KERALA STATE IT MISSION
Department of Information Technology
Government of Kerala

# ALERT

# Phishing Campaign Targeting Users of email.gov.in

**[CERT-K/2020/ALERT-No: 4]**

## INTRODUCTION

The Indian Computer Emergency Response Team (CERT-In) has issued an alert on a "Phishing Campaign Targeting Users of **email.gov.in**".

## ATTACK METHOD

It has been observed that a phishing campaign targeting users of NICs email service for Government of India (email.gov.in). The campaign involves fraudulent websites spoofing the email.gov.in homepage. The URLs of these websites are also often similar to the spoofed website's URL.

***Examples of Phishing URLs***

Some of the phishing URLs which were active in last few weeks are given below:

1. hxxps://loveindiamail.000webhostapp[.]com
2. hxxps://email-gov.in/indexi[.]php
3. hxxps://safebrowsingindia.000webhostapp[.]com/secure.html
4. hxxps://emalegovin.000webhostapp[.]com/secure.html
5. hxxps://email.gov.in.mailgovin[.]com

The campaign often involves emails pretending to be from NIC asking users to "verify" their account or other such pretexts. The email contains a link to one of the spoofed websites which steal the user's login credentials.

Further, it has been observed that successfully phished email accounts are then used to send malware-containing emails to other sensitive Government organizations and users. These mails contain topical and context-aware content to lure the target into opening the malicious attachment, thus infecting their system. The malware can then create persistence inside the targeted organization's network, and be used for various malicious activities such as stealing sensitive data.

KERALA STATE IT MISSION
Department of Information Technology
Government of Kerala

# ALERT

***Proof of Phishing:***

Dear User,

During current wave of cyber attacks it has been observed that on 15th Aug 2020 someone has tried to login your email account with wrong login details.
However you are advised to verify your Account.
If User failed to Verify Email Account it will be disabled for further usage.

VERIFY YOUR ACCOUNT NOW

The failed attempts are from the following IP addresses/locations:
IP Locations on 15th Aug 2020.
==========
49.15.89.145: India Kerala
49.15.89.145: India Kerala
49.15.89.145: India Kerala
49.15.89.145: India Kerala

Rahul Sharma
Messaging Administrator
Monitoring Informatics Cyber Wing
Note: Please do not reply to this email.
This mailbox does not allow incoming messages.

**Fig: Content of Fradulant phising mail pretending to come from NIC**

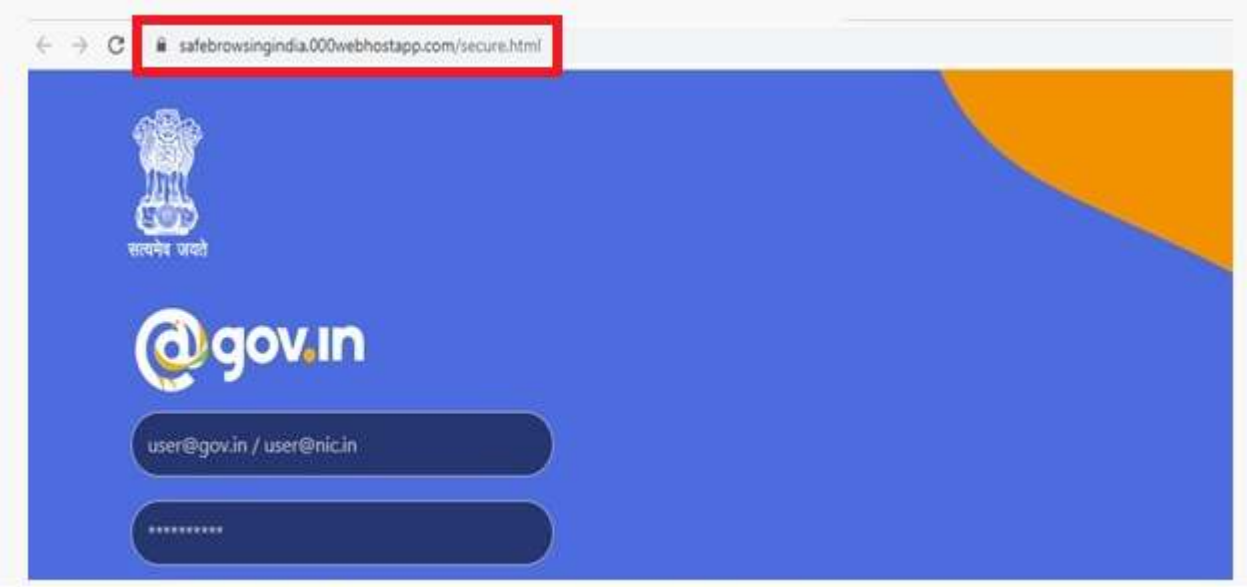


**Fig: Fradulant websites spoofing email.gov.in homepage**

KERALA STATE IT MISSION
Department of Information Technology
Government of Kerala

