THẾ GIỚI THẺ

Bản tin nội bộ của MK Group

Số 169 | tháng 2.2025

NỘI DUNG CHÍNH

https://mkgroup.com.vn contact@mkgroup.com.vn

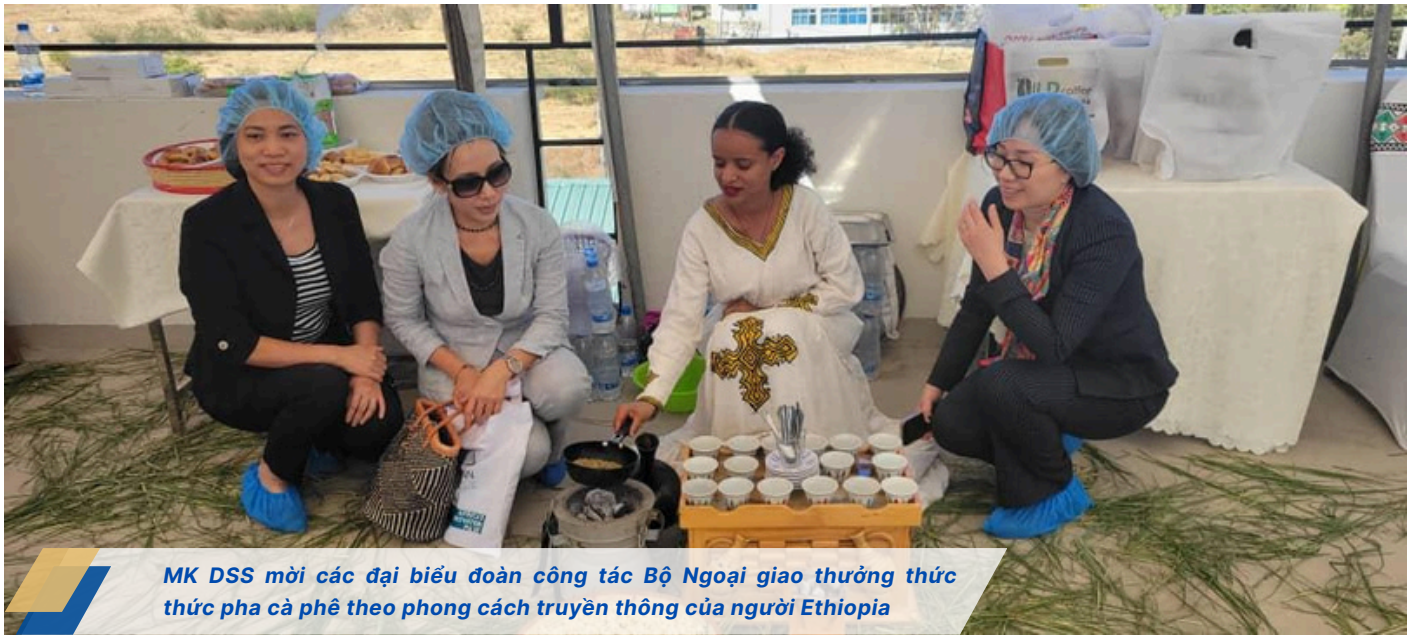
CÔNG TY MK DSS VINH DỰ ĐÓN ĐOÀN BỘ NGOẠI GIAO VIỆT NAM TỚI THAM QUAN VÀ LÀM VIỆC TẠI NHÀ MÁY Ở ETHIOPIA

Đoàn công tác Bộ Ngoại giao Việt Nam trong chuyến thăm quan và làm việc tại Nhà máy MK DSS tại Addis Ababa, Ethiopia

Chiều ngày 18/02/2025, bà Nguyễn Minh Hằng, Thứ trưởng Bộ Ngoại giao Việt Nam đã dẫn đầu đoàn công tác của Bộ Ngoại giao đã tới tham quan và làm việc tại Khu công viên công nghệ cao (ICT Park) và tham quan Nhà máy sản xuất thẻ thông minh của công ty MK DSS – liên doanh giữa Tập đoàn MK (MK Group), Việt Nam và công ty Neuronet, Ethiopia tại thủ đô Addis Ababa, Ethiopia.

Đoàn đại biểu Bộ ngoại giao Việt Nam bao gồm bà Nguyễn Phương Trà, quyền Vụ trưởng Vụ Trung Đông và Châu Phi, bà Vũ Thanh Huyền, Đại sứ Việt Nam tại Tanzania kiêm nhiệm khu vực Đông Phi, ông Trần Chí Thành, Phó Vụ trưởng Vụ Tổng hợp kinh tế, Bộ Ngoại giaovà một số thành viên

Về phía đại diện của công ty MK DSS đón đoàn công tác gồm ông Tsegaye Habtu Teshale, Tổng giám đốc và ông Yidnekachew Bekele, Giám đốc vận hành. Về phía MK Group, có ông Lê Văn Thao, Phó giám đốc nhà máy MK Smart kiêm trưởng đoàn công tác của MK Group cùng đội ngũ chuyên gia của MK đang nhận nhiệm vụ tại Ethiopia.



MK DSS mời các đại biểu đoàn công tác Bộ Ngoại giao thưởng thức thức pha cà phê theo phong cách truyền thông của người Ethiopia

Đoàn công tác của Bộ Ngoại giao Việt Nam đã tới tham quan các dây chuyền sản xuất thẻ thông minh với các giải pháp toàn diện từ khâu in ấn, cá thể hóa, kiểm tra cho tới đóng gói thành phẩm. Với công nghệ và hạ tầng nhà máy được đầu tư nghiêm túc, bài bản, MK DSS hướng tới mục tiêu trở thành đối tác tin cậy hàng đầu trong ngành công nghiệp thẻ thông minh tại khu vực Châu Phi và Trung Đông.

