SeABank

NGÂN HÀNG THƯƠNG MẠI CỔ PHẦN
ĐÔNG NAM Á

HƯỚNG DẪN GIAO DỊCH THẺ AN TOÀN

Để đảm bảo an toàn bảo mật, bảo vệ quyền và lợi ích của chính mình, khi thực hiện giao dịch bằng thẻ của SeABank,Quý khách hàng vui lòng đọc kỹ và tuân theo các thông tin hướng dẫn sau đây. SeABank trân trọng cảm ơn Quý khách hàng!

I. Hướng dẫn giao dịch an toàn với thẻ SeABank

1. Nguyên tắc chung

- Kiểm tra các thông tin trên thẻ đảm bảo đúng với các thông tin Quý khách đã đăng ký
- Ký ngay vào dải chữ ký ở mặt sau thẻ
- Thông báo ngay cho Ngân hàng những thay đổi của Quý khách về địa chỉ cư trú, địa chỉ gửi sao kê, thay đổi số điện thoại liên hệ, chữ ký…
- Đổi mã PIN tại máy ATM ngay sau nhận được thẻ
- Thường xuyên thay đổi mã PIN để bảo mật thông tin
- Không chọn mã PIN gắn liền với các thông tin cá nhân như số di động, ngày sinh…
- Tuyệt đối không tiết lộ mã PIN cho bất kỳ ai
- Luôn lấy tay che bàn phím khi nhập mã PIN đề phòng có người nhìn trộm hoặc quay lén
- Không lưu trữ thẻ và PIN cùng nơi
- Không viết mã PIN trên thẻ
- Không cung cấp thông tin trên thẻ (bao gồm toàn bộ số thẻ, ngày hết hạn thẻ và số CVV) cho bất kỳ ai

2. Nguyên tắc bảo quản thẻ

- Cất giữ thẻ ở nơi an toàn và bảo mật
- Không cung cấp thông tin thẻ (số thẻ, ngày hiệu lực, mã số PIN, địa chỉ, họ tên chủ thẻ...) khi nhận được email/điện thoại yêu cầu cung cấp/xác nhận thông tin hoặc các cuộc gọi nghi ngờ khác
- Không cho bất kỳ ai mượn, sử dụng, sở hữu và quản lý thẻ của Quý khách
- Không để thẻ ở gần những vật từ tính (điện thoại di động, nam châm…), các nơi có độ ẩm cao
- Tránh để thẻ cùng các vật nhọn dễ gây trầy, xước; tránh để thẻ bị cong vênh; tránh để rơi thẻ xuống nước
- Trường hợp thẻ hết hạn, Quý khách thực hiện đục lỗ Chip và cắt dải băng từ trước khi hủy để đảm bảo thẻ không bị làm giả thông tin và gửi lại Ngân hàng.
- Vì lý do bảo mật, Quý khách không lưu giữ bản sao mặt trước và mặt sau thẻ.

3. Nguyên tắc khi giao dịch tại máy ATM.

- Nên thực hiện giao dịch tại các máy ATM vào ban ngày, nơi có đông người qua lại hoặc có bảo vệ
- Quan sát kỹ trước khi thực hiện giao dịch tại ATM. Không giao dịch nếu máy ATM có thiết bị lạ gắn vào khe đọc thẻ/bàn phím hoặc nhiều camera gắn tại cùng 1 ATM. Nếu phát hiện các trường hợp bất thường thì ngừng giao dịch và thông báo ngay cho Ngân hàng qua hotline 1900 555 587
- Khi thực hiện giao dịch khách hàng chú ý dùng tay che bàn phím để tránh lộ PIN
- Luôn kiểm tra tiền và lấy lại thẻ sau khi thực hiện giao dịch.
- Cần đợi máy chi tiền ra, không nên bỏ đi ngay để tránh trường hợp máy ATM nhả tiền chậm và người khác có thể lấy được số tiền này.

