Secure Surfing – Some Pointers

09-May-2017

Internet Banking – Dos and Don’ts

- Look for https in the Address bar
- Look for a lock symbol in the screen
- Check the URL i.e., the website address clearly
- Look for site certification details
- When clicked, a box showing the web certification details would pop up
- Check the URL – Address Bar turning the first part green when the site comes up

E-Banking - Remember

- Avoid using internet banking from public place
- Avoid writing the login id or the password as part of your person or anywhere near your computer system
- Always keep the help-line (ie help-desk) of the bank ready and handy
- Maintain confidentiality of the login details
- Be alert to all the messages and emails from the bank and in case of any doubt or discrepancy, always call the bank immediately

And now the “Don’t’s”

- Never click a link received in your mail to go to a bank website – Always type the URL of the bank website
- Never give any details as a response to a mail reportedly received from bank. Banks never CALL FOR details by email.
- Never respond to any phone call or text message or respond in any manner, to any mail or call claiming to be from a bank

“Don’t’s” ..contd

- Don’t login to internet banking from a browsing center or a public un-trusted computer
- Never do e-banking in a public place, when you suspect someone is watching you
- Never keep the internet banking window open, idle after you finish the transaction
- Do not be distracted by any external calls or by another windows session or otherwise, when doing an internet banking transaciton