Securing Online Banking

As per advisories received from CERT-in (Computer Emergency Response Team-India), online Banking users, need to follow the following best practices-

1. Protect your PC:

a) Install antivirus software and keep it updated on a regular basis to guard against new viruses
b) Install antispyware security software against those programs that monitor, record and extract the personal information you type in your PC (passwords, card numbers, ID numbers, etc.)
c) Install personal firewalls to protect your PC against unauthorized access by hackers
d) Keep your operating system and internet browser up to date, checking for and downloading new versions/security enhancements from the vendor's web site

2. Protect your personal information:

a) Create hard to guess security access codes (User ID & password) for Online Banking and make them unique (e.g. they should not be the same as those you use to access your email account)
b) Change your password (security access codes) periodically
c) Memorize your security access codes, avoid writing them down and keep them strictly personal and confidential
d) Do not disclose to ANYONE your security access codes: Bank will never initiate or contact you for your ebanking or ATM PINs, card or account numbers, personal identification information, neither over the phone nor in any electronic or written message
e) Never leave your PC unattended when logged into Online Banking Always remember to log off from your online session using the "Logoff" button when finished using the e-banking services

3. Use the Internet cautiously:

a) Always access Online Banking internet only by typing the URL in the address bar of your browser.
b) Never attempt to access Online Banking internet through an external link of unknown or suspicious origin appearing on other websites, search engines or emails
c) Before logging in, check for the Bank's Security Certificate details and the various signs (e.g. green address line and Lock, HTTPs) that confirm you are visiting the secure pages of Bank.
d) Ignore and delete immediately suspicious fraudulent (phishing, spoof, hoax) emails that appear to be from Bank, asking you to urgently click a link to a fraudulent (spoof) website that tries to mimic the Bank's site and to lure you into giving out your sensitive personal information (PIN, account or card numbers, personal identification information et al.)

e) Never click on a link contained in suspicious emails

f) Avoid using Online Banking from public shared PCs (as in internet cafes, libraries, etc.) to avoid the risk of having your sensitive private information copied and abused

4. Stay alert:

a) Sign-on to Online Banking regularly and review your account transactions, checking for any fraudulent activity on your account (e.g. transactions you do not recognize)

b) Keep track of your last logon date and time, displayed at the top left side of the Online Banking Home page

c) Once logged into Online Banking, you can also monitor the actions performed online

5. Prompt reporting of suspicious activity:

a) Contact your bank immediately, if you think someone knows your security access code or in case of theft of your code/ money or in case you have forgotten your credentials.

b) Forward any suspicious emails to the bank(soc@denabank.co.in) as well as on CERT-in email incident@certin.org.in

c) Your prompt action is crucial to prevent any (further) damage