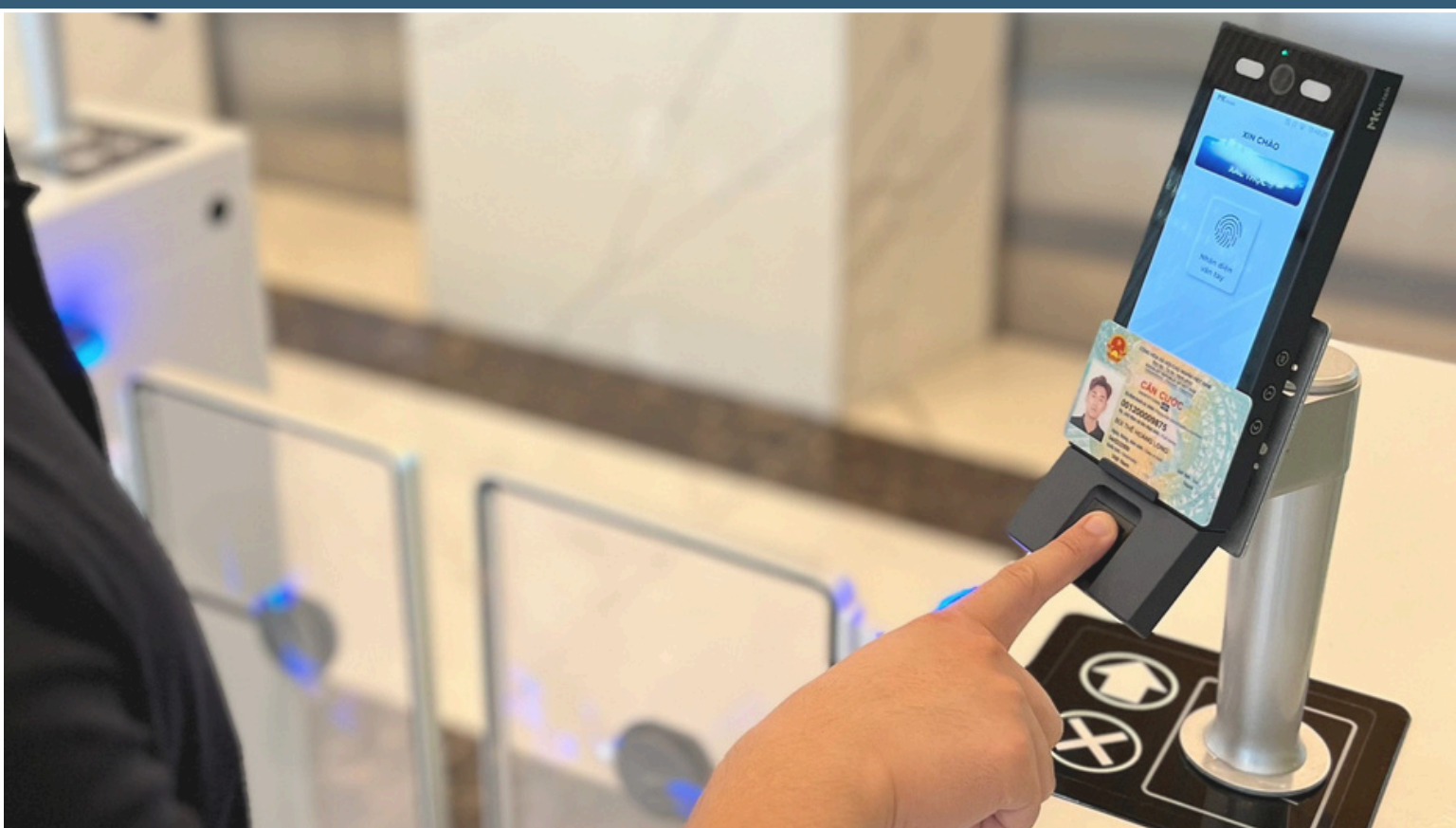


THẺ GIỚI THẺ

Bản tin nội bộ của MK Group

Số 160 | tháng 08.2024



TIN NỔI BẬT

02 MK GROUP ĐỒNG HÀNH CÙNG CÁC TỔ CHỨC TÀI CHÍNH NGÂN HÀNG TRONG HÀNH TRÌNH TUÂN THỦ QUYẾT ĐỊNH 2345/QĐ-NHNN

06 HƠN 21,6 TRIỆU KHÁCH HÀNG ĐÃ XÁC THỰC SINH TRẮC HỌC VỚI DỮ LIỆU DÂN CƯ QUA CĂN CƯỚC GẮN CHIP VÀ VNEID

07 ENTRUST: ĐỒNG HÀNH CÙNG CHÍNH PHỦ TRONG QUÁ TRÌNH CHUYỂN ĐỔI TƯƠNG TÁC CỦA CÔNG DÂN BẰNG DANH TÍNH SỐ

10 CHƯƠNG TRÌNH THANH TOÁN ỨNG DỤNG SINH TRẮC HỌC CỦA MASTERCARD BƯỚC ĐẦU TIẾP CẬN THỊ TRƯỜNG CHÂU ÂU

11 NEPAL YÊU CẦU THẺ ID QUỐC GIA ĐỂ ĐẢM BẢO AN SINH XÃ HỘI TỪ THÁNG 7.2024

12 BÁO CÁO GIAN LẬN DANH TÍNH 2024



MK GROUP ĐỒNG HÀNH CÙNG CÁC TỔ CHỨC TÀI CHÍNH NGÂN HÀNG TRONG

HÀNH TRÌNH TUÂN THỦ QUYẾT ĐỊNH 2345/QĐ-NHNN

Ngày 18/12/2023, NHNN đã ban hành Quyết định số 2345/QĐ-NHNN về triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng (Quyết định 2345). Theo Quyết định số 2345, từ 1/7/2024, các giao dịch chuyển tiền điện tử của cá nhân có giá trị trên 10 triệu đồng hoặc tổng giá trị giao dịch chuyển tiền điện tử trong ngày vượt 20 triệu đồng phải áp dụng một trong các biện pháp xác thực sinh trắc học.

Mục tiêu ban hành Quyết định 2345/QĐ-NHNN là để hướng tới bảo đảm người giao dịch ngân hàng trực tuyến là chính chủ nhằm bảo vệ khách hàng, góp phần giảm thiểu tội phạm lừa đảo chiếm đoạt tài sản của khách hàng, cũng như phòng ngừa những vụ việc cho thuê, mượn, mua bán tài khoản thanh toán, ví điện tử sử dụng cho mục đích bất hợp pháp. Đây cũng là một trong những giải pháp góp phần bảo vệ khách hàng sử dụng dịch vụ ngân hàng.

“

Quyết định 2345/QĐ-NHNN là bước đi quan trọng, giải quyết căn cơ những vấn đề tồn tại trong hoạt động thanh toán số.

Trung tá Triệu Mạnh Tùng,
Phó cục trưởng Cục An ninh mạng và
Phòng, chống tội phạm sử dụng
công nghệ cao (A05), Bộ Công an.

Từ khả năng, lợi thế và kinh nghiệm sẵn có trong suốt 25 năm qua, chúng tôi đã nhanh chóng nghiên cứu, phát triển và triển khai các giải pháp xác thực đa nhân tố tiêu biểu như giải pháp định danh xác thực khách hàng sử dụng căn cước (CC) gắn chip, đối sánh sinh trắc học hoặc các giải pháp xác thực OTP nâng cao... nhằm hỗ trợ các Ngân hàng trong quá trình định danh, xác thực khách hàng sử dụng thẻ CCCD gắn chip, hỗ trợ các Ngân hàng tạo kho dữ liệu đồng bộ, nhất quán từ cơ sở dữ liệu (CSDL) thu thập trong chip của CCCD cũng như hỗ trợ các Ngân hàng làm sạch kho dữ liệu sẵn có của mình, kết hợp với giải pháp nhận dạng, so khớp sinh trắc học trong quá trình thực hiện giao dịch hỗ trợ các Tổ chức, Ngân hàng đáp ứng Quyết định 2345/QĐ-NHNN một cách hiệu quả - nhanh chóng.

