Hướng dẫn bảo mật thanh toán qua VinID Pay

Việc sử dụng ví điện tử và các dịch vụ trực tuyến khác trong hoạt động thanh toán ngày càng trở nên thuận tiện và phổ biến. Tuy nhiên đây cũng là nơi để kẻ xấu lợi dụng để khai thác, thực hiện hoạt động giả mạo, lừa đảo khách hàng để chiếm đoạt tài sản, lấy cắp thông tin cá nhân/ tổ chức. Để các hoạt động thanh toán trên ví điện tử được thực hiện đảm bảo an toàn, VinID Pay đã triển khai nhiều biện pháp tăng cường an ninh bảo mật trên ứng dụng. Tuy nhiên, để các biện pháp này thực sự hiệu quả, sự phối hợp của các Đơn vị chấp nhận thanh toán và Khách hàng là rất quan trọng trong việc phát hiện sớm và ngăn chặn kịp thời các hoạt động bất hợp pháp của đối tượng xấu.

Một số hướng dẫn an toàn bảo mật dành cho Đơn vị chấp nhận thanh toán của VinID Pay

Các hướng dẫn này được khuyến nghị áp dụng cho các thiết bị, phần mềm, ứng dụng, hạ tầng công nghệ thông tin (CNTT) tham gia hoặc hỗ trợ hoạt động thanh toán từ phía các đơn vị chấp nhận thanh toán của VinID Pay

- Sử dụng các thiết bị, phần mềm hợp pháp, có nguồn gốc xuất xứ rõ ràng, còn thời hạn sử dụng hoặc vẫn được hỗ trợ từ nhà sản xuất.
- Thực hiện bảo trì, bảo dưỡng thiết bị, hạ tầng CNTT theo hướng dẫn từ nhà sản xuất.
- Triển khai các giải pháp bảo mật như tưởng lửa, thiết bị phát hiện xâm nhập, phòng chống mã độc, virus…
- Lập danh sách các thiết bị, phần mềm, ứng dụng tham gia hoặc hỗ trợ hoạt động thanh toán, định kỳ kiểm kê, rà soát danh sách quản lý tài sản
- Thực hiện quy trình kiểm soát trước khi triển khai thay đổi, nâng cấp về cấu hình, chức năng trên các thiết bị, phần mềm, ứng dụng.
- Phân quyền truy cập cho người dùng theo đúng chức năng nhiệm vụ, và thực hiện rà soát quyền truy cập của người dùng theo định kỳ.
- Thiết lập mật khẩu mạnh theo tiêu chuẩn bảo mật quốc tế, có thể triển khai giải pháp xác thực đa yếu tố nếu điều kiện công nghệ cho phép.
- Ghi nhật ký hoạt động của hệ thống, hoạt động của người dùng trên hệ thống và thực hiện bảo vệ tính bí mật và toàn vẹn của tập tin nhật ký.

- Thường xuyên rà soát nhật ký hoạt động ghi nhận trên hệ thống để phát hiện kịp thời các hoạt động bất thường.
- Tiến hành đánh giá, rà soát lỗ hổng bảo mật hoặc tấn công kiểm thử trên các hệ thống ứng dụng để phát hiện kịp thời các lỗ hổng bảo mật.
- Đánh giá rủi ro hoạt động CNTT hàng năm nhằm nhận diện các rủi ro và đưa ra các phương án xử lý giảm thiểu rủi ro kịp thời.
- Tiến hành đào tạo và nâng cao nhận thức của nhân viên về an toàn bảo mật khi thực hiện các giao dịch thanh toán với khách hàng sử dụng dịch vụ của VinID Pay.

