



To,

All CGMs
All Telecom Circles/Metro Districts,
Maintenance/Project Circle
Other functional Units

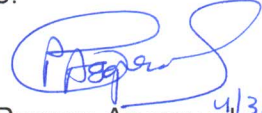
No. 8-8/2008-IT/Vol-III

Dated: 04-03-2013

Subject: General safety tips and Safety tips on using E-mail - (Security aspects on Information Technology).

In light of the recent IT Security incidents that have happened in BSNL, the "General safety tips and Safety tips on using E-mail" are enclosed as annexure. These may be followed by all employees of BSNL.

Necessary action may be taken at your end to circulate the General safety tips and Safety tips on using E-mail and hence to increase the awareness.


Raman Aggarwal 4/3/13
Additional GM (CIT)

Enclosed: General safety tips and Safety tips on using E-mail

Copy to:

2. Office Copy
3. CMD BSNL for favor of kind information please.
4. All Directors BSNL CO for favor of kind information please.
5. All PGMs, Sr GMs, GMs BSNL CO for circulating the General safety tips and Safety tips on using E-mail to all the staff working under them so as to make them aware about IT security aspects.



Annexure

General safety tips

- 1) The sensitive information / data should not be shared with unknown / unauthorized person.
- 2) The contact details of officers at key locations should not be shared with unknown / unauthorized person.
- 3) The mails from unknown / unauthorized persons should not be opened.

Safety tips for using Email

- 1) **Avoid Exposure of email account details**
While opening an email account, do not expose your account details such as name and password to unauthorized/ unknown persons. Ensure that nobody is watching you behind while entering your password. Exposing email account details (such as name or password or both or part of the password) may give way to intruders to hack the email account by guessing password or some password cracking tools.
- 2) **Avoid Unauthorized Disclosure of email contents**
Read email only when it is necessary to avoid exposure to third party or unauthorized persons. Many times the content of an email will contain private or confidential data, so to avoid any type of invasion of privacy, be sure to be cautious of your surroundings and never leave a computer unattended. Lock the computer if having to leave it for any length of time.
- 3) **Avoid clicking web Links in email messages**
Avoid clicking or opening web links or program unchecked in email messages. Following the web links or programs that may be part of an email message may lead to secretly installation a malware (e.g., virus) on the computer.
- 4) **Install Anti-virus software**
User should Install latest Anti-virus software and Anti-spyware, and keep them updating time to time. Anti-virus software helps to protect computer against known viruses. User can detect and remove the virus before it can do any damage to the computer. Attackers are continually writing new viruses, it is important to keep antivirus software up-to-date. Anti-virus software such as AVG, Norton Internet Security, Trend micro, Quick Heal etc is good options. User should not install multiple (more than one) anti-virus software, as multiple installations may give scanning results against each other.
- 5) **Cautious with email Attachments**



- a) Use caution when opening email attachments, even if they appear to have been sent by a known person. Email attachments are a common source of spreading malware such as Virus, Worm and Trojan horse. Some malware can "spoof" the return address, making it look like the message came from some known source. Take the following precautions:
 - b) Do not open an email attachment If it seems suspicious, even if the scanning result indicates that the attachment is clean because that anti-virus software may not have the signature as new viruses are constantly being released.
 - c) Open attachments that come from a trusted source only (not unsolicited email) as many viruses, worms, and Trojan Horses have been known to attach themselves on to them. Opening an infected email attachment may damage or harm the computer.

- 6) Scan an email attachment before opening/downloading
 - a) Scanning email attachment before opening or downloading minimizes the risk of downloading malware (e.g., virus). Opening or Downloading attachment without scanning may damage the computer if it is infected.
 - b) Disable the option to automatically download attachments, if this option is already enabled in the email software.

- 7) Use Encryption for Sending and Receiving Confidential email
 - a) Send and receive confidential or sensitive messages using encryption to ensure that message can only be read by the intended recipients.
 - b) Some messages are too sensitive and confidential. User should use encryption for sending sensitive messages. Email Encryption is used to ensure that both sensitive and personal information cannot be seen by anyone other than the intended recipient.
 - c) Email encryption is a process where the actual body is coded using an encryption key. An e-mail message appears either blank or with a block random combination of integers and alphabets. It is intended for confidential information between the sender and recipient.
 - d) There are few tools and techniques of encryption. Pretty Good Privacy (PGP) is one of the tools to encrypt email messages. The other tools/techniques include public-key encryption like the Secure Sockets Layer (SSL) to encrypt data and PEM Privacy Enhanced Mail) for encryption, authentication, and certificate-based key management.
 - e) The encryption process is as follows. There are two keys: Private Key and Public Key. The sender and the recipient both need to have Private Key and Public Key in the form of a Digital Signature, a PGP key, or the open version of PGP (Open GPG) key. Both sender and recipient need Public key in each other's repository. The repository is like a key-chain. First step is to exchange each other's public keys between sender and recipient through a signed (but not encrypted) e-mail and import keys into repository. After getting the each



other's public keys and putting into repository, create an e-mail as usual and select Encrypt ("Encrypt this to myself,") from the security options and then send the email. The email is encrypted (using a combination of sender's Private key and recipient's Public key) and then sent to the recipient. When recipient gets the email, the indicator at the recipient's email shows whether or not the e-mail has been tampered with or the certificate is valid (typically a green or red icon in the header). As long as the recipient has the sender's Public key in repository, the e-mail will appear normal, otherwise it will be blank page.

- 8) Do Not respond Suspicious/Banking-related emails
 - a) Many suspicious emails are being sent and forwarded to many email accounts for collecting information. Do not respond or follow such emails.
 - b) Emails regarding updation of bank account details or winning lottery or emails from persons (e.g, Nigerians) requesting bank account details for transferring a big amount of money (million dollars) to your account. These are **phishing emails** and are sent from malicious people with intent of collecting bank account details to transfer money from your account to their account. Do not respond/follow such email messages, instead delete them. Keep in mind that bank never sends email messages to any customers/clients asking updation of account details.
- 9) Do Not Open Unknown emails
Lot of emails are received from unknown sources/people for advertising, marketing or any other purpose. They are all junk and often frustrating, unsolicited and unwanted emails called **Spam**. Do not open/respond such emails, instead delete them.
- 10) Enable Spam Filter
Set a Spam filter to reduce "junk" emails that could be part of a potential phishing scam or malware. Enabling spam filter can automatically eliminate a large portion of the risk.
- 11) Keep Strong Password
Keep a strong password so that it is difficult to guess by a third party. A strong password should have a minimum of eight characters, comprising a combination of alphabets (both upper and lowercase), numbers and symbols/special characters, and be as meaningless as possible.
- 12) Do not keep Computer Unattended
Never keep computer system unattended so that unauthorized persons will not have an opportunity to alter any file or information or do mischievous. Always lock/ shutdown the computer when not in use.