1.

Giải pháp định danh, xác thực khách hàng thông qua căn cước điện tử

MK eID

Theo Quyết định 2345/QĐ-NHNN, các tổ chức Tài chính - Ngân hàng cần thu thập, kiểm tra toàn bộ CC gắn chip của khách hàng để đảm bảo CC gắn chip khách hàng sử dụng do đúng Bộ Công an phát hành, đảm bảo dữ liệu trong CSDL của các tổ chức là dữ liệu sạch, đã được bảo đảm và kiểm tra.

Giải pháp định danh - xác thực khách hàng sử dụng CCCD gắn chip của MK như một “chìa khóa” giúp các tổ chức Tài chính - Ngân hàng xác minh danh tính Khách hàng đồng thời giúp Khách hàng chứng minh lý lịch bản thân, tạo profile khi sử dụng dịch vụ:

- Kiểm tra tính đồng nhất giữa khuôn mặt sống/ vân tay sống với dữ liệu sinh trắc học lưu trong thẻ theo cơ chế đối sánh trên thẻ (Matching on Card - MoC), xác thực quan hệ sở hữu giữa thẻ và người sử dụng thẻ
- Kiểm tra tính xác thực của thẻ CCCD gắn chip, chứng thực chữ ký số lưu trong chip của thẻ CCCD, đảm bảo thẻ cho Bộ Công an cấp phát.
- Đọc, giải mã và trích xuất thông tin lưu trữ theo chuẩn ICAO trên ứng dụng định danh (eID) của thẻ CC gắn chip
- MK Group đã có kinh nghiệm triển khai giải pháp định danh - xác thực khách hàng sử dụng CCCD gắn chip trong suốt 4 năm qua, hỗ trợ các Ngân hàng trong quá trình xác thực khách hàng sử dụng CCCD gắn chip trong các luồng nghiệp vụ:



- Mở tài khoản, xác minh khách hàng mới và khách hàng hiện hữu trên kênh Mobile Banking,
- Xác minh khách hàng tại Quầy cùng các thiết bị đầu đọc chuyên dụng,
- Nộp tiền - Rút tiền bằng CCCD gắn chip,...
- Hỗ trợ các Ngân hàng áp dụng tới đa dạng các luồng nghiệp vụ khác nhau theo yêu cầu của mình.

2.

Giải pháp xác thực sinh trắc học khuôn mặt

MK Face Authentication

Giải pháp sinh trắc học của MK được triển khai linh hoạt tại hạ tầng của các tổ chức hoặc triển khai dưới dạng dịch vụ phần mềm (SaaS) với server đặt tại trung tâm RAR của Bộ Công an, giúp các tổ chức linh hoạt lựa chọn phương án triển khai.

Giải pháp sinh trắc học chúng tôi muốn hướng tới không những áp dụng đối với các giao dịch thanh toán trực tuyến, thanh toán thẻ Ngân hàng đáp ứng Quyết định 2345/QĐ-NHNN, chúng tôi hướng tới tất cả dịch vụ khác nhau của các tổ chức, có thể kể đến như thay đổi thông tin cá nhân, đăng ký biến động sổ dư, nâng cao hạn mức giao dịch,...

Các tổ chức tài chính - ngân hàng khi sử dụng giải pháp sinh trắc học của chúng tôi có thể linh hoạt lựa chọn phương án nhận dạng sinh trắc của khách hàng bằng các phương thức:

- Nhận dạng - đối sánh sinh trắc học (khuôn mặt) của khách hàng khớp đúng với dữ liệu sinh trắc học được lưu trong CSDL sinh trắc học về khách hàng đã thu thập và kiểm tra (Match-on-Server);
- Nhận dạng - đối sánh sinh trắc học (khuôn mặt) của khách hàng khớp đúng với dữ liệu sinh trắc học được lưu trong chip của thẻ CCCD gắn chip theo cơ chế đối sánh trực tiếp trên thẻ CCCD gắn chip (Matching on Card - MoC).
- Xử lý hình ảnh, trích xuất và lưu trữ hình ảnh/template hình ảnh khuôn mặt của Khách hàng.

3.

Phương thức xác thực OTP nâng cao

KeyPass OTP

Kết hợp với phương thức xác thực mạnh OTP nâng cao để hoàn thiện bộ giải pháp bảo mật giao dịch trực tuyến, giao dịch thẻ ngân hàng, đáp ứng hạn mức loại D - hạn mức cao nhất theo Quyết định 2345/QĐ-NHNN.

MK Group với hơn 25 năm kinh nghiệm trên thị trường cung cấp giải pháp bảo mật, với gần 15 năm nghiên cứu, triển khai giải pháp xác thực mạnh KeyPass OTP tới 15 Ngân hàng - tổ chức chứng khoán tại Việt Nam. Từ những thời điểm sơ khai khi các NH đẩy mạnh triển khai thanh toán trên Internet Banking - Mobile Banking, chúng tôi đã triển khai các tính năng OTP cơ bản (OTP time-based) dưới dạng ứng dụng độc lập, rồi phát triển các tính năng nâng cao hỗ trợ các NH tuân thủ Quyết định 630/QĐ-NHNN ban hành vào 31/03/2017 cho tới hiện tại MK Group không ngừng phát triển, nâng cấp giải pháp đáp ứng không những các yêu cầu đặc thù của từng Ngân hàng mà còn tuân thủ theo các tiêu chuẩn, xu hướng bảo mật trên toàn thế giới.

Bảo mật:

Giải pháp của MK mang đến khả năng định danh chính xác khách hàng đang yêu cầu giao dịch thông qua việc kiểm tra thực thể sống, so khớp khuôn mặt/ vân tay, xác thực sử dụng thẻ căn cước gắn chip

Tuân thủ văn bản pháp luật:

Hỗ trợ các đơn vị đáp ứng hoàn toàn Quyết định 2345/QĐ-NHNN ban hành ngày 18/12/2023 về triển khai giải pháp về an toàn bảo mật trong thanh toán trực tuyến và thanh toán thẻ dự kiến sẽ có hiệu lực từ 01/07/2024 và các văn bản pháp lý khác.

4.

Lợi ích của các giải pháp đối với các tổ chức tài chính - ngân hàng và người dùng

Phạm vi ứng dụng rộng rãi: Các tổ chức có thể áp dụng rộng rãi trong các luồng nghiệp vụ dịch vụ do các tổ chức cung cấp cho khách hàng như: mở thẻ/tài khoản, đăng ký khoản vay, xác thực trong các giao dịch chuyển tiền, nạp/rút tiền từ ví điện tử, thanh toán, rút tiền qua mã QR tại ATM/STM hay những dịch vụ mà các tổ chức có thể mở rộng trong tương lai đảm bảo xác thực tuân thủ Quyết định 2345/QĐ-NHNN.

