VRB

VIETNAM - RUSSIA BANK

HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN KÊNH NGÂN HÀNG ĐIỆN TỬ

Để đảm bảo an toàn bảo mật, quyền và lợi ích của chính mình, khi thực hiện giao dịch trên các kênh Ngân hàng điện tử của VRB, Quý khách hàng vui lòng đọc kỹ và tuân theo các thông tin hướng dẫn sau đây.

VRB trân trọng cảm ơn Quý khách hàng!

1800 6656

www.vrbank.com.vn

VRB
VIETNAM - RUSSIA BANK

PHỤ LỤC II: CẨM NANG HƯỚNG DẪN AN TOÀN GIAO DỊCH DÀNH CHO IB DOANH NGHIỆP

I. Phạm vi áp dụng

Dịch vụ IB Doanh nghiệp

II. Bảo mật thông tin và an toàn giao dịch

1. Nguyên tắc về bảo mật thông tin

1.1. Những điều quý khách không nên thực hiện

STT	TUYỆT ĐỐI KHÔNG	LÝ DO
1	Tuyệt đối không cung cấp bất kỳ thông tin bảo mật dịch vụ như: Mã truy cập/Tên đăng nhập (username), mật khẩu truy cập (password), mã xác thực giao dịch OTP (Soft Token/hoặc sinh ra trên thiết bị Token) cho bất kỳ ai và qua bất kỳ hình thức nào như: điện thoại, email, mạng xã hội, ứng dụng, trang mạng (website), đường kết nối (link) lạ,… mà không xác định được mục đích và người nhận là ai.	VRB không bao giờ chủ động yêu cầu Quý khách hàng khai báo cùng một lúc cả tên đăng nhập và mật khẩu truy cập của dịch vụ Ngân hàng điện tử qua điện thoại hoặc thư điện tử (email). Quý khách có thể bị hacker/ kẻ gian lợi dụng thông tin nhằm mục đích xấu như lừa đảo, ăn cắp thông tin cho các mục đích xấu
2	Không đăng nhập vào internet banking ngoại trừ đường link https://ebanking.vrbank.com.vn/corp/Login.aspx	Trong một số trường hợp, kẻ gian xây dựng các web giả mạo gần giống với web Internet Banking để lừa lấy username và mật khẩu của khách hàng. Có trường hợp đường link giả mạo được kẻ gian gửi kèm tin nhắn mang thương hiệu (brandname)

VRB
VIETNAM - RUSSIA BANK

		trùng với thương hiệu của ngân hàng làm cho người nhận hiểu lầm là tin nhắn thông báo từ ngân hàng. Chi tiết thủ đoạn lừa đảo xin xem tại 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. Trang web của VRB được bảo mật với công nghệ mã hóa SSL (Secure Sockets Layer). Quý khách đang thực hiện một phiên giao dịch an toàn nếu địa chỉ URL bắt đầu với https:// hoặc có biểu tượng ổ khóa xuất hiện tại cửa sổ trình duyệt của Quý khách. - Về công nghệ mã hóa SSL được sử dụng tại trang web của Ngân hàng để mã hóa các thông tin của Quý khách khi thực hiện kết nối đến VRB để thực hiện giao dịch, các thông tin được truyền từ thiết bị cá nhân của Quý khách đến Ngân hàng sẽ được mã hóa nhằm đảm bảo không ai có thể đọc được thông tin đó.
3	Không Click vào tin nhắn đáng ngờ chứa nội dung liên quan đến sản phẩm, dịch vụ của VRB, đặc biệt các tin nhắn không phải từ VRB.	Các tin nhắn giả mạo thường từ một số điện thoại di động, không có tên VRB và yêu cầu nhập tên đăng nhập cùng mật khẩu vào một trang web bắt chước giao diện của VRB để lừa đảo khách hàng
4	Tuyệt đối từ chối / Không trả lời bất kỳ tin nhắn nào từ những tin nhắn không bắt đầu từ brandname VRB	Tất cả các tin nhắn thông báo/ cảnh báo/ cung cấp thông tin đều từ brand name VRB. Ngoại trừ Brandname này, những tin nhắn đến từ đầu số khác đều là lừa đảo.

