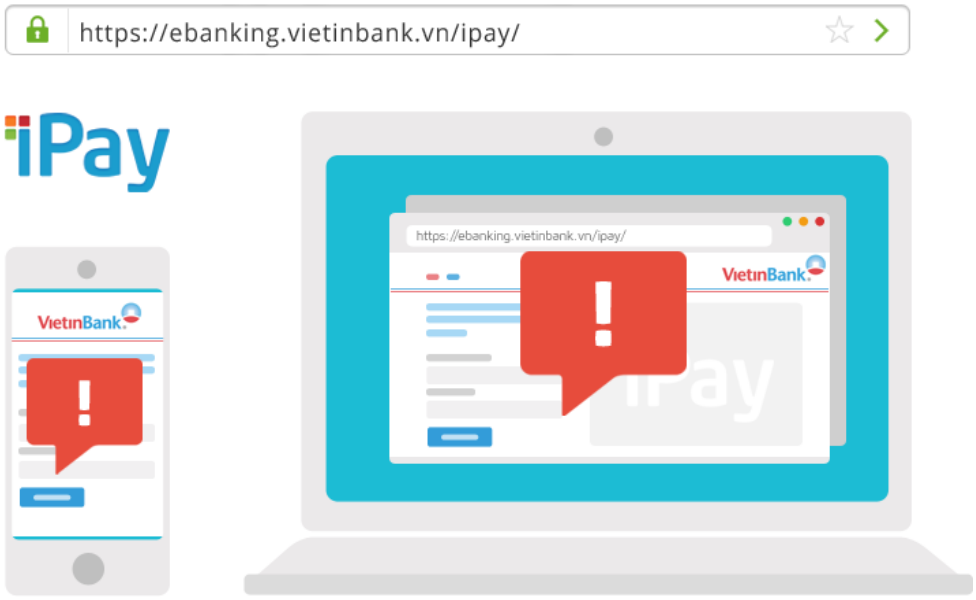
VietinBank iPay

HƯỚNG DẪN GIAO DỊCH AN TOÀN



DANH MỤC

Các biện pháp bảo mật khách hàng cần áp dụng **03**

- Đăng nhập 03
- Thiết lập & sử dụng mật khẩu 03
- Nhận OTP & sử dụng OTP 04
- Bảo mật tài khoản & phòng tránh virus 05
- Tham gia các chương trình khuyến mại 06

Các biện pháp bảo mật từ phía ngân hàng **07**

Thông tin liên lạc khi cần trợ giúp **09**



CÁC BIỆN PHÁP KHÁCH HÀNG CẦN ÁP DỤNG

Lưu ý về đăng nhập

✔ Đối với máy tính để bàn (desktop), máy tính xách tay (laptop): chỉ truy cập dịch vụ VietinBank iPay qua website www.vietinbank.vn hoặc ebanking.vietinbank.vn. Quý khách nên gõ trực tiếp địa chỉ này vào thanh địa chỉ trên trình duyệt, tránh truy cập từ các liên kết đính kèm vào thư điện tử không được gửi từ VietinBank.

✔ Đối với thiết bị di động: ngoài 2 website trên, Quý khách có thể đăng nhập thông qua ứng dụng VietinBank iPay trên thiết bị di động (iPay Mobile). Tuy nhiên, xin lưu ý rằng ứng dụng sẽ hoạt động **không** an toàn khi chạy trên các thiết bị di động **đã bị phá khóa**: jailbreak (iOS) hoặc rooted (Android). Khách hàng không nên sử dụng các thiết bị di động đã bị phá khóa, trường hợp khách hàng vẫn sử dụng những thiết bị này, khách hàng cần phải chấp nhận những rủi ro có thể xảy ra như lộ thông tin tên truy cập, mật khẩu truy cập, virut…. trong quá trình sử dụng dịch vụ ngân hàng điện tử.

"Jailbreak", "Rooted": là cách can thiệp hệ thống để cài ứng dụng bên thứ ba, không thông qua App Store hay CH Play/Play Store.

> Download VietinBank iPay Mobile App phiên bản dành cho: iOS / Android / Windows Phone.

✔ Chỉ đăng nhập qua các thiết bị đáng tin cậy, không đăng nhập qua thiết bị công cộng/dùng chung, không sử dụng các mạng di động, wifi công cộng để sử dụng dịch vụ. Đồng thời ghi nhớ các thiết bị đã từng sử dụng để đăng nhập, và hạn chế đăng nhập qua nhiều thiết bị.

