E-COMMERCE
Enterprise Applications

INTERNET BANKING
Safety checks

BY

JYOTINDRA ZAVERI

Electronic Business Consultant

.com

Online Banking Safety Checks

- With the rapid increase in use of technology by companies, for banking as well as non-banking activities. It is imperative that each user is aware of prudent use of computers and gadgets
- Enjoy the convenience of Online Banking with just a few simple safety checks

PC security

- It is essential to update antivirus software regularly with a personal firewall and spyware programme
- It is also important to ascertain that firewall is ON, if the computer is used in cyber cafes or is not self owned.

Precautions while logging in

- Always access a bank's Internet banking website only by typing the correct URL (website address) into the browser
- <u>Never click a link sent in an e-mail that is supposed to link to the bank's website</u>
- A spurious link could be a fraudster's **phishing** attack designed to collect personal information
  - This information is then used for accessing accounts and making *unauthorized* transfer of funds
  - When in doubt, immediately contact the bank.

Confirm that the website is secured

- When you use the Internet for banking
  - Check that the session is secure by
    - a) checking presence of digital certificate, a padlock or key at the bottom right hand corner. Double click on this icon to view information about the organization with which you have entered into a secure session
    - b) verify the name of the website displayed in the top bar to avoid entering a spoof (false) website.

Ensure to log out

- Always log off completely when you have finished your internet banking activity
  - Simply closing the window may not close the banking session
  - If your computer is virus infected, your session may be hijacked by a fraudster and financial transactions can be made without your knowledge
  - It is also recommended to disconnect from the Internet when you are not using it

Special caution for e-mails from unknown sources.

- Never reply to any e-mail that is received from unknown people asking for confidential information or payment of fees etc., for surprise gifts.
  - E.g. You have won lottery – $100,000
  - Be careful with such email, do not fill up any form given in such emails, most likely it is for phishing (fishing out information from you).
- Be very suspicious of any person who ask for your log-in-ID, password, account details, card details, or similar sensitive information
- Be especially careful about opening an e-mail with an attachment

Check your transactions regularly.

- It is very important to check your bank statements regularly to identify any erroneous or unauthorized transaction
- You can also register for SMS alert services for your banking transactions and electronic statements provided by most banks (e.g. from ATM).

Keep your banking documents safe.

- **Destroy** expired debit / credit cards and other old statements that are not required and may contain sensitive personal information
  - At the same time , it is advisable to store retained documents in a suitably locked/secure place.

Safety First

THANKS

PRESENTATION BY

JYOTINDRA ZAVERI

Electronic Business Consultant

www.dnserp.com

DNS

www.dnserp.com