Đồng bộ trên tất cả các kênh:

Các tổ chức có thể triển khai Giải pháp trên đa kênh: Kênh Mobile, Kênh quầy, Kênh Kiosk, Kênh ATM/CDM hay các kênh lưu động tại quầy, tại ATM/STM,

Linh hoạt cơ chế xác thực:

Sử dụng cơ chế xử lý đối sánh sinh trắc học trực tiếp trong chip (Matching on Card- MoC) của thẻ CCCD, không thu thập ảnh và thông tin của khách hàng, đáp ứng và tuân thủ nghị định 13/2023/NĐ-CP Bảo vệ dữ liệu cá nhân



- **ĐẢM BẢO TÍNH TOÀN VỆ DỮ LIỆU:** Xác thực Chữ ký số của BCA trên thẻ CCCD để xác minh thẻ thật/giả – Ngăn chặn hành vi giả mạo giấy tờ Dữ liệu chỉ có thể đọc – không thể can thiệp.
- **ĐẢM BẢO ĐỘ TIN CẬY CAO:** Công nghệ xác thực sinh trắc học vân tay/khuôn mặt sống MoC ngay trên chip Dữ liệu được xử lý ngay trên chip giúp hạn chế khả năng lộ lọt, đánh cắp dữ liệu.
- **ĐẢM BẢO TÍNH ĐỒNG BỘ:** Quy trình xác thực nhất quán trên tất cả các kênh Trải nghiệm đồng bộ cho người dùng và linh hoạt cho đơn vị triển khai.
- **TỐC ĐỘ XÁC THỰC NHANH CHÓNG:** Giảm thời gian chờ đợi Góp phần gia tăng hiệu quả hoạt động của các dịch vụ công
- **ĐA KÊNH – ĐA DẠNG THIẾT BỊ:** Triển khai trên đa kênh: ATM, kiosk, quầy giao dịch, mobile... Đa dạng các thiết bị đầu đọc
- **TỐI ƯU CHI PHÍ TRIỂN KHAI:** Linh hoạt tùy chỉnh phù hợp với quy mô và ngân sách khác nhau của người dùng

Với 25 năm kinh nghiệm xây dựng và triển khai nhiều chương trình Thẻ thông minh và xác thực bảo mật cho các tổ chức trong nước và quốc tế, đồng thời là đối tác tin cậy của nhiều tổ chức thẻ, tổ chức thanh toán và các ngân hàng, đội ngũ chuyên gia của MK Group tiếp tục nghiên cứu và hoàn thiện các giải pháp xác thực bảo mật sử dụng căn cước điện tử và dữ liệu sinh trắc học với mong muốn thực thi cam kết đồng hành và hỗ trợ các ngân hàng trong hành trình đáp ứng Quyết định 2345/QĐ-NHNN một cách tuân thủ đúng, đủ và hiệu quả.

HỆ SINH THÁI MK BANKID

Các giải pháp xác thực
bảo mật trên không gian số



MK eID

Giải pháp định danh, xác thực khách hàng sử dụng thẻ CCCD gắn chip

Xác thực sinh trắc học

Giải pháp thực hiện đối sánh, xác thực sinh trắc học khuôn mặt, vân tay của khách hàng dựa trên các đặc điểm sinh trắc học duy nhất

MK KeyPass OTP

Giải pháp xác thực mạnh KeyPass™ OTP với các phương thức xác thực từ OTP cơ bản, OTP nâng cao có chức năng ký giao dịch

MK FIDO2

Giải pháp xác thực mạnh tuân thủ chuẩn FIDO2, phương pháp chống phishing hiệu quả

MK SmartCA - Remote signing

Dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa ứng dụng công nghệ đám mây (cloud-based)

Hà Nội: (024) 7100 6781
Tp. Hồ Chí Minh: (028) 3930 1055

HƠN 21,6 TRIỆU KHÁCH HÀNG ĐÃ XÁC THỰC SINH TRẮC HỌC VỚI DỮ LIỆU DÂN CƯ QUA CĂN CƯỚC GẮN CHIP VÀ VNEID

Tại hội thảo "Rủi ro tài chính và thủ đoạn lừa đảo trong hoạt động tài chính ngân hàng" sáng ngày 11/7/2024, bà Nguyễn Thị Thu, Phó Vụ trưởng Vụ Thanh toán, Ngân hàng Nhà nước chia sẻ sau khi Quyết định 2345/QĐ-NHNN về triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng (Quyết định 2345) được ban hành ngày 18/12/2023 và có hiệu lực từ ngày 1/7/2024, các đơn vị trong ngành Ngân hàng đã quan tâm tổ chức triển khai đồng bộ, bước đầu đạt được những kết quả tích cực.

"Theo số liệu cập nhật đến ngày 10/7/2024, ngành Ngân hàng đã xác thực sinh trắc học với dữ liệu dân cư (thông qua CCCD gắn chip và tài khoản VNeID) được hơn 21,6 triệu khách hàng", bà Nguyễn Thị Thu chia sẻ.

Ngày 8/7/2024 vừa qua, Ngân hàng Nhà nước đã có công văn số 5675/NHNN-CNTT về việc triển khai Quyết định 2345/QĐ-NHNN nhằm bảo đảm an ninh, an toàn hơn nữa cho khách hàng thực hiện giao dịch ngân hàng trực tuyến. Tại công văn này, Ngân hàng Nhà nước đề nghị các tổ chức tín dụng, các chi nhánh ngân hàng nước ngoài, các đơn vị trung gian thanh toán thực hiện:

Đối với giao dịch loại C của khách hàng cá nhân theo quy định tại Quyết định 2345, áp dụng biện pháp xác thực sinh trắc học theo quy định và phải kết hợp với biện pháp xác thực OTP gửi qua SMS/Voice hoặc SoftOTP/TokenOTP.

Rà soát, thiết lập các tiêu chí kỹ thuật của giải pháp xác thực sinh trắc học bảo đảm xác định chính xác chủ thể thực hiện giao dịch, có tính năng phát hiện các hành vi giả mạo dấu hiệu sinh trắc học của vật thể sống (liveness detection) để phòng chống gian lận, giả mạo khách hàng qua hình ảnh (ảnh tĩnh, ảnh động), video, mặt nạ 3D và các hình ảnh, video tạo bởi công nghệ deepfake.

Bên cạnh đó, rà soát tài khoản thanh toán của doanh nghiệp. Trong đó, nghiên cứu, có giải pháp áp dụng các biện pháp ngăn chặn các hành vi mạo danh, can thiệp, chỉnh sửa, làm sai lệch việc xác minh thông tin nhận biết khách hàng trong quá trình mở và sử dụng

tài khoản thanh toán và các biện pháp đảm bảo việc sử dụng tài khoản thanh toán được thực hiện bởi chính chủ tài khoản thanh toán hoặc người đại diện hợp pháp.

Theo đại diện Vụ Thanh toán, thời gian tới, Ngân hàng Nhà nước sẽ tiếp tục nghiên cứu, hoàn thiện hành lang pháp lý đảm bảo an ninh, an toàn hoạt động thanh toán.

Đồng thời, tổ chức triển khai các văn bản pháp luật mới được ban hành và tiếp tục chỉ đạo các tổ chức tín dụng; tiếp tục đẩy nhanh thực hiện triển khai, vận hành hệ thống giám sát các tài khoản thanh toán, ví điện tử nghi ngờ gian lận (SIMO); đẩy mạnh truyền thông, thông tin đến các khách hàng dưới nhiều hình thức để hướng dẫn, nâng cao nhận thức, hiểu biết của khách hàng về ứng dụng công nghệ.

Bà Nguyễn Thị Thu khẳng định, Ngân hàng Nhà nước sẽ tiếp tục phối hợp với Bộ Công an chỉ đạo các tổ chức tín dụng đẩy mạnh triển khai Kế hoạch 01 về triển khai Đề án 06 để làm sạch dữ liệu, xác thực khách hàng và ứng dụng, triển khai các hoạt động nghiệp vụ ngân hàng...

(TaichinhTiente)

CHƯƠNG TRÌNH THẺ

- Từ 05/07/2024 cho đến hết ngày 31/10/2024, Ngân hàng Nông nghiệp và Phát triển Nông thôn Việt Nam (Agribank) triển khai chương trình khuyến mại "Thẻ mới trong tay – Hoàn tiền mê say", hoàn tiền lên tới 1 triệu đồng dành cho các khách hàng mở mới và sử dụng thẻ tín dụng và ghi nợ quốc tế Agribank JCB.
- Hưởng ứng Quyết định số 2345/QĐ-NHNN của Ngân hàng Nhà nước từ ngày 01/07/2024, Ngân hàng Quân Đội (MB Bank) bên cạnh việc tăng cường hỗ trợ người dân cập nhật sinh trắc học trong, ngoài giờ hành chính và cả cuối tuần; Ngân hàng còn tặng tài khoản số đẹp và 30.000 đồng cho mỗi khách hàng mở mới App MB Bank và xác thực thành công.
- Từ ngày 08/07 đến hết ngày 30/09/2024, Ngân hàng TMCP Bắc Á (Bac A Bank) triển khai chương trình "Thẻ đặc quyền – Trọn ưu đãi" miễn phí thưởng niên ba năm đầu dành cho các khách hàng mở mới thẻ tín dụng Bac A Bank MasterCard Platinum hoặc Rewards Gold hợp lệ./.

