Protect Yourself Now

	DOs	DONT's
Protect your Personal Information	• In response to any calls / SMS / email, ONLY call the number on BizChannel web • Check transaction activities on your statements or via BizChannel@CIMB regularly. In case of any unusual activity, contact our Business Call Centre.	• Phone scam fraudsters deploy fear tactics on the phone and 'role-play' to induce you to share your User ID / PIN / password. Do not panic. Always contact our Business Call Centre. • Never share your user ID, Password or OTP to anyone
Protect your Internet Banking / BizChannel Mobile Details	• On BizChannel@CIMB, look out for your chosen 'Secureword' after keying in your User ID (fake/bogus websites will not display your chosen 'Secureword'). • To access BizChannel@CIMB, type the entire URL as below: http://www.cimb-bizchannel.com.my/ • Ensure your mobile device is always updated with the latest Operating System [OS]. Stay alert for updates released by your OS/device manufacturer.	• Do not click on links or open email attachments from unknown / unreliable senders/sources. Emails from CIMB will always end with @cimb.com. • Do not enter 'User ID' or 'Password" outside BizChannel@CIMB website. Outside BizChannel@CIMB, CIMB will not ask for your 'User ID' or 'Password' under any circumstances.
Safeguarding your Token	• Keep your token in a safe place.	• Do not write your PIN anywhere which is easily accessible to anyone.

Money Muling Prevention

For fraudsters, transferring stolen funds directly into their accounts would make their whereabouts and activities be easily traced by law enforcement agencies. In efforts to stay under the radar, money mules are recruited or used to help facilitate the movement of funds to the criminals. In other words, money mules are used specifically to receive and transfer out stolen money.

Fraudsters will try to recruit customer to use their personal banking account as intermediary account by promising them rewards. Recruitment will normally be promoted via social media, chat sessions or even newspaper ads offering work-from-home job offers.

Malware Prevention

Malware stands for Malicious Software. It can be viruses, trojans, and spyware to "PC Optimization" programs that harm your electronic devices.

DOs	DONT's
• Check your transactions regularly. • Verify an app's permission and author or publisher before installing it. • Safeguarding your personal details. • Always run a reputable anti-virus on your computer/mobile devised, and keep it up-to-date regularly. • Update the operating system and applications on your computer/mobile devices, including the browser, in order to avoid any malicious exploits of security holes in outdated versions. • Change your password periodically. • Since URL on mobile site appears differently from desktop browser, make sure to verify it first.	• Do not click on adware or suspicious URL sent through SMS/messaging services. Malicious program could be attached to collect user's information. • Do not use public WiFi networks for bank transactions and turn off Bluetooth connection when not in use. These can be open windows for eavesdroppers intercepting the transaction or installing spyware and other malware on user's computer/mobile devices. • Do not enter TAC for activities which you did not initiate. • Do not open unknown or suspicious attachments in emails, even if they are from senders you know. • Do not plug your USB stick into just any computer. • Do not save your Online Banking login details on a public computer.

Phishing Prevention

DOs	DONT's
• Be suspicious of job adverts promising you an easy money for just a few hours of work every month. • Be wary of the overseas company offering employment, as it would be difficult for you to find out who they really are. Do a search on the employing company, confirm their contact details and verify their identity. • If you ever become a victim and someone credited a large amount to your account and requested you transfer it to another account, do not deal. Report this to your bank. • If you think you might already be part of a money mule scam, it is important that you act fast. Contact your bank and the police immediately.	• Never share your account details to anyone, unless you know who they are. • Don't open a new bank account to receive and transfer money from people you don't know anything about. • Do not get carried away by attractive commissions or consent to receive unauthorized money.

Example of Email Recruitment Scam

One of the most popular methods of recruiting mules today is through the Internet. If messages below seem familiar to you, they probably are fraudsters.

1. Earn RM1,500-RM4,000 per week working from home, or
2. Only requires 1-2 hours of availability per day, or
3. A 5-10% commission for “processing payments,” or
4. Work as a ‘Financial Agent’/ 'Money Transfer Agent'

SMS/Phone Call Scam Prevention

DOs	DONT's
• If you're unsure, ask for a reference number and call back on a trusted number (i.e. phone book) to confirm if the call was genuine. • Watch out for poor grammar in the SMS. • Check your transactions regularly. • Change your password periodically. • Safeguard your personal details.	• Do not respond to SMS or call from unknown person asking for your credit/debit card or online banking details. • Do not respond to any SMS or call claiming it's coming from Bank Negara. Their officer will never call you to ask for your credit/debit card or banking particulars. • If someone claiming to be from your card service provider calls you and asks you to confirm the security numbers on the back of the card (the last three digits on the back of the card), you should end the call immediately.