✔ Vui lòng thường xuyên thực hiện xóa history, cache và cookie của trình duyệt internet. Việc xóa các dữ liệu trên sẽ hạn chế việc thông tin liên quan đến hoạt động truy cập được lưu lại trên máy tính, tạo ra cơ hội đánh cắp dữ liệu.

✔ Sử dụng các trình duyệt cập nhật mới nhất có chế độ bảo mật tiêu chuẩn hoặc chế độ cao.

✔ Không sử dụng chế độ tự động lưu thông tin tài khoản/mật khẩu khi sử dụng trình duyệt.

✔ Đảm bảo đã kết nối thành công vào website chính thức của VietinBank hoặc website dịch vụ VietinBank iPay trước khi nhập mọi dữ liệu cá nhân khác.

✔ **Không tiết lộ** tên đăng nhập và mật khẩu cho bất cứ ai khác, dù là người thân tín. Việc này giúp Vietinbank dễ dàng phối hợp với Quý khách khi xảy ra tranh chấp không đáng có.

✔ **Đăng xuất** ngay sau khi kết thúc phiên giao dịch; không nên thoát khỏi trình duyệt mà không sử dụng nút đăng xuất để tránh các lỗi không đáng có; không rời khỏi máy tính khi đang thực hiện giao dịch hoặc khi phiên đăng nhập còn tồn tại.

✔ **Không đăng nhập** vào tài khoản cá nhân của người khác. Việc đăng nhập này là trái pháp luật và đã được quy định rõ tại điều 226 Bộ Luật hình sự.

Lưu ý khi thiết lập & sử dụng mật khẩu

✔ Nên dùng các mật khẩu khác nhau cho các trang web/dịch vụ khác nhau.

✔ Mật khẩu nên bao gồm cả chữ cái và chữ số, có chữ in hoa và in thường. Mật khẩu có giá trị bảo mật tốt hơn khi có cả các ký tự đặc biệt (@ # $ % ^ * ...)

✔ Không nên sử dụng các thông tin cá nhân cơ bản (ngày tháng năm sinh, số điện thoại, tên, tên viết tắt, số chứng minh thư...) để đặt mật khẩu.

✔ Đổi mật khẩu định kỳ tối thiểu 1 năm 1 lần hoặc khi bị lộ, nghi bị lộ. Đặc biệt nên đổi ngay sau khi truy cập dịch vụ từ thiết bị công cộng (vui lòng đổi mật khẩu tại một thiết bị tin cậy khác).

✔ Không nên viết mật khẩu ra giấy hoặc ghi chép dưới bất kỳ hình thức nào cũng như không đọc to mật khẩu để tránh lộ mật khẩu mà Quý khách không kiểm soát được.

✔ Không chia sẻ các thông tin liên quan đến mật khẩu/mã PIN, OTP và các thiết bị lưu trữ các thông tin này với bất kỳ ai.

✔ Không cung cấp/nhập mật khẩu tại bất cứ website nào ngoài website VietinBank.vn và VietinBank iPay.

✔ Riêng đối với iPay Mobile: Ngoài mật khẩu thông thường, Quý khách có thể đăng nhập sử dụng dấu vân tay. Để đảm bảo an toàn, Quý khách lưu ý các điều sau khi sử dụng:

- Hệ thống không hỗ trợ đăng nhập bằng vân tay đối với các thiết bị đã jailbreak hoặc rooted. VietinBank xin miễn trừ trách nhiệm nếu thiết bị của quý khách đã jailbreak hoặc rooted.
- Đảm bảo chỉ có duy nhất dấu vân tay của Quý khách trong điện thoại.
- Không cho mượn điện thoại đã đăng ký hình thức đăng nhập bằng vân tay và không đăng ký hình thức đăng nhập bằng vân tay với các điện thoại dùng chung.
- Không tiết lộ mật khẩu máy cho người khác, không đặt mật khẩu đơn giản có thể dễ dàng truy ra.
- Trước khi đổi điện thoại, khi sửa chữa hay nhờ cài đặt trên thiết bị di động của mình, Quý khách cần hủy đăng ký tiện ích đăng nhập bằng vân tay và đăng xuất khỏi hệ thống.

