SCHOLARS
INDIAN SCHOOL

Email Security

- Use e-mail filtering software to avoid spam so that only messages from authorized users are received. Most e-Mail providers offer filtering services.
- Do not open attachments coming from strangers, since they may contain a virus along with the received message.
- Be careful while downloading attachments from e-Mails into your hard disk. Scan the attachment with updated antivirus software before saving it.
- Do not send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. We can use Rich Text Format instead of the standard .DOC format. RTF will keep your formatting, but will not include any macros. This may prevent you from sending virus to others if you are already infected by it.
- Avoid sending personal information through e-Mails.
- Avoid filling forms that come via e-Mail asking for your personal information. And do not click on links that come via e-Mail.
- Do not click on the e-Mails that you receive from untrusted users as clicking itself may execute some malicious code and spread into your system.