VIETNAM - RUSSIA BANK

5	Không mở tài khoản và đăng ký dịch vụ Ngân hàng điện tử cho người khác sử dụng.	Tài khoản cá nhân là tài sản riêng chứa thông tin và cần được bảo mật của Quý khách hàng. Quý khách không kiểm soát được tài khoản của mình nếu giao cho người khác sử dụng.
6	Không truy cập vào các trang web hay đường link có vấn đề (website độc hại, nhạy cảm, có vẻ đáng ngờ)	Các trang web/đường link loại này có thể lén cài đặt virus, *phần mềm độc hại* vào máy tính, điện thoại thông minh của Quý khách để *ăn cắp thông tin* cá nhân như mật khẩu email, thông tin truy cập Internet Banking v.v .
7	Không bẻ khóa trên thiết bị (điện thoại, laptop, ipad…) của Quý khách.	Việc bẻ khóa trên thiết bị sẽ làm *suy giảm* đáng kể tính năng kiểm tra các ứng dụng được cài lên thiết bị (điện thoại, laptop…) từ cửa hàng ứng dụng của bên thứ ba. Điều này mang đến nhiều nguy cơ cho thiết bị của Quý khách, nguy hiểm nhất là bị các phần mềm gián điệp đánh cắp thông tin, cài mã độc lên thiết bị. Vì vậy, đừng bẻ khóa (root hay jailbreak) thiết bị của Quý khách, đặc biệt là với các thiết bị có chứa thông tin tài chính.
8	Không chuyển tiền, nạp tiền vào số điện thoại chỉ định để làm thủ tục nhận thưởng.	VRB không bao giờ yêu cầu khách hàng chuyển tiền, nạp tiền vào số điện thoại để nhận thưởng bất kỳ chương trình khuyến mại nào của VRB
9	Hạn chế sử dụng Internet Banking với Wifi công cộng	Tránh sử dụng mạng Wi-Fi công cộng. Trong trường hợp thực sự cần thiết, hãy sử dụng đường truyền được mã hóa (Mạng riêng ảo). Wi-Fi công cộng là loại Wi-Fi phổ biến mà Quý khách thường gặp ở quán cà phê, rạp chiếu phim, v.v. Những wifi này thường không yêu cầu mật khẩu để nhiều người có thể truy cập nhanh chóng. Thông qua những mạng

VIETNAM - RUSSIA BANK

		wifi không được bảo vệ, nhiều tin tặc dễ dàng lấy cắp thông tin của người sử dụng.
10	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…	Hạn chế thông tin bị đánh cắp, khiến kẻ gian có thể sử dụng thông tin, tài khoản của Quý khách vào mục đích xấu có thể gây thiệt hại nghiêm trọng về tài sản, uy tín và danh dự của Quý khách.
11	Hạn chế số người có tên sử dụng và mật khẩu của tài khoản doanh nghiệp.	Tránh lộ thông tin tài khoản mà không kiểm soát được hoặc bị người khác lợi dụng sử dụng các giao dịch tài chính trực tiếp trên các thiết bị điện tử này.
12	Không viết tên đăng nhập và mật khẩu, mã PIN Soft token (Soft OTP, Soft Token)/ SMS OTP ra giấy hoặc ghi chép/ lưu dưới bất kỳ hình thức nào	Tránh lộ thông tin tài khoản mà không kiểm soát được hoặc bị người khác lợi dụng sử dụng các giao dịch tài chính trực tiếp trên các thiết bị điện tử này
13	Không cho mượn các thiết bị điện tử có cài đặt/lưu thông tin đăng nhập dịch vụ Internet Banking	
14	Không lưu tự động mật khẩu, tên người dùng trên các trình duyệt.	

VIETNAM - RUSSIA BANK

1.2. Những điều khách hàng nên thực hiện và tuân thủ

QUÝ KHÁCH NÊN	
Thường xuyên cập nhật hướng dẫn giao dịch an toàn để đảm bảo sử dụng các dịch vụ Ngân hàng điện tử đúng cách, an toàn, bảo mật.	
1. Cài đặt mật khẩu	+ Sử dụng mật khẩu đủ tin cậy là mật khẩu đủ có độ dài tối thiểu 6 ký tự, bao gồm các ký tự chữ và số, có chứa chữ hoa, chữ thường hoặc các ký tự đặc biệt (@#$%). + Không sử dụng mật khẩu có chưa thông tin mang tính cá nhân mà người khác dễ dàng suy đoán như ngày tháng năm sinh, số điệm thoại, biển số xe, tên bản thân, tên của người thân như vợ chồng/con, dãy số liên tục đơn giản như 1234567….
2. Bảo mật mật khẩu	+ Đổi mật khẩu, mã PIN truy cập các dịch vụ Ngân hàng điện tử lần đầu trong vòng 24h kể từ khi nhận được. + Thay đổi mật khẩu thường xuyên (tối thiểu định kỳ 03 tháng/lần) để đảm bảo an toàn cho tài khoản. + Không viết tên đăng nhập và mật khẩu ra giấy hoặc ghi chép/lưu dưới bất kỳ hình thức nào để tránh lộ thông tin tài khoản mà không kiểm soát được. + Thay đổi mật khẩu truy cập dịch vụ Ngân hàng điện tử ngay lập tức sau khi phát hiện ra mình vừa click vào các đường link nghi ngờ giả mạo hoặc vô tình trả lời thông tin cho người lạ gọi tới. + Không đặt chế độ lưu mật khẩu đăng nhập Internet Banking trên các thiết bị sử dụng chung (nhiều người sử dụng), trên máy tính công cộng.
3. Giao dịch	+ Nên cài đặt phần mềm diệt virus cho thiết bị khi thực hiện giao dịch

