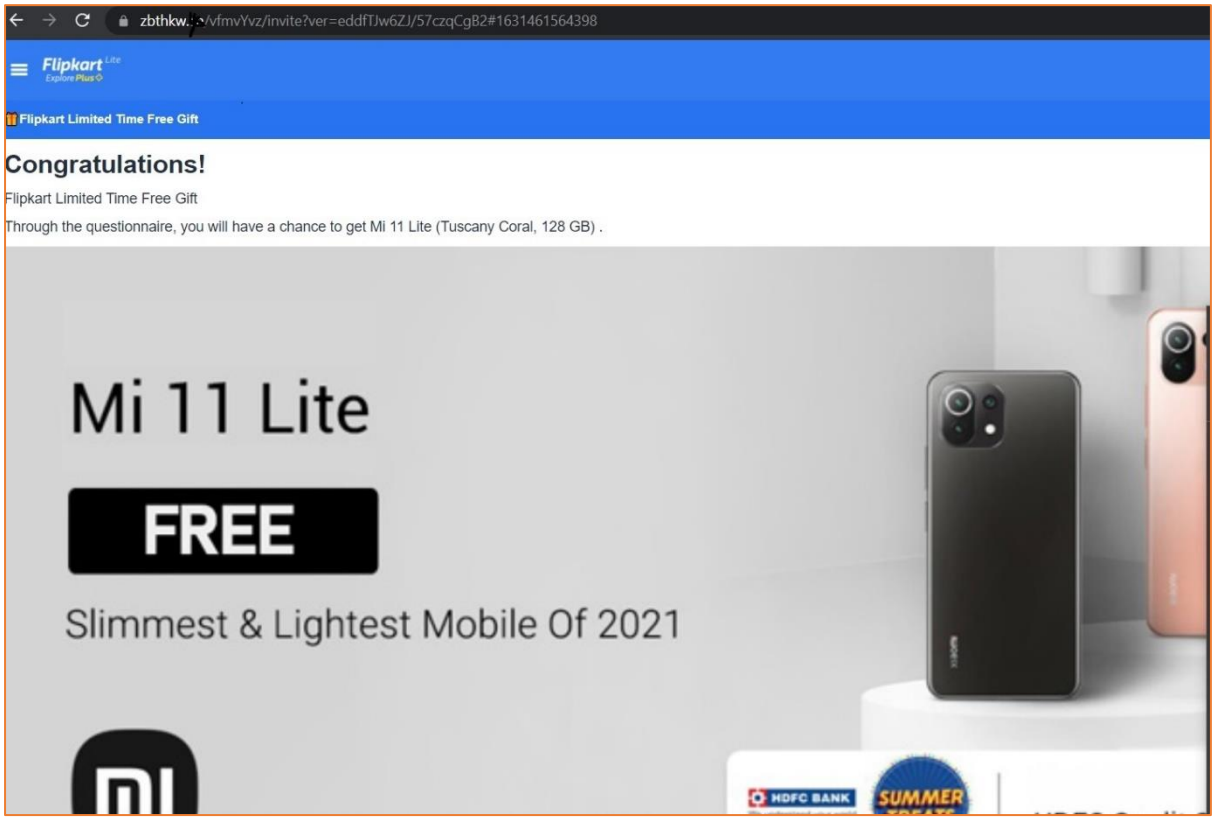


Fig: A phishing page showing offers and have the intention of financial fraud

Question 8: To whom we should report? Who will handle it ?

Question 9 : What if someone has clicked and submitted their personal information?

Question 10? What if it is dropping a spyware/malware within your computer system/android phone? (Worrying situation)

