महाप्रबंधक बिक्री एवं विपणन/आई.टी./बी.पी.
छठवीं मंजिल, बी विंग ,प्रशासनिक भवन जुहू रोड,
सांताकुज़-पश्चिम 400054
General Manager (S&M/ITBP) 6th Floor, B-Wing,
Administrative Building, Juhu Road, Santacruz(W),
Mumbai-400054 Tel: 022 26613072
suhasmankar@bsnl.co.in

BSNL
Connecting India faster

भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)

To,
All BA/SSA Heads,
Maharashtra Telecom Circle.

No: MHCO-IT/12(19)/1/2020-O/o GM IT **Dated:22.04.2021.**

Sub:-Regarding compromise of Computers by Cyber Threat Actors.
Ref: 1.BSNLCO-CIT/20(25)/2/2020-CIT Dated:05.04.2021.
2.MHCO-IT/12(19)/1/2020-O/o GMIT Dated:09/04/2021.
3. MHCO-IT/12(19)/1/2020-O/o GMIT Dated:26/03/2021.

With reference to above cited subject and guidelines issued time to time vide letters under reference, regarding cyber threat actors to compromise the computers. Some of the very common tactics, techniques and procedures adopted by cyber threat actors to compromise the computers like Spear phishing mail, evading the traffic analysis, Exploiting web application vulnerabilities, Creation of dubious Apps, DDoS etc. The best practices that are to be followed at the organization level and at individual's level to mitigate the cyber security threats.

Further, in view of the current situation of COVID-19, many offices have adopted work from home (WFH) concept, where unsecured home computers are extensively used to connect to the organizational/office network. To mitigate the cyber security threats emanating from WFH, users may follow best practice enclosed in Annexure.

In case any infected device observed in organization's network, following action are to be initiated immediately.

1. Immediately disconnected infected device (computers/Laptops) from Network.
2. Take Forensic image of infected device (computers/Laptops) and keep in safe custody.
3. Remove all unused data/software from computer/Laptop particularly remote desktop software, if any.
4. Infected device should be formatted after taking back up of data files & forensic image as above.
5. OS & application should be re-installed from clean software's.
6. Ensure availability of security software available in device.

It is requested to adhere to above Best Practices to keep the cyber security threats at bay.

Encl: Annexure.

(Suhas Mankar)
General Manager (IT)

Copy to: Sr GM(CIT), Corporate Office for kind info pl.

ANNEXURE

Best practices – Cyber Security (User level)

- Always use **genuine software.** Install the latest updates/ patches for Operating System, Antivirus and Application software.
- **Limit user privileges** on the computer. Always access Internet as a standard user but not as Administrator.
- **Restrict remote access.** If file sharing is not required in your day-to-day work, disable file and print sharing.
- Be wary of **storing personal information** on various Social Media and other platforms.
- **Do not share financial details,** e-wallet details or banking details with anyone.
- Beware of **unsolicited contacts from individuals** in person, on the phone, or on the Internet who are seeking organizational or personal data
- **Do not share usernames,** passwords, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.
- **Do not provide information about yourself** that will allow others to answer your security questions- such as when using "I forgot my password" feature. Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends and co-workers on Social Media platforms.
- **Check and verify email** sender IDs and web links before opening file attachments and clicking on links in emails and web pages.
- Be **cautious of tiny URLs** in Email contents.
- **Do not open attachment** having extension: VBS, U64, SHS, PIF, SCR.
- **Protect against social engineering attacks.** Phishing emails and SMS are used to get user credentials like username, passwords, credit card and PIN numbers etc.
- Regularly **check the last log-in details** of emails accounts.
- **Internet-connected computers should not be used for drafting storing classified official documents / correspondences.**

*****