CIS Governance Division
Cyber and Information Security Group,
National Informatics Centre,
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
csg-advisory@nic.in

NIC-CISG/2024-09/515
Dated: 03-09-2024

राष्ट्रीय सूचना विज्ञान केंद्र
National Informatics Centre

Advisory for Phishing Domains mimicking Department of Defence

Description:

Two phishing domains are found mimicking Department of Defence under Ministry of Defence, 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. The domains are:

1. mod.gov.in.aboutcase.nl/publications.html
2. mod.gov.in.army.aboutcase.nl/publications.html

Both the phishing URL's are consisting of a 'Download' button. Upon clicking download button, a login prompt appears which asks NIC credentials of the government officials before downloading of the fake document titled 'Hackers Targeted Defence Personnel in Mass Cyber Attack'. Upon entering NIC login credentials it redirects to a 'login-error.html' page. Further investigations revealed that both the phishing URLs have mirrored original MoD website (www.mod.gov.in) to lure end users into believing they are legitimate MoD websites.

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.