DIR-IFP/20 20 20 21 / 229

Dated: 24 / 06 / 20 20

24/06/2020

IT cell for wide Distribution / Circulation

From: HEAD IT/icfre
To: ALL_USERS
Cc: Assistant Director General Admin/ICFRE/icfre@ICFRE, Deputy Director General Admin/ICFRE/icfre@icfre

Date: Wednesday, June 24, 2020 03:36AM
Subject: Advisory regarding Phishing Attack Campaign by Malicious Actors

---

Dear All Users,

Please go through the Cert-IN Advisory regarding Phishing Attack Campaign by Malicious Actors

Description:

It has been reported that malicious actors are planning a large-scale phishing attack campaign against Indian individuals and businesses (small, medium, and large enterprises).
The phishing campaign is expected to use malicious emails under the pretext of local authorities in charge of dispensing government-funded Covid-19 support initiatives. Such emails are designed to drive recipients towards fake websites where they are deceived into downloading malicious files or entering personal and financial information.
The phishing campaign is expected to be designed to impersonate government agencies, departments, and trade associations who have been tasked to oversee the disbursement of the government fiscal aid. The malicious actors are claiming to have 2 million individual / citizen email IDs and are planning to send emails with the subject: free COVID-19 testing for all residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad, inciting them to provide personal information.
It has been reported that these malicious actors are planning to spoof or create fake email IDs impersonating various authorities. The email id expected to be used for the phishing campaign towards Indian individuals and businesses is expected to be from email such as "ncov2019@gov.in" .

Best Practices

Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
Leverage Pretty Good Privacy in mail communications. Additionally, it is being recommended to encrypt / protect the sensitive documents stored in the internet facing machines to avoid potential leakage
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).
Check the integrity of URLs before providing login credentials or clicking a link.

Do not submit personal information to unknown and unfamiliar websites.
Beware of clicking form phishing URLs providing special offers like winning prize, rewards, cashback offers.

For any suspicious website link or email received, please do not respond and contact servicedesk , ICFRE

Regards

Head
Information Technology Division
ICFRE, PO: New Forest, Dehra Dun 248001
Phone : +91-135-2753099, 2224848(O) 2750297 (Fax)
e-mail: head_it@icfre.org
Website: http://www.icfre.gov.in

Disclaimer:Please do not print this email unless it is absolutely necessary.
This email is exclusively intended for the addressee(s) and may contain proprietary, confidential or privileged information. If you are not the intended recipient, you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately and destroy all copies of this message and any attachments.
Warning: Computer viruses can be transmitted via email. The recipient should check this email and any attachments for the presence of viruses. ICFRE accepts no liability for any damage caused by any virus transmitted by this email.
www.icfre.gov.in