ICMR
INDIAN COUNCIL OF MEDICAL RESEARCH
Serving the nation since 1911

भारतीय आयुर्विज्ञान अनुसंधान परिषद
स्वास्थ्य अनुसंधान विभाग, स्वास्थ्य एवं परिवार कल्याण मंत्रालय, भारत सरकार

Indian Council of Medical Research
Department of Health Research, Ministry of Health and Family Welfare, Government of India

No.18/1/2020-Admn-II

Dated: 14.7.2020.

To

The Directors/Directors-in-Charge of
permanent Institutes/Centres of ICMR.

Subject : Large Scale Phishing campaign regarding.

Sir/Madam,

I am directed to refer a copy of OM No. 4-21/2017-IC/E.IIIA dated 28.11.2019 on the subject mentioned above issued by the Ministry of Finance, Department of Expenditure, New Delhi for information and necessary action.

Yours faithfully,

14/07/2020

(Jagdish Rajesh)
Asstt. Director General (Admn.)

Encl: As above

Copy to:-

1. PS to DG/PS to Addl. DG/PS to Sr. DDG (A)/PS to Sr. FA
2. All Divisional Heads
3. Dy. Director-General (Admn.) /ADG(A) 1/II
4. Dr. L.K.Sharma, Scientist 'E' – soft copy of the same has been mailed at your email ID(sharma.lk@icmr.gov.in) for website upload.

Sr. DDG (A) Office
Dy. No. :..798.....
Dated :..30/6/2020...

File number T-21016/128/2020-eHealth
Government of India
Ministry of Health and Family Welfare
eHealth section
*****

Nirman Bhawan, New Delhi
23rd June 2020

Subject:- Large Scale phishing campaign regarding

A reference has been received stating 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.

2. 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 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.

3. A copy of the Advisory is enclosed. All Senior Officers are requested to kindly take necessary action as per Advisory and issue the instructions to the staff/ Attached/ Subordinate offices and Autonomous Institutions.

Dr. Sachin Mittal
Director (eHealth), MoHFW 06/7/2020
01123063523

To

All Senior Officers, DoHFW/ Secretary (DHR)/ Director General, Dte. GHS
All officers and Staff, MoHFW (Through eOffice Notice Board)

p. circulate to
Heads / Directors
[redacted]

GM
26/6

ADG I
for 30/6

ADG II

30/6

5.0 (Admin-I)

CERT-In Advisory CIAD

COVID 19-related Phishing Attack Campaign by Malicious Actors

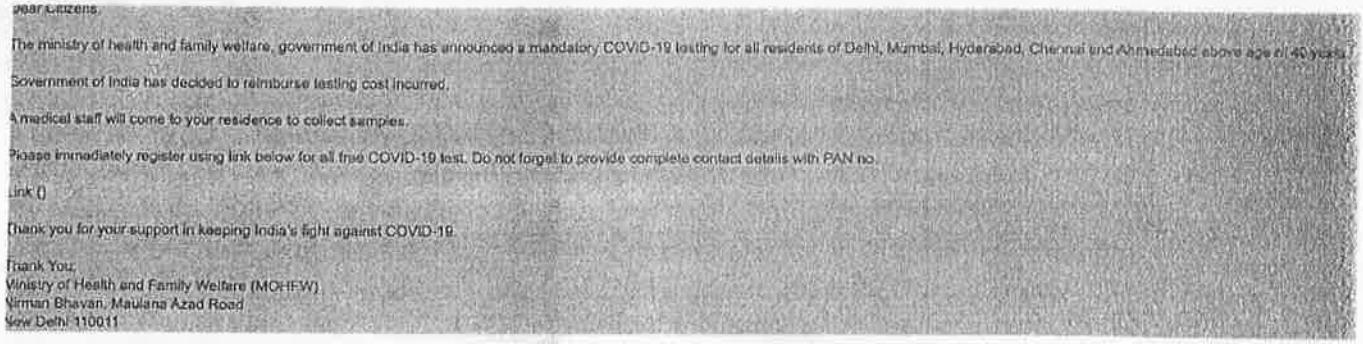
It has been reported that malicious actors are planning a large-scale phishing attack campaign against Indian individuals and businesses (small, medium, and large enterprises).

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.

Description

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" and the attack campaign is expected to start on 21st June 2020.The email may look as follows:



Dear Citizens,

The ministry of health and family welfare, government of India has announced a mandatory COVID-19 testing for all residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad above age of 40 years.

Government of India has decided to reimburse testing cost incurred.

A medical staff will come to your residence to collect samples.

Please immediately register using link below for all free COVID-19 test. Do not forget to provide complete contact details with PAN no.

Link ()

Thank you for your support in keeping India's fight against COVID-19.

Thank You,
Ministry of Health and Family Welfare (MOHFW)
Nirman Bhavan, Maulana Azad Road
New Delhi 110011

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, advise the users 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). Block the attachments of file types, "exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf"
- Beware about phishing domain, spelling errors in emails, websites and unfamiliar email senders
- 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.
- Consider using Safe Browsing tools, filtering tools (antivirus and content-based filtering) in your antivirus, firewall, and filtering services.
- Update spam filters with latest spam mail contents
- Any unusual activity or attack should be reported immediately at incident@cert-in.org.in. with the relevant logs, email headers for the analysis of the attacks and taking further appropriate actions

References

- https://www.cyfirma.com/early-warning/global-covid-19-related-phishing-campaign-by-north-korean-operatives-lazarus-group-exposed-by-cyfirma-researchers/
- https://zeenews.india.com/india/north-koreas-lazarus-hackers-plan-phishing-attack-in-india-to-steal-covid-aid-2290701.html