Bảo vệ quyền và lợi ích hợp pháp của khách hàng cá nhân trước tội phạm công nghệ cao

Nguyễn Thị Tú Trinh, Vũ Minh Hường, Hà Nhật Minh, Nguyễn Văn Mạnh
Khoa Luật, Học viện Ngân hàng

Tội phạm công nghệ cao trong hoạt động của các ngân hàng thương mại tại Việt Nam đang gia tăng với thủ đoạn ngày càng tinh vi, gây hậu quả nặng nề cho xã hội, đặc biệt là đối với khách hàng cá nhân. Xuất phát từ tình hình thực tiễn còn nhiều bất cập trong công tác phòng, chống tội phạm công nghệ cao của các ngân hàng thương mại, nhóm tác giả đã có những tìm hiểu về thực trạng công tác bảo vệ khách hàng cá nhân của các ngân hàng thương mại Việt Nam, từ đó đề xuất những giải pháp có thể áp dụng để bảo vệ tốt hơn trong thời gian tới.

Sự bùng nổ của cuộc Cách mạng công nghiệp lần thứ tư (CMCN 4.0) kéo theo sự gia tăng nhanh chóng về nhu cầu sử dụng các sản phẩm dịch vụ ngân hàng ứng dụng công nghệ hiện đại của nhiều khách hàng. Phân khúc khách hàng cá nhân trở thành một thị trường đầy tiềm năng và chiếm một vị trí quan trọng trong các ngân hàng thương mại. Tuy nhiên, với sự tiến bộ của công nghệ, các khách hàng cá nhân sử dụng những sản phẩm dịch vụ ứng dụng công nghệ hiện đại của các ngân hàng thương mại cũng phải đối mặt với nguy cơ bị tấn công bởi tội phạm công nghệ cao. Do đó, để hội nhập và phát triển, vấn đề bảo vệ quyền và lợi ích hợp pháp của khách hàng cá nhân càng trở nên cấp thiết.

Mối nguy trước sự tấn công của tội phạm công nghệ cao

Theo Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (PA05) - Công an TP Hà Nội, trong năm 2020 có 5 phương thức phạm tội phổ biến của tội phạm công nghệ cao trong lĩnh vực ngân hàng, bao gồm: 1) Trộm cắp dữ liệu của ngân hàng, thông tin tài khoản khách hàng, thông tin thẻ tín dụng; 2) Thủ đoạn phishing câu nhử, lấy cắp thông tin tài khoản; 3) Lợi dụng kẽ hở trong quy trình, lỗ hổng bảo mật để chiếm quyền quản trị hệ thống; 4) Tấn công vào cơ sở dữ liệu, chiếm quyền điều khiển hệ thống để chiếm đoạt tiền của tổ chức tín dụng; 5) Sử dụng tài khoản, thẻ ngân hàng, thẻ cào trong quá trình thực hiện hành vi vi phạm pháp luật. Trong 5 phương thức trên, phương thức được đánh giá phổ biến nhất là trộm cắp dữ liệu của ngân hàng, thông tin tài khoản khách hàng, thông tin thẻ tín dụng. Phương thức này được thực hiện thông qua việc lắp đặt thiết bị đánh cắp thông tin thẻ và mật khẩu tại máy ATM (skimming), lấy cắp/mua thông tin thẻ tín dụng, làm thẻ giả rồi sử dụng trái phép để thanh toán dịch vụ nhà hàng, khách sạn, các dịch vụ trên mạng internet, thậm chí lấy cắp tài khoản, mật khẩu truy cập hệ thống kế toán để chiếm đoạt tiền của khách hàng… Gần đây, nhiều chiêu thức ăn cắp tiền trong thẻ ATM, tài khoản ngân hàng đã được tội phạm công nghệ cao sử dụng là giả danh điều tra viên, cán bộ cơ quan công an, viện kiểm sát, tòa án... liên hệ với nạn nhân bằng

số cố định, khai thác thông tin bằng cách nói rằng chủ tài khoản đang bị điều tra, cần cung cấp thông tin tài khoản, số chứng minh nhân dân…

Trong thời gian vừa qua, trước sự tấn công của tội phạm công nghệ cao vào đối tượng là khách hàng cá nhân, các ngân hàng thương mại đã chú trọng đến công tác phòng, chống thông qua việc nâng cấp nền tảng công nghệ về bảo mật, khắc phục những lỗ hổng thông tin… Một số ngân hàng thương mại đã thường xuyên tổ chức các buổi hội thảo, tập huấn để nâng cao nhận thức cho các cán bộ và nhân viên trong việc phát hiện, điều tra, phòng chống tội phạm công nghệ cao cũng như tìm ra các giải pháp hữu hiệu để bảo vệ các khách hàng của mình. Mặt khác, nhiều ngân hàng đã liên tục phát đi các cảnh báo tới khách hàng về những hành vi nguy hiểm mà tội phạm công nghệ cao thường sử dụng trên chính các website của ngân hàng hay qua tin nhắn trực tiếp tới khách hàng. Tuy nhiên, các biện pháp đang được áp dụng vẫn còn bộc lộ một số hạn chế:

Một là, việc áp dụng khoa học và công nghệ nâng cấp hạ tầng, nền tảng công nghệ trong nhiệm vụ phòng chống tội phạm còn gặp nhiều khó khăn. Nhiều ngân hàng được trang bị hạ tầng công nghệ thông tin còn khá lạc hậu (hầu hết các số liệu cần thiết cho việc báo cáo, quản trị, điều hành hàng ngày hiện vẫn phải tập hợp, tính toán thủ công…). Hệ thống ngân hàng thương mại là đối tượng chịu ảnh hưởng trực tiếp từ nhóm tội phạm công nghệ cao, song việc chưa có một phòng/ban cụ thể để giải quyết những yêu cầu đối với việc bảo vệ quyền và lợi ích hợp pháp cho khách hàng cá nhân đang là một bất cập.

Hai là, sự gia tăng của tội phạm công nghệ cao có tổ chức, mang tính chất quốc tế, với sự liều lĩnh và ngày càng tinh vi hơn. Tính chất quốc tế của tội phạm xuất phát từ sự giao lưu dễ dàng thông qua các kết nối công nghệ trong thời đại CMCN 4.0, kẻ phạm tội từ các quốc gia khác nhau đã gây khó khăn cho công tác truy vết và bắt giữ của các cơ quan chức năng. Bên cạnh đó, các đối tượng phạm tội thường có trình độ về công nghệ thông tin cao, cách thức phạm tội và thủ đoạn che giấu tinh vi, không gian phạm tội "ảo" trên internet nên rất khó xác định được danh tính và địa chỉ thật… cũng là những khó khăn trong hoạt động phòng, chống tội phạm công nghệ cao trong lĩnh vực ngân hàng.

Ba là, nhiều ngân hàng thương mại hiện nay đang phải đối mặt với tình trạng thiếu hụt nhân sự chất lượng cao trong các lĩnh vực chuyên sâu gắn với công nghệ. Việc đảm bảo an toàn, an ninh trong lĩnh vực ngân hàng đòi hỏi phải có lực lượng nhân sự nắm vững về các công nghệ mới nổi của cuộc CMCN 4.0 như trí tuệ nhân tạo, Big Data, Data analytics hay Blockchain... trong khi đó, nguồn nhân lực được đào tạo trong nước chưa đáp ứng được và còn thay đổi chậm so với sự gia tăng của tội phạm công nghệ cao.

Bốn là, các khách hàng cá nhân xuất phát từ nhiều bộ phận dân cư, với trình độ và nhận thức khác nhau nên khả năng tiếp cận công nghệ còn hạn chế. Bên cạnh đó, khả năng bảo mật dữ liệu của các khách hàng cá nhân nhìn chung còn rất khiêm tốn, rất nhiều khách hàng cá nhân dễ dàng đăng tải những thông tin cá nhân quan trọng trên những trang mạng xã hội, lại không thường xuyên cập nhật phần mềm bảo mật cho các thiết bị và ứng dụng chứa nhiều thông tin, tạo rất nhiều sơ hở cho tội phạm công nghệ cao tấn công.

Theo dự báo của nhiều chuyên gia, cùng với sự phát triển mạnh của khoa học và công nghệ, tình hình tội phạm công nghệ cao trong lĩnh vực ngân hàng ở Việt Nam trong những năm tới sẽ càng phức tạp, tính chất, quy mô, thủ đoạn ngày càng tinh vi, xảo quyệt hơn và có chiều hướng ngày càng tăng.

Giải pháp hiệu quả để bảo vệ quyền và lợi ích hợp pháp của khách hàng cá nhân

Việt Nam đang hội nhập và tham gia sâu vào sân chơi của khu vực và thế giới, điều đó mang lại nhiều cơ hội nhưng cũng đặt ra không ít thách thức cho nền kinh tế nói chung và ngành ngân hàng nói riêng. Cuộc CMCN 4.0 đang diễn ra mạnh mẽ, kèm theo dịch vụ ngân hàng số nở rộ, tội phạm công nghệ cao tấn công vào lĩnh vực ngân hàng tại Việt Nam có xu hướng gia tăng cả về số lượng và mức độ ngày càng tinh vi hơn.