By -R G Singh

#Incident4: Email Compromise

The ID: xyz@gov[.]in; is suspected to be compromised and has been involved in sending phishing mails.

```
Return-Path: <trailer@gov.in>
Received: from abc(LHLO abc) (1.5.6.7) by
 Received: from pqr(unknown [192.168.1.166])
      by abc(Postfix) with ESMTP id 3538741B97B1;
      Mon, 30 Aug 2021 12:43:51 +0530 (IST)


RmGexjYtIA7fJmpT9VtOpHMnequ6StW4C23h9wbJe24IUIfJZeaTmrndP3EpiSqR8A6F
5FKJI7
 A9a23:mQjbyqDGMwhC0iblHemS55DYdb4zR+YMi2TDtnoBLCC9Hfb3qy
 Subject: PASSWORD CHANGE EMAIL!!
MIME-Version: 1.0
Content-Type: multipart/alternative;
      boundary="=_3c4a14ba-6132-4892-ba8f-16be3adba2d6"
X-Originating-IP: [1.2.3.4, 4.5.6.7]
X-Mailer: Zimbra 8.8.15_GA_2148 (ZimbraWebClient - FF91
(Win)/8.8.15_GA_2148)
Thread-Index: EAJCNQhUZSCR/RczbJ1/1CjhFgu1hQ==
Thread-Topic: PASSWORD CHANGE EMAIL!!
To:

--=_3c4a14ba-6132-4892-ba8f-16be3adba2d6
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable

Dear user,
eG&IT Division has received reports from Govt officials regarding
receipt of a phishing emails. Malicious received emails have already
been forwarded to NIC for necessary actions.

In this connection, eG&IT Division urge users to change their
password immediately using following link:

[ https://www.xyz.in/NewSite/Admin/try/PassApp.php | https://=
PassApp.mail.gov.in/ChangePassword ]=20

Kind regards,
SO(IT Security)
```

Question11: Here the phishing email is coming from original Email ID (Seems to be compromise)? What action you will take?

Question 12: How you will analyze?

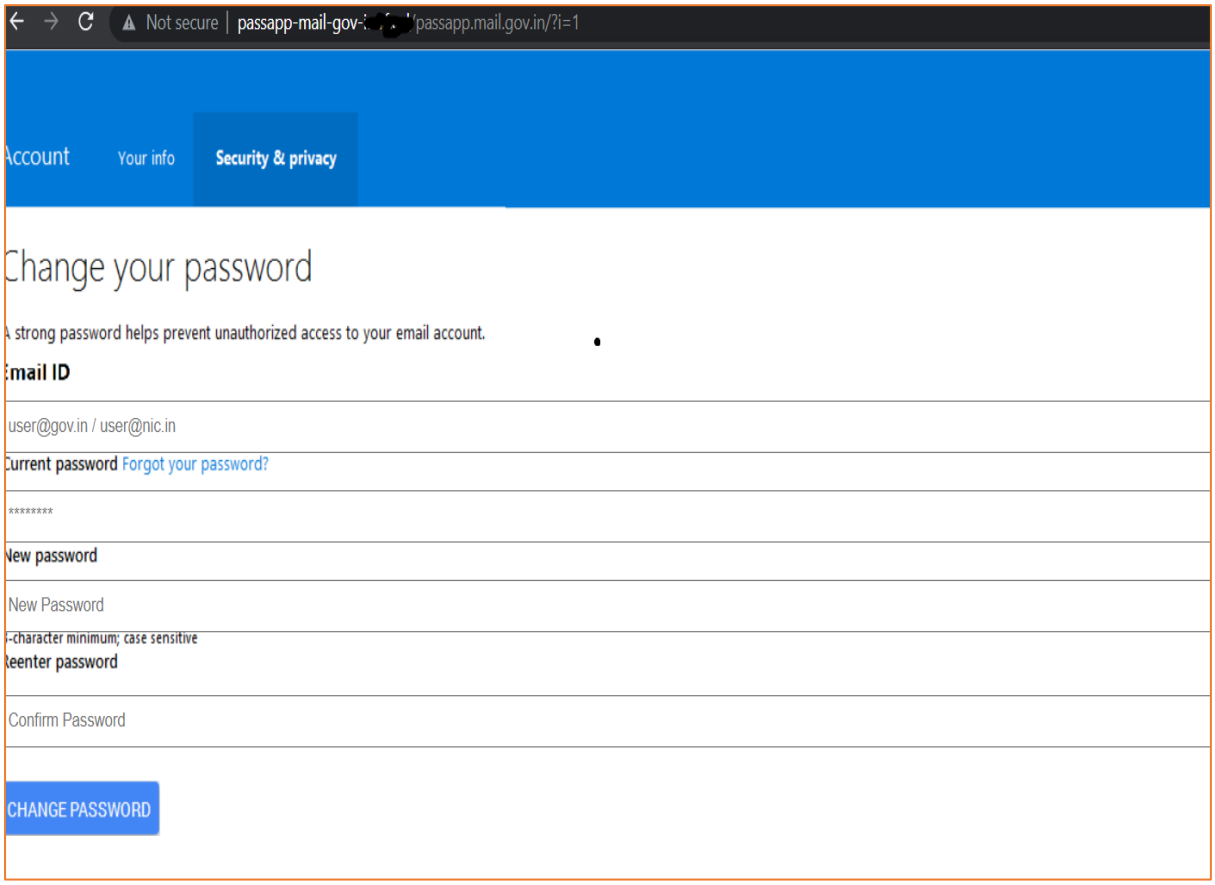
Question 13: What if some has submitted their personal information, believing with assumption the received email is correct?

