**Cảnh giác với 3 thủ đoạn lừa đảo của tội phạm công nghệ cao**

THEO DANTRI

16:14 21/04/2020

Lừa đảo qua điện thoại, "bẫy tình" qua mạng xã hội và hack email doanh nghiệp là 3 thủ đoạn phổ biến, gây thiệt hại nặng nhất của bọn tội phạm công nghệ cao hiện nay.

**

*Thượng tá Nguyễn Đăng Nam, Trưởng Phòng Cảnh sát hình sự Công an TP HCM cho biết, phương thức, thủ đoạn của bọn tội phạm lừa đảo qua mạng luôn đổi mới, tinh vi và xảo quyệt.*

**Cảnh giác với 3 thủ đoạn**

Theo Công an TP HCM, thời gian qua tình hình hoạt động của tội phạm lợi dụng công nghệ cao thực hiện hành vi lừa đảo chiếm đoạt tài sản diễn biến phức tạp, gây thiệt hại nghiêm trọng về tài sản cho người dân lẫn doanh nghiệp.

Mặc dù, công an đã tổ chức nhiều đợt tuyên truyền, cảnh báo nhưng vẫn còn nhiều người trở thành nạn nhân của loại tội phạm này. Thủ đoạn phổ biến là lừa đảo qua điện thoại, "bẫy tình" qua mạng xã hội và tội phạm lừa đảo hack email doanh nghiệp.

Thượng tá Nguyễn Đăng Nam, Trưởng Phòng Cảnh sát hình sự Công an TP HCM cho biết, hiện nay các đối tượng lừa đảo qua mạng rất tinh vi, xảo quyệt, phương thức thủ đoạn của bọn chúng luôn luôn đổi mới.

“Các đối tượng phạm tội dùng công nghệ số giả danh các số điện thoại của bưu chính, bưu cục, thậm chí mã số hoá đầu số 069 của Bộ Công an gọi điện đến người dân để thực hiện hành vi lừa đảo”, Thượng tá Nam thông tin.

**

*Các đối tượng lừa đảo sử dụng các thiết bị hiện đại để thực hiện hành vi phạm tội.*

Theo đó, dấu hiệu nhận biết của loại tội phạm lừa đảo qua điện thoại là khi có cuộc gọi đến điện thoại bàn, đầu dây bên kia (đối tượng lừa đảo) xưng danh là cơ quan pháp luật (Công an, Tòa án, Viện kiểm sát) thông báo nợ cước điện thoại hoặc liên quan một vụ án rửa tiền...

Các đối tượng này dọa nạt, yêu cầu nạn nhân phải hợp tác điều tra và làm theo hướng dẫn nếu không sẽ bắt tạm giam 3 tháng, bị xử lý về hình sự. Sau khi dò hỏi được thông tin cá nhân, số tài khoản, những khoản tiền đang gửi ở đâu, bọn chúng yêu cầu nạn nhân chuyển vào tài khoản cho "cơ quan pháp luật" kiểm tra và sẽ trả lại trong vài giờ.

Sau đó, bọn chúng đưa ra số tài khoản do người Việt Nam đứng tên đã chuẩn bị sẵn và yêu cầu chuyển tiền vào. Ngoài ra, đối tượng lừa đảo còn yêu cầu nạn nhân giữ bí mật không được báo cho người thân biết.

Về loại tội phạm dùng chiêu thức "bẫy tình" qua mạng xã hội, đối tượng lừa đảo đóng giả thành người có nhiều tiền, địa vị trong xã hội, giới thiệu là thương gia đang sinh sống tại nước ngoài hoặc quân nhân đang chiến đấu tại Afghanistan, Syria... ngỏ ý làm quen, kết bạn qua các trang mạng xã hội.

