HƯỚNG DẪN GIAO DỊCH AN TOÀN TRÊN GP.IB

* * *

Mọi yêu cầu trợ giúp, vui lòng liên hệ
Trung tâm Dịch vụ khách hàng GPBank
1800585866 / 02435149094 / info@gpbank.com.vn

1. Lưu ý về đăng nhập

- Chỉ truy cập dịch vụ GP.IB qua website www.gpbank.com.vn hoặc https://ib.gpbank.com.vn. Quý khách nên gõ trực tiếp địa chỉ này vào thanh địa chỉ trên trình duyệt, không truy cập từ các liên kết đính kèm vào thư điện tử không được gửi từ GPBank.
- Lưu ý đối với thiết bị di động: ứng dụng sẽ hoạt động an toàn hơn khi chạy trên các thiết bị không jailbreak (iOS) hoặc rooted (Android).
- Chỉ đăng nhập qua các thiết bị đáng tin cậy, không đăng nhập qua thiết bị công cộng/dùng chung. Đồng thời không ghi nhớ mật khẩu trên các thiết bị đã từng sử dụng để đăng nhập, và hạn chế đăng nhập qua nhiều thiết bị.
- 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 website được lưu lại trên máy tính, tạo ra cơ hội đánh cắp dữ liệu.
- Đảm bảo đã kết nối thành công vào website chính thức của GPBank hoặc website dịch vụ GP.IB trước khi nhập mọi dữ liệu cá nhân khác.
- Không tiết lộ tên đăng nhập, mật khẩu và SMS OTP cho bất cứ ai khác, dù là người thân tín, bao gồm cả cán bộ tự xưng là nhân viên của GPBank, cán bộ công tác tại cơ quan nhà nước như Công an, toà án, …. Việc này giúp GPBank 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 thiết bị khi đang thực hiện giao dịch hoặc khi phiên đăng nhập còn tồn tại.

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 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...) để đặt mật khẩu.
- Nên đổi mật khẩu định kỳ. 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/lưu 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 cung cấp/nhập mật khẩu tại bất cứ website nào ngoài website của GPBank và GP.IB.

3. Lưu ý về OTP và sử dụng OTP

- OTP là mã số bảo mật được sinh ra ngẫu nhiên từ hệ thống và tự động hết hạn sau một khoảng thời gian nhất định, dùng để xác nhận việc thực hiện một giao dịch nào đó, đồng thời là biện pháp bảo mật và là chữ ký điện tử. OTP sẽ được cung cấp qua số điện thoại mà Quý khách đăng ký với GPBank.
- Đối với khách hàng doanh nghiệp áp dụng mô hình 2 cấp/3 cấp. Quý khách thực hiện tuân

Mọi yêu cầu trợ giúp, vui lòng liên hệ
Trung tâm Dịch vụ khách hàng GPBank
1800585866 / 02435149094 / info@gpbank.com.vn

thủ đúng mỗi người chỉ thực hiện một bước trong khi thực hiện giao dịch, nhập đầy đủ, chính xác OTP gửi đến các số điện thoại khác nhau tại mỗi bước.

- Việc sử dụng OTP nên theo các khuyến cáo dưới đây:
  - Khi nhận được tin nhắn OTP, cần kiểm tra các nội dung liên quan đến giao dịch (số tiền, số tài khoản nhận, ...). Trong trường hợp thông tin không khớp đúng, Quý khách tuyệt đối không nhập OTP vào bất cứ màn hình nào. Nếu có nghi ngờ, Quý khách báo ngay cho GPBank theo số điện thoại 1800585866/02435149094 của Trung tâm dịch vụ khách hàng.
  - Không nhập/nhập tạm OTP vào bất cứ website/màn hình hiển thị nào khác không có các dấu hiệu nhận biết của GPBank.
  - Trường hợp tin nhắn OTP đến chậm, Quý khách nên kiểm tra lại kết nối mạng điện thoại trước khi thực hiện lại.
  - Không nhờ cá nhân khác đăng nhập vào tài khoản và thực hiện giao dịch cũng như không cung cấp OTP cho bất cứ ai dưới bất kỳ hình thức nào (điện thoại, email, ghi chú...).

4. Lưu ý khác về cách bảo mật tài khoản và phòng tránh virus

- Cài dặt, sử dụng và 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.
- Lưu ý dịch vụ GP.SMS của GPBank 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 đã từng chuyển tiền đến thành công, sử dụng chức năng "Chọn từ các tài khoản đã giao dịch" để tránh sai thông tin, chuyển nhầm cho người khác.
- Không nên truy cập vào các trang website lạ (các trang website 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

Mọi yêu cầu trợ giúp, vui lòng liên hệ
Trung tâm Dịch vụ khách hàng GPBank
1800585866 / 02435149094 / info@gpbank.com.vn

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...).

- 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, GPBank 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 về xác thực ngẫu nhiên giao dịch qua điện thoại đối với giao dịch chuyển tiền của khách hàng doanh nghiệp

- GPBank sẽ thực hiện gọi điện thoại đến số điện thoại đã đăng ký của Quý khách (Người nhập lệnh/người kiểm soát/người phê duyệt) để xác thực thông tin giao dịch chuyển tiền của khách hàng doanh nghiệp. Khi Quý khách nhận được điện thoại từ GPBank, Quý khách chỉ cung cấp thông tin về giao dịch chuyển tiền đã thực hiện (số tiền chuyển, thời gian chuyển tiền, người thụ hưởng…), KHÔNG cung cấp thông tin về tên đăng nhập, mật khẩu truy cập, thông tin OTP.

Chúc Quý khách giao dịch an toàn, thuận tiện

với dịch vụ GP.IB của GPBank !

Mọi yêu cầu trợ giúp, vui lòng liên hệ
Trung tâm Dịch vụ khách hàng GPBank
1800585866 / 02435149094 / info@gpbank.com.vn