**** Note that here the phishing page is hosted on a xyz website. It may possible that xyz.in may be compromised by the attacker.

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

By -R G Singh

#Incident5: Are you Using Kavach (Page impersonating pass mail)



A phishing redirector site hosted on Domain "xyz.in" / which is redirecting to a phishing page

hxxps://www.xyz.in/figure/news /PassApp.php

redirects to url

http://passapp-mail-gov-in.rf.gd/passapp.mail.gov.in/?i=1

By -R G Singh

#Incident6: Email Dropping malware

Description:

Dear Sir,

We have received a suspicious mail from an user having an attachment "Bill_rupesh_Section_Officer.zip".

Question 14: What will be your approach to verify and handle this incident?

Question 15: Should we open it? (No, if you feel it is not genuine, always use safe environment)

Question 16: What is the safe environment? (Cuckoo sandbox, Linux machine (for .exe), sandboxie)

Question 17: How the analysis will be performed? (Malware analysis)

Question 18: Can we do some basic analysis using common tools? (Virus total)

** The suspicious file may be escalated to a dedicated team, if the user is not able to verify it. It is strictly followed to AVOID download and open suspicious files. The file sample may also be escalated to other CERT or National CERT(CERT-In)

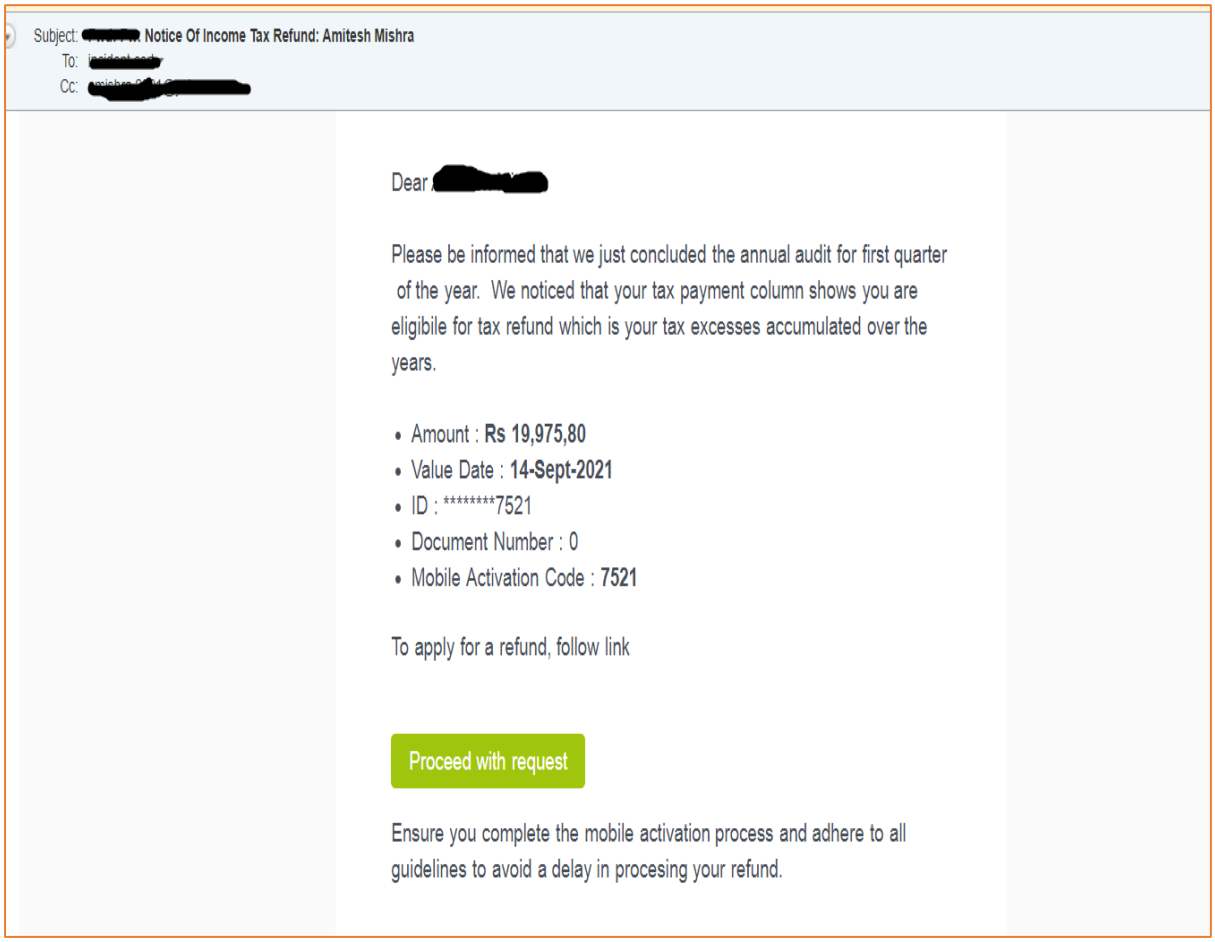
**https://www.virustotal.com/

** https://www.sandboxie.com/

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

By -R G Singh

#Incident8: Income Tax (Targeting the Mass)



Subject: [redacted] Notice Of Income Tax Refund: Amitesh Mishra
To: [redacted]
Cc: [redacted]

Dear [redacted]

Please be informed that we just concluded the annual audit for first quarter of the year. We noticed that your tax payment column shows you are eligibile for tax refund which is your tax excesses accumulated over the years.

- Amount : **Rs 19,975,80**
- Value Date : **14-Sept-2021**
- ID : ********7521
- Document Number : 0
- Mobile Activation Code : **7521**

To apply for a refund, follow link

Proceed with request

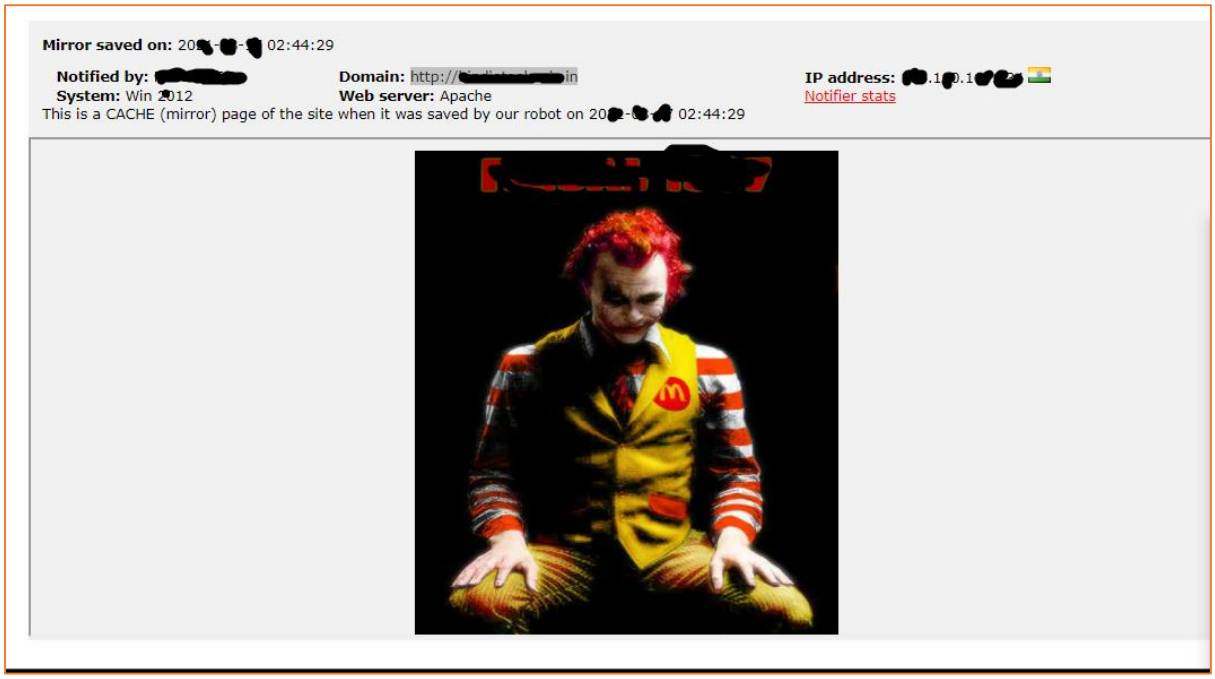
Ensure you complete the mobile activation process and adhere to all guidelines to avoid a delay in procesing your refund.

