Hướng dẫn giao dịch an toàn trên VietinBank eFAST

Kính thưa Quý Khách hàng,

Bên cạnh các giải pháp bảo mật thông tin giao dịch được VietinBank áp dụng, chúng tôi cũng khuyến nghị Quý khách hàng lưu ý những điểm sau khi thực hiện giao dịch tài chính trên dịch vụ Internet Banking:

Lưu ý về đăng nhập

1. Chỉ nên thực hiện giao dịch trên máy tính hoặc thiết bị di động cá nhân có cài đặt mật khẩu truy cập và phần mềm chống virus được cập nhật thường xuyên.
2. Chỉ nên truy cập vào website ngân hàng điện tử chính thức của VietinBank tại địa chỉ https://ebanking.vietinbank.vn/efast/; tuyệt đối không truy cập vào các đường link lạ được gửi tới email hoặc qua tin nhắn SMS.
3. Chỉ đăng nhập qua các thiết bị đáng tin cậy, không đăng nhập qua thiết bị công cộng/dùng chung. Đồng thời ghi nhớ các thiết bị đã từng sử dụng để đăng nhập, và hạn chế đăng nhập qua nhiều thiết bị.
4. Đảm bảo đã kết nối thành công vào website chính thức của VietinBank hoặc website dịch vụ VietinBank eFAST trước khi nhập mọi dữ liệu cá nhân khác.
5. Đăng xuất ngay sau khi kết thúc phiên giao dịch; hạn chế đóng cửa sổ trình duyệt thay cho đăng xuất trực tiếp; không rời khỏi máy tính khi đang thực hiện giao dịch hoặc khi phiên đăng nhập còn tồn tại.
6. Không tiết lộ tên đăng nhập và mật khẩu cho các đối tượng khác.
7. Không đăng nhập vào tài khoản cá nhân của người khác. Việc đăng nhập này là trái pháp luật theo điều 226 Bộ Luật hình sự.

Lưu ý khi thiết lập & sử dụng mật khẩu

1. Không dùng chung mật khẩu cho nhiều website khác nhau.
2. 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 (@ # $ % ^ * ...)

3. Không sử dụng các thông tin cá nhân cơ bản (ngày tháng năm sinh, số điện thoại, tên,...) để đặt mật khẩu.
4. Đổi mật khẩu định kỳ. Đặc biệt nên đổi ngay sau khi sử dụng tại thiết bị công cộng (vui lòng đổi mật khẩu tại một thiết bị tin cậy khác).
5. Không copy mật khẩu ra văn bản hoặc ghi chép lại dưới bất kỳ hình thức nào.
6. Không cung cấp mật khẩu cho bất cứ người nào kể cả nhân viên VietinBank. Chúng tôi không bao giờ yêu cầu Quý khách cung cấp thông tin mật khẩu qua email, SMS hay điện thoại.

Lưu ý khác về cách bảo mật tài khoản & phòng tránh virus

1. Sử dụng 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.
2. Sử dụng tường lửa (firewall) thường xuyên: tường lửa sẽ giúp bạn ngăn chặn các truy cập trái phép vào máy tính cá nhân.
3. Chặn các phần mềm gián điệp (spyware): các phần mềm này có thể theo dõi và ăn cắp thông tin trực tuyến của bạn. Vui lòng kiểm tra cài đặt và liên tục cập nhật các phần mềm an ninh nêu trên.
4. Bảo mật kết nối internet của bạn: nếu kết nối internet (cable/wifi) không được bảo mật đúng cách, các đối tượng khác có thể can thiệp vào thiết bị của bạn. 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.
5. Nên sử dụng đồng thời dịch vụ thông báo biến động số dư qua tin nhắn SMS Banking để liên tục cập nhật những thay đổi trên tài khoản của Quý khách.
6. Bảo quản thiết bị bảo mật RSA cẩn thận. Trong trường hợp mất hoặc thất lạc thẻ RSA, Quý khách cần nhanh chóng liên hệ với cán bộ Ngân hàng để khóa thẻ.
7. Không nên chia sẻ, dùng chung tài khoản giao dịch, thẻ RSA giữa các thành viên trong công ty.
8. Không truy cập vào các website lạ, không tải các nội dung không có bản quyền để tránh virus được gắn vào link download khó nhận diện. Cẩn thận trước các

đường link lạ, các tập tin không rõ nguồn gốc (lưu 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 gõ mật khẩu. Để phòng tránh keylogger, vui lòng tham khảo các cách 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 delete 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 di chuyển lại ô mật khẩu để gõ tiếp;
- Nhập xen kẽ giữa phần tên đăng nhập và mật khẩu;

Sử dụng bàn phím ảo (virtual keyboard).

Các biện pháp trên có thể ngăn chặn việc keylogger nhận diện mật khẩu. VietinBank khuyến cáo Quý khách áp dụng đầy đủ các biện pháp bảo mật để đạt hiệu quả tối đa.

Khi có thắc mắc, nghi ngờ, Quý khách vui lòng liên hệ ngay với VietinBank thông qua Trung tâm dịch vụ Khách hàng 24/7: 1900 55 88 68 hoặc liên hệ với Chi nhánh/ Phòng giao dịch VietinBank nơi gần nhất để được hỗ trợ, giải đáp.

VietinBank trân trọng cảm ơn sự hợp tác của Quý khách hàng!