Vui lòng truy cập vào website của các ngân hàng và tổ chức thẻ để biết thêm chi tiết.

ENTRUST: ĐỒNG HÀNH CÙNG CHÍNH PHỦ TRONG QUÁ TRÌNH CHUYỂN ĐỔI TƯƠNG TÁC CỦA CÔNG DÂN BẰNG DANH TÍNH SỐ

Entrust, công ty hàng đầu thế giới về các giải pháp bảo mật tập trung vào danh tính cho chính phủ và doanh nghiệp trên toàn thế giới, đã công bố giải pháp Điều phối Nhận dạng Công dân. Giờ đây, các chính phủ có thể triển khai cung cấp dịch vụ công thông qua danh tính số bảo mật, tạo dựng niềm tin vào mọi tương tác của người dân.

Giải pháp đổi mới và thiết kế theo mô-đun này từ Entrust được ra mắt khi các chính phủ trên toàn thế giới nhận thấy nhu cầu cung cấp dịch vụ liền mạch, minh bạch và nhanh chóng ngày càng tăng. Việc số hóa các dịch vụ công có thể giúp đáp ứng những kỳ vọng này, nhưng để mang lại tính hiệu quả, các kênh dịch vụ kỹ thuật số phải sử dụng thuận tiện và trực quan hơn so với các phương án hiện có. Và khi hành vi gian lận danh tính do AI điều khiển tiếp tục gia tăng, chính phủ cần xác minh và xác thực công dân khi truy cập các dịch vụ trực tuyến.

Với giải pháp này, người dân sẽ được hưởng lợi nhờ khả năng truy cập tin cậy, minh bạch và toàn diện vào các dịch vụ của chính phủ, được tăng cường với trải nghiệm kỹ thuật số liền mạch và an toàn. Chính phủ có thể đảm bảo các tiêu chuẩn cao nhất về bảo mật và quyền riêng tư cho các tương tác kỹ thuật số giữa chính phủ với công dân (G2C) đối với các hoạt động kiểm soát biên giới liền mạch, cung cấp phúc lợi, nộp thuế, tiếp cận dịch vụ chăm sóc sức khỏe và nhiều hoạt động khác.

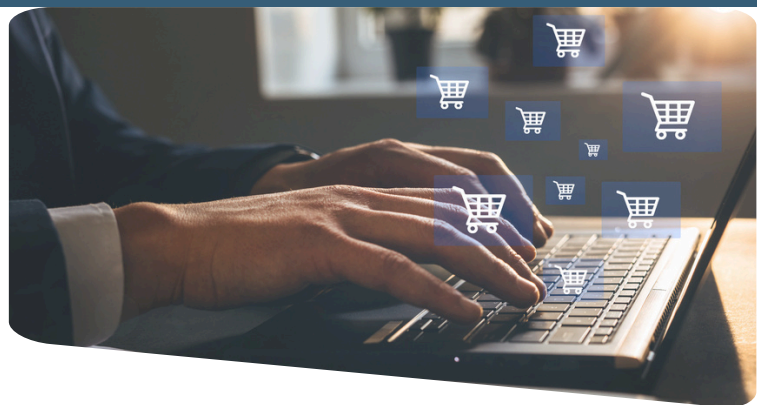
Tony Ball, Chủ tịch về Thanh toán & Danh tính của Entrust cho biết: “Khi bạn thiết lập danh tính của một cá nhân trực tuyến và cung cấp cơ sở hạ tầng phù hợp cho phép tin cậy danh tính đó, bạn có thể mở ra cho công dân và doanh nghiệp những khả năng không giới hạn bằng cách củng cố các dịch vụ của chính phủ, giúp các dịch vụ này trở nên thuận tiện, dễ tiếp cận và an toàn hơn. Mặc dù nhu cầu số hóa các dịch vụ công ngày càng mở rộng, nhưng công dân vẫn chậm thích nghi, ngoại trừ một số trường hợp ngoại lệ như Estonia.



Giải pháp Điều phối Nhận dạng Công dân của Entrust áp dụng cách tiếp cận lấy danh tính làm trung tâm. Giải pháp được thiết kế để hỗ trợ các sáng kiến chuyển đổi số giữa chính phủ và công dân (G2C).

Lợi ích của giải pháp:

- Kiến trúc tổng hợp: Cho phép dễ dàng tích hợp với cơ sở hạ tầng hiện có và hợp lý hóa quy trình giữa chính phủ và công dân bằng cách sử dụng dịch vụ dạng đơn nhất và yêu cầu người sử dụng ít hoặc không cần viết code, đảm bảo tính sẵn sàng trong tương lai và khả năng tương tác với các hệ thống hiện có.
- Thiết kế trải nghiệm tổng thể: Tăng cường sự chấp nhận của người dân đối với các dịch vụ công nghệ số với giao diện trực quan trên web hoặc trên thiết bị di động, thúc đẩy người dân tham gia nhiều hơn vào các hoạt động của chính phủ.
- Dựa trên tiêu chuẩn: Cho phép chính phủ đáp ứng các tiêu chuẩn NIST IAL 1, 2 và 3, eIDAS và GDPR, đồng thời có thể dễ dàng cấu hình để tuân thủ các tiêu chuẩn quy định của địa phương, đảm bảo tiêu chuẩn bảo mật và quyền riêng tư cao nhất cho các hoạt động số hóa.
- Xây dựng sự tin cậy: Đưa niềm tin vào các tương tác kỹ thuật số với tính năng phát hiện gian lận tích hợp công nghệ AI để xác minh danh tính, xác thực mạnh mẽ và mã hóa PKI để cung cấp dịch vụ đáng tin cậy.



Giải pháp cung cấp các tính năng chính bao gồm tích hợp kỹ thuật số với tính năng phát hiện gian lận do AI cung cấp để xác minh danh tính, cấp thông tin xác thực số liền mạch, quản lý vòng đời danh tính và các kênh kỹ thuật số tự phục vụ trên web hoặc thiết bị di động, kết hợp với khả năng xác thực đa yếu tố khi truy cập các dịch vụ của chính phủ.

Giải pháp góp phần quan trọng giúp hoạt động di chuyển xuyên biên giới trở nên liền mạch, hỗ trợ đa phương thức (đường bộ, đường sắt, đường hàng không, đường biển). Giải pháp cho phép triển khai các biện pháp sinh trắc học thông minh mà không yêu cầu cổng tự động hay hệ thống ki-ốt tốn kém, cho phép khách du lịch hợp pháp có thể xuất nhập cảnh một cách liền mạch thông qua việc đăng ký trước đơn giản trên thiết bị di động, qua đó giúp bảo vệ biên giới đồng thời thay đổi trải nghiệm di chuyển của công dân./.

(Entrust)

MK[®]group
Smart Digital Security

ENTRUST



MÁY IN THẺ ENTRUST SIGMA DS

LỰA CHỌN SỐ 1 CHO CÁC
CHƯƠNG TRÌNH THẺ THÀNH CÔNG

- ✓ ĐƠN GIẢN
- ✓ THÔNG MINH
- ✓ BẢO MẬT



HOTLINE: 0903.481.456



contact@mkgroup.com.vn

Google Wallet thay thế Fitbit Pay, bổ sung hỗ trợ American Express

Google gần đây đã công bố kế hoạch loại bỏ dần ứng dụng Fitbit Pay bắt đầu từ ngày 29 tháng 7 năm 2024 với những thay đổi ban đầu được áp dụng với các thiết bị Android từ đầu tháng 6. Là một phần của bản cập nhật hệ thống, Dịch vụ Google Play phiên bản 24.25 đã cho phép Google Wallet hỗ trợ American Express.

