

Cảnh giác phương thức thủ đoạn lừa đảo mới khi truy cập đường link do shipper gửi

19:00 12/11/2024

Theo Công an TP. Hà Nội, thời gian qua, thủ đoạn giả danh nhân viên giao hàng (shipper) gọi điện lừa đảo chiếm đoạt tài sản của người dân ngày càng nở rộ với nhiều phương thức tinh vi hơn.

Thời gian gần đây đối tượng lừa đảo đã sử dụng phương thức lừa đảo tinh vi hơn, thông qua việc hướng dẫn người dân cài đặt phần mềm giả mạo với "hướng dẫn" để hoàn tiền thanh toán đơn hàng.

Khi cài đặt phần mềm giả mạo, người dân có nguy cơ sẽ bị chiếm quyền điều khiển toàn bộ điện thoại.

Các tin nhắn, cuộc gọi đến điện thoại của nạn nhân sẽ được ứng dụng kiểm soát, ngầm chuyển về máy chủ do đối tượng quản lý, không hiển thị trên điện thoại của nạn nhân.

Nguy hiểm hơn, các đối tượng chiếm quyền điều khiển điện thoại di động từ xa, sau đó truy cập vào tài khoản, chuyển tiền của bị hại.

GIẢ DANH SHIPPER CHIẾM ĐOẠT TÀI SẢN NGƯỜI MUA HÀNG



Cảnh báo thủ đoạn lừa đảo khi truy cập đường link do shipper gửi.
Ảnh minh họa

Ngày 11/11, Công an quận Cầu Giấy (Hà Nội) cho biết, đang điều tra, xác minh vụ người phụ nữ bị kẻ giả danh nhân viên giao hàng (shipper) gọi điện lừa đảo chiếm đoạt gần 100 triệu đồng.

Cụ thể, vào khoảng 9h ngày 1/11, chị B. (SN 2001) nhận được điện thoại của đối tượng nhận là shipper, thông báo có đơn hàng gửi đến. Chị B. trao đổi với đối tượng là để hàng vào nhà và bảo đưa số tài khoản để thanh toán.

Sau khi chuyển khoản, đối tượng gọi lại thông báo là gửi nhầm tài khoản thanh toán của shipper khác và yêu cầu chị phải truy cập vào một đường link của công ty giao hàng để nhận lại tiền gửi nhầm.

Khi truy cập vào đường link, thực hiện theo hướng dẫn và quét mã QR code thì tài khoản của chị B. bị trừ gần 100 triệu đồng. Phát hiện mình bị lừa, chị B. đã đến Công an phường Dịch Vọng Hậu (quận Cầu Giấy) trình báo sự việc.

Nếu như trước đây, các đối tượng chỉ lợi dụng những khách hàng mua sắm nhiều, dễ quên đơn hàng để gọi điện yêu cầu chuyển khoản thanh toán; thì thời gian gần đây đối tượng lừa đảo đã áp dụng phương thức lừa đảo tinh vi hơn, thông qua việc hướng dẫn người dân cài đặt phần mềm giả mạo với “hướng dẫn” để hoàn tiền thanh toán đơn hàng.

Khi cài đặt phần mềm giả mạo, có nguy cơ sẽ bị chiếm quyền điều khiển toàn bộ điện thoại. Các tin nhắn, cuộc gọi đến điện thoại của nạn nhân sẽ được ứng dụng kiểm soát, ngấm chuyển về máy chủ do đối tượng quản lý, không hiển thị trên điện thoại của nạn nhân. Nguy hiểm hơn, các đối tượng chiếm quyền điều khiển điện thoại di động từ xa, sau đó truy cập vào tài khoản, chuyển tiền của bị hại.

Từ thủ đoạn nêu trên, cơ quan công an khuyến cáo người dân hết sức cảnh giác khi nhận số điện thoại lạ, không chuyển khoản khi chưa trực tiếp nhận hàng đã đặt và cần xác minh thật kỹ các thông tin trước khi chuyển khoản. Tuyệt đối không đăng nhập vào các đường link do người lạ gửi tới để tránh mắc bẫy lừa đảo.

Hiện nay, các doanh nghiệp bưu chính, chuyển phát đều có website và ứng dụng để tra cứu thông tin mã vận đơn, do đó người dân nên chủ động truy cập để theo dõi đường đi của đơn hàng, đảm bảo đúng đơn hàng đã đặt trước khi nhận hàng.

Khi bị các đối tượng lừa đảo, chiếm đoạt tài sản người dân cần đến cơ quan công an gần nhất trình báo để được hỗ trợ kịp thời.

Thiên Trường