Đoàn cũng ghi nhận và đánh giá cao tinh thần lao động của các MKers trong quá trình xây dựng và hoàn thiện nhà máy sản xuất thẻ thông mình đầu tiên tại Ethiopia, nỗ lực mở rộng thị trường của MK Group, từ đó mang lại những giá trị thiết thực cho sự phát triển quan hệ đối tác của hai doanh nghiệp cũng như góp phần củng cố quan hệ hợp tác giữa hai quốc gia Ethiopia và Việt Nam.

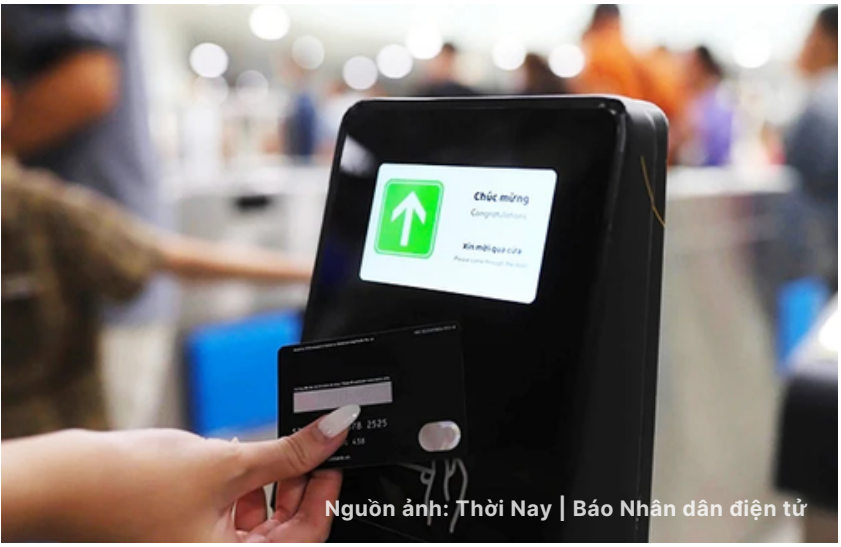
Theo phát biểu của Thứ trưởng Nguyễn Minh Hằng tại buổi làm việc, việc MK Group đầu tư xây dựng nhà máy sản xuất thông minh đầu tiên tại Ethiopia có thể coi là hình mẫu của hoạt động liên doanh và đầu tư của doanh nghiệp Việt Nam tại khu vực Châu Phi, vốn chưa thu hút được nhiều doanh nghiệp Việt.

Bên cạnh đấy, đoàn công tác cũng nhận định các hoạt động đầu tư của MK Group tại Ethiopia phù hợp với định hướng mở rộng thị trường và xuất khẩu công nghệ cao của Việt Nam ra quốc tế trong giai đoạn hiện nay. thông, Bộ Thông tin và Truyền thông thực hiện.

Ông Tsegaye Habtu Teshale, Tổng giám đốc MK DSS giới thiệu với Thứ trưởng Nguyễn Minh Hằng và các đại biểu công ty.

THANH TOÁN BẰNG THẺ NGÂN HÀNG KHI ĐI METRO

Nhằm giúp người dân trải nghiệm dịch vụ đường sắt đô thị nhanh chóng và hiện đại hơn, Công ty cổ phần Thanh toán quốc gia Việt Nam (NAPAS) phối hợp Công ty TNHH MTV Đường sắt đô thị số 1 Thành phố Hồ Chí Minh (HURC1) cùng 25 ngân hàng trong hệ thống NAPAS vừa triển khai dịch vụ thanh toán bằng thẻ trên tuyến metro số 1



Nguồn ảnh: Thời Nay | Báo Nhân dân điện tử

Danh sách các ngân hàng tham gia bao gồm: Sacombank, BIDV, Agribank, TPBank, SHB, BVBank, VietBank, SeABank, NamABank, Vietcombank, Wooribank, Techcombank, VIB, NCB, VietABank, Bảo Việt Bank, PBVN, Kienlongbank, Saigonbank, BAB, Eximbank, MB, ACB, OCB, Vietinbank.

Theo đó, khách hàng có thể thanh toán tiện lợi với các loại thẻ ngân hàng không tiếp xúc dựa trên nền tảng hệ thống vé điện tử công nghệ "open-loop" của HURC1. Dịch vụ thanh toán này được triển khai với dòng thẻ ghi nợ và thẻ tín dụng sử dụng công nghệ không tiếp xúc của NAPAS.

Hành khách chỉ cần chạm thẻ lên thiết bị kiểm soát tại cổng vào (tap-in) và sau khi kết thúc hành trình tại cổng ra (tap-out), giao dịch thanh toán cho chuyến đi sẽ được hoàn tất một cách nhanh chóng và thuận tiện.

Đại diện NAPAS cho biết, những năm gần đây, với sự phát triển của các giải pháp trong lĩnh vực thẻ, vé điện tử và sự phổ biến của thẻ thanh toán ngân hàng sử dụng công nghệ không tiếp xúc theo tiêu chuẩn EMV, nhiều quốc gia đã nghiên cứu và chuyển dần sang thanh toán giao thông với cơ chế mở.

Điều này cho phép khách hàng thanh toán phí giao thông công cộng trực tiếp bằng thẻ ngân hàng, với đa dạng các phương tiện di chuyển từ bus, metro mà không cần sử dụng nhiều thẻ vé khác nhau. Việc sử dụng thẻ ngân hàng cũng giúp bỏ qua công đoạn xếp hàng để mua vé hoặc nạp tiền vào thẻ vé, góp phần giảm bớt chi phí vận hành của các đơn vị cung cấp dịch vụ.