Lưu ý về phương thức xác thực & sử dụng mã xác thực

Hiện tại VietinBank triển khai hai giải pháp xác thực: Xác thực qua tin nhắn OTP (OTP SMS) và xác thực qua Soft OTP

OTP là mật khẩu chỉ có giá trị **một lần duy nhất** khi xác nhận giao dịch, và chỉ có hiệu lực trong một khoảng thời gian nhất định.

Mã OTP SMS của VietinBank iPay được cung cấp theo cú pháp như minh họa.

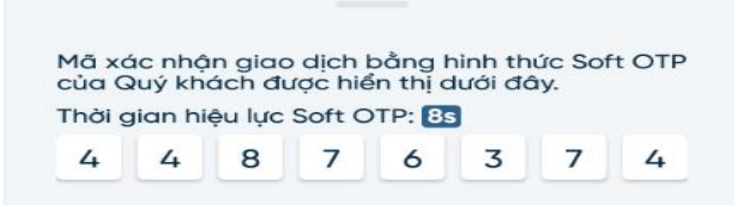




****Mã giao dịch gồm 4 chữ số.*

****Mã OTP gồm 6 chữ số.*

Soft OTP là một giải pháp xác thực sinh mã OTP ngẫu nhiên theo thời gian, căn cứ theo các thông tin khách hàng và giao dịch cụ thể. Đây là giải pháp xác thực giao dịch loại D theo quy định của NHNN an toàn cao, được tích hợp với iPay mobile để khách hàng có trải nghiệm tốt nhất.



Thẻ RSA là một thiết bị sinh mã dùng một lần để xác thực giao dịch. Mã xác thực hiển thị trên màn hình sẽ thay đổi 60 giây một lần.



Việc sử dụng mã xác thực nên theo các khuyến cáo dưới đây:

✔ Chỉ yêu cầu mã xác thực một lần duy nhất khi thực hiện một giao dịch (chỉ nhấn "Chấp nhận" một lần để yêu cầu mã xác thực).

✔ Khi nhận được tin nhắn OTP, cần kiểm tra các nội dung: kênh giao dịch, loại giao dịch, mã giao dịch, khớp đúng với giao dịch đang thực hiện. Trường hợp tin nhắn OTP đến chậm, Quý khách nên kiểm tra lại kết nối mạng điện thoại trước khi thực hiện lại giao dịch.

✔ Không nhập/nhập tạm mã xác thực vào bất cứ website/màn hình hiển thị nào khác không có các dấu hiệu nhận biết của VietinBank.

✔ Không nhờ cá nhân khác đăng nhập vào tài khoản và thực hiện giao dịch

✔ Không cung cấp mã xác thực cho bất cứ ai dưới bất kỳ hình thức nào (điện thoại, email, ghi chú…), đặc biệt không cung cấp mã xác thực cho bất cứ bên thứ ba nào đề nghị để nhận quà/nhận thưởng.

✔ *Lưu ý: đối với hình thức xác thực RSA, VietinBank đã dừng phát hành thẻ RSA mới và chỉ hỗ trợ khách hàng sử dụng thiết bị xác thực có thời gian giao nhận muộn nhất là ngày 31/12/2018 cho đến khi hết hạn thẻ RSA. Khách hàng vui lòng chuyển sang sử dụng xác thực bằng soft otp để có hạn mức cao hơn.*

Lưu ý khác về cách bảo mật tài khoản, phòng tránh virus và cảnh báo rủi ro

✔ Cài đặt, sử dụng & cập nhật thường xuyên phần mềm chống virus (anti-virus): các phần mềm này giúp ngăn chặn virus, trojans và các tác nhân gây hại khác. Anti-virus không chỉ được cung cấp cho máy tính cá nhân, vui lòng cài đặt và sử dụng phần mềm anti-virus tương ứng cho các thiết bị cần sử dụng khác.

✔ Sử dụng tường lửa (firewall) sẽ giúp Quý khách ngăn chặn các truy cập trái phép vào máy tính cá nhân.

✔ Chặn các phần mềm gián điệp (spyware): các phần mềm này có thể theo dõi và ăn cắp thông tin trực tuyến của Quý khách. Vui lòng kiểm tra cài đặt và liên tục cập nhật các chương trình chặn phần mềm gián điệp.

✔ Bảo mật kết nối internet của Quý khách: nếu kết nối internet (cable/wifi) không được bảo mật đúng cách, các đối tượng khác có thể can thiệp vào thiết bị của Quý khách. Vui lòng cài đặt mật khẩu cho kết nối internet hoặc áp dụng các biện pháp bảo mật theo hướng dẫn của nhà cung cấp.

