

Cảnh báo hành vi lừa đảo thay SIM 4G để chiếm đoạt tiền

17:00 05/04/2021

Khi nhận được tin nhắn hay thư điện tử có chứa đường dẫn lạ, người tiêu dùng không nên vội vàng truy cập hoặc nhấp vào đường dẫn đó.

Thời gian gần đây, Tổng đài Tư vấn, hỗ trợ người tiêu dùng 1800.6838 và Hệ thống tiếp nhận, giải quyết yêu cầu, kiến nghị, khiếu nại của người tiêu dùng của Cục Cảnh tranh và Bảo vệ người tiêu dùng (Cục CT&BVNTD) đã tiếp nhận hàng chục cuộc gọi, đơn thư phản ánh về việc bị một số đối tượng mạo danh là nhân viên của các nhà mạng Vinaphone, Mobifone gọi điện, nhắn tin hướng dẫn cú pháp để thực hiện nâng cấp sim 3G thành sim 4G nhằm lừa đảo, chiếm đoạt quyền kiểm soát sim điện thoại, đánh cắp các thông tin thẻ tín dụng, lấy mã OTP và thanh toán hàng chục triệu đồng cho các đơn hàng online bằng thẻ tín dụng của người tiêu dùng.



Ảnh minh họa. (Ảnh: internet)

Lợi dụng chính sách hỗ trợ đổi sim 4G của các nhà mạng và đưa ra những lý lẽ đầy thuyết phục như thực hiện đổi sim theo cú pháp, không giao sim trực tiếp

nhằm hạn chế tiếp xúc, tránh lây lan của dịch bệnh Covid-19; đổi sim ngay để được miễn phí và nhận được các ưu đãi, khuyến mãi; nếu không nâng cấp lên 4G sẽ không thể tiếp tục sử dụng dịch vụ..., các đối tượng lừa đảo đã dễ dàng chiếm được lòng tin của người tiêu dùng.

Khi nhận được tin nhắn hay thư điện tử có chứa đường dẫn lạ, người tiêu dùng không nên vội vàng truy cập hoặc nhấp vào đường dẫn đó. Đối tượng lừa đảo thường tạo ra các website có tên miền gần giống với tên website của các doanh nghiệp có thương hiệu, uy tín nhằm cố ý gây nhầm lẫn cho người tiêu dùng.

Người tiêu dùng cần tìm hiểu thêm thông tin trên website chính thức của các doanh nghiệp viễn thông, tổ chức tín dụng, ngân hàng... thông qua các công cụ tìm kiếm của bên thứ ba như Google, Bing..., sử dụng các thông tin liên lạc (chẳng hạn, gọi điện đến tổng đài chăm sóc khách hàng; đường dây nóng...) được cung cấp trên website chính thức đó để kiểm chứng, xác thực thông tin.

Hà Trần