



INSTRUCTIONS FOR SAFE TRANSACTIONS ON E-BANKING CHANNEL

To ensure your own safety, rights and benefits, when performing transactions on VRB's e-banking channels, please read carefully and follow the following instructions.

VRB sincerely thanks you!

 1800 6656

www.vrbank.com.vn

APPENDIX I: INSTRUCTIONS FOR SAFE TRANSACTIONS

FOR INDIVIDUAL IBMB

I. Scope of application

Scope of application: IB / MB for individuals

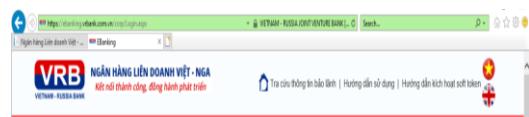
II. Information security and transaction safety

1. Principles of information security

1.1. Things you should not do



No	ABSOLUTATE NO	REASON
1	- Do not provide security information for e-banking service (include of: access code, access password, transaction authentication code, PIN Soft token) for anyone, even “Bank”, “Police”, “The supervisory institute”,... and in any way, such as: telephone, email, social networking, apps, website, strange links (does not contain VRB domain name),...	VRB or other Financial Institutions would never ask customer to provide any information security. Customer might be exploited by hacker/ fraudsters for bad purpose such as fraud, information theft
2	Do not log into internet banking except for the link https://ibanking.vrbank.com.vn / or on the VRB Mobile Baking app.	In some cases, fraudsters setup fake websites that closely resemble Internet Banking websites in order to trick customer’s usernames and passwords. There are cases where a fake link is sent by a fraudster with a brand name message coinciding with

		<p>the VRB's brand name, causing the customer to misunderstand that it is a message from the bank.</p> <p>For details of the scam, please see at: https://vrbank.com.vn/en/tin-tuc-vrb/vrb-canhh-bao-hinh-thuc-lua-dao-moi-thong-qua-tin-nhan-va-website-gia-mao.html.</p> <p>The VRB website is secured with SSL (Secure Sockets Layer) encryption technology. You are performing a secure session if the URL address starts with https: // or a padlock icon appears in your browser window.</p> <p>- Regarding the SSL encryption technology used at the Bank's website to encrypt your information when connecting to VRB to make transactions, information transmitted from your personal device to the Bank will be encrypted to ensure that no one can read it.</p> 
3	Do not Click on suspicious messages containing content related to VRB's products or services, especially non-VRB messages.	Fake messages are usually from a mobile phone number without a VRB name and require entering a username and password on a website mimics the VRB's interface to deceive customers
4	Absolutely refuse / Do not reply to any messages from messages that	All notification / warning / informational messages are from VRB brand name. Except for this

	do not start with the VRB brand name	Brand name, the messages coming from other numbers are all scams.
5	Do not open account and resist e-banking service for other people	Personal Account is privately property which contain customer's information and need to be secured. Customer could not control account if assigning it to someone else to use
6	Do not visit questionable websites or links (website is malicious, sensitive, looks suspicious)	These websites / links can secretly install viruses and <i>malware</i> on your computers, smartphones to <i>steal personal information</i> such as email passwords, Internet Banking access information, etc.
7	Do not unlock (jailbreak or root) on your device (phone, laptop, ipad...).	Rooting in Android phone or jail breaking an iPhone will significantly affect the ability to check applications installed on the device (phone, laptop ...) from the third-party application store. This bring a significant amount of risk for device, most dangerous is the possibility of stealing information by spyware, install malicious code on the device, therefore, please don't root or jailbreak any device, particularly those are contain financial information.
8	Do not transfer, recharge money into the telephone number which already assisted for processing the prize gifts	VRB would be never request customer to transfer, recharge money in the telephone number to receive prize of any promotion program of VRB


9	Restrict use of Internet Banking with public Wi-Fi	Avoid to use Public Wi-Fi network. In case of high necessity, use encrypted lines (Virtual Private Network). Public Wi-Fi is common type of Wi-Fi which you can usually meet at café, cinema, etc. These Wi-Fi generally do not require a password in order for many people could access quickly, and through unprotected Wi-Fi network, many hackers easily steal user's information.
10	Do not use password which contain personal information that easily recognize by other people such as date of birth, phone number, license plate, personal name, name of relatives such as husband/wife, serial number simple continuity like 1234567...	Limiting stolen information, making it possible for crooks to use your information and account for bad purposes that can cause serious damage to your property, reputation and honor.
11	Do not write user and password, PIN Soft token (Soft OTP, Soft Token)/SMS OTP in the note or record/save in any way	Avoid exposing account's information without controlling or being exploited by others who use financial transaction directly on these electronic devices.
12	Do not lend electronic devices to any one which have Internet Banking service login with installed/saved information	
13	Do not automatically save passwords, usernames on website	