# ALERT

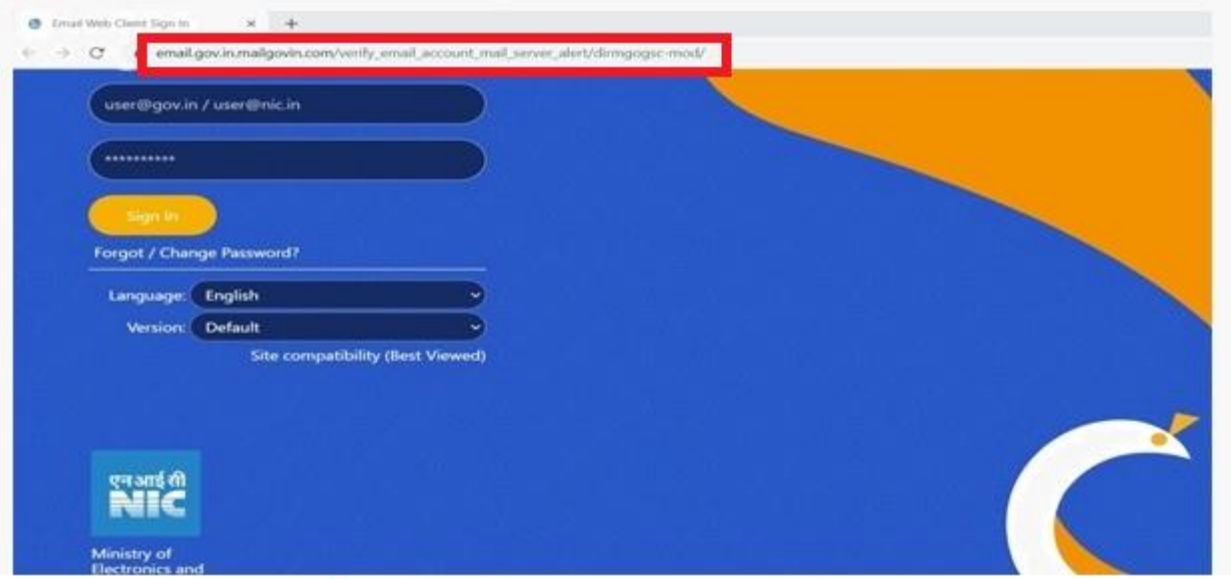


**Fig: Fradulant websites spoofing email.gov.in homepage**

## DOMAINS

- hxxps://loveindiamail.000webhostapp[.]com
- hxxps://email-gov.in/indexi[.]php
- hxxps://safebrowsingindia.000webhostapp[.]com/secure.html
- hxxps://emalegovin.000webhostapp[.]com/secure.html
- hxxps://email.gov.in.mailgovin[.]com

## BEST PRACTICES

1. Always ensure that the URL in the address bar is exactly https://email.gov.in whenever you are entering your credentials for the website. Ensure that no other characters (hyphen, numerals etc.) are present in the URL.
2. Do not open attachments in unsolicited e-mails, even if they come from people in your contact list. Never click on a URL contained in an unsolicited e-mail, even if the link seems benign.
3. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known. Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e. the extension matches the file header).
4. Inform the security team of the organization, if any suspicious mails, files etc. are received
5. In cases of genuine URLs, close the e-mail and go to the organization's website directly through browser's address bar.

# ALERT

6. Leverage Pretty Good Privacy (PGP) in mail communications. Additionally, it is advised to encrypt / protect the sensitive documents stored in the internet facing machines to avoid potential leakage.
7. Check the integrity of URLs before providing login credentials or clicking a link. Do not submit personal information to unknown and unfamiliar websites.
8. Beware of emails and webpages providing special offers like winning prize, rewards, cashback offers etc.
9. Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
10. Update spam filters with latest spam mail contents.
11. If you suspect to have been phished, change the password immediately and inform the mail administrator.

## CONCLUSION

You are advised to follow the best practices to protect your networks and information from similar attacks.

***Note: Any unusual activity or attack should be reported immediately at incident@cert-in.org.in, cert.ksitm@kerala.gov.in with the relevant logs, email headers etc. for analysis and taking further appropriate actions.***