✔ Sử dụng dịch vụ **thông báo biến động số dư** qua SMS của VietinBank để được lập tức thông báo về mọi biến động số dư của tài khoản, tăng khả năng phát hiện sớm các giao dịch gian lận/giao dịch nghi ngờ.

✔ Đối với các tài khoản Quý khách thường xuyên chuyển tiền đến, Quý khách nên lưu tên người được chuyển vào mục **Lưu danh bạ** (sau khi thực hiện chuyển khoản) để sử dụng cho các lần tiếp theo, tránh chuyển nhầm cho người khác. Thông tin này sẽ được ghi nhớ tại mục **Danh bạ.**

✔ Không nên truy cập vào các trang web lạ (các trang web lạ tải phần mềm không có bản quyền, key crack, tải nhạc, hình ảnh miễn phí…), các website nghi ngờ giả mạo, các liên kết đính kèm thư điện tử vì các website/liên kết này có thể đính kèm virus vào các link download, link hình ảnh mà người sử dụng không nhận biết được. Trường hợp buộc phải truy cập để tải dữ liệu, nên bật phần mềm antivirus, antispyware trước khi tải. Cẩn thận trước các đường link lạ, các tập tin không rõ nguồn gốc (đặc biệt chú ý các tập tin có đuôi *.exe, *.com, *.bat, *.scr, *.swf, *.zip, *.rar, *.js…).

✔ Không cung cấp thông tin cá nhân như số thẻ ATM, mã PIN thẻ, mã OTP xác thực… dưới mọi hình thức hoặc với bất kỳ người nào kể cả nhân viên ngân hàng.

✔ Trường hợp phát hiện dấu hiệu lừa đảo hoặc có dấu hiệu nghi ngờ, Quý khách vui lòng liên hệ ngay với tổng đài chăm sóc khách hàng 1900558868 để được hỗ trợ và hướng dẫn.

✔ Trường hợp bắt buộc phải dùng máy tính công cộng để đăng nhập sử dụng dịch vụ, xin hết sức lưu ý trong quá trình nhập tên đăng nhập và mật khẩu để bảo vệ tài khoản của mình. Quý khách nên tìm hiểu các cách nhập mật khẩu phòng tránh keylogger, có thể tham khảo một vài cách như sau:

- Nhập vài ký tự trong ô mật khẩu xen kẽ với các ký tự không nằm trong mật khẩu, sau đó dùng phím backspace/delete xóa đi các ký tự thừa (một lần nhấn phím cần xóa tối thiểu 02 ký tự), sau đó nhập tiếp và lặp lại quá trình này đến khi hoàn thành;
- Nhập đoạn sau của mật khẩu trước, sau đó di chuyển lên vị trí đầu để nhập bổ sung phần đầu của mật khẩu;
- Nhập vài ký tự của mật khẩu rồi di chuyển tới vị trí khác trên màn hình (ngoài ô mật khẩu) để gõ, sau đó chuyển chuột lại ô mật khẩu để gõ tiếp;
- Nhập xen kẽ giữa ô tên đăng nhập và mật khẩu bằng cách di chuyển chuột;
- Sử dụng bàn phím ảo (virtual keyboard).

Tuy nhiên các cách trên đây chỉ phòng tránh được phần nào đối với các keylogger thông thường, làm kéo dài quá trình keylogger nhận diện mật khẩu khách hàng. Đối với các virus nguy hiểm, Vietinbank vẫn khuyến cáo Quý khách hàng áp dụng đầy đủ các biện pháp bảo mật trước khi áp dụng các biện pháp qua mặt keylogger để đạt được hiệu quả tối đa.

Lưu ý khi tham gia các chương trình khuyến mại

✔ Quý khách lưu ý chỉ xem **các thông tin và tin tức khuyến mại** của dịch vụ internet banking tại địa chỉ website www.vietinbank.vn hoặc ebanking.vietinbank.vn. Quý khách cần cảnh giác với các chương trình trúng thưởng hoặc nhận tiền từ nước ngoài chuyển về qua mạng xã hội (Facebook..), đây là hình thức lừa đảo phổ biến hiện nay.

✔ Vui lòng tham khảo đầy đủ thể lệ của chương trình tại website chính thức.

