DIRECTORATE GENERAL
CENTRAL INDUSTRIAL SECURITY FORCE
(MINISTRY OF HOME AFFAIRS)

BLOCK-13, CGO COMPLEX,
LODHI RAOD, NEW DELHI

No.E-32099/4/CYBER ALERT/EDP CELL/39741/2020-1265-(E) Dated : 21-06-2020

To,

ALL SECTOR ISG
DIRECTOR NISA HYDERABAD

Subject :-**CYBER ALERT:REG.**

It is submitted that Computer Emergency Response Team-India(CERT-In) has issued an advisory regarding a potential cyber offensive attack from the Chinese Army. In the guise of a Free Covid-19Test, Chinese cyber warriors could be carrying out a massive phishing attack. Watch out for IDs like * ncov2019@gov.in*. Beware of Malicious Phishing E-mails/ SMS/ Messages on Social Media inciting you to provide personal and financial information.

Key Points

i. Phishing campaign is expected to impersonate government agencies, departments and trade associations who have been tasked to oversee the disbursement of the government fiscal aid.

ii. Spoofed Email ID which could be used for the phishing email is expected to be **ncov2019@gov.in**.

iii. Phishing E-mail Subject Line: **Free Covid-19 testing for all residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad.**

iv. The malicious group claims to have 2 million individual email addresses and the attack campaign is expected to start on June 21.

Preventive Measures

i. Don\'t open or click on attachment in unsolicited e-mail, SMS or messages through Social Media.

ii. Exercise extra caution in opening attachments, even if the sender appears to be known.

iii. Beware of e-mail addresses, spelling errors in e-mails, websites and unfamiliar e-mail senders.

iv. Do not submit personal financial details on unfamiliar or unknown websites / links.

v. Beware of e-mails, links providing special offers like Covid-19 testing, Aid, Winning prize, Rewards, Cashback offers.

vi. Check the integrity of URLs before providing login credentials or clicking a link.

vii. 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.

viii. 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.

ix. 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.

2. In view of all of the above, it is therefore requested to direct all units under your administrative control regarding potential cyber offensive attack/ Phishing attack campaign to strictly adhere to preventive measures suggested as above and also to educate and spread awareness amongst all force personnel and their family members through regimental activities like Sainik Sammelan, Daily briefing session etc so that it can be fully avoided.

3. It is seen that, a well educated/ aware person is likely to be less prone in falling prey to such kind of cyber attacks. Therefore, it is hereby once again requested to educate/ spread awareness amongst all force personnel regularly/ daily on the above mentioned points and preventive measures.

Digitally signed by
B S N REDDY,
SR. COMMANDANT/AIG TECH,
FHQ NEW DELHI,
21-06-2020

Copy to:-

1. PS TO DG CISF - FOR KIND INFORMATION OF DG/CISF PLEASE
2. PS TO SDG/APS - FROM KIND INFORMATION OF SDG/APS PLEASE
3. PS TO ADG (HQRS) - FOR KIND INFORMATION OF SDG/HQRS PLEASE
4. ALL BRANCHES OF FHQ