CÔNG AN TP. HỒ CHÍ MINH
CÔNG AN QUẬN 1

Số: 1697/CV-CAQ1(PT)

V/v phát hành tài liệu tuyên truyền phương thức đánh cắp thông tin và làm giả thẻ ngân hàng tại các máy ATM.

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

Quận 1, ngày 27 tháng 05 năm 2019.

Kính gửi: - Trưởng Công An 10 Phường

Thực hiện Thông báo số 687/TB-CAQ1-TH ngày 16 tháng 05 năm 2019 của Công an Quận 1 về việc đảm bảo an ninh, an toàn hoạt động thanh toán thẻ ngân hàng. Nhằm giúp người dân hiểu rõ về thủ đoạn hoạt động của các loại tội phạm và đề cao tinh thần cảnh giác trong việc sử dụng dịch vụ tại các máy ATM, Công an quận đã biên soạn tài liệu tuyên truyền về phương thức đánh cắp thông tin và làm giả thẻ ngân hàng tại các máy ATM. Đề nghị Trưởng Công an 10 phường triển khai đến CBCS để thực hiện tuyên truyền xuống địa phương. Mọi thắc mắc liên hệ về CAQ1 (qua Đội XDPT) để được giải đáp./.

KT. TRƯỞNG CÔNG AN QUẬN 1
PHÓ TRƯỞNG CÔNG AN QUẬN 1

Thượng tá Nguyễn Thanh Liêm

Nơi nhận:
- Như trên (để thực hiện);
- UBMTTQVN Q1 và các tổ chức thành viên (để phối hợp tuyên truyền);
- Trưởng CAQ1 (thay báo cáo);
- Đội AN (để theo dõi);
- Lưu CAQ1 (PT).

TÀI LIỆU TUYÊN TRUYỀN
PHƯƠNG THỨC ĐÁNH CẮP THÔNG TIN VÀ LÀM GIẢ THẺ NGÂN HÀNG TẠI CÁC MÁY ATM

Trong thời gian vừa qua, tình trạng người nước ngoài nhập cảnh vào Việt Nam theo đường du lịch hoặc tiểu ngạch và di chuyển trên nhiều địa bàn để lắp đặt thiết bị sao chép thông tin (thiết bị Skimming) tại máy ATM nhằm đánh cắp thông tin, làm giả thẻ ngân hàng, rút tiền chiếm đoạt diễn biến phức tạp, thủ đoạn ngày càng tinh vi. Đối tượng chủ yếu tập trung vào các trụ ATM của các ngân hàng như: Vietcombank, Viettinbank, BIDV, Sacombank, Đông Á. Trong năm 2018, cả nước xảy ra 178 vụ đánh cắp dữ liệu, thiệt hại hơn 6,2 tỷ đồng; Quý I/2019 xảy ra 89 vụ đánh cắp dữ liệu, gây thiệt hại 5,4 tỷ đồng.

Thiết bị Skimming là những thiết bị gồm: camera siêu nhỏ, khuôn bàn phím giả để ốp trên bàn phím thật của máy ATM, thiết bị đặt ở khe đút thẻ để sao chép lại thông tin dữ liệu trên thẻ. Việc lắp thiết bị trộm cắp dữ liệu được các đối tượng tiến hành ở những trạm ATM vắng vẻ và thường vào các dịp ngày nghỉ, lễ hội, Tết, tập trung vào các dòng máy ATM cũ như S, SS22, SS34 hoặc các máy ATM có tầng suất giao dịch lớn, tại các vị trí thuận lợi. Các đối tượng thường chia thành nhiều nhóm khác nhau: nhóm điều hành, nhóm trộm cắp dữ liệu, nhóm làm thẻ giả, nhóm trực tiếp đi rút tiền. Khi người dùng thẻ ATM tại các máy có gắn thiết bị Skimming thì thao tác gõ mật khẩu sẽ bị khuôn bàn phím giả và camera ghi lại, khi thẻ được đút vào khe thì sẽ bị thiết bị sao chép lại dữ liệu. Từ đây các đối tượng tiến hành đánh cắp thông tin của khách hàng và dùng thẻ giả để rút hết tiền trong tài khoản rồi chiếm đoạt.

Nhằm tránh thiệt hại về tài sản, khi giao dịch tại các trụ ATM và máy POS (loại máy tính tiền chấp nhận thẻ ngân hàng để thanh toán hóa đơn), người dùng cần chú ý những điểm bất thường như sau:

- Khe đút thẻ, khe quẹt thẻ bỗng nhưng dài hơn mọi khi, thẻ nhét vào khó khăn hơn, khe đút thẻ có dấu hiệu bị tháo gỡ, có vết băng keo hoặc có sự can thiệp từ bên ngoài.

- Bàn phím dày hơn bình thường, nhô cao bất thường, khó nhấn hơn, nhập PIN cảm giác có khoảng trống phía dưới hoặc phát ra âm thanh lạ.

- Chú ý quan sát xung quanh máy ATM, nhất là tại các vị trí có thể nhìn thấy rõ bàn phím như nóc máy ATM, hông màn hình ATM... và nhớ che tay khi nhập mã PIN.

Khi phát hiện những điều bất thường trên thì người dùng phải ngừng ngay hoạt động giao dịch, lấy thẻ ra và báo cho ngân hàng, cơ quan Công an gần nhất để kịp thời xử lý.

Công an Quận 1, ngày 27 tháng 05 năm 2019