Một số hướng dẫn an toàn bảo mật thông tin dành cho Khách hàng khi sử dụng dịch vụ thanh toán của VinID Pay

Khi sử dụng ví điện tử VinID Pay và các dịch vụ thanh toán trực tuyến khác, Khách hàng có thể gặp phải những rủi ro sau:

- Đối tượng lừa đảo mạo danh là cơ quan công an, nhân viên ngân hàng, nhân viên của VinID Pay… liên hệ với khách hàng để đưa ra các thông tin như tài khoản khách hàng thực hiện giao dịch bất hợp pháp, vi phạm pháp luật, hay tài khoản sẽ bị trừ tiền hoặc bị khóa; và yêu cầu khách hàng cung cấp các thông tin cá nhân như thông tin đăng nhập, mật khẩu, mã PIN …

- Đối tượng lừa đảo mạo danh là người thân, người quen, bạn bè để nhờ khách hàng chuyển tiền, vay tiền, nạp tiền điện thoại, thanh toán các khoản tiền mua hàng online …

- Đối tượng lừa đảo thông báo khách hàng nhận được gói bưu kiện, hay hàng hóa mua online trên các trang thương mại điện tử, và yêu cầu khách hàng thanh toán cước phí vận chuyển, phí lưu kho …

- Đối tượng lừa đảo giả mạo là người nước ngoài, nhà đầu tư, chủ doanh nghiệp ... để kêu gọi góp vốn, đầu tư kinh doanh (mua bán bất động sản, chứng khoán, tiền ảo …) hoặc giả mạo thành người mua hàng hoặc bán hàng online để yêu cầu khách hàng chuyển tiền vào tài khoản.

- Đối tượng lừa đảo thông báo khách hàng trúng các giải thưởng lớn, các phần thưởng có giá trị và yêu cầu khách hàng cung cấp thông tin cá nhân để xác thực, hoặc chuyển tiền vào tài khoản để nhận giải thưởng.
- Đối tượng lừa đảo tạo dựng các trang web, các fanpage trên mạng xã hội giả mạo của VinID Pay để thực hiện tiếp cận, chăm sóc, tư vấn khách hàng, từ đó yêu cầu khách hàng cung cấp thông tin cá nhân, thông tin tài khoản để phục vụ mục đích lừa đảo.

Để đảm bảo an toàn trước các hành vi lừa đảo, giả mạo, Khách hàng có thể áp dụng các khuyến nghị sau trong việc sử dụng các dịch vụ thanh toán trực tuyến/thanh toán qua ứng dụng di động:

- Không chia sẻ mật khẩu đăng nhập tài khoản VinID, mật khẩu xác nhận thực hiện dịch vụ thanh toán cho người khác, kể cả người thân hay bạn bè.
- Không chia sẻ mã xác thực OTP (mật khẩu sử dụng một lần One Time Password) do Ngân hàng/VinID Pay cung cấp cho khách hàng (qua tin nhắn SMS hoặc trên ứng dụng).
- Khi nhận được tin nhắn thông báo mã xác thực OTP, cần kiểm tra các nội dung được thông báo (như loại giao dịch, số tiền, mục đích của OTP …). Trong trường hợp thông tin không khớp đúng, Quý khách tuyệt đối không nhập OTP vào bất cứ màn hình nào.
- Không chia sẻ thông tin cá nhân, thông tin tài khoản, thông tin thẻ, thông tin đăng nhập vào ứng dụng VinID hoặc dịch vụ thanh toán VinID Pay.
- Thực hiện đổi mật khẩu đăng nhập/mật khẩu thanh toán theo định kỳ tối thiểu 3 tháng một lần hoặc ngay khi bị lộ hay nghi ngờ bị lộ.
- Thiết lập phương thức lấy lại mật khẩu theo hướng dẫn của VinID
- Thoát khỏi ứng dụng VinID khi không có nhu cầu sử dụng
- Thiết lập tính năng tự động khóa ứng dụng sau một khoảng thời gian nhất định
- Thiết lập cơ chế xác thực đa yếu tố nếu nền tảng công nghệ cho phép