VRB
VIETNAM - RUSSIA BANK

	+ Kiểm tra kỹ thông tin trước khi giao dịch (thông tin người nhận, số tài khoản, tên người thụ hưởng, ngân hàng thụ hưởng, số tiền giao dịch)
4. Hình thức xác thực	Hiện nay VRB đang có 02 hình thức xác thực khi giao dịch chuyển khoản: OTP Hard Token/ Soft Token (có 3 hình thức): Soft OTP, Soft Token, QR Code + Hình thức xác thực giao dịch áp dụng tương ứng theo số tiền giao dịch (Quyết định 630/2017/QĐ-NHNN về áp dụng hình thức xác thực trong giao dịch trực tuyến) + Quý khách nên cài đặt sử dụng Soft Token khi thực hiện giao dịch trên IB/MB (phần mềm Entrust Identity Guard Mobile, trên các kho ứng dụng của Google Play và Apple Store)
5. Sử dụng thiết bị an toàn	+ Quý khách nên bảo vệ máy tính, điện thoại, các thiết bị di động bằng cách cài đặt và sử dụng các phần mềm diệt virus như Kapersky, BKAV anti-virus hoặc các phần mềm diệt virus uy tín và được cập nhật liên tục từ nhà cung cấp. + Chỉ tải/ cài đặt các phần mềm từ kho lưu trữ chính thống của hệ điều hành Android (Play Store), iOS (Apple Store), Windows Phone/ Windows Mobile (Microsoft Store). + Virus & Worms, Trojans, Phishing, Pharming, Rootkit, Hacking, Keylogger,..: Là bất kỳ loại phần mềm nào được thiết kế để gây hại máy tính hoặc thiết bị di động. Phần mềm độc hại có thể lấy cắp thông tin nhạy cảm từ các thiết bị, làm chậm hoạt động của thiết bị hay thậm chí gửi email giả mạo từ tài khoản email của Quý khách mà Quý khách không biết.
Thông báo ngay cho VRB khi: 	- Thông báo ngay cho VRB khi Quý khách có bất kỳ thay đổi nào về thông tin, số lượng người sử dụng (quản trị/nhập/duyệt), số chứng minh thư/hộ chiếu, số điện thoại, địa chỉ email,… hoặc xảy ra các trường hợp mất/thất lạc thiết bị di động, thiết bị Token. - Nếu bị mất điện thoại hoặc có bất kỳ sự thay đổi nào về số điện thoại đã đăng ký sử dụng gắn với dịch vụ ngân hàng điện

	tử, Quý khách cần liên hệ VRB hoặc chủ động truy cập dịch vụ Ngân hàng điện tử để hủy dịch vụ gắn với số điện thoại đó. - Khi có bất kỳ sự thay đổi về địa chỉ email, số điện thoại, địa chỉ cư trú, địa chỉ nhận sao kê, chữ ký… - Khi nghi ngờ địa chỉ email, số điện thoại đang sử dụng cho dịch vụ ngân hàng điện tử bị lợi dụng - Vô tình click vào các đường link nghi ngờ giả mạo hoặc trả lời thông tin qua điện thoại với đối tượng nghi ngờ mạo danh. - Khi có bất cứ băn khoăn, thắc mắc hay lo ngại nào về dịch vụ và cách sử dụng dịch vụ Ngân hàng điện tử của VRB hoặc khi gặp bất kỳ lỗi và sự cố trong quá trình sử dụng dịch vụ, Quý khách vui lòng liên hệ tới Tổng đài Chăm sóc Khách hàng 24/7 - Hotline: **1800 6656/ hoặc +84 24 3942 9365** để được hỗ trợ.

