



## Security Newsletter

15<sup>th</sup> November, 2010

*As internet is becoming an integral part of our lives, it is important that we are aware of the threats we face in the Cyberspace. The need of the hour is to be aware and adequately equipped to protect ourselves online.*

*Keeping this in view, with the support of **Indian Computer Emergency Response Team (Certin), Department of Information Technology, VeriSign India and Sify Technologies Ltd.** we are releasing the third edition of our **fortnightly Security Newsletter**.*

## Safe Internet Banking

The last decade has witnessed the growth of Internet banking as it provides the consumers the ease to do commercial transactions like paying bills, checking bank details etc almost instantaneously. However along with the exponential growth of internet banking, there has been a significant increase in online financial theft, with hacking and phishing being the predominant activity behind these thefts.

A few safety measures are shared below for ensuring Safe Internet Banking experience:

- Always try accessing the bank website by correctly typing the URL in address field as there can be websites having almost similar names(to capture the typing mistakes) and looks (to create illusion) as the original bank website. Practice some caution here.
- Never save your banking password on your laptop or computer and for safety, Always enter the banking password manually.
- Always be alert while accessing and entering your password in public places and from public access points.
- Never leave your computer unattended when you are conducting your Internet transactions.
- Log out immediately after you have completed your Internet transaction and clear the cache, cookies, saved passwords, files, and user names in the browser after use.
- Change passwords periodically, so that the chances of unknowingly compromised passwords being exploited are reduced
- Never use same password for all your accounts.
- Delete suspicious mails in particular if they contain attachment and always share such incident with others in your reach for such information might save someone from being victim of these emails.
- Always scan all your new files and software before installations.



- Watch out for ploys designed to get your bank account numbers and passwords like - “phishing” emails that ask you to log in through a link in the email and reconfirm your account, or emails that warn you that your account is suspended and ask you to call a toll free number to unlock it, or telemarketer calls and ask you for your password and account information, or job ads that ask you to receive or send wires using a bank account in your name. Remember, guard your password and account number zealously.
- Lastly, if your bank account has been compromised, act fast and inform your bank immediately.