Dear MTNL Customer,

Kindly find the following advisory regarding the Malicious e-mails in circulation which has been reported to intending target the computers of Telecom Service Providers/internet service providers and customers.

You are requested to follow the advisory from the Department of Telecommunications attached.

It is, therefore, advised to initiate the following step immediately for preventing and limiting any possible damage from such offensives;

1. Officers/official are also advised not to open any mail from unknown source/ any suspicious mail and not to download/save/open any attachment without scanning virus;
2. Not to open attachments having extension EXE, DLL, VBS,U64,SHS,PIF (typical examples: txt.exe, doc.exe);
3. Not to click any URL mentioned in the body of any email text unless one is assured of the identity and credentials of the sender;
4. To disable the option: (view->layout->uncheck->' show preview pane') as some malicious programs start executing as soon as they appear on the Outlook Express preview pane;
5. Not to use officials e-mail IDs to subscribe internet services like RSS, feeds, blogs, groups, social networking sites etc;
6. Not to open any files attached to an e-mail if the subject matters appears questionable or unexpected, notwithstanding e-mail originating from known source/e-mail ID;
7. Not to leave an e-mail account unattended once logged on, unless password protected screen saver enabled on the system;
8. Officers/official are also advised not to use private e-mail for official purpose, All official information is sent through NIC e-mail accounts only. Not to use personal e-mail ID for official communications;
9. Do not forward chain/junk e-mails;
10. To set MS Word application macros security to High;
11. To minimize exposure of e-mail addresses in public domain (websites/ blogs etc) unless official work related to public interaction.