CENTRAL WAREHOUSING CORPORATION
(A GOVT. OF INDIA UNDERTAKING)
4/1 Siri Institutional Area, Hauz Khas, August Kranti Marg,
New Delhi-110016 **Email : warehouse@nic.in**
Tel: 26602576, 26566107

NO. CWC/MIS-Gen/Email Security/2019-20 **Dated 02-08-2019**

CIRCULAR

Subject : Advisory on safety precautions for email frauds and Digital Signature Certificate – reg.

1. Email Frauds

Instances of email frauds or phishing or cybercrime have come to our notice, wherein emails are often sent out in mass, tricking the user in providing personal information, bank account details or to make funds transfer to the fraudulent account. Following are some of the widely email frauds/cybercrime:-

a) Often cyber criminals send an email to a lower level employee typically someone who work in Account or Finance Department, while pretending to be senior executive, the goal of such attack is to get their victims, to transfer fund to a fake account.

b) Sending offensive messages to friends and relatives or asking for some ransom.

c) Sending phishing emails, purportedly from genuine email accounts, but actually fake. The email may contain links that prompt to visit a page for updating your password and other credentials on the pretext of some system update, data loss, technology upgrade, regulatory compliance, etc. The links will direct you to a fake page where, once you enter your login ID and password, the same get stealthily stolen by the fraudsters.

d) Sending you unsolicited/spam mails containing attachments that have malwares/viruses embedded in them. Once such emails are opened and attachments activated the malware/virus gets discreetly downloaded and installed on your device. The malware could be a key logger that captures and sends all keyboard taps to the fraudsters, which includes your account passwords. The other possible malwares/viruses could be ones that capture screenshot or read and transmit saved passwords.

CENTRAL WAREHOUSING CORPORATION
(A GOVT. OF INDIA UNDERTAKING)
4/1 Siri Institutional Area, Hauz Khas, August Kranti Marg,
New Delhi-110016 **Email : warehouse@nic.in**
Tel: 26602576, 26566107

Following preventive measures/precautions are suggested to keep your email account safe as far as possible:

a) Do not open SPAM mails or e-mails sent from unknown senders. Do not click on any link sent on such mails.

b) Be cautious while opening links sent in unsolicited e-mails, even if they are sent from someone in your contact list. Such known contacts email account may have been compromised and thereafter, used to send malicious codes to unsuspecting contacts.

c) Do not click on attractive and tempting links sent over a WhatsApp message or routine SMS. They may lead you to malicious pages and cause malware intrusion on your system/device. Hackers use social engineering to trick you in clicking links. Don't fall for it.

d) Don't disclose your password to anyone and keep changing it at regular intervals (2-4 months).

e) Keep your e-mail password long and difficult. Password should have at least 8 characters and there should be at least one upper-case, one lower-case, one numeral and one special character in your password.

f) Don't store your passwords in your device (phone/tablet). Anyone getting access (physical or remote) to your device will easily get to know your passwords.

g) Always have a lock screen on your smart phone, tablet, laptop, etc protected by a PIN or password. Do not keep your device open and unattended, even for a minute, especially in public work place.

h) All employees should use CWC email id (xxx@cewacor.nic.in) for communication. In case any employee does not have CWC email id, the same should be created within a week's time by sending request at warehouse@nic.in. The request format, password policy and user manual are available on CWC website, under MIS Division circular.

i) It has also come to our notice that email id of Senior Officer are being used by Junior Officials for sending mails. This should be stopped forthwith.

2. Action to be taken in case wrong opening of SPAM/ phishing email :-

a) Change the password immediately as explained at point number (d) and (e) above.

b) Contact MIS Division, CO to temporarily block the email account for preventing its misuse by hacker.

c) Send email messages to all your contact from your alternate email account requesting and alerting them to not to respond to emails coming from hacked email.

d) Write to all service providers that your hacked email account is given as communication mail, to not to entertain any request from the compromised email account without secondary manual check with you, over the alternate mode of communication.

e) It is also suggested to lodge complaint with cyber crime cell of nearest police station, in case of email cyber attack as enumerated at sr. no.1 on page no.1.

f) The devices like desktop, laptop, mobile should be updated with latest Antivirus/Anti-Malware .Deploy Firewall/UTM on internet gateway for preventing malwares over Local Area Network.

3. Digital Signature Certificate (DSC):-

As per the IT Act 2000 and subsequent amendment, Digital Signature certificates are considered at par with ink signature. The Digital Signature certificates have varied use in electronic transaction and therefore at most precautions should be used in its operation. Following are the do's and don'ts:-

a) Do not share your Digital Certificate with anyone including e-procurement service provider.

b) Do not reveal your DSC password to anyone.

c) Use the DSC only for Authorized and Legal purposes.

CENTRAL WAREHOUSING CORPORATION
(A GOVT. OF INDIA UNDERTAKING)
4/1 Siri Institutional Area, Hauz Khas, August Kranti Marg,
New Delhi-110016 **Email : warehouse@nic.in**
Tel: 26602576, 26566107

d) Tender committee members should use their own DSC for opening of technical and price bid.

e) Loss of DSC:-

In case, the DSC is lost or misplaced, FIR should be lodged by the concerned employee. MIS Division, CO, should be informed immediately with a copy of FIR for deactivation of service in e-procurement portal. Effort should be made to obtain another copy of DSC from the DSC provider and till such period the date of opening of Tenders in which he/she has already been assigned the role of Bid Opener will have to be extended, if required. In case it is not possible to procure the DSC due to any reason, then the Tender, which are yet to be opened may have to be cancelled and re-tendered, if other bid openers also fail to open the bid.

This issues with the approval of Competent Authority for compliance.

2/8/19.

(A.M. Rao)
GM (System)

Copy to:

1. All HoDs, CWC, CO, New Delhi, for information and necessary action.
2. All RMs, CWC, ROs, for further circulation and necessary action as above.
3. Sr. PA to MD/ PS to Dir. (M&CP)/ SAM to Dir. (Fin.)/ PS to Dir. (Pers.)/ PA to CVO, CWC, CO, New Delhi, for information please.
4. MIS Division, CWC, CO, New Delhi, for arranging to upload on the CWC's website.