Động thái loại bỏ dần các sản phẩm và dịch vụ của Fitbit không hoàn toàn suôn sẻ. Người dùng đã gặp phải một số vấn đề như không có hỗ trợ của American Express và cần phải cập nhật lại thẻ Visa vào Google Wallet để thanh toán qua thiết bị Fitbit, đặc biệt được lưu ý ở những người dùng iOS.

Gần đây, Google cũng đã thêm 29 ngân hàng mới có trụ sở tại Mỹ vào ứng dụng. Cũng theo nguồn tin này, những bước đi này nhấn mạnh nỗ lực của Google trong việc củng cố sự hiện diện của mình trong không gian thương mại điện tử.

(ThePaypers)



MuchBetter ra mắt nhẫn thanh toán không tiếp xúc ‘miễn phí’

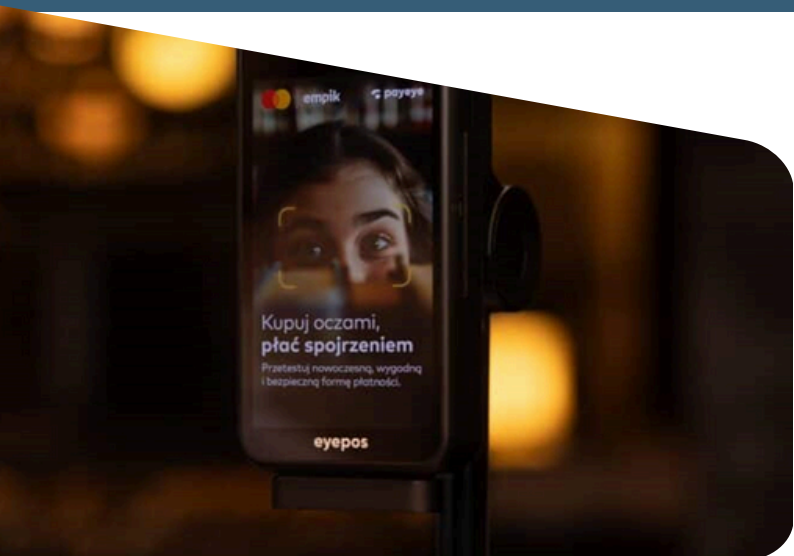


Nhà cung cấp công nghệ thanh toán thiết bị đeo MuchBetter đã ra mắt một dòng sản phẩm nhẫn thanh toán không tiếp xúc “hoàn toàn miễn phí” tại Ý – miễn là người dùng nạp €100 thông qua ứng dụng được liên kết.

Có sẵn để đặt hàng trên website MuchBetter, khách hàng chỉ cần trả €5.99 phí giao hàng để có được chiếc nhẫn được làm từ gốm, không dùng pin và có khả năng chống nước này trên tay. Khi nhận được nhẫn, khách hàng chỉ cần giữ nhẫn gần vùng giao tiếp NFC trên điện thoại thông minh để kết nối với ứng dụng ví MuchBetter trên điện thoại. Sau khi nạp tiền, chiếc nhẫn có thể ngay lập tức được sử dụng để thực hiện thanh toán không tiếp xúc.

Theo sau phát hành tại Ý, MuchBetter đã lên sẵn kế hoạch để phát hành sản phẩm này tại các quốc gia khác như Đức, Áo, Anh, Ireland và Ba Lan.

(Finextra)



Chương trình thanh toán ứng dụng sinh trắc học của Mastercard bước đầu tiếp cận thị trường Châu Âu

Mastercard lần đầu tiên triển khai thanh toán bán lẻ ứng dụng sinh trắc học tại thị trường châu Âu. Công ty dự kiến sẽ thí điểm Chương trình thanh toán ứng dụng sinh trắc học ở Ba Lan kết hợp với công ty fintech PayEye tại đây để cung cấp công nghệ sinh trắc học mống mắt và khuôn mặt.

Từ ngày 10 tháng 6, người mua hàng có thể thanh toán bằng cách quét mống mắt tại 5 cửa hàng trên khắp Ba Lan thuộc sở hữu của chuỗi cửa hàng sách Empik. Một đối tác khác trong chương trình này là Planet Pay.

Các cửa hàng sẽ được trang bị thiết bị đầu cuối eyePOS của PayEye. Trong một thông cáo mới đây, Công ty cho biết quy trình này yêu cầu hiệu chuẩn chính xác để tránh nguy cơ vô tình nhìn vào thiết bị đầu cuối và thanh toán. Thiết bị đầu cuối eyePOS 3, sử dụng kết hợp sinh trắc học khuôn mặt và mống mắt, đã nhận được chứng nhận Ngành Thẻ Thanh toán (PCI) vào năm ngoái.

Mastercard bắt đầu triển khai Chương trình thanh toán ứng dụng sinh trắc học từ năm 2022 tại Brazil, nơi họ triển khai chương trình thanh toán nhận dạng khuôn mặt "thanh toán bằng nụ cười" với Payface của Brazil. Năm ngoái, công ty đã công bố mở rộng chương trình sang khu vực Châu Á Thái Bình Dương và triển khai thí điểm lần hai tại Châu Mỹ Latinh vào đầu tháng 6 này. Nhiều chương trình thí điểm trên toàn cầu đã được lên kế hoạch triển khai vào cuối năm nay.

(BiometricUpdate)

Ngân hàng Singapore dần loại bỏ Mật khẩu dùng một lần (OTP) qua SMS

Các ngân hàng ở Singapore sẽ loại bỏ dần việc sử dụng Mật khẩu một lần (OTP) được gửi qua tin nhắn SMS bởi chúng dễ bị đánh cắp để thay thế bằng mã thông báo kỹ thuật số để giúp khách hàng truy cập tài khoản ngân hàng an toàn hơn trong tương lai.

Tính năng OTP lần đầu được giới thiệu vào những năm 2000 như một tùy chọn xác thực đa yếu tố nhằm tăng cường bảo mật trực tuyến.

Tuy nhiên, hiện tại với sự phát triển đa công nghệ không ngừng cùng với cơ cấu xã hội phức tạp hơn đã khiến cho những kẻ gian có nhiều cơ hội lừa đảo lấy được OTP gửi qua SMS của khách hàng một cách dễ dàng. Ví dụ như việc thiết lập các trang web giả gần giống với web Ngân hàng cũng đã giúp tăng khả năng lừa đảo thành công lên đáng kể. Đề xuất của các Ngân hàng về việc chuyển sang hệ thống mã thông báo kỹ thuật số để đăng nhập tài khoản trên thiết bị di động và các trang web trực tuyến sẽ được tiến hành hình thức dần dần trong 3 tháng tới.

Ngài Ong-Ang Ai Boon, giám đốc Hiệp hội Ngân hàng ở Singapore, cho biết: "Biện pháp này cung cấp cho khách hàng sự bảo vệ tốt hơn và giúp tăng cường ngăn chặn truy cập trái phép vào tài khoản ngân hàng của họ. Mặc dù chúng có thể gây ra một số bất tiện nhưng những biện pháp như vậy là cần thiết để giúp ngăn chặn lừa đảo và bảo vệ khách hàng trong thời đại công nghệ luôn biến đổi hiện nay."

Lừa đảo xen giữa nằm trong số Top 5 hình thức lừa đảo hàng đầu tại Singapore được liệt kê trong Báo cáo tóm tắt về tội phạm mạng và lừa đảo thường niên năm 2023 của Lực lượng cảnh sát Singapore, với ít nhất 14,2 triệu USD bị đánh cắp từ hình thức này.

(Finextra)

Nepal yêu cầu thẻ ID quốc gia để đảm bảo an sinh xã hội từ tháng 7.2024

Theo báo Kantipur đưa tin, Chính phủ Nepal đã ra quyết định yêu cầu người dân buộc phải sử dụng Thẻ ID quốc gia (NID) cho tất cả các dịch vụ công của Chính phủ.

