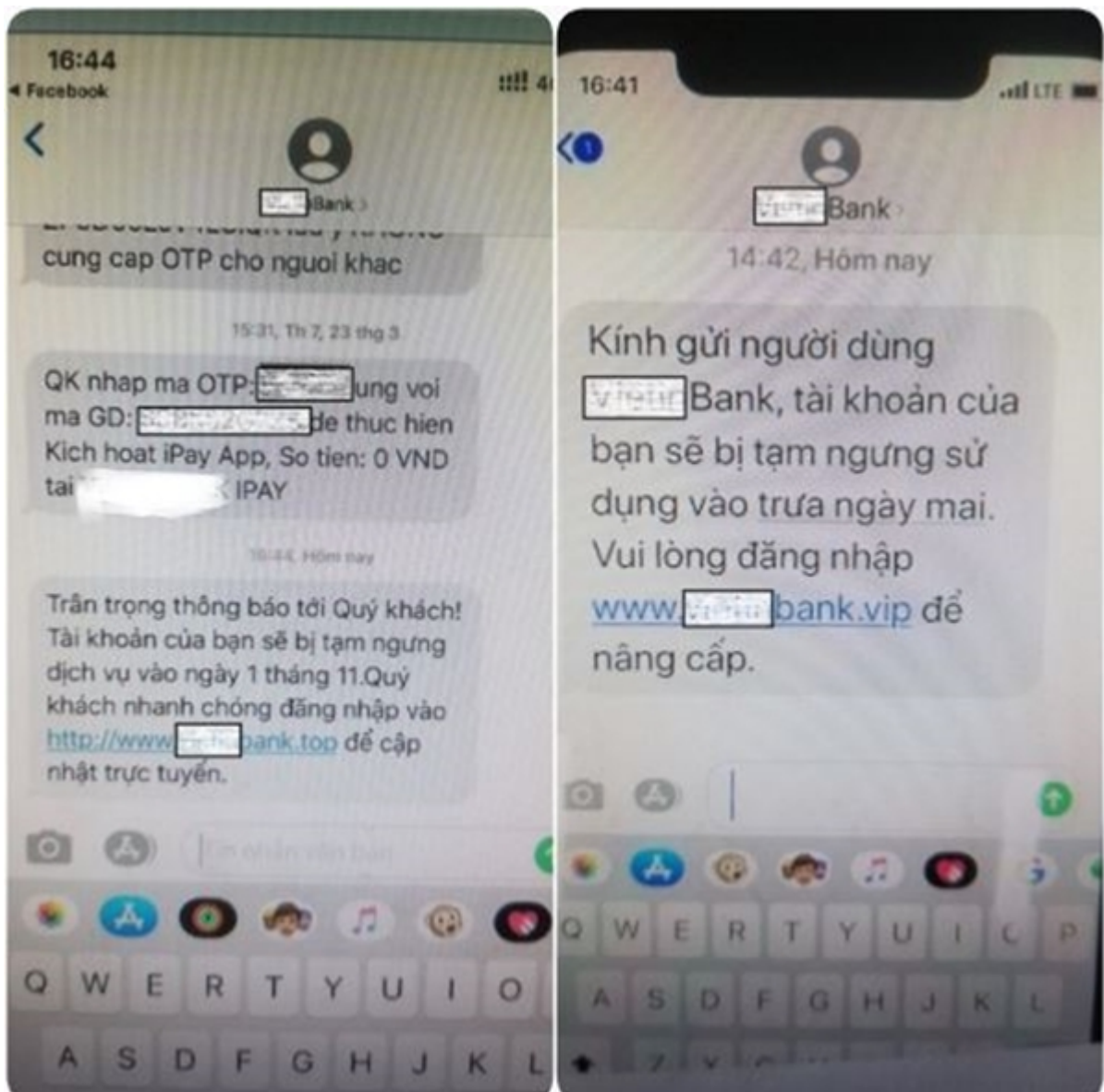


## Bộ Công an cảnh báo thủ đoạn lừa đảo mới rất tinh vi

15:16 12/12/2019

Ngày 12/12, Bộ Công an phát đi cảnh báo về tình trạng các đối tượng phạm tội dùng thủ đoạn giả mạo tin nhắn thương hiệu (SMS Brand Name) để chiếm đoạt tài sản với số tiền lớn. Đây là thủ đoạn hoàn toàn mới, rất tinh vi.