✔ Mã dự thưởng hợp lệ (nếu có) chỉ được cung cấp sau khi Quý khách đã đăng nhập thành công vào dịch vụ NHĐT do VietinBank cung cấp và thực hiện các điều kiện khác của chương trình (VD: chuyển khoản ngoài hệ thống, thanh toán hóa đơn thành công,...)

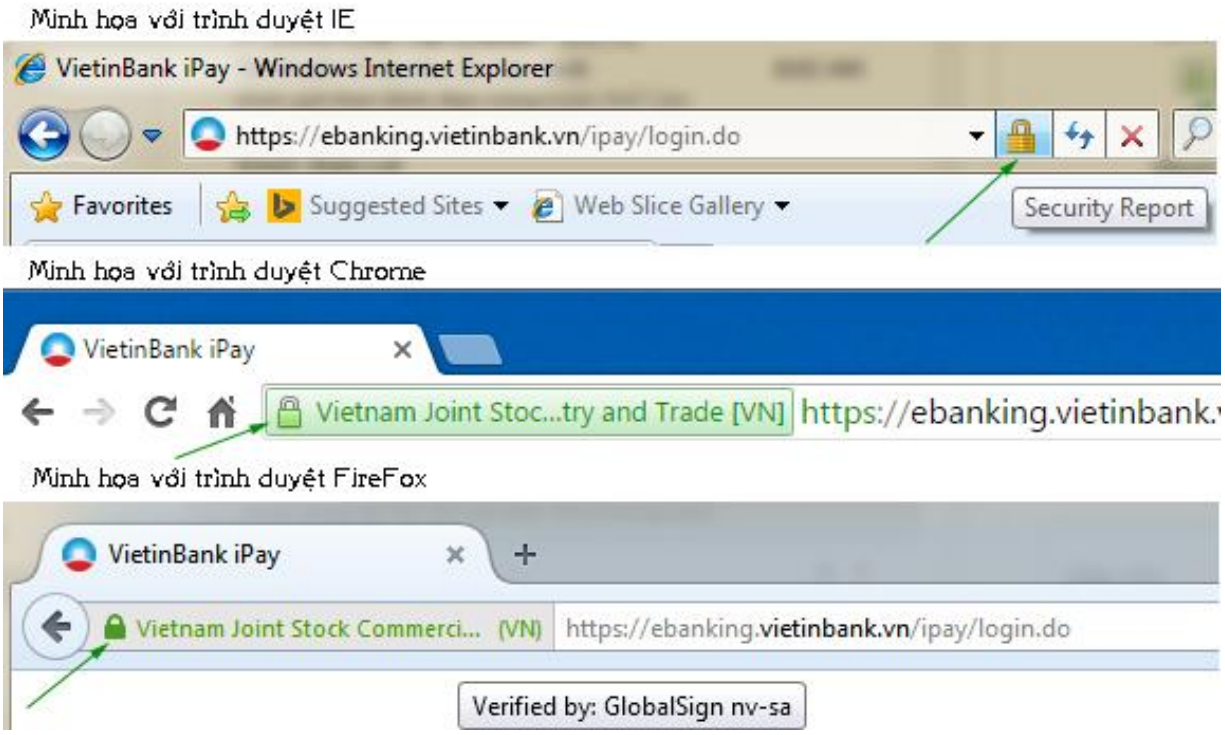
✔ Không truy cập vào các website khác để kiểm tra mã số dự thưởng.

✔ Không nhập thông tin cá nhân tại các website khác, đặc biệt là các website quảng cáo đăng nhập để trúng thưởng dựa trên thương hiệu VietinBank nhưng không xuất phát từ website chính thức của VietinBank.

CÁC BIỆN PHÁP BẢO MẬT TỪ PHÍA NGÂN HÀNG

VietinBank sử dụng biện pháp mã hoá theo tiêu chuẩn ngành trong các dịch vụ ngân hàng trực tuyến để bảo vệ tài khoản và các thông tin cá nhân của Quý khách. Các tầng an ninh và hệ thống bảo mật liên tục được cập nhật.

