











**Malaysian Cyber Security Agency**  
(formerly known as NISER)  
**13 Security Tips To Safe Internet Banking**

- Keep your password/PIN code safe and memorize them. Make sure you change them regularly (recommended every 3 months). If you conduct Internet transactions in a number of websites, use different passwords for each website. Create unique passwords that are difficult to guess, e.g. use a 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 of the security icon (locked padlock) when you visit the bank site. Double click on the padlock and ensure that it has a valid digital certificate.

Web Browser	Secured	Not Secured
<b>Microsoft Windows Platform</b>		
Internet Explorer		
Netscape Navigator		
Firefox		
<b>Apple MAC Platform</b>		
Apple Safari		
Firefox		

- Log out immediately after you have completed your Internet transaction. Then, clear the browser cache, cookies and history (refer to your bank's website for online guidance). Ensure that you log out properly after every Internet banking session and not just close the browser.
- Never leave your computer unattended when you are conducting your Internet transactions.
- If you are unsure of the security of the computer, do not use it for Internet transactions.
- Use an anti-virus, anti-spyware and personal firewall and keep it updated. Some of this software are freely available on the Internet.
- Ensure that your PC and browser are updated with the latest patches/fixes. Use the Automated Update feature of your Operating System (e.g. **Windows Update** for Windows users).
- Do not be influenced by appealing offers, especially from unknown parties. Do not click on any links attached in your emails. Do not copy and paste any website address (URL). Retype the website address to surf or use your *Bookmark*.
- Do not respond to emails asking for personal information, log in information or on changing password notification. Report to your bank or Malaysian Cyber Security Agency.
- 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 Internet transactions.
- Always check your account balance/statement to ensure that no unauthorized withdrawal has taken place.
- When visiting your Internet 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 Malaysian Cyber Security Agency (<http://www.niser.org.my> or <http://www.mycert.org.my>)
  - **Tel - 03-89926969**
  - **Fax: 03-89453442**
  - **Email: [mycert@mycert.org.my](mailto:mycert@mycert.org.my)**
  - **SMS: 019-2813801**
  - **MyCERT 24x7 call incident reporting : 019-2665850**