Hình thức thanh toán bằng thẻ NAPAS trên tuyến metro số 1 giúp đẩy mạnh thói quen thanh toán không tiền mặt khi tham gia giao thông, mang lại sự tiện lợi và an toàn cho hành khách tại Thành phố Hồ Chí Minh, góp phần bảo vệ môi trường. Đồng thời, điều này cho thấy những lợi ích khi hạ tầng thanh toán được tích hợp và đồng bộ, góp phần thúc đẩy giao thông xanh tại Việt Nam và đưa hệ thống thanh toán tại các tuyến đường sắt đô thị trong nước bắt kịp với các quốc gia khác trên thế giới.

Với đối tượng được hỗ trợ miễn phí vé xe bus trên các tuyến xe có trợ giá bao gồm: Người có công với cách mạng được xác định theo khoản 1 điều 3 Pháp lệnh Ưu đãi người có công với cách mạng; Người khuyết tật; Người cao tuổi theo quy định tại Điều 2 Luật Người cao tuổi (là công dân Việt Nam từ đủ 60 tuổi trở lên) và trẻ em dưới 6 tuổi.

Những hành khách này chỉ cần xuất trình Căn cước công dân hoặc thẻ căn cước hoặc giấy tờ chứng minh do cơ quan có thẩm quyền cấp để được hưởng quyền lợi theo quy định. Với doanh nghiệp vận tải phải niêm yết đầy đủ các thông tin về chính sách miễn giảm vé cho người dân được biết để phối hợp đối chiếu giấy tờ chứng minh khi đi xe bus.

BaoNhanDan

MASTERCARD RA MẮT THẺ GHI NỢ KHÔNG SỐ TẠI ÚC

Nằm trong kế hoạch nhằm xóa bỏ 16 số thông tin thẻ trên các dòng thẻ tín dụng và ghi nợ của Mastercard đến năm 2030, Ngân hàng AMP của Úc đang ra mắt thẻ ghi nợ không số đầu tiên dành cho các doanh nghiệp.

Nguồn ảnh: news.com.au

Ngân hàng di động AMP đang bắt đầu đưa dòng thẻ mới này cho các khách hàng doanh nghiệp và cá nhân. Các ngân hàng khác của Úc cũng đang có kế hoạch tung ra loại thẻ tương tự trong năm tới.

Mastercard đang quảng bá các loại thẻ này như một cách để cung cấp cho khách hàng của Ngân hàng AMP công nghệ thanh toán liền mạch và an toàn. Họ tuyên bố rằng việc xóa bỏ số 16 chữ số khỏi thẻ ghi nợ sẽ giúp xóa bỏ tình trạng trộm cắp danh tính và gian lận. Các số thẻ truyền thống sẽ được thay thế bằng sự kết hợp của mã khóa thông báo và xác thực sinh trắc học.

Khách hàng vẫn sẽ có thẻ vật lý để thanh toán trực tiếp, nhưng Mastercard có kế hoạch thay thế số thẻ tín dụng 16 chữ số tĩnh bằng mã thông báo do ứng dụng ngân hàng của khách hàng tạo ra, đảm bảo rằng thông tin thẻ thực tế không bao giờ phải lộ ra. Khoảng 25% giao dịch Mastercard trên toàn thế giới đã được mã hóa và công ty báo cáo rằng các giao dịch này đang tăng trưởng với tốc độ 50% theo năm.

(Theo PaymentJournal)

TIN VẮN NGÂN HÀNG

- **Từ nay cho đến hết ngày 31/03/2025, Ngân hàng Thương mại cổ phần Kỹ Thương Việt Nam (Techcombank)** triển khai chương trình ưu đãi hoàn tiền lên tới 350.000 nghìn đồng dành cho các khách hàng là chủ thẻ tín dụng Techcombank và có phát sinh chi tiêu hợp lệ.

- **Từ nay đến hết 19/10/2024, Ngân hàng TMCP Đầu tư và Phát triển Việt Nam (BIDV)** triển khai khuyến mãi hoàn tiền dành cho các khách hàng mở mới thẻ BIDV Mastercard Moneyverse BIDV.

- **Từ nay đến hết 31/12/2025, Ngân hàng TMCP Ngoại thương Việt Nam (Vietcombank)** thực hiện chương trình "Ưu đãi bất tận cùng thẻ VIETCOMBANK VISA". Cụ thể, các khách hàng mở mới thẻ Vietcombank Vibe và Vietcombank Vibe Platinum sẽ được nhận các phần quà bao gồm Voucher mua sắm và voucher giảm giá khi ăn uống.

- **Từ nay đến hết 31/12/2025, Ngân hàng TMCP Tiên Phong (TPBank)** tặng dịch vụ phòng chờ cho chủ thẻ tín dụng TPBank Visa Signature tại App Lounge Key cho các Chủ thẻ Tín dụng quốc tế TPBank Visa Signature có đầu mã BIN 401286 (bao gồm thẻ Chính và thẻ Phụ) có trạng thái hoạt động (Valid Card) tại hệ thống TPBank

Quý độc giả vui lòng truy cập vào website chính thức hoặc gọi điện trực tiếp cho các ngân hàng và tổ chức thẻ để biết thêm chi tiết.

Anh: Thanh toán ví kỹ thuật số gia tăng đáng kể

Theo nghiên cứu do Cơ quan quản lý tài chính Anh (FCA) thực hiện đã chỉ ra rằng 20% người tiêu dùng thẻ của Anh đã sử dụng ví kỹ thuật số cho hơn 50% giao dịch thẻ của họ và một trong mười người (10%) sử dụng ví kỹ thuật số cho hơn 75% giao dịch của họ.

