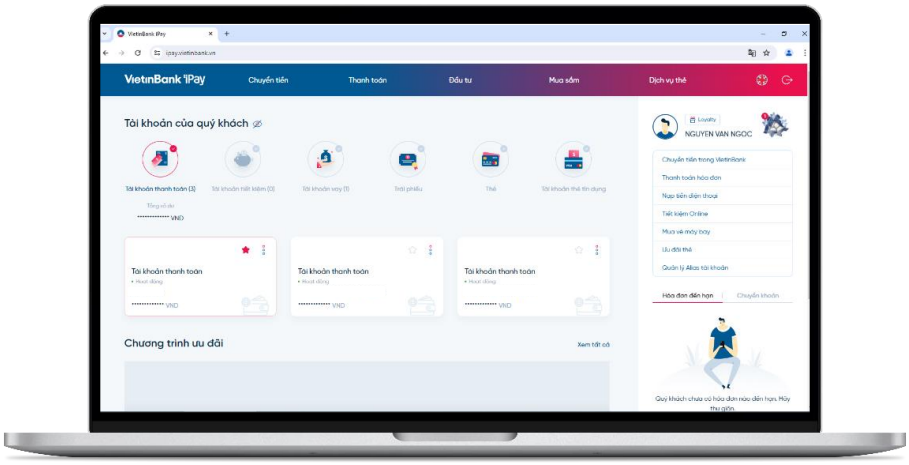
VietinBank iPay

HƯỚNG DẪN GIAO DỊCH AN TOÀN



DANH MỤC

I. CÁC BIỆN PHÁP KHÁCH HÀNG CẦN ÁP DỤNG

1. 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 ipay.vietinbank.vn. Quý khách nên gõ trực tiếp địa chỉ này vào thanh địa chỉ trên trình duyệt, tránh truy cập trực tiếp từ các liên kết (link) gửi kèm tin nhắn, chat, hoặc từ thư điện tử.

➔ Đối với thiết bị di động: Ngoài 2 link trên, Quý khách có thể đăng nhập thông qua ứng dụng VietinBank iPay trên thiết bị di động (iPay Mobile). Ứng dụng iPay Mobile chỉ xuất bản chính thức trên các trên chợ ứng dụng App Store/Google Play (CH Play) mà không qua bên nào gửi đường dẫn để tải ứng dụng.

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). Vì vậy, Quý khách không nên sử dụng các thiết bị di động đã bị phá khóa. Trường hợp vẫn sử dụng những thiết bị này, quý khách 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 thuật ngữ mô tả việc can thiệp vào hệ thống để cài ứng dụng bên thứ ba, không thông qua App Store hay Google Play (CH play).

> Download VietinBank iPay Mobile App <

➔ Chỉ đăng nhập dịch vụ từ các thiết bị đáng tin cậy, không nên đăng nhập qua thiết bị công cộng/dùng chung. Quý khách không nên sử dụng các mạng wifi công cộng để sử dụng dịch vụ. Lưu ý đổi mật khẩu đăng nhập sau khi truy cập dịch vụ từ các thiết bị hoặc mạng công cộng. Hạn chế đăng nhập từ nhiều thiết bị.

➔ Vui lòng thường xuyên thực hiện xóa lịch sử (history), bộ nhớ đệm (cache, 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, khiếu nại.
➔ **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.

2. Lưu ý khi thiết lập và sử dụng mật khẩu

➔ Nên dùng các mật khẩu khác nhau cho các trang web/dịch vụ khác nhau.
➔ Mật khẩu bao gồm chữ cái, chữ số (có chữ in hoa và in thường) và 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, CCCD...) để đặt mật khẩu.
➔ Đổi mật khẩu định kỳ 1 năm 1 lần theo đúng quy định 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, ứng dụng nào ngoài website www.vietinbank.vn hoặc ipay.vietinbank.vn và ứng dụng VietinBank iPay Mobile
➔ Riêng đối với iPay Mobile: Ngoài mật khẩu thông thường, Quý khách có thể đăng nhập sử dụng dấu vân tay hoặc FaceID. 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/FaceID đối với các thiết bị đã jailbreak hoặc rooted. VietinBank 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/FaceID và không đăng ký hình thức đăng nhập bằng vân tay/FaceID 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/FaceID và đăng xuất khỏi hệ thống.

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

Hiện tại, VietinBank cung cấp 03 phương thức xác thực:

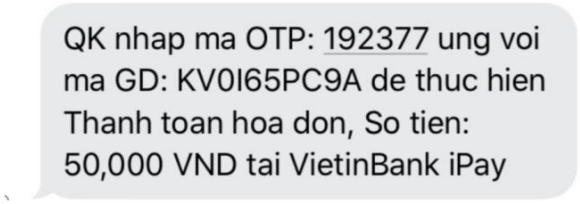
(i) Xác thực bằng mã OTP gửi qua tin nhắn SMS (SMS OTP)

(ii) Xác thực qua SoftOTP

(iii) Xác thực qua FacePay

OTP (One time password) là chuỗi số ngẫu nhiên do hệ thống Ngân hàng cung cấp để Quý khách xác nhận giao dịch do chính Quý khách thực hiện. Để đảm bảo an toàn cho giao dịch của Quý khách, OTP chỉ có giá trị **một lần duy nhất**, và chỉ có hiệu lực trong một khoảng thời gian ngắn.

