


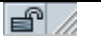








Safe Internet Banking

- Keep your password/PIN code safe and memorize them. Make sure you change them regularly (at least every 3 months). If you conduct transactions in a number of websites, use different passwords for each. Create unique passwords that are difficult to guess, e.g. use combination of letters and numbers.
- How do you know the website is secured?
 - Look for https:// in the URL and not http:// when you login
 - Look at the status bar for the security icon (locked padlock) when you visit the bank site. Ensure the icon is within the browser frame.

| Web Browser | Secured | Not Secured |
|--------------------------|---|--|
| Microsoft Windows | | |
| Internet Explorer |  |  |
| Netscape Navigator |  |  |
| Firefox |  |  |
| Apple MAC | | |
| Apple Safari |  |  |
| Firefox |  |  |

- When using a public computer, clear the browser cache, cookies and history once you complete your online transaction and logout (refer to you bank's website for online guidance). Make sure you logout properly after every Internet banking session and they must not just close the browser.
- Be aware of your surrounding and never leave your computer unattended when you are conducting your transactions. If you are unsure of the security of the computer, do not use it for online transactions.
- Use an antivirus, anti-spyware and personal firewall that is trusted and well supported by the vendor. Make sure the programs are regularly updated with the current version.
- Make sure your PC and browser are updated with the latest patches/fixes.
- Be sure that all email attachments are scanned with your anti-virus and are from trusted sources before opening them. Make sure you do not click on any links attached in your emails.
- Do not respond to emails asking for personal information, login information or change password notification. If you are not sure of the sender, contact your bank.
- If you decide to go to other websites linked via your internet banking website, read the privacy and policy information of that website first before conducting any online transactions.
- Always check your account balances/statement to ensure that no unauthorized withdrawal has taken place.
- When making any online payment, use a credit card. Credit cards usually have stronger protection for personal liability. Keep a copy of transaction receipt.
- When visiting your online banking site, always check that the Date and Time, matches the date and time when you last signed in.
- If your bank account has been compromised, act fast and inform the bank, or contact the Malaysia Cyber Security Centre (<http://www.niser.org.my> or <http://www.mycert.org.my>)
 - Tel - 03-89961901
 - Fax: 03-89960827
 - Email: mycert@mycert.org.my
 - SMS: 019-2813801
 - MyCERT 24x7 call incident reporting : 019-2665850

