Tội phạm sử dụng công nghệ deepfake trong giao dịch ngân hàng [3].

Nguy cơ tội phạm sử dụng công nghệ deepfake trong giao dịch ngân hàng

TS Phạm Ngọc Minh[1], PGS.TS Hồ Tú Cường[2]

[1]Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam
[2]Học viện Khoa học và Công nghệ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Công nghệ deepfake là một lĩnh vực của trí tuệ nhân tạo (AI) và học máy (machine learning), với khả năng tạo ra các hình ảnh, video hoặc âm thanh giả mạo một cách rất chân thực, đang trở thành mối đe dọa ngày càng lớn trong lĩnh vực ngân hàng. Tội phạm có thể lợi dụng công nghệ này để thực hiện các hành vi gian lận và lừa đảo tinh vi. Bài viết khái quát về công nghệ deepfake, qua đó nhận diện một số thủ đoạn lừa đảo sử dụng công nghệ này trong hoạt động ngân hàng, từ đó đưa ra một số giải pháp khắc phục, phòng tránh.

Deepfake là gì?

Công nghệ deepfake dựa chủ yếu vào GANs (Generative Adversarial Networks), một kỹ thuật học máy được giới thiệu bởi Ian Goodfellow và các cộng sự vào năm 2014. GANs bao gồm hai mạng neural: một mạng sinh (generator) tạo ra dữ liệu giả, và một mạng phân biệt (discriminator) đánh giá dữ liệu đó. Cả hai mạng này cạnh tranh với nhau để cải thiện khả năng tạo ra dữ liệu giả mạo ngày càng chân thực. Công nghệ này bắt đầu được biết đến rộng rãi vào năm 2017 khi một người dùng Reddit

(trang cộng đồng trực tuyến) chia sẻ các video giả mạo sử dụng công nghệ GANs để hoán đổi khuôn mặt của người nổi tiếng trong các video giả mạo. Mặc dù mục đích ban đầu của các video này gây tranh cãi và lo ngại, nhưng nó nhanh chóng thu hút sự chú ý vì khả năng tạo ra các hình ảnh giả mạo chất lượng cao.

Thực trạng tội phạm sử dụng công nghệ deepfake trong giao dịch ngân hàng

Theo báo cáo của Công ty Bảo mật dữ liệu Sumsub có trụ sở tại London (Vương quốc Anh), công bố vào tháng 11/2023, tình trạng lừa đảo sử dụng công nghệ deepfake đã gia tăng đáng lo ngại trên toàn cầu. Mức độ sử dụng deepfake đã tăng mạnh từ năm 2022, với sự khác biệt rõ rệt theo khu vực: đạt 1740% ở Bắc Mỹ, 1530% ở khu vực châu Á - Thái Bình Dương (APAC), 780% ở châu Âu (bao gồm cả Vương quốc Anh), 450% ở Trung Đông và Bắc Phi (MEA), 410% ở Mỹ Latinh. Tây Ban Nha là quốc gia bị tấn công nhiều nhất bởi deepfake, còn hộ chiếu quốc gia vùng Trung Đông đứng đầu danh sách các loại giấy tờ giả mạo phổ biến toàn cầu. Đặc biệt, Mỹ Latinh chứng kiến sự gia tăng gian lận ở hầu hết các quốc gia trong khu vực [1].

Đầu năm 2024, một nhân viên của một công ty có trụ sở tại Hồng Kông đã chuyển 25 triệu USD cho những kẻ lừa đảo, sau khi nhận được chỉ thị từ người được cho là giám đốc tài chính của cô trong cuộc gọi video với các đồng nghiệp khác. Tuy nhiên tất cả những cá nhân trong cuộc gọi đều không phải là "chính chủ". Những kẻ lừa đảo đã sử dụng deepfake để sao chép hình ảnh các thành viên trong công ty nhằm lừa nhân viên thực hiện giao dịch chuyển tiền [2].

Các công ty dịch vụ tài chính ngày càng lo ngại về gian lận AI tạo ra nhắm vào tài khoản khách hàng. Một báo cáo cho thấy sự gia tăng 700% các sự cố deepfake trong công nghệ tài chính trong năm 2023. Trung tâm dịch vụ tài chính của Deloitte (Anh) dự đoán rằng, AI có thể khiến tổn thất do gian lận ở Mỹ tăng từ 12,3 tỷ USD (năm 2023) lên tới 40 tỷ USD (năm 2027), tương ứng với tốc độ tăng trưởng kép hàng năm là 32% [3].

Xu hướng công nghệ chống deepfake

So sánh khuôn mặt với dữ liệu nhận dạng: Giải pháp cơ bản này yêu cầu so sánh khuôn mặt của người dùng với dữ liệu nhận dạng mà họ cung cấp. Tuy nhiên, phương pháp này dễ bị qua mặt và cần được kết hợp với các giải pháp phức tạp hơn.