- Trường hợp máy báo nhập sai số PIN, kiểm tra kỹ số PIN, sau đó thực hiện lại giao dịch. Nếu nhập sai PIN 03 lần liên tiếp, thẻ sẽ bị khóa do nghi ngờ gian lận. Trường hợp thẻ bị khóa, Quý khách vui lòng đến Chi nhánh/ Phòng Giao dịch của Ngân hàng để mở khóa thẻ và phát hành lại PIN.

4. Nguyên tắc khi thanh toán bằng thẻ tại các đơn vị chấp nhận thẻ (ĐVCNT)

- Luôn yêu cầu thực hiện thanh toán thẻ qua đầu đọc Chip, và chỉ đồng ý thực hiện giao dịch qua dải từ trong trường hợp máy cà thẻ không có đầu đọc Chip.
- Đảm bảo giao dịch phải được thực hiện trong tầm mắt của Quý khách để quan sát việc cà thẻ của thu ngân
- Nếu phát hiện thu ngân thực hiện giao dịch nhiều lần, yêu cầu thu ngân dừng lại và liên hệ với Hỗ trợ khách hàng 24/7 CallCenter để kiểm tra số dư tài khoản thẻ. Sau đó yêu cầu thu ngân xác nhận số tiền giao dịch, hủy các hóa đơn thẻ không chính xác.
- Chú ý kiểm tra các thông tin trên hóa đơn thanh toán thẻ, đảm bảo các thông tin chính xác, đầy đủ.
- Chỉ ký nhận thanh toán khi đồng ý về tất cả các thông tin trên hóa đơn.
- Đảm bảo tất cả các giao dịch bằng thẻ tại các ĐVCNT phải được tiến hành trước mắt Quý khách.
- Đảm bảo được nhận lại thẻ sau khi thực hiện xong giao dịch tại các ĐVCNT.
- Giữ lại các hóa đơn thanh toán thẻ và các chứng từ có liên quan để phục vụ việc tra soát khiếu nại sau này (nếu có).

II. Hướng dẫn giao dịch an toàn trên các kênh Ngân hàng điện tử

1. Nguyên tắc về bảo mật thông tin

QUÝ KHÁCH HÀNG KHÔNG NÊN:

- Mở tài khoản và đăng ký dịch vụ Ngân hàng điện tử cho người khác sử dụng.
- Cung cấp số thẻ, ngày hiệu lực thẻ, số CVV2, PIN, mật khẩu, tên truy cập (username) của bất kỳ dịch vụ Ngân hàng điện tử nào cho bất cứ ai qua bất kỳ kênh nào như điện thoại, email, đường link….
- Click vào các đường link lạ và khai báo thông tin cá nhân cho bất kỳ địa chỉ email đã gửi đến hoặc điện thoại gọi tới. SeABank 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 email.
- Chuyển tiền, nạp tiền vào số điện thoại chỉ định để làm thủ tục nhận thưởng. SeABank không bao giờ yêu cầu khách hàng chuyển tiền, nạp tiền vào số tài khoản nào đó để nhận thưởng bất kỳ chương trình khuyến mại nào của SeABank.

QUÝ KHÁCH HÀNG NÊN:

- Về cài đặt mật khẩu: Sử dụng mật khẩu đủ tin cậy là mật khẩu đủ độ dài (từ 8 ký tự), có sự kết hợp giữa chữ hoa với chữ thường, chữ số…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 123456…
- Về 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. Tránh viết mật khẩu ra giấy hoặc ghi chép dưới hình thức khác.
- Thay đổi mật khẩu truy cập SeANet, Mobile Banking 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.

