

## GUIDELINES FOR SAFE TRANSACTIONS ON EPLUS ELECTRONIC BANKING CHANNEL FOR CORPORATE CUSTOMERS



## APPENDIX II: GUIDELINES FOR SAFE TRANSACTIONS ON EPLUS ELECTRONIC BANKING CHANNEL FOR CORPORATE CUSTOMERS

### I. Scope of application

EPlus Electronic Banking Service for Corporate Customers

### II. Information security and transaction safety

#### 1. Principles of information security

##### 1.1. Things you should not do



STT	ABSOLUTELY NO	REASONS
1	- Do not provide e-Banking information (username, password, OTP transaction authentication code (SMS OTP, Smart OTP)) to anyone through any methods. Any method of communication such as: phone, email, text message, social network, application, website, strange link, oral communication... without identifying the purpose and the receiver.	<p>VRB never proactively requires customers to declare both the login name and access password of the e-banking service at the same time via phone or email.</p> <p>You may have your information used by hackers/crooks for bad purposes such as fraud, stealing information for bad purposes.</p>
2	<p>Do not log in to any other e-banking link except this link:  <a href="https://eplus.vrbank.com.vn/corp/login">https://eplus.vrbank.com.vn/corp/login</a></p>	<p>In some cases, crooks build fake websites similar to VRB's Internet Banking website to trick customers into taking usernames and passwords. There are cases where a fake link is sent by a fraudster with a message having the same brand name as the bank's brand, causing the recipient to misunderstand that</p>



VIETNAM - RUSSIA BANK

		<p>it is a notification message from the bank. For details of the scam, please see <a href="https://vrbank.com.vn/vi/tin-tuc-vrb/vrb-canh-bao-hinh-thuc-lua-dao-moi-thong-qua-tin-nhan-va-website-gia-mao.html">https://vrbank.com.vn/vi/tin-tuc-vrb/vrb-canh-bao-hinh-thuc-lua-dao-moi-thong-qua-tin-nhan-va-website-gia-mao.html</a>.</p> <p>VRB's website is secured with SSL (Secure Sockets Layer) encryption technology. You are conducting a secure transaction if the URL begins with https:// or a padlock icon appears in your browser window.</p> <p>- Regarding SSL encryption technology used on the Bank's website to encrypt your information when connecting to VRB to perform transactions, information is transmitted from your personal device. Customers coming to the Bank will be encrypted to ensure that no one can read that information.</p>
3	Do not click on suspicious messages containing content related to VRB products and services, especially messages that are not from VRB.	The fake messages are usually from a mobile phone number, do not have a VRB name, and require entering a login name and password on a website that mimics the VRB interface to scam customers.
5	Do not open an account and register for e-banking services for others to use.	Your personal account is your private property containing information and needs to be kept confidential. You cannot control your account if you let someone else use it.



VIETNAM - RUSSIA BANK

6	Do not access questionable websites or links (malicious, sensitive, suspicious websites).	Websites/links of this type can secretly install viruses and malware on your computer or smartphone to steal personal information such as email passwords, Internet Banking access information, etc.
7	Do not jailbreak your device (phone, laptop, iPad...).	Jailbreaking a device will significantly reduce the ability to check applications installed on the device (phone, laptop, etc.) from third-party app stores. This brings many risks to your device, the most dangerous is spyware stealing information and installing malicious code on the device. Therefore, do not root or jailbreak your device, especially devices that contain financial information.
8	Do not transfer money or deposit money to the designated phone number to complete the procedure to receive rewards.	VRB never requires customers to transfer money or top up their phone number to receive rewards for any of VRB's promotional programs.
9	Limit use of Internet Banking with public Wifi.	Avoid using public Wi-Fi networks. In case of absolute necessity, use an encrypted connection (Virtual Private Network). Public Wi-Fi is the common type of Wi-Fi that you often encounter in coffee shops, movie theaters, etc. These wifi usually do not require a password so many people can access it quickly. Through unprotected wifi networks, many hackers easily steal users' information.



