I/3052215/2022

भारत सरकार Government of India
रेल मंत्रालय Ministry of Railways
(रेलवे बोर्ड) (Railway Board)
****

CIRCULAR

NATIONAL CYBER SECURITY AWARENESS MONTH-OCTOBER 2022

The Month of October is globally observed as the National Cyber Security Awareness Month (NCSAM), with an aim of increasing Cyber Security Awareness among the public and private sectors, which in turn will enhance the overall cyber resilience of the nation.

2. The theme for NCSAM 2022 is *"**See Yourself in Cyber**"* which demonstrates that while cyber security may seem like a complex subject, ultimately, it's really all about people. This October therefore, we will focus on the "**People**" part of cyber security.

3. A dedicated webpage for October-NCSAM (cert-rail.railnet.gov.in/CSAM-2022.asp) is being created on the CERT-Rail Website by Railway Board Computer Centre. This webpage is accessible only on intranet' (i.e. Railnet) from 1st October 2022. Information will be provided for awareness and safeguarding, which can be accessed through the links directly from the website. NSCS has indicated the broad areas for creating awareness as indicated below:

(a) Enable Multi-Factor Authentication • Text Message (SMS) or Email • Authenticator App • Push notification	**(b) Use Strong Passwords** • Password shall contain more than 8 characters. • Password shall be a combination of upper, lower case characters, digits, punctuation characters and other characters • Never use common information in your password. • Never use the same password twice. • User shall be required to change their passwords periodically
(c) Recognise and Report Phishing/ Smishing/ Vishing • **Phishing** is a method of cyber attack that attempts to trick victims into clicking on fraudulent links in emails. The link typically takes the victim to a seemingly legitimate form that asks them to type in their usernames, passwords, account numbers or other private information. • **Smishing** is a kind of fraud similar to phishing, except that it comes in the form of a text message. A smishing text will often contain a fraudulent link that takes victims to a form that's used to steal their information. • Fraudulent calls or voicemails fall under the category of **"vishing"** Scammers call potential victims, often using prerecorded robocalls, pretending to be a legitimate company to solicit personal information from a victim.	**(d) Do not fall into any financial fraud trap.** **Ponzi-schemes** • Investment schemes that promise to pay relatively high rates of returns for fixed term investments. • They are fraudulent investment plans - money is not invested at all. **Identity fraud** – Someone impersonates you and uses your personal information to steal money. Identity fraud is common on Internet. **Card Fraud** • Starts with the theft of your bank card. • Stolen /loss cards remain usable. • Thieves make unauthorized purchases with the card until you notify your bank. **Skimming** – This involves stealing information off a credit card during a legitimate transaction. • Fraudsters swipe the card through an electronic device known as a "wedge" or "skimming device" which records all information contained on the magnetic strip. **International lottery fraud/Fake prizes** • A perpetrator claims that you have won a non-existent prize.

(e) **Update your Software**	(f) **Be cyber security aware on Social Media.**
• Software and application updates contain important security fixes that can help keep your devices safe from cyber criminals.	• Lock Down Privacy Settings • Use Text Messaging to Prevent Unauthorized Logins • Be Discreet about Your Whereabouts • Avoid (and Report) Duplicate Friend Requests • Don't Use Social Credentials to Sign Into Third-Party Sites • Avoid Quizzes and Games that Require Access to Profile Information • Handle Passwords With Care • If You Have Kids, Pay Attention to Their Accounts as Well
Note: In case of any suspicious activity is noticed in the system, kindly inform the Helpdesk (Computer Complaints).	

All are, therefore, requested to regularly check the latest updates on the CERT- Rail Website, which would enable safe and secure working in the cyberspace.

Signed by Bharat Bhushan Harit
Date: 28-09-2022 10:59:26

(Bharat Bhushan Harit)
JDME (C&IS)

2022/RBCC/7/7/Misc. Activities Dated: 28.09.2022

All Officers and Branches in Board's Office and at Dayabasti, New Delhi.

Copy for information to:-

PS/EDPG to MR/MOSR(D)/MOSR(J)
PSOs/PPSs to CRB & CEO, M/O&BD, MF, M/TRS, and M/Infra
Secretary/Railway Board