TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Giải pháp cho người tiêu dùng trước thực trạng giả mạo tin nhắn thương hiệu

11:00 04/10/2021

Tình hình dịch bệnh Covid-19 đang diễn biến phức tạp, đã có nhiều người tiêu dùng bị các đối tượng giả mạo tin nhắn thương hiệu (SMS Brand Name) để phạm tội chiếm đoạt tài sản.

Đây là thủ đoạn rất tinh vi, cần được người tiêu dùng nhận biết, quan tâm, nâng cao cảnh giác để tự bảo vệ tài sản của chính mình, nhất là trong giai đoạn hiện nay khi khối lượng giao dịch ngân hàng theo phương thức online là rất lớn, do tình hình dịch bệnh nên người dân chủ yếu mua bán hàng hóa thông qua hình thức online và thanh toán qua phương thức chuyển khoản. Chính vì lẽ đó đối tượng phạm tội đã lợi dụng cơ hội này để gia tăng hoạt động.



Ảnh minh họa

Hình thức lừa đảo

SMS Brand Name là một hình thức 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, gọi điện hàng loạt đến các khách hàng, để chăm sóc, quảng bá hình ảnh, thông báo nội dung, chính sách mới… đến khách hàng. Theo nguyên tắc, khi tin nhắn, cuộc gọi Brand Name đã được đăng ký tại các nhà mạng thì các tổ chức, cá nhân khác không được phép đăng ký trùng tên thương hiệu.
Phương thức thủ đoạn lừa đảo phổ biến của các đối tượng 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 tiêu dùng bằng nhiều hình thức khác nhau. Tuy nhiên, thời gian gần đây, các đối tượng lừa đảo đã thay đổi phương thức, thủ đoạn là giả mạo tin nhắn, cuộc gọi thương hiệu - Brand Name của các ngân hàng, công ty điện lực… nguy hiểm hơn là các tin nhắn, cuộc gọi 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. Do đó, người dùng, khách hàng của các ngân hàng, công ty điện lực… sẽ rất dễ nhầm tưởng đây là thông báo chính thức từ các ngân hàng hay các cơ quan hữu quan. Đây là thủ đoạn rất tinh vi và nguy hiểm.
Bằng nhiều nguồn khác nhau, sau khi có được thông tin khách hàng của các ngân hàng, tổ chức… các đối tượng sẽ gửi các tin nhắn, cuộc gọi giả mạo 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 các đối tượng quản lý (các trang web này có tên gần giống với các trang web chính thức của ngân hàng, tổ chức…) nên người dùng dễ lầm tưởng, mất cảnh giác. Khi người dùng 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, tổ chức… và được yêu cầu điền các thông tin như: tên đăng nhập, mật khẩu, mã OTP….
Khi có được các thông tin, các đối tượng 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…

Giải pháp cho người tiêu dùng

Bằng các phương thức, thủ đoạn trên, thời gian qua, các đối tượng đã lừa đảo chiếm đoạt tài sản của nhiều khách hàng với số tiền lớn, xảy ra tại nhiều địa phương trong cả nước. Với phương thức phát tán tin nhắn Brand Name giả mạo ngân hàng, tổ chức… khách hàng rất khó để phân biệt được thật giả. Một số tổ chức đã gửi khuyến cáo về các hình thức lừa đảo để cảnh báo khách hàng của mình nhưng không phải người tiêu dùng nào cũng nhận được thông tin hay hiểu hết được mức độ tinh vi và nguy hiểm của những thủ đoạn trên.
Khi nhận được những tin nhăn như trên, người tiêu dùng cần:

Kiểm tra kỹ nội dung tin nhắn nhận được, kể cả các tin nhắn thương hiệu từ Ngân hàng, tổ chức... để phát hiện các tin nhắn giả mạo ngân hàng, tổ chức... 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 tiêu dùng có thể gọi điện trực tiếp lên tổng đài chăm sóc khách hàng của các ngân hàng, tổ chức... 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, tổ chức... và các cơ quan chức năng để có biện pháp xử lý kịp thời.

Thường xuyên thay đổi mật khẩu đăng nhập tài khoản Internet banking, Smartbanking và có biện pháp để quản lý, bảo mật các thông tin này.

Anh Minh