Let's treat convenience responsibly.

INTERNET BANKING
One of the biggest risks in banking online is identity theft

DOs	DON'Ts
Be sure to key in the CIMB Clicks URL yourself *Do not click on any hyperlinks in emails or pop-up windows. Secure Word is used to verify that you are logging in to the genuine CIMB Clicks website.*	**Do not disclose your User ID, Passwords and TAC via email, SMS or voice call** *Vital information such as these provide access to your internet banking account.*
Make sure your PC and CIMB Clicks website are secure ▶ *Install anti-virus software and use a firewall.* ▶ *Ensure there is a* ***padlock icon*** *at the top right corner of the browser's status when logging in to the secured website*	**Do not respond to emails, open attachments or click on suspicious links** *CIMB will never ask you to validate or restore your internet banking access via emails or pop-up windows.*
Create passwords that are hard to decipher *Avoid using personal information as your password.*	**Do not store your User ID and password in your computer or mobile phone**
Always log off and clear your computer's cache after each banking session *Avoid unauthorized people from using your internet banking account.*	**Do not let anyone else access your internet banking account** *Avoid allowing others to perform your online banking transactions on your behalf.*
Keep tabs on your money *Be sure to regularly check for unusual / fraudulent transactions in your bank statement.*	**Do not share your personal information with anyone, online or verbally** *Avoid sharing personal information such as answers to personal verification questions. Prevent placing your privacy at risk.*

ATM

DOs	DON'Ts
Change your PIN when you first receive it	**Do not use your personal information as your ATM PIN** *(e.g. birth date, telephone numbers)*
Keep your ATM card in a safe place	**Do not reveal your PIN to anyone else, not even your bank**
Block the view of the keypad and screen when using ATMs	**Do not keep your PIN and ATM Card together**
Collect your cash immediately from the cash slot as soon as it is presented *Prevent others from seeing how much you have withdrawn.*	**Do not accept the help of unknown persons when using the ATM**
Report lost or stolen ATM cards immediately *Contact the CIMB Call Centre at 1300 880 900 or email callcentre@cimb.com*	**Do not leave the ATM until you have completed the transaction** *Prevent unauthorized people from accessing your bank account.*

Phishing Scams - Request for disclosure of personal information, by disguising as CIMB Bank through emails, SMS or any other form of communication.

Transaction Authorization Code (TAC) - Required to perform online transactions. It will be sent via SMS to the mobile number that you have registered via CIMB ATM

For more information on how to protect yourself further from malicious scams, log on to www.cimbbank.com.my