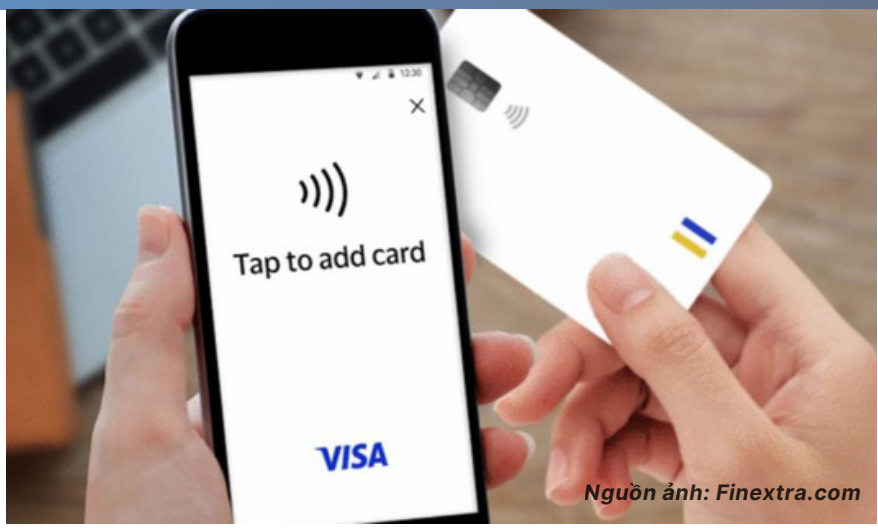
Tuy nhiên, nghiên cứu này cũng chỉ ra rằng khoảng 59% người dùng thẻ tại Anh hiện vẫn chưa hề sử dụng ví kỹ thuật số.

Tổng cộng, hơn 9 tỷ giao dịch đã được thực hiện bằng ví kỹ thuật số tại Anh vào năm 2023, tăng trừ chỉ 1 tỷ giao dịch ví kỹ thuật số được ghi nhận vào năm 2019.

Tỷ lệ giao dịch thẻ được thực hiện thông qua ví kỹ thuật số cũng tăng đáng kể, tăng từ 8% vào năm 2019 lên 29% vào năm 2023.

Các cơ quan quản lý cho biết: "Nhìn chung, các số liệu thống kê này cho thấy các công cụ ví kỹ thuật số, đặc biệt là Apple Pay và Google Pay, đang ngày càng phổ biến và một số khách hàng ngày càng phụ thuộc vào chúng".

(NFCW)



Nguồn ảnh: Finextra.com

Visa ra mắt dịch vụ "Tap to Add Card" tại 3 quốc gia mới

Visa đã ra mắt dịch vụ "Tap to Add Card" tại 3 quốc gia mới gồm Ukraine, Georgia và Nam Phi, cho phép chủ thẻ dễ dàng thêm thẻ ngân hàng vào ví di động của họ thông qua NFC chỉ bằng cách chạm thẻ vào điện thoại di động.

Visa cho biết "Với tính năng bảo mật và tiện lợi được nâng cao, Tap to Add Card loại bỏ quy trình nhập thông tin thẻ thủ công - thao tác dễ tạo lỗi phổ biến và tạo lỗ hổng giúp làm lộ lọt thông tin nhạy cảm cho kẻ gian lợi dụng".

"Tap thẻ trên điện thoại di động sẽ tạo ra một mã xác thực một lần duy nhất bằng dịch vụ Xác thực Chip của Visa, đảm bảo cung cấp thông tin xác thực thẻ an toàn và cung cấp giải pháp thay thế nhanh hơn và an toàn hơn đáng kể so với các phương pháp truyền thống".

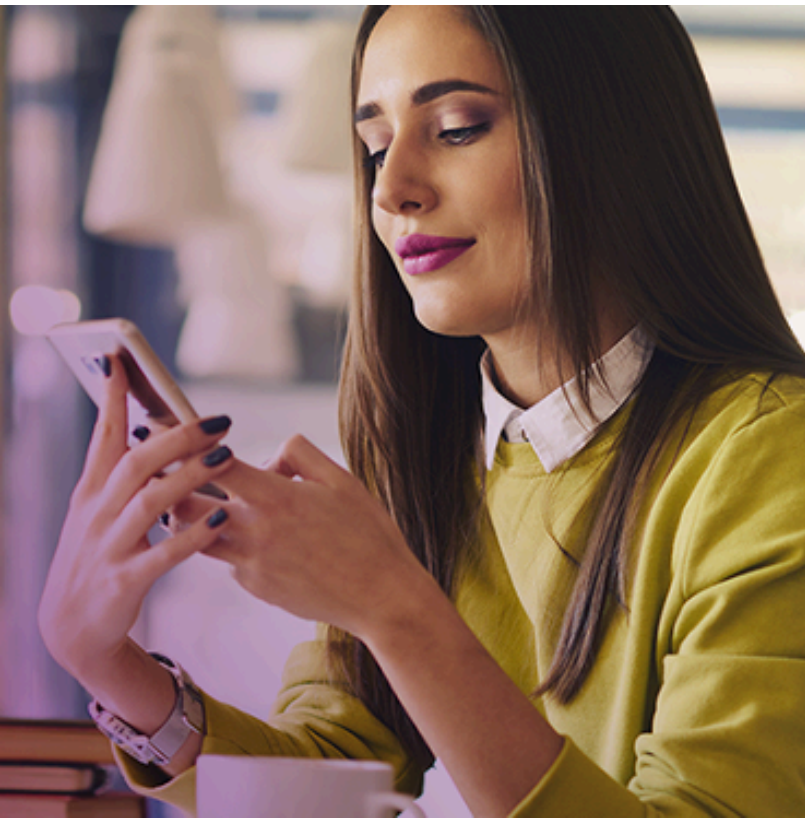
Visa cho biết thêm: "Dịch vụ Tap to Add Card được thiết kế để mang lại lợi ích cho tất cả các bên liên quan trong hệ sinh thái thanh toán. Với trải nghiệm tương tự như thanh toán tại cửa hàng, chủ thẻ có thể tận hưởng cách thanh toán nhanh hơn, thuận tiện và an toàn hơn với việc thêm thẻ vào ví kỹ thuật số, nhằm khuyến khích áp dụng thanh toán kỹ thuật số nhanh hơn."