2. Nguyên tắc về sử dụng dịch vụ an toàn

- Chỉ nên sử dụng máy tính cá nhân để thực hiện các giao dịch điện tử
- Sử dụng trình duyệt web an toàn: Hãy tìm ký tự "s" sau "http" trong địa chỉ trang web hoặc URL của các cửa hàng trực tuyến mà bạn đang truy cập. Chỉ thực hiện giao dịch tại các website uy tín, các địa chỉ mua hàng tin cậy
- Không lưu thông tin thẻ để người khác có thể lợi dụng
- Cẩn trọng trước bất kỳ thông báo yêu cầu cung cấp thông tin thẻ (để nâng hạng, đổi thẻ, tăng hạn mức,…) từ các website/email tương tự với website/email của Ngân hàng phát hành thẻ; liên hệ với CN phát hành thẻ của ngân hàng thẻ để xác minh thông tin; chỉ cung cấp thông tin bằng văn bản tại CN phát hành.
- 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.
- Nên đăng ký sử dụng dịch vụ nhận tin nhắn/email 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.

III. Cảnh báo các loại hình rủi ro thẻ

Để Quý khách chủ động phòng ngừa rủi ro, giảm thiểu tổn thất, SeABank liệt kê ở đây một số loại hình rủi ro thẻ mà tội phạm thường sử dụng hiện nay:

1. Rủi ro trực tuyến

- Lừa đảo tài chính: tội phạm gửi email hoặc gọi điện cho Khách hàng thông báo KH sẽ nhận được một khoản tiền lớn và yêu cầu nộp một khoản tiền để nhận thưởng. KH tin tưởng và tiến hành nộp tiền vào tài khoản của tội phạm và chịu rủi ro
- Trộm danh tính: là hành vi của cá nhân, tổ chức thu thập các thông tin cá nhân của khách hàng để kiếm các lợi ích tài chính. Chủ thẻ thường không chú ý đến vấn đề bảo mật thông tin thẻ (số thẻ, ngày hết hạn, số CVV) dẫn đến để lộ thông tin và bị tội phạm thực hiện giao dịch trục lợi gây tổn thất cho khách hàng.
- Virus, phising: là những chương trình hay đoạn mã phá hoại máy tính của nạn nhân bị lây nhiễm để lấy cắp các thông tin cả nhân và tiến hành trục lợi, đặc biệt là các thông tin về thẻ của KH

2. Rủi ro tại ATM, POS

- Tội phạm lắp thiết bị công nghệ cao tại ATM/POS để đánh cắp thông tin trên thẻ của khách hàng làm thẻ giả và trục lợi gây tổn thất tài chính cho khách hàng.

IV. Các giải pháp bảo mật tại SeABank

- Thẻ và các thiết bị chấp nhận thanh toán thẻ của SeABank đạt chuẩn EMV – chuẩn bảo mật cao nhất của Tổ chức thẻ quốc tế Visa. Master, hạn chế được tối đa khả năng bị đánh cắp thông tin thẻ cho khách hàng trong quá trình giao dịch
- Sử dụng công nghệ bảo mật xác thực hai yếu tố thông qua thiết bị bảo mật tin nhắn One Time Password. Mỗi mật khẩu sinh ra chỉ được sử dụng một lần duy nhất và không trùng lặp nên tin tặc không thể xâm nhập vào tài khoản của Quý khách để thực hiện giao dịch bất hợp pháp.
- Cơ chế tự động khóa tài khoản SeANet: Sau 5 lần đăng nhập không thành công, SeABank sẽ tạm khóa tài khoản của Quý khách. Để kích hoạt lại tài khoản, khách hàng cần liên hệ với SeABank để được hỗ trợ.
- Bảo mật toàn bộ thông tin thẻ của khách hàng theo chuẩn bảo mật quốc tế PCI DSS.
- Các giải pháp khác được thực hiện đồng bộ trong các khâu thiết kế và vận hành dịch vụ dựa trên nền tảng công nghệ hiện đại, tiên tiến và các chế độ cảnh báo rủi ro đáp ứng các thông lệ quốc tế.

V. Liên hệ với SeABank

Trong trường hợp thẻ bị nuốt, mất cắp, thất lạc, thẻ bị lợi dụng, hoặc nghi ngờ gian lận, Quý khách liên hệ với ContactCenter theo số điện thoại **1900 555 587** đối với các cuộc gọi trong nước hoặc **(043) 6276 629** đối với trường hợp ở nước ngoài để được hỗ trợ.