- Không chia sẻ thiết bị cài đặt ứng dụng cho người khác sử dụng ngoài tầm kiểm soát của khách hàng, hoặc nhờ người khác đăng nhập vào ứng dụng và thực hiện giao dịch.
- Cài đặt các tính năng phòng chống mã độc, virus trên thiết bị di động cài đặt ứng dụng VinID, và đảm bảo các tính năng này được cập nhật liên tục.
- Không sử dụng các thiết bị di động với các phiên bản hệ điều hành đã bị bẻ khóa, hoặc không còn hỗ trợ từ nhà sản xuất để cài đặt và sử dụng ứng dụng VinID.
- Tải ứng dụng từ những nguồn tin cậy và thường xuyên cập nhật các phiên bản mới nhất của ứng dụng thanh toán ví điện tử.
- Thực hiện các hoạt động thanh toán trên ứng dụng khi đảm bảo thiết bị được kết nối vào hệ thống mạng đáng tin cậy.
- Trong các trường hợp bị mất, thất lạc, hư hỏng thiết bị cài đặt ứng dụng VinID hoặc số điện thoại nhận tin nhắn SMS; bị lừa đảo hoặc nghi ngờ bị lừa đảo; bị tin tặc hoặc nghi ngờ bị tin tặc tấn công, Quý khách cần ngay lập tức thông báo cho VinID Pay và thực hiện các thủ tục cần thiết để được hỗ trợ tạm ngừng/tạm khóa tài khoản ví và thẻ/tài khoản ngân hàng.
- Chỉ liên hệ với VinID thông qua các kênh hỗ trợ chính thống như hotline 19006959, hộp thư: cskh@vinid.net hoặc fanpage chính thức facebook.com/vinid.net; và liên hệ Ngân hàng quản lý thẻ/tài khoản để được hỗ trợ.

Điều kiện cần thiết về trang thiết bị cài đặt và sử dụng ứng dụng

- Không sử dụng các thiết bị di động có hệ điều hành bị bẻ khóa để cài đặt ứng dụng VinID và/hoặc VinID Partner.
- Các thiết bị nên kích hoạt tính năng tự động khóa màn hình sau một khoảng thời gian nhất định.
- Chỉ cài đặt ứng dụng VinID trên thiết bị có phiên bản hệ điều hành tối thiểu theo yêu cầu được mô tả trên kho ứng dụng.
- Nên cài đặt thêm các ứng dụng bảo mật trên thiết bị di động.

Các thiết bị không đáp ứng điều kiện, bao gồm nhưng không giới hạn việc thiết bị của người dùng có trạng thái root/ jailbreak, có thể bị chặn khi mở và sử dụng tài khoản ví VinID Pay do không đảm bảo các vấn đề về bảo mật thông tin người dùng. Cụ thể:

- "thiết bị có trạng thái jailbreak" có nghĩa là việc người dùng can thiệp vào hệ thống trên thiết bị để vượt qua rào cản bảo mật của nhà sản xuất cho mục đích thực hiện những tính năng không được phép;
- "thiết bị có trạng thái root" có nghĩa là việc người dùng can thiệp vào hệ thống trên thiết bị để mở quyền tiếp cận gốc cho các ứng dụng và vượt qua rào cản bảo mật của nhà sản xuất cho mục đích thực hiện những tính năng không được phép.

Trong trường hợp này, Khách Hàng có thể tiến hành thao tác trên các thiết bị khác hoặc liên hệ chăm sóc khách hàng để được tư vấn.

Chúng tôi mong muốn Quý đối tác và Khách hàng không ngừng nâng cao nhận thức và cảnh giác trong các hoạt động thanh toán trên ví điện tử VinID Pay nói riêng và các hình thức thanh toán trên nền tảng trực tuyến nói chung, nhằm giảm thiểu các rủi ro không đáng có và góp phần nâng cao trải nghiệm của người dùng trên các nền tảng thanh toán công nghệ số.