Bắt đầu từ tháng 7 này, các công dân sẽ cần NID để nhận trợ cấp an sinh xã hội và gia hạn lương hưu thông qua xác minh sinh trắc học. Sáng kiến này nhằm mục đích xác thực hóa các dịch vụ, ngăn chặn gian lận và tiết kiệm thời gian cho những người cao tuổi. Theo Cục Đăng ký và Chứng minh nhân dân quốc gia, hệ thống này hiện đang hỗ trợ các quyền lợi an sinh xã hội cho khoảng 3,8 triệu người cao tuổi trên cả nước.

Bộ đang tích hợp thông tin chi tiết NID với nhiều lĩnh vực khác, bao gồm như ngân hàng, bảo hiểm y tế và đăng ký xe, nhằm gia tăng tiện ích của thẻ ID quốc gia và giảm thiểu tối đa chi phí phải in nhiều loại giấy tờ khác. Các quan chức cho biết mọi nỗ lực nhằm ngăn chặn việc giả mạo danh tính, chẳng hạn như giả mạo sinh trắc học.

Tổng giám đốc Yuvraj Kattel cho biết một đề xuất đang được xây dựng để tất cả các cơ quan nhà nước sử dụng giấy chứng nhận công dân Nepal chuyển sang số chứng minh nhân dân./.

(BiometricUpdate)

GIẢI PHÁP MÃ HÓA DỮ LIỆU CẤP CAO

BẢO MẬT - TIN CẬY - AN TOÀN



Giải pháp Prim'X áp dụng mã hóa theo một phương thức mới trong tổ chức doanh nghiệp nhằm bảo vệ tốt hơn nguồn tài nguyên dữ liệu, chống thất thoát, bị đánh cắp, rò rỉ và gián điệp kinh tế.

Các giải pháp của Prim'X mang tính tổng thể và trong suốt, có khả năng triển khai quy mô lớn, đáp ứng yêu cầu quản lý bảo mật thông tin qua việc quản lý quyền được biết nhằm chống lại những xâm nhập từ bên ngoài và bên trong tổ chức.

CÁC CHỨNG CHỈ CỦA GIẢI PHÁP PRIM'X



Hà Nội: (024) 7100 6781

Tp. Hồ Chí Minh: (028) 3930 1055



BÁO CÁO GIAN LẬN ĐỊNH DANH 2024:

BỨC TRANH GIAN LẬN ĐẦY NHỮNG ÂU LO

(Phần 1)



Trong môi trường ngày nay - nơi phần lớn cách thức chúng ta tương tác, làm việc và kinh doanh đều ưu tiên kênh số hóa, mọi thứ từ bảo mật doanh nghiệp đến bảo vệ dữ liệu, hay quyền riêng tư của người dùng đều ngày càng bị đe dọa.

Nhìn về tương lai, tăng cường an ninh mạng và phòng, chống gian lận là những hành động cần thiết để xây dựng nền tảng niềm tin cho tương lai số.

Entrust Identity Fraud Report 2024 chia sẻ những xu hướng gian lận đặc biệt mà các doanh nghiệp nhận thấy trong thời điểm quan trọng khi bắt đầu triển khai và cung cấp thông tin chi tiết về giải pháp phòng chống. Dữ liệu phân tích trong báo cáo được trích dẫn từ giai đoạn 1/9/2022 - 1/9/2023. Trong một số trường hợp, Onfido - đơn vị xây dựng báo cáo - so sánh dữ liệu này với các năm trước để hiểu rõ hơn và chính xác hơn về xu hướng chung.

Trong đây là một số nét chính trong báo cáo:

1. Các hành vi giả mạo kỹ thuật số tiếp tục gia tăng:

Năm ngoái, các hành vi giả mạo kỹ thuật số chiếm 16,7% tổng số nỗ lực gian lận tài liệu. 6 tháng qua, con số đó đã tăng hơn gấp đôi - 34,8% nỗ lực gian lận tài liệu hiện bao gồm một số thủ đoạn thao túng kỹ thuật số. Phần lớn tình trạng này có thể là do sự xuất hiện của các trang web như OnlyFake - dịch vụ trực tuyến cung cấp khả năng tạo hình ảnh của các tài liệu nhận dạng bằng trí tuệ nhân tạo (AI). Hiện nay, OnlyFake đã ngừng hoạt động, tuy nhiên, các doanh nghiệp nên cảnh giác trước những mối đe dọa tương tự mà các đối tượng lừa đảo sẽ cố gắng lợi dụng.

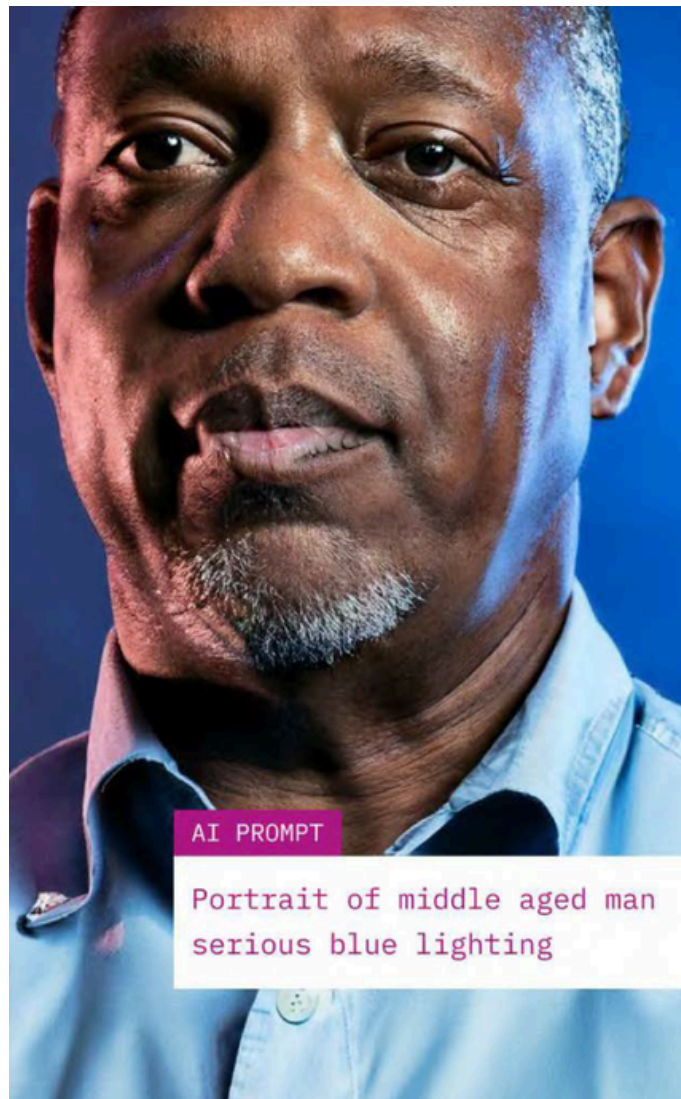
2. Gian lận tiếp tục trở nên khó nắm bắt hơn:

Vài năm gần đây chứng kiến xu hướng chuyển đổi sang thủ đoạn lừa đảo ít tinh vi hơn, bởi kẻ gian ưa chuộng số lượng hơn là mức độ phức tạp. Năm 2023, 80,3% tổng số vụ lừa đảo mà Onfido phát hiện được phân loại "dễ dàng" (mức độ phức tạp thấp hơn). Tuy vậy, trong 6 tháng qua, số vụ gian lận ở mức độ "trung bình" và "khó" đã gia tăng. 36,4% nỗ lực gian lận trong 6 tháng qua được phân loại là "trung bình" (tăng so với mức 19,6% của năm 2023) và 1,4% là "khó" (so với tỷ lệ 0,1% của năm 2023). Chiều hướng này có liên quan đến sự gia tăng của các hành vi giả mạo kỹ thuật số, vốn khó có thể phát hiện bằng mắt thường.

