Internet Banking Security Measures [1/]

1. Secure Log-in ID and Password or PIN
   - Dot not disclose Log-in and Password or PIN.
   - Do not store Log-in and Password or Pin on the computer.
   - Regularly change password or PIN and avoid using easy-to-guess passwords such as names or birthdays. Password should be a combination of characters (uppercase and lowercase) and numbers and should be at least 6 digits in length.
2. Keep personal information private.
   Do not disclose personal information such as address, mother's maiden name, telephone number, social security number, GSIS number, bank account number or e-mail address – unless the one collecting the information is reliable and trustworthy.
3. Keep records of online transactions
   - Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
   - Review and reconcile monthly credit card and bank statements for any errors or unauthorized transactions promptly and thoroughly.
   - Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories.
   - Immediately notify the bank if there are unauthorized entries or transactions in the account.
4. Check for the right and secure website
   - Before doing any online transactions or sending personal information, make sure that correct website has been accessed. Beware of bogus or "look alike" websites which are designed to deceive consumers.
   - Check if the website is "secure" by checking the Universal Resource Locators (URLs) which should begin with "https" and closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display a security certificate information of the site.
   - Always enter the URL of the website directly into the web browser. Avoid being re-directed to the website, or hyperlink to it from a website that may not be as secure.
   - If possible, use software that encrypts or scrambles the information when sending sensitive information or performing e-banking transactions online.
5. Protect personal computer from hackers, viruses and malicious programs
   - Install a personal firewall and a reputable anti-virus program to protect personal computer from virus attacks or malicious programs.
   - Ensure that the anti-virus program is updated and runs at all times.
   - Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities.
   - Always check with an updated anti-virus program when downloading a program or opening an attachment to ensure that it does not contain any virus.
   - Install updated scanner softwares to detect and eliminate malicious programs capable of capturing personal or financial information online.
   - Never download any file or software from sites or sources, which are not familiar or hyperlinks sent by strangers. Opening such files could expose the system to a computer virus that could hijack personal information, including password or PIN.
6. Do not leave computer unattended when logged-in
   - Log-off from the internet banking site when computer is unattended, even if it is for a short while.
   - Always remember to log-off when e-banking transactions have been completed.
   - Clear the memory cache and transaction history after logging-out from the website to remove account information. This would avoid incidents of the stored information being retrieved by unwanted parties.
7. Check the site's privacy policy and disclosures
   - Read and understand website disclosures specifically on refund, shipping account debit/credit policies and other bank terms and conditions.
   - Before providing any personal financial information to a website, determine how the information will be used or shared with others.
   - Check the site's statements about the security provided for the information divulged.
   - Some websites' disclosure are easier to find than others - look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a sites. If the customer is not comfortable with the policy, consider doing business elsewhere.
8. Other internet security measures:
   - Do not send any personal information particularly password or PIN via ordinary e-mail.
   - Do no open other browser windows while banking online.
   - Avoid using shared or public personal computer in conducting e-banking transactions.
   - Disable the "file and the printer sharing" feature on the operating system if conducting banking transactions online.
   - Contacts the banking institution to discuss security concerns and remedies to any online e-banking account issues.