- Các trang thông tin giao dịch trong suốt phiên đăng nhập được áp dụng giao thức **bảo mật SSL** (https) để đảm bảo an toàn, các thông tin trên không được lưu trên cookie của máy tính.
- Hệ thống không cho phép ghi nhớ tên đăng nhập cũng như mật khẩu của khách hàng.
- Hệ thống sẽ **tự động đăng xuất** nếu người dùng không sử dụng trong vòng 10 phút, hoặc quên đăng xuất, hoặc tắt trình duyệt trước khi đăng xuất, hoặc để quên thiết bị trong tình trạng còn đăng nhập.
- Áp dụng cơ chế phòng chống chương trình đăng nhập tự động/dò tìm mật khẩu: sau 3 lần đăng nhập sai mật khẩu, hệ thống sẽ yêu cầu nhập **captcha** – mã xác nhận để tránh các chương trình đăng nhập tự động.
- Cung cấp cơ chế đăng nhập bằng bàn phím ảo mỗi khi đăng nhập vào iPay để tránh việc ghi lại thao tác bàn phím của một số phần mềm độc hại.
- Áp dụng cơ chế bảo mật xác thực 2 yếu tố: tên đăng nhập, mật khẩu kết hợp với **mã xác thực** trong mỗi giao dịch, giúp giao dịch luôn được đảm bảo an toàn.
- **Các thông tin và tin tức khuyến mại** của dịch vụ internet banking **chỉ được cung cấp** tại địa chỉ website www.vietinbank.vn hoặc ebanking.vietinbank.vn để tránh nhầm lẫn cho khách hàng.
- Đối với các giao dịch qua Vietinbank iPay, Vietinbank chỉ chấp thuận việc nhập mã xác thực duy nhất tại màn hình mà Quý khách đã đăng nhập hợp lệ theo đúng cách hướng dẫn phía trên. Quý khách không nhập OTP vào bất cứ trang web, màn hình popup nào khác để tránh các giao dịch lừa đảo.
- Website chính thức của VietinBank chỉ có giá trị khi thanh địa chỉ của trình duyệt hiển thị chính xác: https://www.vietinbank.vn/web/home/vn/index.html. VietinBank đã được GlobalSign - nhà cung cấp chứng thực số uy tín và nổi tiếng trên thế giới xác thực cho các trang web cung cấp dịch vụ trực tuyến của VietinBank. Vì vậy, khi truy cập các dịch vụ trên website của VietinBank, Quý khách sẽ nhìn thấy màu xanh an toàn hiện rõ trên thanh địa chỉ. Khi truy cập các dịch vụ trên website của VietinBank (bằng trình duyệt phiên bản mới nhất), Quý khách sẽ nhìn thấy biểu tượng thông tin xác thực trên thanh địa chỉ như dưới đây.



Xin cảnh giác với những **website giả mạo** có giao diện giống với giao diện của website VietinBank. Việc giả mạo trên thường nhằm mục đích đánh cắp các thông tin của Quý khách như tên đăng nhập, mật khẩu, số tài khoản, OTP… để thực hiện các giao dịch gian lận. Hình website giả mạo minh họa:

Vui lòng liên lạc Trung tâm chăm sóc khách hàng VietinBank ☎ **1900-55-88-68** hoặc phòng giao dịch gần nhất trong các trường hợp:

- ✔ Quý khách phát hiện các giao dịch bất thường

✔ Quý khách nhận được bất cứ một liên kết khả nghi yêu cầu đăng nhập, một thông báo hay một tin nhắn khuyến mại nghi vấn giả mạo (các chương trình khuyến mại không có trên website chính thức)

✔ Quý khách nhận được một cuộc điện thoại hay một thư điện tử yêu cầu cung cấp các thông tin đăng nhập của Quý khách (địa chỉ email không có tên miền của Vietinbank).

✔ Quy khách bị **mất máy điện thoại** hoặc có bất kỳ sự thay đổi nào về số điện thoại đã đăng ký

✔ Quý khách phát hiện bị mất hoặc bị lộ thông tin tài khoản

✔ Quý khách bị mất/thất lạc/hư hỏng thiết bị tạo OTP; bị lừa đảo hoặc nghi ngờ bị lừa đảo; bị tin tặc hoặc nghi ngờ bị tin tặc tấn công.

VietinBank sẽ tiến hành kiểm tra mọi yêu cầu, khiếu nại của khách hàng về các giao dịch điện tử có nghi vấn, và tiến hành mọi thủ tục cần thiết để tiếp tục ngăn chặn các rủi ro tiềm tàng.



MỌI YÊU CẦU TRỢ GIÚP XIN VUI LÒNG LIÊN LẠC

Trung tâm chăm sóc khách hàng VietinBank

Điện thoại: 1900-55-88-68 (24h/7)

Email: contact@vietinbank.vn

Chúc Quý khách giao dịch an toàn với VietinBank iPay.