"Với các đơn vị phát hành, Tap to Add Card có thể giúp giảm rủi ro và các chi phí liên quan đến gian lận, đơn giản hóa quy trình và giúp nâng cao tỷ lệ phê duyệt giao dịch"

(Finextra)

ENTRUST ĐƯỢC CÔNG NHẬN LÀ NHÀ LÃNH ĐẠO ĐỔI MỚI TẠI FROST RADAR™ NĂM 2024

MINNEAPOLIS, MN (ngày 16 tháng 1 năm 2025) – Entrust, công ty hàng đầu toàn cầu về các giải pháp bảo mật lấy danh tính làm trọng tâm đã thông báo rằng công ty được xếp hạng là Nhà lãnh đạo về Chỉ số đổi mới tại Frost Radar năm 2024 của Frost & Sullivan về Quản lý danh tính và quyền truy cập của khách hàng (CIAM). Công ty cũng đạt được vị trí thứ hai trong Chỉ số tăng trưởng.



Bhagwat Swaroop - Chủ tịch Giải pháp bảo mật kỹ thuật số tại Entrust cho biết, *"Được công nhận là Nhà lãnh đạo tại Frost Radar năm 2024 của Frost & Sullivan là minh chứng cho động lực không ngừng nghỉ của chúng tôi đối với sự đổi mới và xuất sắc. Vị trí này báo hiệu với khách hàng của chúng tôi rằng Entrust đang đi đầu trong các giải pháp nhận dạng tiên tiến, vừa đáp ứng được thách thức liên tục phát triển của các mối đe dọa mạng tiên tiến vừa đảm bảo trải nghiệm của người dùng thúc đẩy tăng trưởng cho doanh nghiệp. Nền tảng bảo mật toàn diện, hỗ trợ AI của chúng tôi cung cấp khả năng bảo vệ và khả năng mở rộng vô song, cho phép các tổ chức quản lý danh tính và quyền truy cập một cách an toàn trong một môi trường phức tạp và kết nối với nhau."*

Lợi ích của các giải pháp CIAM

Việc Entrust được công nhận tại Frost Radar năm 2024 nhấn mạnh những lợi thế riêng biệt của các giải pháp CIAM. Nền tảng bảo mật có thể mở rộng và hỗ trợ AI của Entrust mang lại nhiều lợi ích bao gồm:

- **Đổi mới tiên tiến:** Giải pháp CIAM của Entrust được thiết kế để đáp ứng và vượt qua các tiêu chuẩn bảo mật mới nhất với các công nghệ tiên tiến.
- **Bảo vệ toàn diện:** Entrust bảo mật toàn bộ hành trình của khách hàng từ khi đưa lên máy chủ kỹ thuật số đến khi rời khỏi máy chủ và quyền truy cập hàng ngày, kết hợp Xác minh danh tính tài liệu và sinh trắc học hỗ trợ AI (IDV), xác thực đảm bảo cao không cần mật khẩu, xác thực tăng dần dựa trên rủi ro và khả năng ký kỹ thuật số. Nền tảng toàn diện của Entrust đảm bảo khả năng bảo vệ mạnh mẽ để quản lý danh tính và quyền truy cập từ đầu đến cuối, bảo vệ các tổ chức trong môi trường được kết nối, đồng thời luôn đặt trải nghiệm người dùng (UX) lên hàng đầu.
- **Phòng ngừa gian lận nâng cao:** Nền tảng phòng ngừa gian lận toàn diện của Entrust tận dụng IDV sinh trắc học tiên tiến và xác thực dựa trên rủi ro thích ứng để giảm thiểu gian lận và xâm phạm thông tin xác thực trong khi tối ưu hóa trải nghiệm của người dùng.
- **Khả năng mở rộng và tích hợp:** Các giải pháp CIAM của Entrust cung cấp các khả năng IDV và CIAM được tích hợp sẵn, mang lại thời gian đạt giá trị nhanh hơn và tổng chi phí sở hữu thấp hơn. Các giải pháp linh hoạt và có khả năng mở rộng để đơn giản hóa quá trình tích hợp và giúp chúng thích ứng với nhiều trường hợp sử dụng khác nhau.
- **Khẳng định vị thế hàng đầu trong ngành:** Entrust có sự hiện diện mạnh mẽ trong các tổ chức tài chính và chính phủ, đặc biệt là ở Liên minh Châu Âu và Bắc Mỹ.
- **Tối ưu chi phí và thời gian triển khai:** Được thiết kế để triển khai nhanh chóng và hiện thực hóa lợi ích nhanh chóng, Entrust giảm thời gian và nguồn lực cần thiết để đạt được hệ thống quản lý danh tính khách hàng an toàn và hiệu quả. Công cụ điều phối mã thấp/không mã cho phép tùy chỉnh dễ dàng và tích hợp liền mạch với các công cụ hiện có như hệ thống CRM và nền tảng tiếp thị.

(Entrust)

Anh sẽ ra mắt giấy phép lái xe kỹ thuật số năm nay

Theo BBC đưa tin. Chính phủ Anh đang có kế hoạch ra mắt một ứng dụng di động mà các tài xế có thể sử dụng để lưu trữ phiên bản kỹ thuật số của giấy phép lái xe trên điện thoại thông minh của họ.