➔ **SMS OTP:** Là phương thức mã OTP được cung cấp qua tin nhắn SMS gửi từ hệ thống VietinBank theo cú pháp như minh họa.



Mã OTP gồm 6 chữ số

➔ **SoftOTP:** Là phương thức mã OTP được sinh ngẫu nhiên ngay trên ứng dụng VietinBank iPay mobile. 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 Quý khách có trải nghiệm tốt nhất.

➔ **FacePay:** là phương thức xác thực giao dịch bằng nhận diện khuôn mặt có độ an toàn và bảo mật cao. Quý khách nên sử dụng FacePay cho các giao dịch tài chính, đặc biệt với các giao dịch có giá trị cao.

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: Mã giao dịch, loại giao dịch, số tiền và kênh giao dịch, đảm bảo 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 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 **cá nhân/bên thứ ba nào đề nghị để nhận quà/nhận thưởng/nhận khuyến mãi.**

➔ Đặt mã PIN cho SoftOTP.

4. Lưu ý khác về cách bảo mật tài khoản, phòng tránh virus và giảm thiểu 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 OTT/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** trên VietinBank iPay.

➔ 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: Tên đăng nhập, mật khẩu, số thẻ ATM, mã PIN thẻ, mã OTP,... cho bất kỳ ai dưới bất kỳ hình thức nào, kể cả cơ quan công an hay nhân viên ngân hàng.

➔ Không cài đặt phần mềm giả mạo dịch vụ công (Bộ Công an, VNEID, Tổng Cục Quản lý đất đai, Tổng Cục Thuế...) từ các website/đường link/QRCode lạ hoặc tập tin APK.

➔ Chỉ nên cài đặt phần mềm trên chợ ứng dụng App Store/Google Play (CH Play).

➔ Khi cài đặt bất kỳ ứng dụng nào, người dùng nên đọc kỹ thông tin trước khi đồng ý tất cả điều khoản, kiểm tra thông tin tác giả (nhà phát triển) và đọc các bài đánh giá về ứng dụng.

➔ Nên thường xuyên cập nhật các phương thức, thủ đoạn của tội phạm trên các phương tiện thông tin đại chúng và website VietinBank, ứng dụng VietinBank iPay Mobile.

➔ Trường hợp phát hiện dấu hiệu lừa đảo hoặc có dấu hiệu nghi ngờ, Quý khách liên hệ ngay với **Trung tâm Dịch vụ Khách hàng VietinBank 1900 55 88 68** và cơ quan công an để được hỗ trợ và hướng dẫn kịp thời.

➔ 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.

5. Lưu ý khi tham gia các chương trình khuyến mãi

➔ Quý khách lưu ý chỉ xem các thông tin khuyến mãi, chương trình ưu đãi của dịch vụ tại địa chỉ website www.vietinbank.vn hoặc ipay.vietinbank.vn.

➔ 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 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.

➔ Quý khách cần cảnh giác với các chương trình trúng thưởng hoặc nhận tiền từ nước ngoài chuyển về qua mạng xã hội (Facebook, Zalo...). Đây là hình thức lừa đảo phổ biến hiện nay.

II. 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** trong các trường hợp:

- Người dùng không sử dụng trong vòng 10 phút,
- Người dùng quên đăng xuất, quên tắt trình duyệt trước khi đăng xuất
- Người dùng 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.

➔ 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 mãi** của VietinBank **chỉ được cung cấp tại địa chỉ** website www.vietinbank.vn hoặc ipay.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 các 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.

➔ VietinBank đã được GlobalSign - nhà cung cấp chứng thực số uy tín và nổi tiếng trên thế giới xác thực cho các trang web của VietinBank. Vì vậy, khi truy cập các dịch vụ trên website của VietinBank, Quý khách sẽ nhìn thấy biểu tượng khóa an toàn trên thanh địa chỉ.

↗ 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.

Vui lòng liên lạc **Trung tâm Dịch vụ Khách hàng VietinBank** theo số **1900 55 88 68** hoặc điểm 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 mãi nghi vấn giả mạo (các chương trình khuyến mãi 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).

– Quý khách nhận được cuộc điện thoại hay liên hệ từ đối tượng lạ (tự nhận là cơ quan chức năng) yêu cầu cung cấp, kê khai các thông tin của Quý khách hoặc hướng dẫn cài đặt phần mềm theo đường link hay tải tập tin lạ.

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

MỌI YÊU CẦU TRỢ GIÚP XIN VUI LÒNG LIÊN HỆ
Trung tâm Dịch vụ Khách hàng VietinBank
Điện thoại: **1900 55 88 68** (24/7)
Email: contact@vietinbank.vn
Kính chúc Quý khách giao dịch an toàn với VietinBank iPay!