Nhằm đón đầu xu hướng phát triển của khoa học và công nghệ, các ngân hàng Việt Nam đang chủ động nghiên cứu, đầu tư mạnh mẽ vào ứng dụng một số thành tựu của CMCN 4.0 trong sản phẩm, dịch vụ, hoạt động và quản trị của mình. Nổi bật nhất là việc triển khai các công nghệ số nền tảng như: điện toán đám mây, phân tích dữ liệu lớn, trí tuệ nhân tạo, các ứng dụng và giải pháp mới như xác thực sinh trắc học, trao đổi dữ liệu mở qua giao diện lập trình ứng dụng (Open API)... nhằm nâng cao hiệu quả hoạt động, làm phong phú thêm những trải nghiệm của khách hàng. Bên cạnh đó, các ngân hàng cũng đã có sự đầu tư lớn về hạ tầng công nghệ thông tin, phần mềm lõi (corebank) thế hệ mới, ứng dụng các giải pháp sáng tạo theo xu hướng chung về chuyển đổi số, số hóa dịch vụ của ngành với mục tiêu cuối cùng là cung cấp các sản phẩm, dịch vụ theo hướng đơn giản, thông minh.

Là đối tượng vừa chịu sự tấn công của tội phạm công nghệ cao, vừa phải bảo vệ quyền và lợi ích cho các khách hàng của mình, nên việc chủ động tìm ra và áp dụng những giải pháp phòng chống và xử lý kịp thời tội phạm, bảo vệ khách hàng là hết sức quan trọng và cấp bách đối với mỗi ngân hàng thương mại. Để làm được điều đó, các ngân hàng thương mại cần thực hiện đồng bộ một số giải pháp sau:

Thứ nhất, các ngân hàng thương mại cần sớm triển khai đồng bộ các biện pháp bảo vệ dữ liệu của khách hàng và đảm bảo sự hoạt động liên tục của hệ thống thông tin trong ngân hàng, cụ thể: nâng cấp công nghệ bảo mật và các giải pháp an ninh mà các ngân hàng đang triển khai như tường lửa, hệ thống phòng chống virus, hệ thống phát hiện xâm nhập (IPS/IDS), mã hóa dữ liệu đối với các hệ thống quan trọng... nhằm ngăn chặn, cảnh báo và bảo vệ cho các server, website, cơ sở dữ liệu của ngân hàng.

Thứ hai, tuyển chọn và đào tạo đội ngũ cán bộ nhân viên có trình độ cao về công nghệ, hiểu biết về pháp luật để ứng biến, xử lý kịp thời khi xảy ra nguy cơ tội phạm xâm nhập và xử lý tình huống khi khách hàng bị tấn công; thường xuyên đào tạo, huấn luyện về nghiệp vụ tin học, kỹ thuật nhằm đảm bảo lực lượng cán bộ có thể thích ứng được với mọi tình huống thực tế diễn biến phức tạp.

Thứ ba, đẩy mạnh công tác tuyên truyền, nâng cao ý thức cảnh giác và tự bảo vệ của các khách hàng trong việc phòng chống tội phạm công nghệ cao. Thường xuyên cảnh báo tới khách hàng việc cẩn trọng trong cung cấp thông tin cá nhân, mật khẩu hoặc số OTP khi thực hiện các giao dịch thanh toán hoặc thực hiện bất kỳ yêu cầu thay đổi thông tin trên mạng xã hội, website, email, điện thoại... Đặc biệt, cần khuyến cáo khách hàng sử dụng các phần mềm có bản quyền, sử dụng mật khẩu có tính bảo mật cao, thường xuyên thay đổi mật khẩu...

Thứ tư, bên cạnh việc tuân thủ nghiêm ngặt các quy trình nghiệp vụ, các quy định của pháp luật, chỉ đạo từ phía các cơ quan quản lý về việc phòng chống tội phạm công nghệ cao…, các ngân hàng thương mại cũng cần có sự tác động ngược lại, nhiều chiều xuất phát từ việc lắng nghe những vướng mắc thực tế của khách hàng cũng như từ những bất cập mà chính ngân hàng gặp phải khi đối mặt với tội phạm để tự hoàn thiện những giải pháp, khắc phục lỗ hổng cho riêng mình.

Thứ năm, tăng cường hợp tác quốc tế trong lĩnh vực đấu tranh phòng, chống tội phạm sử dụng công nghệ cao. Tập trung trao đổi thông tin tội phạm, tiếp nhận sự tài trợ các thiết bị kỹ thuật, công nghệ hiện đại và đào tạo cán bộ trình độ cao từ các tổ chức quốc tế, phục vụ cho công tác đấu tranh phòng chống tội phạm sử dụng công nghệ cao.

Có thể khẳng định, cuộc đấu tranh phòng chống tội phạm công nghệ cao là cuộc chiến không tiếng súng, cuộc chiến của trí tuệ và công nghệ từ 3 bên: ngân hàng, khách hàng và các cơ quan quản lý. Để hạn chế tình trạng gia tăng tội phạm công nghệ cao, cần thúc đẩy hơn nữa sự phối hợp chặt chẽ giữa cơ quan thực thi pháp luật, ngân hàng và người dân nhằm đấu tranh hiệu quả với loại tội phạm này ✍