BBC cũng cho biết "Ứng dụng mang tên Gov.uk được dự kiến sẽ ra mắt trong năm nay, có thể giúp lưu trữ thông tin chi tiết về giấy phép an toàn và cho phép người dân sử dụng chúng như một dạng tài liệu ID để mua các sản phẩm bị hạn chế độ tuổi như rượu, bỏ phiếu hoặc đi trên các chuyến bay nội địa".

"Ứng dụng cũng sẽ cho phép khách hàng xác minh độ tuổi của họ tại các quầy hàng tự phục vụ, loại bỏ nhu cầu phải chờ đợi nhân viên làm các thủ tục xác minh và phiên bản giấy phép lái xe kỹ thuật số này cũng sẽ được cập nhật thường xuyên. Nó cũng giúp người lái xe có thể xuất trình giấy phép khi cần thiết mà không cần phải mang theo thẻ vật lý, tránh bi hỏng hoặc làm mất".

Tin tức được thông báo trong một chuỗi các hoạt động của Chính phủ Anh trong việc mở đường cho "các danh tính kỹ thuật số được chấp nhận và có hiệu lực trong việc xác minh độ tuổi, danh tính bên cạnh các tài liệu truyền thống như hộ chiếu, thẻ bằng lái xe và thẻ ID vật lý".

(NFCW)

Tương lai phổ biến của sinh trắc học tĩnh mạch bàn tay

Sinh trắc học tĩnh mạch bàn tay đang được chú trọng hiện nay, với việc được đầu tư từ các công ty hàng đầu ngành tài chính công nghệ. Xác minh tĩnh mạch bàn tay đang trở thành lựa chọn hàng đầu cho các ngành bán lẻ, ngân hàng và kiểm soát ra vào

Quét sinh trắc học tĩnh mạch bàn tay trong tương lai sẽ ngày càng được sử dụng nhiều hơn, với việc các công ty quốc tế như Tencent, Visa, Amazon, J.P. Morgan và Mastercard đang thúc đẩy hỗ trợ các hệ thống thanh toán dựa trên công nghệ xác minh sinh trắc học này.

Trước đây, Visa đã giới thiệu công nghệ thanh toán sinh trắc học tĩnh mạch lòng bàn tay, trong khi Tencent Cloud đã giới thiệu riêng một hệ thống xác minh lòng bàn tay sử dụng camera hồng ngoại để chụp và phân tích các mẫu tĩnh mạch cùng dấu vân tay kết hợp.

J.P. Morgan đang có kế hoạch triển khai công nghệ thanh toán dựa trên lòng bàn tay của riêng mình vào năm tới, trong khi Mastercard đã tích hợp sinh trắc học lòng bàn tay vào chương trình thanh toán sinh trắc học của họ.

Tại UAE, chính quyền Dubai đang có kế hoạch hợp lý hóa các khoản thanh toán tại tàu điện ngầm và bán lẻ bằng công nghệ xác minh sinh trắc tĩnh mạch lòng bàn tay vào năm tới. Công nghệ này đã được triển khai để tạo điều kiện thuận lợi cho việc kiểm tra hành khách tại các cảng hàng không và cảng biển của quốc gia.

(Biometric Update)

Top 10 xu hướng an ninh mạng trong năm 2025

Năm 2024 ghi dấu sự tồn tại phổ biến của tình trạng gián đoạn mạng máy tính. Những cuộc tấn công bằng mã độc tống tiền (ransomware) đã làm tê liệt các hệ thống y tế lớn, hoạt động kinh doanh và các cơ quan chính phủ. Một bản cập nhật phần mềm bị lỗi khiến hệ thống công nghệ thông tin (CNTT) trên toàn cầu "chết lâm sàng". Hoạt động gián điệp mạng thậm chí còn trở nên táo tợn hơn. Và mức độ cường điệu xoay quanh Trí tuệ nhân tạo (AI) đã lên đến đỉnh điểm, phá vỡ toàn bộ không gian công nghệ.

Liệu năm 2025 có chứng kiến nhiều sự cố gián đoạn hơn nữa không? Các chuyên gia an ninh mạng có thể lập lại trật tự sau sự hỗn loạn? Hội đồng gồm 10 nhà lãnh đạo, chuyên gia phân tích và giáo dục an ninh mạng của GovInfoSecurity sẽ chia sẻ quan điểm về 10 xu hướng hàng đầu cần theo dõi trong năm 2025:

1. Ngày càng có nhiều đối tượng khai thác ransomware nhắm vào các mục tiêu có giá trị cao để đòi số tiền chuộc lớn hơn, trong khi các nhóm khác sẽ tăng cường đánh cắp dữ liệu, tấn công các nhà cung cấp bên thứ ba và nhà cung cấp phần mềm

2. Tội phạm mạng sẽ đẩy mạnh các hoạt động tấn công bộ phận hỗ trợ CNTT, quản trị viên và lãnh đạo cấp cao thông qua thủ đoạn sử dụng tính năng deepfake video và nhân bản giọng nói dựa trên AI để đánh cắp thông tin đăng nhập và thực hiện hành vi lừa đảo.

3. Do mối quan hệ cộng tác ngày càng chặt chẽ giữa các nhóm quốc gia-nhà nước và tổ chức tội phạm, các sự kiện địa chính trị có thể dẫn đến nhiều cuộc tấn công gây gián đoạn hơn nữa nhằm vào hệ thống cơ sở hạ tầng trọng yếu.

4. Giới điều tra sẽ phát hiện thêm bằng chứng về việc các đối thủ trên không gian mạng sắp đặt trước các vụ xâm nhập nhằm vào hệ thống công nghệ vận hành (OT), thiết bị biên và công nghệ thông minh.

