

Advisory for Phishing Domain mimicking National Investigation Agency

Description:

A phishing URL (<https://nia.gov.in.incidentreports.info>) created on June 10, 2024 is mimicking National Investigation Agency (NIA) under Government of India. The phishing campaign is primarily aimed to harvest the NIC credentials of Government officials, to steal sensitive documents pertaining to Indian government and to get unauthorized access to government servers.

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

1. In case such a phishing mail is received, do not enter your NIC Login Credentials when redirected login prompt appears.
2. Delete these phishing emails from your inbox.
3. In case, you have already clicked the phishing URL
 - a. Take your device offline – Disable your internet connection.
 - b. Change your password - You need to change the passwords for any accounts that might have been hit in the cyberattack.
 - c. Change your passwords from a different device to ensure that the hacker can't access your new information.
 - d. Turn on multi-factor authentication for the account that might have been attacked.
 - e. Back up your files - To protect your data from the phishing attack, back up your files to an external hard drive or USB.
 - f. Scan your device with anti-virus software.
 - g. Update your Operating System, Web Browsers, and other Software with the latest security patches.
 - h. Report suspicious message to your email service provider or NIC designated mail address
 - i. Avoid sharing personal information.

By following above steps, you can effectively sanitize your system and mitigate the potential risks associated with clicking on a phishing URL.

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 E.g. nlc.in where the first "i" has been replaced by "l", or gov.in, where the "o" has been replaced by a "0" (zero).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.