1.2 Some notes that customer should comply with



CUSTOMER SHOULD	
Updating safety transaction instructions regularly to ensure proper, safe and secure use of e-banking services.	
1. Install password	+ Password should have the length of minimum 6 characters, include alphanumeric characters, contain uppercase, lowercase letters, or special characters (@ # \$% ...).
2. Secure password	+ Change password, access PIN into e-banking services for the first time within 24 hours after receiving it + Change password regularly (at least 03 months/time) to ensure account's safety + Change access password into VRB Internet Banking, Mobile Banking immediately after discovering that I have clicked on suspected fake links or accidentally answered information to strangers calling. + Creating habit of periodically changing password, or when you suspect information is leaked, or receiving request from VRB
3. Transaction	+ It is advisable to install anti-virus software on the device when making transactions. + Check information carefully before transaction (receiver's information, account number, beneficiary, beneficiary bank, transaction amount)
4. Authentication form	Recently VRB is having 3 forms of authentication when transfer transaction: SMS/OTP Hard Token/Soft Token (3 forms): Soft OTP, Soft Token, QR Code

	<p>+ The transaction authentication method is applied according to the transaction amount (Decision 630/2017 / QD-NHNN on application of authentication form in online transactions)</p> <p>+ Customer should install and use Soft Token when making transaction on IB/MB (Entrust Identity Guard Mobile, on Google Play and Apple Store app)</p>
5. Use safety your device	<p>+ Customer should protect computers, phones, mobile devices by installing and using anti-virus software such as Kapersky, BKAV anti-virus or reputable anti-virus software and is continuously updated from the supplier.</p> <p>+ Only download / install software from the official store of Android operating system (Play Store), iOS (Apple Store), Windows Phone / Windows Mobile (Microsoft Store).</p> <p>+ Virus & Worms, Trojans, Phishing, Pharming, Rootkit, Hacking, Keylogger,... : Is any kind of software designed to harm computers or mobile devices. Malware can steal sensitive information from devices, slow down device performance, or even send fake emails from your email accounts without your knowledge.</p>

<p>▶ Immediately announce to VRB when</p> 	<p>(1) There is any change in personal information: identity card number/passport, mobile number, email address,... or</p> <p>(2) There are cases of lost / misplaced mobile device, or Token device</p> <p>(3) Detect fake links, website, apps or calls impersonating a banker or have messages asking for username, password, personal information, authentication code OTP, PIN Soft Token,...</p> <p>- If you have any concerns, questions or worries about VRB's services and how to use E-banking services. Please kindly contact VRB's 24/7 Hotline at : 1800 6656/ +84 24 3942 9365 for support</p>
--	---

2. Safe transaction principles

- *Safe registration*
 - + Only using personal computer/electronic devices to minimize the possibility of stealing information when accessing or using VRB's Internet Banking/Mobile Banking
 - + In order to access in VRB's Internet Banking/Mobile Banking, customer should only access in official website of VRB at www.vrbank.com.vn, and select e-banking (Vietnamese website)
 - + VRB would lock the service if customer enter incorrect password more than 05 times in a row
- *Safe use*
 - + Read carefully the merchant's policies before accepting the payment.
 - + Check transaction information fully and accurately before entering OTP (authentication code) to confirm the transaction.
 - + Only use card information for payment at reputable websites, do not use public computers to make online payment transactions.
 - + When receiving OTP message from VRBank, it is necessary to carefully check the content of the message, including: transaction type, transaction channel ... If the



message content does not match the current transaction, you absolutely do not enter the OTP on any website or disclose it to anyone.

+ When the system is processing the transaction: You need to wait until there is transaction result notification from the system, not exit the transaction screen to make another transaction or exit the system.

- *Safe transaction*

+ When making transaction on VRB Internet Banking/Mobile Banking, Customer will receive SMS informing the OTP verification code from VRB. Customer absolutely do not enter this OTP on any Website other than VRB Internet Banking/Mobile Banking or disclose it to anyone.

+ When the system is processing transaction, could not exit from transaction screen, and wait for the result announcement from the system before performing others

+ Always remember log out/exit from the system after every access in e-banking services

+ Should register to use banking services via SMS at the same time to receive SMS notifications of balance fluctuations in order to immediately know the transactions on your account, minimize risks and losses to the lowest level.

+ Checking account balance on VRB Mobile Banking/Internet Banking interface after performing consecutive transactions.

+ Immediately change the login password or contact with VRB if customer do not make a transaction but receive OTP or a debit message.

We would like to give our sincere thanks to your trust and use of VRB's products and services.