VIETNAM - RUSSIA BANK

10	Do not use a password that contains personal information that others can easily guess such as date of birth, phone number, license plate number, personal name, names of relatives such as spouse/children, serial numbers. continuously as simple as 1234567...You should change your password/PIN code regularly.	Limit stolen information, allowing thieves to use your information and accounts for bad purposes, which can cause serious damage to your property, reputation and honor.
11	Limit the number of people who have corporate account usernames and passwords.	Avoid revealing account information without control or being taken advantage of by others to use financial transactions directly on these electronic devices.
12	Do not write your username and password, SMS OTP/Smart OTP on paper or record/save it in any form.	Avoid revealing account information without control or being taken advantage of by others to use financial transactions directly on these electronic devices.
13	Do not lend electronic devices that have Internet Banking service login information installed/saved.	
14	<p>- Do not save e-Banking security information on electronic devices and websites or in any form. Restrict access to bank accounts and conduct financial transactions on unfamiliar devices.</p> <p>Always exit VRB's services and applications (including ePlus on web browsers/mobile applications...) as well as other financial applications linked to VRB's e-Banking services and websites. e-commerce right after you have completed the transaction session.</p>	



VIETNAM - RUSSIA BANK

	<p><b>Note:</b> <i>VRB never requires customers to provide card security information and e-banking services.</i></p>	
--	--	--


## 1.2. Things customers should do and comply with



YOU SHOULD	
Regularly update safe transaction instructions to ensure proper, safe and secure use of e-banking services.	
<p><b>1. Set password</b></p>	<ul style="list-style-type: none"> <li>+ Use a sufficiently reliable password with a minimum length of 08 characters, containing at least 4 numeric characters, at least 3 alphanumeric characters (at least 01 uppercase character, at least 01 lowercase character) and at least 01 special character: (@#\$% !&amp;*^?()&lt;&gt;/. For example Abc@0123.</li> <li>+ Không sử dụng mật khẩu có chứa thông tin mang tính cá nhân mà người khác dễ dàng suy đoán như ngày tháng năm sinh, số điện thoại, biển số xe, tên bản thân, tên của người thân như vợ chồng/con, dãy số liên tục đơn giản như 1234567....</li> </ul>
<p><b>2. Password security</b></p>	<ul style="list-style-type: none"> <li>+ Change password and PIN to access e-Banking services for the first time within <b>24 hours</b> of receipt.</li> <li>+ Change your password regularly (at least every 3 months) to ensure account security.</li> <li>+ Do not write your login name and password on paper or record/save it in any form to avoid uncontrollable disclosure of account information.</li> <li>+ Change the password to access e-banking services immediately after discovering that you have clicked on suspected fake links or accidentally replied to information to a stranger who called.</li> <li>+ Do not set the mode to save Internet Banking login passwords on shared devices (multiple users), on public computers.</li> </ul>



VIETNAM - RUSSIA BANK

<p><b>3. Transaction</b></p>	<ul style="list-style-type: none"> <li>+ You should install anti-virus software on your device when making transactions;</li> <li>+ Carefully check information before transaction (recipient information, account number, beneficiary name, beneficiary bank, transaction amount).</li> </ul>
<p><b>4. Authentication form</b></p>	<ul style="list-style-type: none"> <li>+ Currently VRB has 2 forms of authentication when transferring money: OTP (SMS OTP và Smart OTP).</li> <li>+ The form of transaction authentication is applied corresponding to the transaction amount (Decision No. 2345/QĐ-NHNN on implementing safe and secure solutions in online payment and bank card payment).</li> </ul>
<p><b>5. Use equipment safely</b></p>	<ul style="list-style-type: none"> <li>+ You should protect your computer, phone, and mobile devices by installing and using anti-virus software such as Kaspersky, BKAV anti-virus or other reputable and continuously updated anti-virus software from suppliers.</li> <li>+ Only download/install software from VRB's official website <a href="https://eplus.vrbank.com.vn/corp/login">https://eplus.vrbank.com.vn/corp/login</a> or the official repository of the iOS operating system (Apple Store), Windows Phone/Windows Mobile (Microsoft Store).</li> <li>+ Viruses &amp; Worms, Trojans, Phishing, Pharming, Rootkits, Hacking, Keyloggers, ... is type 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 account without your knowledge.</li> </ul>
<p><b>Notify VRB immediately when:</b></p> 	<ul style="list-style-type: none"> <li>- Immediately notify VRB when you have any changes in information, number of users (administrator/import/browse), citizen identification number/passport, phone number, email address, etc. or cases of loss/misplacement of mobile devices.</li> <li>- If you lose your phone or have any changes in the phone number registered to use the e-banking service, you need to contact VRB or actively access the e-Banking service to cancel service associated with that phone number.</li> </ul>