3. Deepfake tiếp tục hoành hành:

Số nỗ lực deepfake tăng cực mạnh trong giai đoạn 2022 - 2023, lên tới 3.000%. Năm 2022, rất hiếm khi thấy các đối tượng lừa đảo sử dụng deepfake để cố gắng vượt qua quá trình xác minh sinh trắc học. Bước sang năm 2023, mọi việc đã thay đổi. Do sự phổ biến ngày càng rộng rãi của phần mềm deepfake và những cải tiến trong lĩnh vực AI, số lượng và mức độ tinh vi của các nỗ lực deepfake có thể sẽ tăng lên trong năm 2024. 6 tháng qua, deepfake chiếm khoảng 30-40% tổng số vụ gian lận sinh trắc học mà Onfido phát hiện.

Trở thành đối tượng lừa đảo chưa bao giờ dễ dàng và ít tốn kém hơn thế. Các trang web như OnlyFake, sự sẵn có của phần mềm deepfake và lượng lớn dữ liệu cá nhân có sẵn trên web đen đồng nghĩa với việc có thêm nhiều kẻ gian tiếp cận các phương tiện tấn công ngày càng tinh vi. Ngày nay, các đối tượng lừa đảo thường là những doanh nghiệp tội phạm có tổ chức, hoạt động giống như các công ty. Các nỗ lực gian lận và an ninh mạng đã chuyển từ những nỗ lực mang tính cơ hội, chỉ diễn ra một lần sang các cuộc tấn công có chủ đích, có thể mở rộng. Hết lần này đến lần khác, kẻ gian tiếp tục điều chỉnh các thủ đoạn để cố gắng vượt qua các hệ thống bảo mật. Trước những mối đe dọa này, nhiệm vụ đảm bảo tương lai số cho các doanh nghiệp cũng như người tiêu dùng là ưu tiên hàng đầu.



Bức tranh toàn cầu về gian lận

Dữ liệu năm nay cho thấy các đối tượng lừa đảo bắt đầu chú trọng hơn đến gian lận sinh trắc học. Tỷ lệ gian lận tài liệu tiếp tục diễn biến theo xu hướng nhất quán. Sau khi đạt đỉnh vào năm 2021, gian lận tài liệu đã chững lại trong vài năm qua, trung bình là 4,4% trong năm 2023.

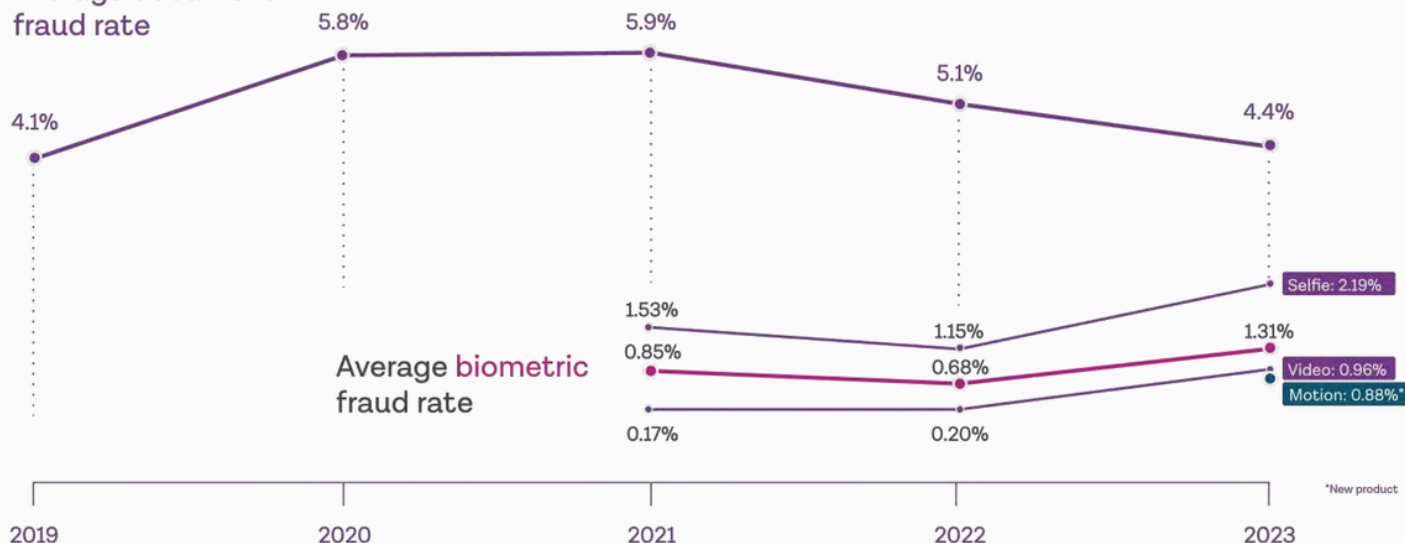
Tương tự, gian lận sinh trắc học tăng nhẹ trong năm qua. Tỷ lệ gian lận sinh trắc học bình quân năm 2023 (1,31%) tăng gấp 2 lần so với năm 2022 (0,68%). Ngày càng có nhiều đối tượng lừa đảo sử dụng tài liệu thật (có được do rò rỉ dữ liệu) để kiểm tra mức độ xác thực của tài liệu, sau đó thay đổi khuôn mặt của chúng để lọt qua khâu kiểm tra sinh trắc học.

Diễn biến trên củng cố một xu hướng mới nổi khác, đó là kẻ gian đang chuyển sang sử dụng các kỹ thuật như cheapfake và deepfake làm phương tiện tấn công sinh trắc học.

Tuy nhiên, sinh trắc học vẫn cho thấy tỷ lệ gian lận thấp hơn rõ rệt so với tài liệu - ở mức ít hơn khoảng 3 lần. Vì vậy, sinh trắc học tiếp tục đóng vai trò là công cụ ngăn chặn hiệu quả, đặc biệt là các giải pháp có yếu tố "thực thể sống" (liveness).

Average fraud rates

Average document fraud rate



Từ giả mạo tài liệu truyền thống đến giả mạo tài liệu số

Số vụ giả mạo tài liệu số tăng 18% trong năm qua (và số vụ giả mạo tài liệu số trong năm 2023 tăng khoảng 5 lần so với năm 2021). Xu hướng này có nguy cơ tiếp diễn vì hình ảnh giả mạo số hóa được tạo ra nhanh hơn và rẻ hơn so với các loại tài liệu giả mạo truyền thống, đặc biệt là khi các công cụ AI ngày càng sẵn có.

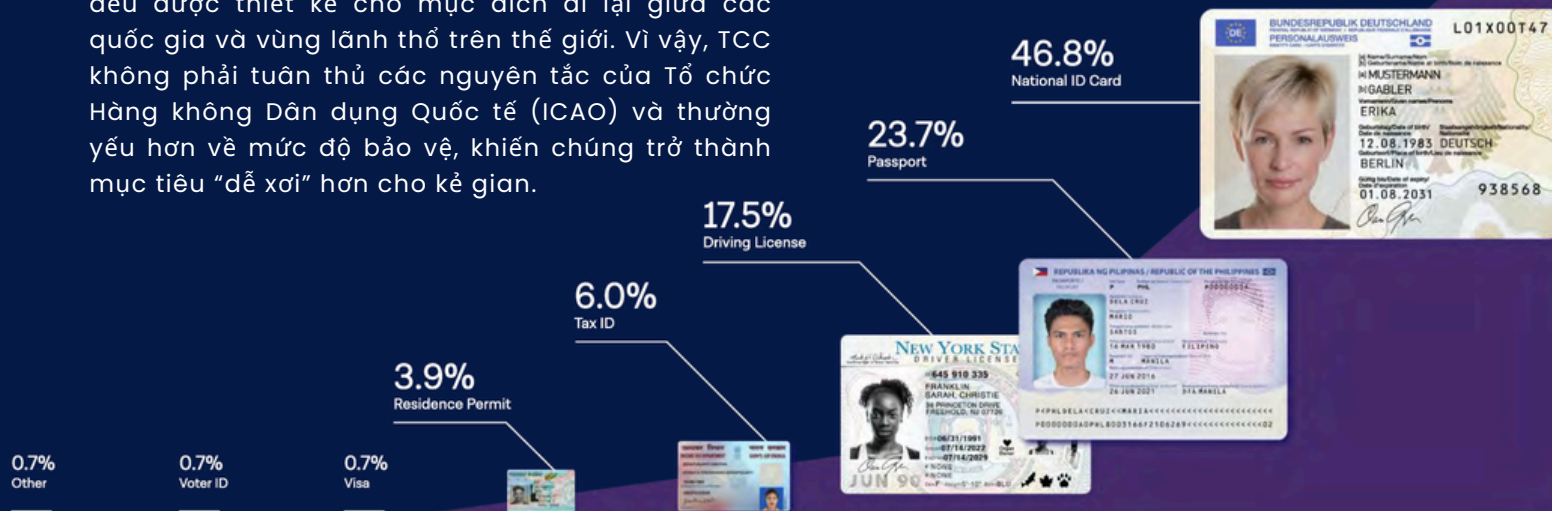


Kẻ gian trở lại với hướng tấn công thẻ căn cước (TCC)

