

Email Security Practices

Internet users may be advised to follow the basic email security practices mentioned below:

1. Not to open/reply email links (hyperlinks/web links/URLs mentioned in the body of such mails) claiming to offer anti-spyware software. The links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
2. Scan mail attachments before downloading / opening.
3. Use different email accounts for personal and professional purposes.
4. Periodically check last log-in activity for any unauthorized access.
5. Change passwords of all their online accounts (emails and others) from another secure computer, if any suspicious activities like email access from foreign IP addresses, etc. are noticed.

NIC Mail Usage

1. Do not open emails or attachments from unknown email IDs.
2. Check for any shared folder under Preferences option in NIC mail. If any shared folder is found, disable it immediately.
3. Check Login History for account access details.
4. Don't save login credentials in browser and logout, once the session is over.
5. Enable Kavach on all NIC Email accounts.