Sau thời gian nói chuyện, các đối tượng này hứa kết hôn, bảo lãnh đi nước ngoài, ngỏ ý tặng quà có giá trị lớn (tiền, vàng) để mua nhà tại Việt Nam hoặc làm từ thiện… rồi cho người giả làm nhân viên giao nhận, hải quan, thuế vụ... thông báo thùng quà biếu bị tạm giữ vì bên trong có nhiều ngoại tệ, hàng hóa giá trị... và yêu cầu nạn nhân phải nộp thuế, lệ phí hoặc lo lót để nhận hàng. Các đối tượng giả danh này cung cấp số tài khoản ngân hàng cho nạn nhân nộp tiền rồi bọn chúng rút ra để chiếm đoạt.

**

*Nhiều phụ nữ sập “bẫy tình” sau khi kết bạn với các “thương gia” qua mạng xã hội.*

*Ảnh Hoàng Lam.*

Đối với thủ đoạn lừa đảo hack mail thì nạn nhân là các doanh nghiệp có quan hệ mua bán với công ty nước ngoài, thường liên lạc giao dịch qua email nên các đối tượng lừa đảo xâm nhập email của doanh nghiệp để lấy thông tin về các hợp đồng mua bán hàng hóa, thanh toán tiền.

Sau đó, bọn chúng tạo email giả mạo (giống với email thật của hai bên hoặc chỉ sai khác một ký tự) của đối tác thanh toán tiền hàng và gửi email yêu cầu thanh toán tiền vào một số tài khoản khác với lý do tài khoản thường giao dịch đang gặp trục trặc (do doanh nghiệp đang bị thanh, kiểm tra hoặc tài khoản bị phong tỏa...).

**Người dân cần làm gì**

Đối với loại tội phạm lừa đảo qua điện thoại, Công an TP HCM khuyến cáo người dân dứt khoát từ chối làm việc qua điện thoại, tuyệt đối không làm theo hướng dẫn như bấm phím số trên máy điện thoại, xác minh số điện thoại...; không cung cấp số điện thoại riêng, số tài khoản, thẻ tín dụng, thông tin cá nhân cho bất kỳ ai.

“Nhiều người dân mất cảnh giác, thiếu hiểu biết về pháp luật, sợ bị bắt giam nên cung cấp thông tin cá nhân lẫn người thân và chuyển tiền cho các đối tượng lừa đảo. Có nạn nhân ở quận Tân Phú chuyển 2 lần 500 triệu đồng, có trường hợp ở các tỉnh thành khác chuyển hàng tỷ đồng”, Thượng tá Nam cho hay.

**

*Tang vật trong vụ Công an TP HCM bắt giữ 20 người Trung Quốc sử dụng công nghệ cao, giả danh cơ quan nhà nước để lừa đảo chiếm đoạt tài sản hồi tháng 6/2019.*

Để tránh sập “bẫy tình” qua mạng, người dân không nên làm quen, kết bạn với người nước ngoài hoặc người lạ qua mạng xã hội; không trao đổi hoặc làm theo yêu cầu của các đối tượng giả danh nhân viên giao nhận, hải quan, thuế...

Đối với các doanh nghiệp thì cần phải kiểm tra địa chỉ email của đối tác đảm bảo chính xác 100%. Trường hợp nhận được email yêu cầu thay đổi số tài khoản thụ hưởng thì tuyệt đối không được chuyển tiền mà phải trực tiếp liên lạc ngay với doanh nghiệp đối tác bằng điện thoại để tránh bị lừa đảo.

Trong cả 3 trường hợp trên, nếu người dân đã chuyển tiền thì phải báo ngân hàng phong tỏa ngay số tiền đã chuyển và thông báo cho cơ quan công an gần nhất để xử lý.

“Khi có vụ việc, vụ án nào đó mà liên quan đến một người dân bình thường, cơ quan điều tra sẽ gửi giấy mời, giấy triệu tập được kí tên, đóng dấu, ghi ngày tháng, địa chỉ trụ sở cơ quan rất rõ ràng. Những giấy mời, giấy triệu tập này đều được gửi qua cảnh sát khu vực để chuyển đến cho người dân. Tất cả các hành vi điện thoại cho người dân nói rằng có lệnh bắt, tạm giam, tạm giữ đều là phương thức của bọn lừa đảo”, Thượng tá Nam khuyến cáo./.

(nguồn: <http://daidoanket.vn)>