*Các đối tượng hack gửi tin nhắn Brand Name (Ảnh: BCA)*

Theo đó, SMS Brand Name là tin nhắn thương hiệu, được các tổ chức, cá nhân đăng ký độc quyền tại các nhà mạng viễn thông và sử dụng làm dịch vụ gửi tin nhắn hàng loạt đến các khách hàng để chăm sóc khách hàng, quảng bá hình ảnh, thông báo nội dung, chính sách mới...

Trước đây, phương thức thủ đoạn lừa đảo phổ biến vẫn là sử dụng số điện thoại bất kỳ (SIM rác) để phát tán nội dung lừa đảo. Hành vi lừa đảo này đã được cảnh báo, tuyên truyền đến người dân bằng nhiều hình thức khác nhau.

Tuy nhiên gần đây, tội phạm lừa đảo giả mạo tin nhắn thương hiệu - SMS Brand Name của các ngân hàng, nguy hiểm hơn là các tin nhắn giả mạo này lại được lưu trữ cùng thư mục với các tin nhắn thương hiệu “thật” của các ngân hàng trên điện thoại di động của người dùng.

Người dân, khách hàng của các ngân hàng sẽ rất dễ nhầm tưởng đây là thông báo chính thức từ các ngân hàng hay các cơ quan hữu quan.

Bộ Công an cho biết, bằng nhiều nguồn khác nhau, sau khi có được thông tin khách hàng của các ngân hàng, các đối tượng sẽ gửi các tin nhắn giả mạo SMS Brand Name đến khách hàng đó. Trong nội dung các tin nhắn giả mạo này luôn kèm đường dẫn đến các trang web giả mạo do họ quản lý (các trang web này có tên gần giống với các trang web chính thức của ngân hàng) nên người dân dễ lầm tưởng, mất cảnh giác.

Khi người dân truy cập vào đường dẫn trong nội dung tin nhắn, hệ thống sẽ tự động hiển thị một trang web giả mạo, có giao diện, logo tương tự các website chính thức của ngân hàng và được yêu cầu điền các thông tin như tên đăng nhập, mật khẩu, mã OTP...

Như vậy, nhóm tội phạm sẽ kiểm soát được tài khoản chuyển tiền trực tuyến của khách hàng và thực hiện được các hành vi như: chuyển khoản, mở thấu chi, topup thẻ tín dụng, đăng ký vay online...

Bộ Công an nhận định, thủ đoạn này sẽ đặc biệt nguy hiểm khi bị các đối tượng xấu lợi dụng để giả mạo các thông báo chính thức của cơ quan nhà nước, gửi tin nhắn xuyên tạc, không đúng sự thật đến người dân.

Do vậy, Bộ Công an khuyến cáo người dân cần kiểm tra kỹ nội dung tin nhắn nhận được, kể cả các tin nhắn thương hiệu từ ngân hàng để phát hiện các tin nhắn giả mạo ngân hàng, không vội vã trả lời hay thực hiện theo nội dung trong tin nhắn. Website chính thức của các tổ chức, doanh nghiệp sẽ được đăng ký với các cơ quan có thẩm quyền và được đánh dấu an toàn bằng hình ổ khóa bên cạnh tên miền website (giao thức https).

Khi nhận các tin nhắn nghi vấn, không rõ ràng, người dân có thể gọi điện thoại trực tiếp lên tổng đài chăm sóc khách hàng của các ngân hàng để kiểm tra lại thông tin hoặc nhờ những người có kinh nghiệm tư vấn; phản ánh các tin nhắn giả mạo tới ngân hàng và các cơ quan chức năng để có biện pháp xử lý kịp thời...

**Hàng Vương**