Xác minh thực thể sống: Đây là một công nghệ tiên tiến giúp xác định liệu đối tượng tương tác có phải người thật hay không, nhằm ngăn chặn hành vi lừa đảo. Công nghệ này dựa trên các phương pháp như: xác định chuyển động để phát hiện các hành vi giả mạo khuôn mặt tĩnh, sử dụng các thuật toán phức tạp và bộ mô tả trực quan để phân biệt giữa người dùng thật và giả mạo, mô hình mạng nơron học sâu, sử dụng các lớp nơron để xử lý hình ảnh và xác định tính xác thực của người dùng…

Sinh trắc học đa phương thức: Việc kết hợp nhiều phương thức sinh trắc học để tăng cường bảo mật và độ chính xác đang trở thành xu hướng nổi bật. Thay vì chỉ dựa vào một phương thức duy nhất, chẳng hạn như

Xu hướng phát triển trong tương lai của xác thực sinh trắc học [4].

nhận diện khuôn mặt hoặc quét vân tay, các ứng dụng ngân hàng hiện đại đang kết hợp cả hai để xác minh danh tính người dùng. Cách tiếp cận này không chỉ khắc phục được những hạn chế riêng lẻ của từng phương thức mà còn nâng cao mức độ an toàn tổng thể [4].

Sinh trắc học hành vi: Sinh trắc học hành vi đang mở ra một hướng đi mới trong bảo mật, bằng cách phân tích các mẫu hành vi đặc trưng của người dùng như tốc độ gõ phím, cách di chuyển chuột và thói quen sử dụng. Những đặc điểm này rất khó để giả mạo, mang lại một lớp bảo vệ bổ sung cho hệ thống. Đặc biệt, sinh trắc học hành vi cho phép xác thực liên tục, nghĩa là hệ thống có thể liên tục kiểm tra danh tính người dùng trong suốt phiên làm việc, đảm bảo an toàn tối đa [4].

Thẻ thanh toán sinh trắc học: Một bước tiến mới trong công nghệ thanh toán là tích hợp cảm biến sinh trắc học trực tiếp vào thẻ thanh toán. Những thẻ này sử dụng nhận diện vân tay để xác thực giao dịch, loại bỏ nhu cầu nhập mã PIN. Công nghệ này không chỉ tăng cường bảo mật mà còn mang đến sự tiện lợi và dễ sử dụng, giúp người tiêu dùng có trải nghiệm thanh toán an toàn và quen thuộc hơn [4].

Tích hợp công nghệ 4.0 vào xác thực sinh trắc học

Khi công nghệ sinh trắc học tiếp tục tiến bộ, ứng dụng của nó trong ngân hàng dự kiến sẽ phát triển theo những cách thú vị và mang tính đột phá. Các phát triển trong tương lai có thể tập trung vào việc tăng cường bảo mật, cải thiện độ chính xác và mở rộng khả năng sử dụng của các hệ thống sinh trắc học. Những đổi mới như tích hợp sinh trắc học với công nghệ blockchain, các tiến bộ trong AI, và nhu cầu ngày càng tăng về các giải pháp ngân hàng từ xa an toàn đang định hình tương lai của xác thực sinh trắc học trong ngành ngân hàng. Cụ thể:

Tích hợp với công nghệ Blockchain: Tương lai của xác thực sinh trắc học trong ngân hàng có thể bao gồm tích hợp với công nghệ blockchain. Blockchain, với tính phi tập trung và không thể giả mạo, sẽ tăng cường bảo mật cho dữ liệu sinh trắc học, lưu trữ chúng một cách an toàn và không thể thay đổi. Sự kết hợp này có khả năng cách mạng hóa quản lý danh tính và phòng chống gian lận trong ngành ngân hàng.

Trí tuệ nhân tạo tiên tiến và học máy: AI và học máy sẽ tiếp tục nâng cao khả năng xác thực sinh trắc học bằng cách cải thiện độ chính xác và khả năng thích ứng với các mẫu mới. Trong tương lai, các hệ thống sinh trắc học do AI điều khiển có thể phát hiện và phản ứng ngay lập tức với các nỗ lực làm giả tinh vi theo thời gian thực.

Sử dụng xác thực sinh trắc học tại các chi nhánh ngân hàng: Việc xác thực sinh trắc học trực tiếp tại các chi nhánh ngân hàng, như qua nhận diện vân tay hoặc khuôn mặt tại cây ATM hoặc văn phòng, đảm bảo mức độ an toàn và tin cậy cao nhất. Phương pháp này cung cấp một cách xác minh danh tính đáng tin cậy và chính xác, giảm thiểu nguy cơ trộm cắp danh tính và gian lận nhờ vào tính duy nhất và khó sao chép của các đặc điểm sinh trắc học. Đồng thời, nó mang lại trải nghiệm xác thực liền mạch và thuận tiện, nâng cao sự hài lòng của khách hàng bằng cách loại bỏ nhu cầu sử dụng các phương pháp truyền thống như thẻ căn cước hoặc mật khẩu ✍

TÀI LIỆU THAM KHẢO

[1] Identity Fraud Report (2023), *Sumsub Research: Global Deepfake Incidents Surge Tenfold from 2022 to 2023*.

[2] H. Chen, K. Magramo (2024), “Finance worker pays out $25 million after video call with deepfake 'chief financial officer'”, https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html, truy cập ngày 14/6/2024.

[3] K. Araullo (2024), “Shielding from deepfake risks - how exposed are FIs and banks?”, https://www.insurancebusinessmag.com/us/risk-management/news/shielding-from-deepfake-risks--how-exposed-are-fis-and-banks-497226, truy cập ngày 14/6/2024.

[4] Panini (2024), "The future of biometric authentication in banking", https://www.panini.com/blog/the-future-of-biometric-authentication-in-banking, truy cập ngày 14/6/2024.