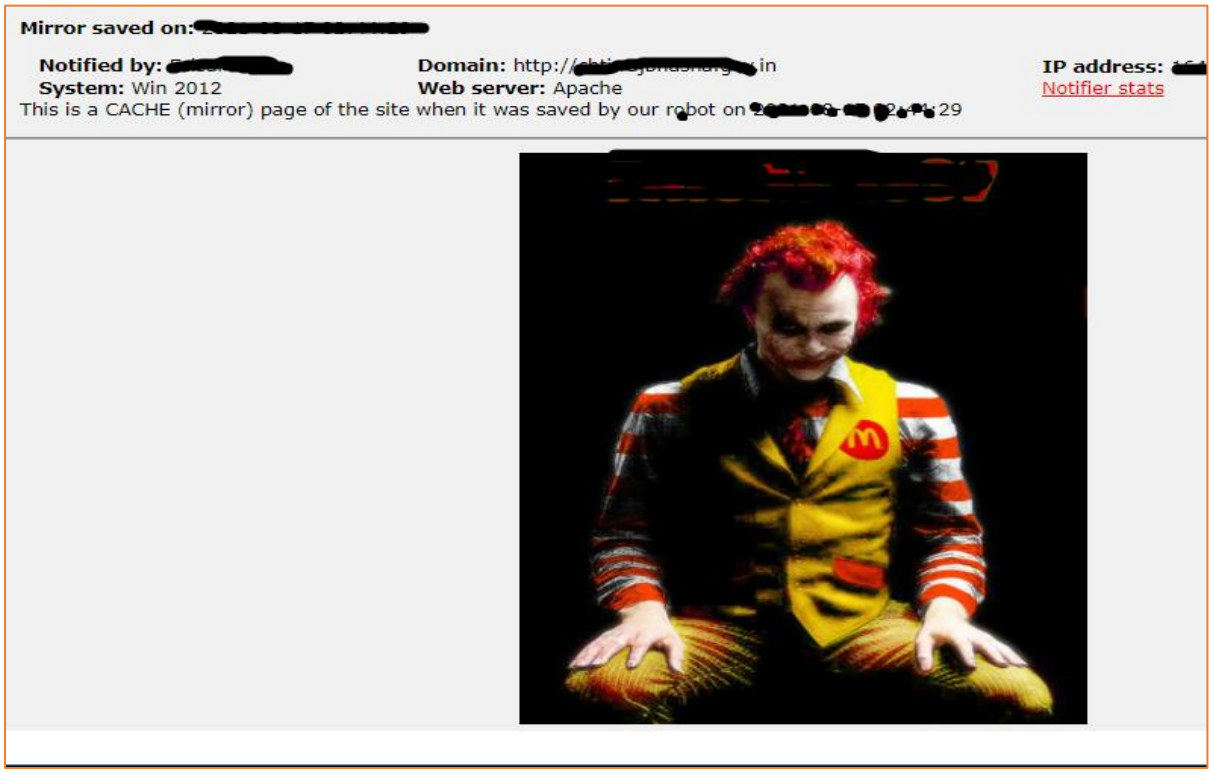
https://mandrillapp.com/track/click/30235690/Incometax.com?p=eyJzIjoiRkdHZ2pMQ1J0a0FhTVlfRHVNY2RQTHB3QXlnIiwidiI6MSwicCI6IntcInVcIjozMDIzNTY5MCxcInZcIjoxLFwidXJsXCI6XCJodHRwczpcXFwvXFxcL2xuY29tZXRheC5jb21cXFwvc2VjdXJlXFxcL0EwXFxcL3NlbmRcXFwvcmVzMTkuaW1nOTc1P2lkPWFtaXNocmEuMjg5MUB5YWhvby5jb21cIixcImlkXCI6XCIxOWRkOTU2ODM2NGQ0MjUxOTFiYTlkYzNmMGIzYzQzN1wiLFwidXJsX2lkc1wiOltcIjU0OTFhMTA3YTA4ZDg0NGFkZmYxYjUyMjYxOTI4ZWE3M2Q5NzIwYjRcIl19In0

Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

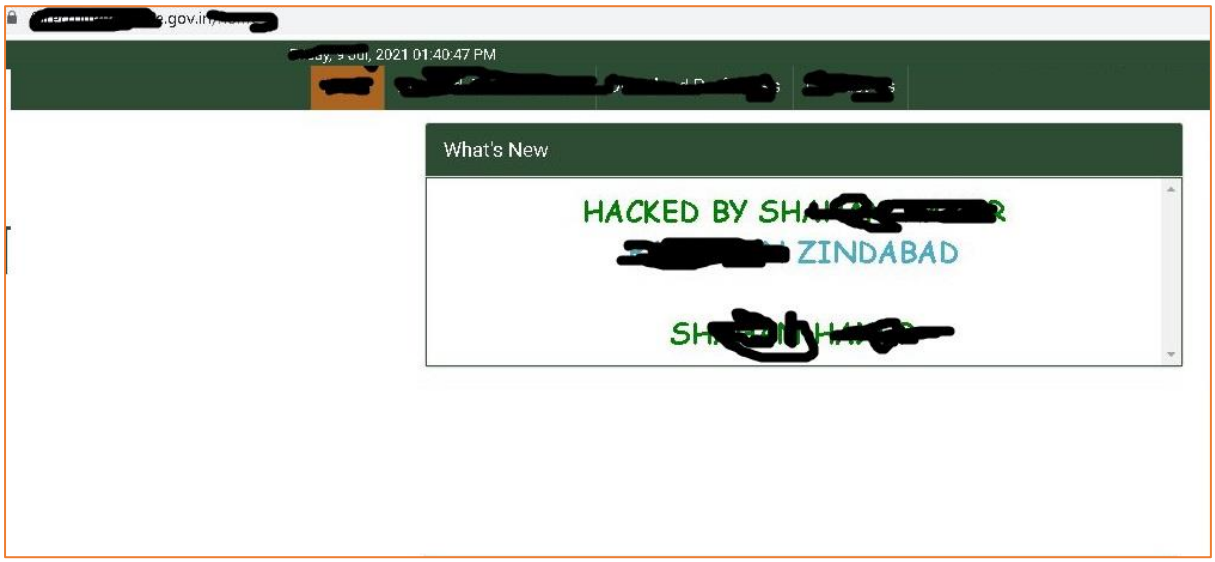
By -R G Singh

#Incident9: Web Defacement (Compromised Website)





By -R G Singh



Question 20: Why this website got compromised? (Perform Root Cause analysis RCA?)

Question 21: When the first time this incident was reported? (Reported by?)

Question 22: Who has compromised the website? (**Log analysis, Firewall log, Database access log, error log, web access log etc**)

Question 23? Whether any data has been stolen? (Data Breach?)

Qustion 24: Was there any vulnerability? (Because many times attacker tris to find out some vulnerability in order to compromise your website)?

Question 25: Suppose some one sees your website is compromise , whom should he report? Do you have any contact number/Email ID (POC) with us? (incident@cert-in.org.in)

Question 26: Who will perform all of the above? (Incident analysis?)

Question 27: What will be your plan after the incident (Post incident plan)

- **What we have to handle:**
    - Contacting with website administrator/owner of the website
    - Find the source of attack
    - Find the cause and vulnerabilities
    - Find the data exfiltereted? Inform to the users.
    - Fixes and patches
    - Sharing of findings

*** Analysis becomes an important task here.