Advisory and Resource Facilitation
National Informatics Centre.
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
IP No 5578
Csg-advisory@nic.in

NIC-CSG/2024-08/502
Dated: 16-08-2024
CVE Ids: Multiple
Severity: High

राष्ट्रीय सूचना विज्ञान केंद्र
National Informatics Centre

Advisory for Phishing Domains mimicking Central Bureau of Investigation

Description:

During cyber investigation below mentioned 2 phishing domains are found mimicking Central Bureau of Investigation (CBI) under Government of India. The phishing campaign is primarily aimed to harvest confidential documents of Indian Citizens like their Aadhar Cards, PAN cards and to gather documents of Indian Citizens like their Aadhar Cards, PAN cards and to gather their financial details to carry out malicious activities in Indian Cyber Space.

1. cbigovins.top/app-in2/
2. cbigovins.site/app-in2/

It is pertinent to mention that there is an “Upload Aadhar Card (JPG)” button which is collecting Front and Back Images of the Aadhar Card and the PAN Card. There is also a “Self-Declaration Form” which is collecting financial details such as Bank Name, Account Number, Mobile banking user id, Credit/Debit card details etc. of Indian citizens so as to carry out malicious activities in the Indian Cyber Space.

In view of above, NIC-Cyber Security Group advises following:

1. In case such a phishing mail is received, do not enter or upload your any personal information/document, when redirected to any upload/login page.
2. Delete these phishing emails from your inbox.
3. In case, you have already clicked the phishing URL and uploaded/submitted your confidential information:
    a. Change your internet banking/mobile banking password - You need to change the passwords for any accounts that might have been hit in the cyberattack.
    b. Turn on multi-factor authentication for the account that might have been attacked.
    c. Review your bank account and credit card statements on a regular basis
    d. Make sure there are no unauthorized transactions
    e. Report any unauthorized transactions immediately
    f. Block your credit/debit card - Your cards can be misused by hackers even if they do not know the PIN.

By following these steps you can effectively mitigate the potential risks associated with clicking on the above-mentioned phishing URL.

Steps to sanitise the system after one has clicked on phishing link:

a. Disconnect from the Internet.
b. Scan your device with anti-virus software.
c. Enable Two-Factor (2FA) Authentication on all critical accounts to add an extra layer of security.
d. Review and Update Security Settings – review the security settings on your digital accounts and devices and ensure that your software and applications are up to date to defend against new threats.
e. Back up your files.
f. Report it to your security team.

Some ways to recognise a phishing email, are given below:

a. Be suspicious of emails that claim you must click, call, or open an attachment immediately or urgently.
b. If a mail received from unknown source, this may be a source of phishing.
c. If an email message has obvious spelling or grammatical errors, it might be a scam. E.g. nlc.in where the first "i" has been replaced by “l”, or gov.in, where the "o" has been replaced by a "0" (zero).
d. Images of text used in place of text (in messages or on linked web pages) may be scam.
e. Be cautious of links shortened by using Bit.Ly or other link shortening techniques.