

CÔNG AN TỈNH QUẢNG TRỊ
CÔNG AN THÀNH PHỐ ĐÔNG HÀ

Số: 455 /CATP-PT
V/v thông báo thủ đoạn lừa đảo
qua tin nhắn điện thoại

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Đông Hà, ngày 30 tháng 3 năm 2022

Kính gửi:

UBND THÀNH PHỐ ĐÔNG HÀ - Thủ trưởng cơ quan, nhà trường, doanh nghiệp trên địa bàn thành phố;
Số: 2080
Ban Điều hành các mô hình ANTT trên địa bàn thành phố;
Ngày: 5/4/2022
UBND các phường.

Chuyển:.....

Lưu hồ sơ số:.....
Hiện nay, hoạt động của tội phạm sử dụng công nghệ cao diễn biến hết sức phức tạp. Đáng chú ý, gần đây, các đối tượng lừa đảo, tội phạm công nghệ cao mạo danh nhân viên chăm sóc khách hàng của các nhà mạng, ngân hàng, ví điện tử để hỗ trợ giải quyết sự cố. Sau đó, đối tượng yêu cầu khách hàng nhắn tin theo cú pháp mà đối tượng đưa ra, rồi chiếm quyền điều khiển sim điện thoại, từ đó lấy tiền trong tài khoản ngân hàng và ví điện tử, sử dụng các dịch vụ mua hàng trực tuyến khác. Cụ thể, các bước đối tượng thực hiện như sau:

- Bước 1: Các đối tượng giả danh nhân viên chăm sóc khách hàng của các nhà mạng, ngân hàng, ví điện tử để hỗ trợ giải quyết sự cố hoặc giả danh nhân viên nhà mạng hỗ trợ nâng cấp SIM lên SIM 4G, 5G. Sau đó, đối tượng yêu cầu khách hàng nhắn tin theo cú pháp ****21*<số điện thoại>#** hoặc **DS <số seri SIM>** gửi 901.

Cú pháp ****21*<số điện thoại>#** thực chất là cú pháp chuyển hướng cuộc gọi (call forward) – dịch vụ của các nhà mạng như Mobifone, Vinaphone, Vietnamobile cho phép thuê bao di động chuyển hướng cuộc gọi đến một số điện thoại nội mạng hoặc ngoại mạng. Sau khi người dùng gửi thành công tin nhắn đã soạn theo cú pháp trên mọi cuộc gọi đến thuê bao của người dùng lập tức được chuyển tiếp đến số điện thoại mà đối tượng lừa đảo cung cấp, trong đó có cuộc gọi cung cấp mã xác thực (OTP) từ ngân hàng, ví điện tử.

Cú pháp **DS <số seri SIM>** gửi 901 là cú pháp đổi SIM điện thoại qua phôi sim trắng theo phương thức nhắn tin. Khi thao tác thành công, người dùng sẽ mất quyền kiểm soát SIM.

- Bước 2: Sau khi người dùng thực hiện theo yêu cầu của đối tượng, đối tượng dễ dàng chiếm đoạt tài khoản mạng xã hội, tài khoản ngân hàng, ví điện tử của nạn nhân bằng cách đăng nhập và chọn tính năng “Quên mật khẩu”. Trường hợp có đầy đủ thông tin cá nhân khác thì rất dễ dàng kích hoạt mật khẩu mới để chiếm đoạt tiền. Ngoài ra, người dùng còn có nguy cơ phải gánh khoản nợ, bởi các đối tượng này có thể sử dụng các thông tin có được để vay tiền từ các ứng dụng, thậm chí là tổ chức tín dụng.

Để phòng ngừa các vụ lừa đảo tương tự, Công an thành phố Đông Hà đề nghị Thủ trưởng cơ quan, nhà trường, doanh nghiệp trên địa bàn thành phố, UBND các phường, Ban điều hành các mô hình về ANTT tổ chức tuyên truyền cho người dân, cán bộ, công nhân, viên chức được biết và nâng cao cảnh giác, chủ động phòng ngừa. Đề bảo vệ tài sản của chính mình, người dân không cung cấp mật khẩu và mã xác thực (OTP) của ví điện tử cho bất kỳ ai bên ngoài ứng dụng. Người dân không bấm vào đường link lạ để nhập mật khẩu và mã xác thực (OTP); đồng thời luôn tra cứu, tìm hiểu thông tin để nắm chắc mục đích, ý nghĩa của các cú pháp tin nhắn trước khi thực hiện.

Khi phát hiện sự việc, đối tượng nghi vấn, đề nghị tập thể, cá nhân thông tin kịp thời đến Công an phường nơi gần nhất hoặc Trục ban Công an thành phố Đông Hà (số điện thoại: 02333.852.250) để có biện pháp đấu tranh kịp thời. /.

Nơi nhận:

- Như trên;
- Phòng PV05 - Công an tỉnh;
- Lưu: VT, PT.

**KT. TRƯỞNG CÔNG AN THÀNH PHỐ
PHÓ TRƯỞNG CÔNG AN THÀNH PHỐ**



Thượng tá Nguyễn Hoài Nam