VIETNAM - RUSSIA BANK

	<ul style="list-style-type: none"> <li>- When there is any change in email address, phone number, residential address, statement receiving address, signature...</li> <li>- When it is suspected that the email address or phone number being used for electronic banking services is being exploited</li> <li>- Accidentally clicking on links suspected of being fake or replying information over the phone to a suspected impersonator.</li> <li>- If you have any concerns, questions or concerns about VRB's e-banking services and how to use them, or if you encounter any errors or problems while using the service, please contact us. Contact the 24/7 Customer Care Center - Hotline: 1800 6656 for support.</li> </ul>
--	--

## 2. Principles for safe use of services

### - Secure login:

- + You should only use personal computers/electronic devices to minimize the possibility of information being stolen when accessing and using VRB Internet Banking/Mobile Banking services.
- + Only use public computers to access and perform Internet Banking transactions if absolutely necessary and then immediately change the login password.
- + To log in to the VRB internet banking program, you should only access VRB's official website at <https://eplus.vrbank.com.vn/>.
- + VRB will lock the service if you enter the wrong password more than 5 times in a row.

### - Safe use:

- + Check the transaction information for complete accuracy before entering the OTP code (authentication code) to confirm the transaction.
- + When receiving an OTP message from VRB, you need to carefully check the message content, including: **transaction type, transaction amount, transaction channel**. If the content of the message does not match the transaction being performed, you absolutely do not enter this OTP code on any website or disclose it to anyone.
- + When the system is processing a transaction: You need to wait until there is a transaction result notification from the system, do not exit the transaction screen to make another transaction or exit the system.





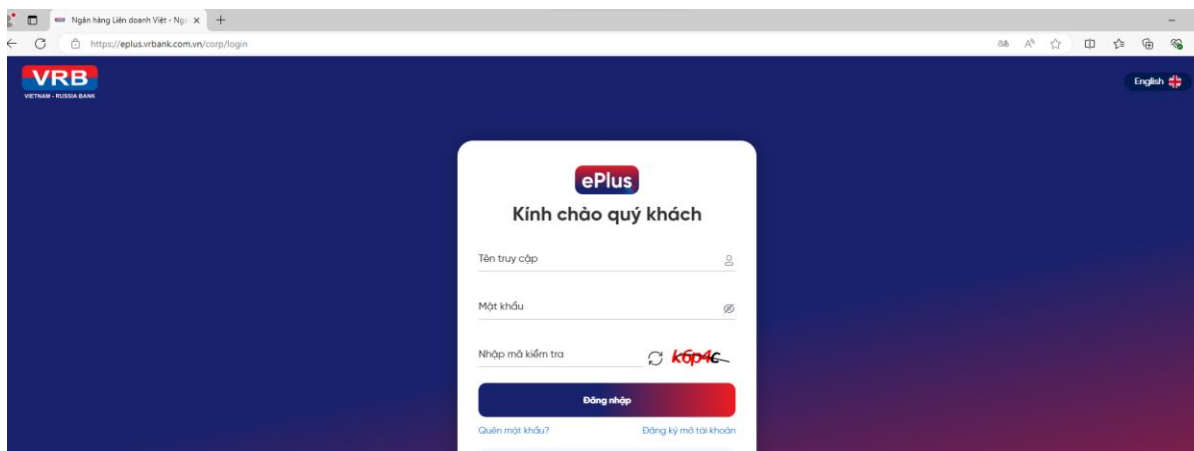
VIETNAM - RUSSIA BANK

+ Do not automatically save passwords and usernames on the browser due to easy information disclosure.

- Safe transactions:

+ Before submitting information via a website, look for the "lock" icon in your browser's status bar or note that the website address should start with <https://>, not just "http ://". When you see such security details, it means your information is in a secured transaction.

VRB's actual website interface with the described features as follows:



+ When the system is processing a transaction, do not exit the transaction screen and wait for result notification from the system before performing other transactions.

+ Always remember to log out/exit the system after each access to e-banking services because of closing the browser/application.

+ You should register to use banking services via SMS at the same time to receive text messages notifying balance changes to immediately know transactions on your account, limiting risks and losses to the lowest level. .

+ Check account balance on VRB Internet banking interface after making consecutive transactions.

+ Immediately change your login password or contact VRB if you do not make a transaction but receive an OTP or a message to deduct money.

**Sincerely thank you for your always trusting and choosing VRB's products and services.**