West Bengal State Electricity Distribution Company Limited
(A Government of West Bengal Enterprise)
Bidhan Nagar, Block-DJ, Sec-II, Kolkata-700091
Website: www.wbsedcl.in,
CIN: U40109WB2007SGC113473

Cyber Security alert for COVID 19-related Phishing Attack Campaign by Malicious Actors

It is submitted that **Computer Emergency Response Team-India (CERT-In)** has issued an advisory regarding a potential cyber offensive attack 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.

Best Practices

- **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.**
- 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.
- 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 personnel regularly/ daily on the above-mentioned points and preventive measures.

End of Document