5. Các khoản tiền phạt đầu tiên được áp dụng theo Đạo luật AI của Liên minh châu Âu (EU) và những các kết quả khác nhau từ các dự án thí điểm AI tạo sinh (GenAI) sẽ làm chậm các sáng kiến AI của doanh nghiệp và làm gia tăng nhu cầu về kiểm soát bảo mật, quyền riêng tư và quản trị.

6. Tình trạng gia tăng những cuộc tấn công nhắm vào các doanh nghiệp vừa và nhỏ sẽ thúc đẩy nhu cầu về các dịch vụ bảo mật được quản lý.

7. Nhu cầu về các giải pháp quản lý tình trạng bảo mật dữ liệu và chống mất mát dữ liệu tích hợp sẽ tăng lên khi ban lãnh đạo của các tổ chức tìm cách giảm thiểu rủi ro xâm phạm dữ liệu.

8. Ngày càng có nhiều tổ chức triển khai xác thực đa yếu tố chống lừa đảo trên quy mô lớn để tăng cường sức mạnh của công nghệ này, đồng thời khắc chế các chiêu trò tấn công phi kỹ thuật.

9. Giáo dục về an ninh mạng sẽ trở nên toàn cầu hóa hơn, do các mối quan hệ hợp tác xuyên biên giới cho phép chia sẻ chương trình giảng dạy, chương trình trao đổi ảo, hệ thống tiêu chuẩn và các bài học thực tiễn tốt nhất.

10. Các vụ kiện tụng liên quan đến xâm phạm dữ liệu và gián đoạn CNTT sẽ gia tăng, khi các nguyên đơn và công tố viên cố gắng buộc đội ngũ Giám đốc an toàn thông tin (CISO) và giám đốc điều hành hàng đầu phải gánh trách nhiệm về các sự cố mạng.

Các sự cố gián đoạn trên không gian mạng sẽ tiếp diễn trong năm 2025, song vẫn có hy vọng rằng các hàng rào phòng thủ CNTT của chúng ta, cùng hàng triệu chuyên gia trong ngành, sẽ giải quyết được những thách thức trước mắt./.

(GovInfoSecurity)

CÁC MỐI ĐE DỌA GIAN LẬN THANH TOÁN NGÀY CÀNG TRỞ NÊN NGHIÊM TRỌNG HƠN

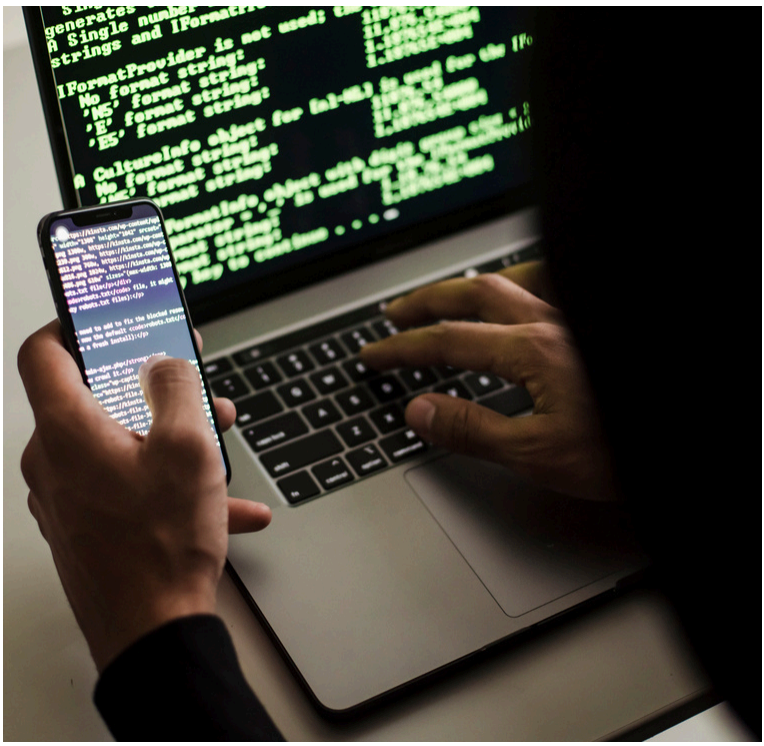
Báo cáo mới đây của Visa đã liệt kê các âm mưu và thủ đoạn lừa đảo qua mạng trực tuyến khiến công ty phải đầu tư 11 tỷ USD trong vòng 5 năm qua để cải thiện các hệ thống. Tội phạm mạng đã lợi dụng những lỗ hổng trong thanh toán và sử dụng trí tuệ nhân tạo (AI) để đẩy nhanh tốc độ thực hiện các hành vi sai trái.

Trong báo cáo nửa đầu năm 2024, Visa đã xác định những chiêu trò gian lận thanh toán đang gây rủi ro cho các công ty và người tiêu dùng (NTD) như: giao dịch hoàn trả mua hàng giả mạo; tấn công bằng mã độc tống tiền (ransomware) và xâm phạm dữ liệu; tấn công đánh cắp thông tin số (digital skimming); mạo danh.

Visa nhận định tội phạm gian lận ngày càng đi sâu thảo luận trên các diễn đàn ngầm về việc sử dụng AI cho mục đích gian lận thanh toán. Theo thông cáo báo chí được công bố cùng với báo cáo, Visa đã đầu tư 11 tỷ USD trong vòng 5 năm qua vào công nghệ và các chương trình cải tiến cơ sở hạ tầng khác nhằm giúp hệ thống của "gã khổng lồ thẻ" trở nên an toàn hơn.

Báo cáo phân tích "những mối đe dọa và chiêu trò lừa đảo mới nổi nhắm vào các ngân hàng và NTD, trong đó có sự hồi phục bất ngờ của tội phạm quy mô nhỏ". Thông cáo dẫn lời ông Paul Fabara - Giám đốc rủi ro và dịch vụ khách hàng của Visa - chia sẻ: "Khi các phương thức thanh toán trở nên an toàn hơn, tội phạm gian lận đang sử dụng trở lại những chiến thuật đã được kiểm chứng, nhắm vào mắt xích yếu nhất trong hệ sinh thái: đó là NTD".

