certin
Handling Computer Security Incidents

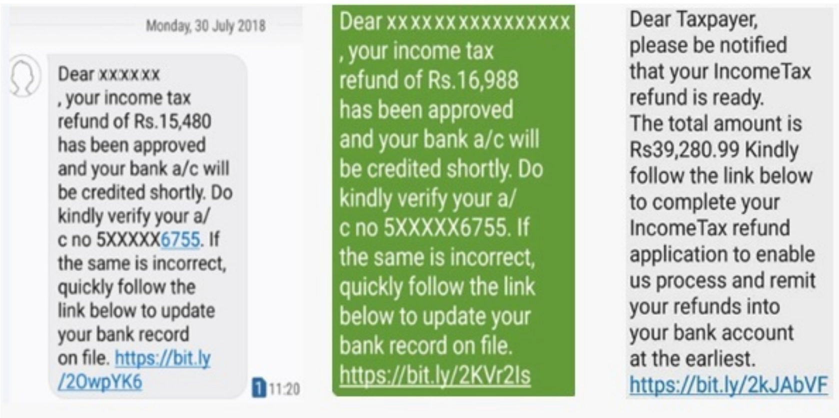
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CURRENT ACTIVITIES

Safeguarding from SMShing income tax refund attacks

Original Issue Date:August 07, 2018

There have been increased reports of incidents related to fake SMS purportedly from Income Tax department as the filing of Income Tax Return nears. This SMShing campaign uses popular URL shortening services such as bit.ly,goo.gl,ow.ly and t.co etc.



Monday, 30 July 2018

Dear xxxxxx
, your income tax refund of Rs.15,480 has been approved and your bank a/c will be credited shortly. Do kindly verify your a/c no 5XXXXX6755. If the same is incorrect, quickly follow the link below to update your bank record on file. https://bit.ly/2OwpYK6

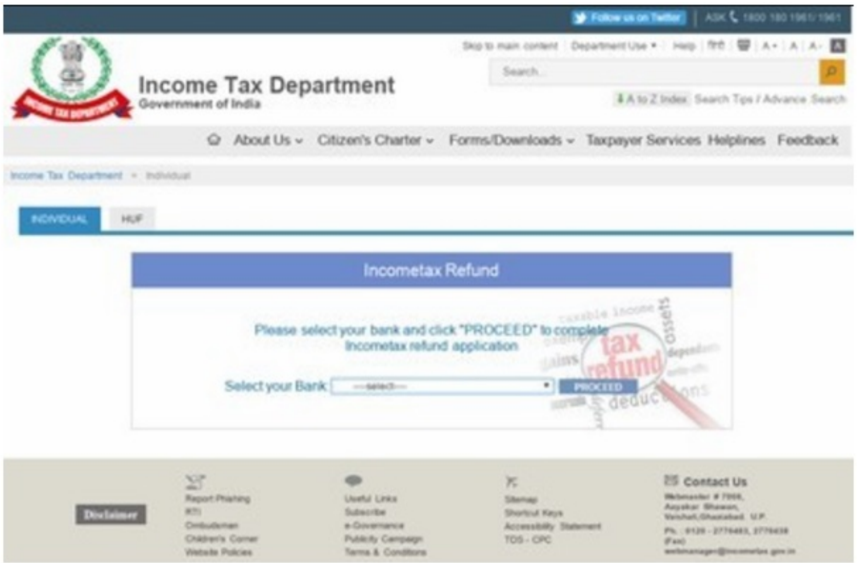
1 11:20

Dear xxxxxxxxxxxxxxxxx, your income tax refund of Rs.16,988 has been approved and your bank a/c will be credited shortly. Do kindly verify your a/c no 5XXXXX6755. If the same is incorrect, quickly follow the link below to update your bank record on file. https://bit.ly/2KVr2Is

Dear Taxpayer,
please be notified that your IncomeTax refund is ready. The total amount is Rs39,280.99 Kindly follow the link below to complete your IncomeTax refund application to enable us process and remit your refunds into your bank account at the earliest. https://bit.ly/2kJAbVF

The message in the SMS tells the recipient that their income tax refund for a certain amount has been approved and will be credited shortly in his bank account. This is followed by an incorrect bank account number. Message reads to the recipient to verify the given bank account number and if found wrong, then visit the shortened bit.ly link given in the message to update his bank record. The bit.ly link is leading to phishing web-pages. Since the bank account number in the SMS is wrong, a number of recipients are enticed to click on the website link. Clicking on the link in the SMS, opens a website which is lookalike to the Income Tax department e-filing website.

The recipient is asked to enter his bank details to complete his income tax refund application and then enter his login ID and password on the next phishing web-page. Therefore, the details entered by the victim SMS recipient are harvested as sensitive data by the cyber criminals running this campaign for a later use in identity-thefts or for putting up for sale on the dark web or for even altering the user's details in the Income Tax Department's records.



Please select your bank and click "PROCEED" to complete Incometax refund application

IOCs:

Phishing Servers

a) IPs:

116.206.105[.]47
50.63.185[.]184
188.42.96[.]48
62.149.158[.]89
31.131.18[.]240
67.227.166[.]88

181.214.31[.]78

b) Domains:

strandgamp[.]com
cdv22[.]com
anmoune[.]com
yalcinsigorta[.]net
bikeme[.]co[.]in
smartcmd0189[.]aruba[.]it
nomadschronicle[.]com

Security Recommendation for Users

In the wake of this scam, users are advised to take diligent best practices to safeguard against disclosing their sensitive details:

- Do not reply to the suspicious SMS and emails. Such social engineering tactics can be identified as these SMS and emails have errors in spelling or grammar errors. Also, the letters in the URL could be jumbled. Even if the SMS or emails came from someone you know, be wary about opening the attachment or click on links. Some malicious emails may be spoofing the sender.
- Do not click on any links. In case if the hyperlink has been clicked then do not enter confidential information like bank account, credit card details etc.
- Do not cut and paste the link from the message into your device's browsers, fraudsters can make the link look like real, but it actually redirects to different websites.
- Use anti-virus software and a firewall for the mobile device and for every other devices used for accessing emails and keep them updated for protection against inadvertently accepting any unwanted files that gets downloaded in the SMShing,phishing links.
- Enterprise IT administrators can roll out group policies which forbid users from enabling macros in Word, Excel, or PowerPoint files originating from outside the company and block known malicious macros, such as the documents used in these social engineering attacks, from running.
- Report any incidents of phishing,SMShing,data theft or data loss to the appropriate stakeholders.

References

https://www.incometaxindia.gov.in/pages/report-phishing.aspx
https://cloudblogs.microsoft.com/microsoftsecure/2017/03/20/tax-themed-phishing-and-malware-attacks-proliferate-during-the-tax-filing-season/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email:info@cert-in.org.in
Phone: +91-11-24368572

Postal Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India