HƯỚNG DẪN GIAO DỊCH THẺ AN TOÀN

!!!CHÚ Ý

Một số thủ đoạn gian lận trong giao dịch thẻ:

- **ATM Skimming:** Hình thức đánh cắp thông tin khi giao dịch ATM bằng cách **gắn thiết bị lạ** vào đầu đọc thẻ hoặc gắn camera/bàn phím giả để đánh cắp thông tin thẻ
- **Nhân viên tại ĐVCNT sao chép, đánh cắp** thông tin thẻ trong quá trình giao dịch, thanh toán
- Phishing/Vishing/Smishing: Tội phạm **gửi email/cuộc gọi/tin nhắn giả danh** nhân viên ngân hàng, các cơ quan nhà nước,... yêu cầu chủ thẻ đăng nhập vào các trang web/ứng dụng giả mạo chứa mã độc để chiếm đoạt thông tin thẻ của khách hàng

	NÊN	KHÔNG NÊN
BẢO MẬT THÔNG TIN THẺ	- **Kiểm tra thông tin trên thẻ**, bảo đảm thông tin trên thẻ trùng khớp với thông tin Quý khách đã đăng ký khi nhận thẻ - **Thay đổi mã PIN** ngay khi nhận được thẻ - **Dán che số CVV** ở mặt sau của thẻ - **Thường xuyên theo dõi biến động** số dư thẻ và sao kê thẻ	- Cung cấp thông tin thẻ **(số thẻ/mã PIN/ngày hết hạn/mã CVV)** cho bất kỳ ai thông qua bất kỳ phương thức giao tiếp nào (email, tin nhắn, trao đổi miệng...) - Lưu trữ thông tin thẻ trên các thiết bị điện tử và các website cũng như dưới bất kỳ hình thức nào.
KHI GIAO DỊCH TẠI ATM VÀ POS	- Chủ động kiểm tra vị trí bàn phím, camera, đầu đọc thẻ trước khi thực hiện giao dịch để đề phòng thẻ bị đánh cắp thông tin - Dùng tay che bàn phím khi nhập mã **PIN** - Trực tiếp quan sát quá trình thực hiện giao dịch - Thường xuyên **thay đổi PIN** hoặc khi có dấu hiệu bất thường - Đối chiếu số tiền hóa đơn với số tiền bị trừ trên tài khoản - Giữ lại hóa đơn thanh toán sau khi giao dịch - Ngay lập tức ngừng giao dịch và liên hệ với SeABank khi có dấu hiệu bất thường	- Bỏ đi khi giao dịch tại **ATM** chưa hoàn thành - Đưa thẻ cho người khác thanh toán hộ - Không giữ lại hóa đơn thanh toán sau khi thực hiện giao dịch - Đọc/cung cấp thông tin thẻ **(số thẻ/mã PIN/ngày hết hạn/mã CVV)** cho bất kỳ ai
KHI GIAO DỊCH TRỰC TUYẾN	- Chủ động **khóa/mở khóa** tính năng giao dịch trực tuyến theo nhu cầu sử dụng - **Cài đặt hạn mức** giao dịch trực tuyến phù hợp với nhu cầu - **Chủ động gỡ bỏ thông tin thẻ** khỏi các trang web khi không còn nhu cầu thanh toán, sử dụng dịch vụ - **Hạn chế thực hiện giao dịch** tài chính trên các trang web lạ	- Luôn luôn mở tính năng thanh toán trực tuyến ngay cả khi không có nhu cầu sử dụng - Cài đặt hạn mức giao dịch trực tuyến quá cao so với nhu cầu thực tế - Thanh toán tại các trang web, địa chỉ không rõ nguồn gốc - **Tiết lộ, cung cấp mã OTP** cho bất kỳ đối tượng nào, kể cả nhân viên ngân hàng

Trong bất kỳ trường hợp nào, nếu Quý khách nghi ngờ thẻ của mình bị mất hoặc bị lợi dụng, gian lận Quý khách vui lòng thực hiện:

- **Ngay lập tức khóa thẻ** trên App SeAMobile/SeANet
- **Liên hệ tổng đài theo** hotline CSKH: KHCN 1900 555 587 – KHDN 1900 599 952 - KHUT 1800 558 899
- **Email đến CSKH:** contact@seabank.com.vn và khut@seabank.com.vn (dành cho KH ưu tiên)
- **Hoặc đến các CN/PGD** gần nhất của SeABank để được hỗ trợ

TẢI SEAMOBILE NGAY