Năm 2023, các đối tượng lừa đảo nhằm mục tiêu vào TCC nhiều hơn bất kỳ loại giấy tờ nào khác, chiếm 46,8% tổng số vụ gian lận giấy tờ.

Không giống như hộ chiếu, không phải tất cả TCC đều được thiết kế cho mục đích đi lại giữa các quốc gia và vùng lãnh thổ trên thế giới. Vì vậy, TCC không phải tuân thủ các nguyên tắc của Tổ chức Hàng không Dân dụng Quốc tế (ICAO) và thường yếu hơn về mức độ bảo vệ, khiến chúng trở thành mục tiêu "dễ xơi" hơn cho kẻ gian.

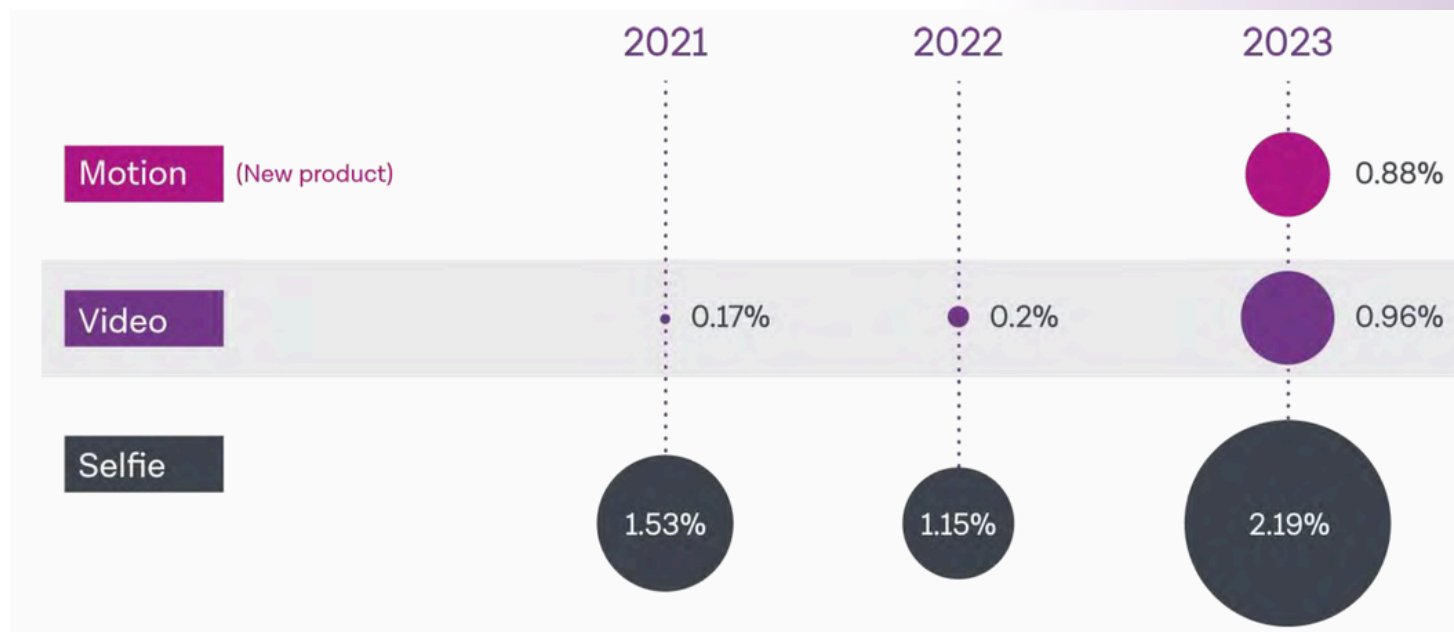
Fraud by document type



Công nghệ sinh trắc học cũng có những điểm yếu

Khi các nhà cung cấp danh tính cũng như các doanh nghiệp triển khai những biện pháp phòng vệ mạnh mẽ hơn, các đối tượng lừa đảo đang cố gắng tìm ra những cách thức mới mẻ và sáng tạo hơn để vượt qua hàng rào bảo mật. Dòng công cụ hỗ trợ AI trực tuyến sẵn có, chẳng hạn như ứng dụng hoán đổi khuôn mặt, cũng mang đến cho chúng con đường mới để thực hiện hành vi lừa đảo sinh trắc học.

Dữ liệu thống kê cho thấy các nỗ lực gian lận sinh trắc học trong năm 2023 cao hơn so với những năm trước.



Thông điệp rất rõ ràng! Các mối đe dọa nghiêm trọng hơn cần hàng rào phòng thủ mạnh mẽ hơn. Xác minh sinh trắc học cung cấp thêm một lớp bảo vệ ngoài xác minh tài liệu. Kết hợp sinh trắc học khuôn mặt với ảnh ID sẽ giúp xác định:

- Có một người thực sự đang cố gắng đăng ký dịch vụ;
- Giấy tờ tùy thân thuộc về người xuất trình.

Để đối phó với các kỹ thuật gian lận sinh trắc học ngày càng tinh vi, chẳng hạn như deepfake, Onfido – một công ty của Entrust đã ra mắt Motion – giải pháp sinh trắc học hoàn toàn tự động, chỉ yêu cầu người dùng xoay đầu khi quay video.

Motion sử dụng công nghệ xác minh thực thể sống và chống giả mạo tiên tiến để mang lại trải nghiệm liền mạch cho người dùng, đồng thời đối phó hiệu quả trước những thủ đoạn gian lận mới nổi như deepfake và tấn công tiêm nhiễm (injection attack).

Motion đã được chứng minh là mang lại sự cải thiện hiệu suất chống giả mạo gấp 10 lần, với 95% số lần kiểm tra được trả về trong chưa đến 15 giây.



Mời các bạn đón đọc tiếp Phần 2 của Báo cáo Gian lận định danh - Identity Fraud Report 2024 trong bản tin Thế Giới Thẻ điện tử số 161 - Tháng 8.2024 với các nội dung về:

- Bản đồ gian lận tại các khu vực trên thế giới
- Khuyến nghị của Ofindo về đảm bảo an toàn cho doanh nghiệp



Smart Digital Security

ĐỐI TÁC TIN CẬY VỀ THẺ THÔNG MINH | XÁC THỰC BẢO MẬT TÀI LIỆU BẢO AN | AI CAMERA



<https://mkgroup.com.vn>



contact@mkgroup.com.vn

Trong trường hợp Quý độc giả không muốn nhận bản tin, hãy phản hồi cho chúng tôi theo địa chỉ:

- **Email:** contact@mkgroup.com.vn
- **Tiêu đề thư:** Không nhận bản tin Thế Giới Thẻ MK



Xin vui lòng truy cập vào website MK Group để hiểu rõ hơn về **Chính sách bảo mật và xử lý dữ liệu cá nhân** của chúng tôi.