Một trong những lỗ hổng mà các tác nhân đe dọa đang khai thác là các giao dịch ủy quyền mua và hoàn trả bị sai sót - trường hợp xảy ra khi các công ty cung cấp dịch vụ thanh toán bị lầm lẫn trong quá trình phê duyệt giao dịch. Theo báo cáo, trong 6 tháng đầu năm 2024, số cuộc điều tra gian lận mà Visa mở tăng 81% so với giai đoạn 6 tháng cuối năm 2023. Mỗi vụ tấn công như vậy đã dẫn đến "những khoản thiệt hại tiềm tàng" trị giá 184.000 USD đối với các đối tác phát hành thẻ của Visa.



Theo Visa, để thực hiện những cuộc tấn công ransomware và xâm phạm dữ liệu, kẻ gian ngày càng nhắm mục tiêu vào các nhà cung cấp bên thứ ba.

Mặc dù ghi nhận mức giảm 12,3% về số sự cố ransomware và xâm phạm dữ liệu riêng lẻ trong 6 tháng đầu năm 2024, song Visa lại chứng kiến mức tăng 24% về số vụ tấn công nhắm vào các nhà cung cấp dịch vụ bên thứ ba.

Báo cáo ghi nhận số vụ tấn công đánh cắp thông tin số, sử dụng mã độc để đánh cắp thông tin nhạy cảm của khách hàng từ các trang web doanh nghiệp, vẫn duy trì ổn định trong nửa đầu năm 2024. Tuy nhiên, Visa dự đoán loại hình gian lận này sẽ gia tăng trong mùa mua sắm cuối năm. Gã khổng lồ thẻ cũng "vạch mặt chỉ tên" những thủ đoạn tấn công phi kỹ thuật nâng cao mà kẻ gian đang sử dụng để lừa gạt các dịch vụ điện tử của các nhà bán lẻ, thông qua việc tạo ra các kế hoạch mạo danh phức tạp và lợi dụng dữ liệu xác thực, chẳng hạn như mật khẩu sử dụng một lần (OTP).

HỖ TRỢ LỰC LƯỢNG THỰC THI PHÁP LUẬT

Visa đã nêu bật những nỗ lực của công ty trong công tác hỗ trợ lực lượng thực thi pháp luật truy bắt các đối tượng gian lận khai thác lỗ hổng thanh toán. Hồi tháng 4, Visa thông báo đã hỗ trợ Cơ quan Mật vụ Mỹ (USSS) và lực lượng thực thi pháp luật địa phương trong "Chiến dịch April Fools", dẫn đến việc bắt giữ 33 nghi phạm ở bang California bị cáo buộc thực hiện các vụ gian lận chuyển tiền điện tử (EBT).

Visa cũng đã hỗ trợ Cục Điều tra Liên bang (FBI) trong quá trình điều tra 22 nghi phạm bị cáo buộc mua và sử dụng thẻ thanh toán bị đánh cắp từ một nhà bán lẻ lớn ở Bắc Mỹ, trong khuôn khổ vụ án năm 2021. Tháng 2 năm nay, 20 bị cáo đã bị kết án vì hành vi sử dụng thông tin thẻ quà tặng, thẻ tín dụng và thẻ ghi nợ bị đánh cắp trong một cuộc tấn công mạng, gây tổng thiệt hại lên đến 25 triệu USD.

Ngoài việc công khai hợp tác với các cơ quan thực thi pháp luật, Visa còn chia sẻ những lời mách nước từ các cơ quan liên bang về cách thức mà NTD có thể bảo vệ bản thân.

Các đối tượng tội phạm lợi dụng thẻ EBT thường nhắm vào những hệ thống thiết bị thanh toán đầu cuối (POS) hoặc ATM, nơi kẻ gian cài đặt thiết bị đánh cắp thông tin để chiếm đoạt số thẻ thanh toán của NTD.

USSS lưu ý chủ thẻ nên kiểm tra đầu đọc thẻ để phát hiện thiết bị chôm chỉa thông tin, đặc biệt là ở các khu du lịch. Cơ quan này cũng khuyến cáo nên che bàn phím ATM khi nhập mã PIN, vì một số đối tượng tội phạm lắp đặt camera giấu kín ở gần bàn phím để đánh cắp mã PIN.

NHỮNG MỐI NGUY HẠI TRONG TƯƠNG LAI

Visa dự đoán một hình thức gian lận khác được gọi là "trích xuất" (enumeration) sẽ vẫn phổ biến đối với giới tội phạm. Khi thi triển thủ đoạn gian lận này, kẻ gian sử dụng chương trình máy tính để đoán mã nhận dạng thanh toán phổ biến cho các giao dịch trực tuyến, thử nhập số tài khoản, mã bảo mật và ngày hết hạn cho đến khi xác định được bộ thông tin chính xác.

Visa cũng nghi ngờ tình trạng gian lận thẻ tại các trạm xăng dầu, những chiêu trò bất lương với thẻ trả trước và các âm mưu ủy quyền hoàn trả mua hàng sẽ tiếp tục tồn tại.

Các công ty lưu trữ đám mây, nhà cung cấp phần mềm từ xa, dịch vụ truyền file và các nhà cung cấp bên thứ ba khác cũng sẽ tiếp tục là những mục tiêu hàng đầu của các vụ tấn công ransomware.

Ngoài ra, Visa dự đoán email lừa đảo (phishing) sẽ ngày càng có sức thuyết phục và thực tế hơn./.

(Payments Dive)

MK® group

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