2. Nguyên tắc về sử dụng dịch vụ an toàn

- *Đăng nhập an toàn:*

+ Chỉ nên sử dụng máy tính/thiết bị điện tử cá nhân để hạn chế tối đa khả năng bị đánh cắp thông tin khi thực hiện truy cập và sử dụng dịch vụ VRB Internet Banking/Mobile Banking

+ Chỉ dùng máy tính công cộng để truy cập, thực hiện giao dịch Internet Banking trong trường hợp thật sự cần thiết và sau đó nên thay đổi ngay mật khẩu đăng nhập.

+ Để đăng nhập vào chương trình VRB internet banking, Quý khách chỉ nên truy cập vào website chính thức của VRB tại địa chỉ https://vrbank.com.vn/ và chọn mục Ngân hàng điện tử (website Tiếng Việt)

+ VRB sẽ thực hiện khóa dịch vụ nếu Quý khách nhập sai mật khẩu quá 05 lần liên tiếp.

- *Sử dụng an toàn:*

+ Kiểm tra đầy đủ chính xác các thông tin giao dịch trước khi nhập mã OTP (mã xác thực) để xác nhận giao dịch.

+ Khi nhận được tin nhắn OTP từ VRB, cần kiểm tra kỹ nội dung tin nhắn, bao gồm: **loại giao dịch, số tiền giao dịch, kênh giao dịch**. Nếu nội dung tin nhắn không khớp đúng với giao dịch đang thực hiện, Quý khách tuyệt đối không nhập mã OTP này vào bất kỳ trang web nào hoặc tiết lộ cho bất kỳ ai.

VRB
VIETNAM - RUSSIA BANK

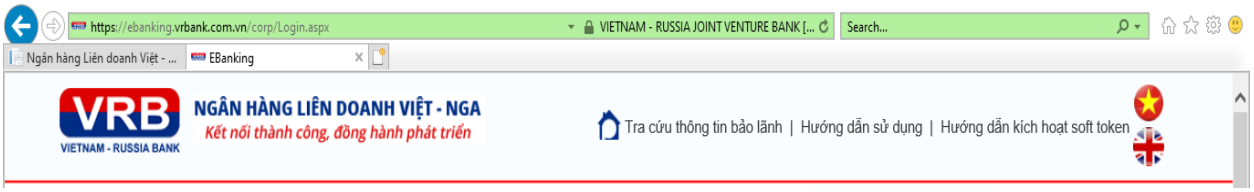
+ Khi hệ thống đang xử lý giao dịch: Quý khách cần chờ cho đến khi có thông báo kết quả giao dịch từ hệ thống, không thoát khỏi màn hình đang giao dịch để thực hiện giao dịch khác hoặc thoát khỏi hệ thống.

+ Không lưu tự động mật khẩu, tên người dùng trên trình duyệt do dễ bị lộ thông tin.

- *Giao dịch an toàn*:

+ Trước khi gửi thông tin qua trang web, hãy tìm biểu tượng hình “chiếc khoá" trên thanh trạng thái của trình duyệt hoặc chú ý rằng địa chỉ trang web nên bắt đầu với "https://" chứ không chỉ là"http://" Khi thấy các chi tiết bảo mật như vậy, thì có nghĩa thông tin của Quý khách đang nằm trong một phiên giao dịch bảo đảm.

Hình Website thật của VRB với các đặc điểm như mô tả được minh họa trong hình sau:



+ Khi hệ thống đang xử lý giao dịch, không thoát khỏi màn hình giao dịch và chờ thông báo kết quả từ hệ thống trước khi thực hiện các giao dịch khác.

+ Luôn nhớ Đăng xuất/Thoát khỏi hệ thống sau mỗi lần truy cập các dịch vụ Ngân hàng điện tử vì đóng trình duyệt/ứng dụng.

+ Nên đăng ký sử dụng đồng thời dịch vụ ngân hàng qua tin nhắn SMS để nhận tin nhắn thông báo biến động số dư nhằm ngay lập tức biết được những giao dịch trên tài khoản, hạn chế rủi ro và tổn thất đến mức thấp nhất.

+ Kiểm tra số dư tài khoản trên giao diện VRB Internet banking sau khi thực hiện các giao dịch liên tiếp nhau.

+ Ngay lập tức thay đổi mật khẩu đăng nhập hoặc liên hệ VRB nếu Quý khách không thực hiện giao dịch nhưng nhận được OTP hoặc tin nhắn báo trừ tiền.

Trân trọng cảm ơn Quý khách hàng luôn tin tưởng lựa chọn và sử dụng sản phẩm dịch vụ của VRB.