MK group
Smart Digital Security

THẾ GIỚI THẺ

Bản tin nội bộ của MK Group

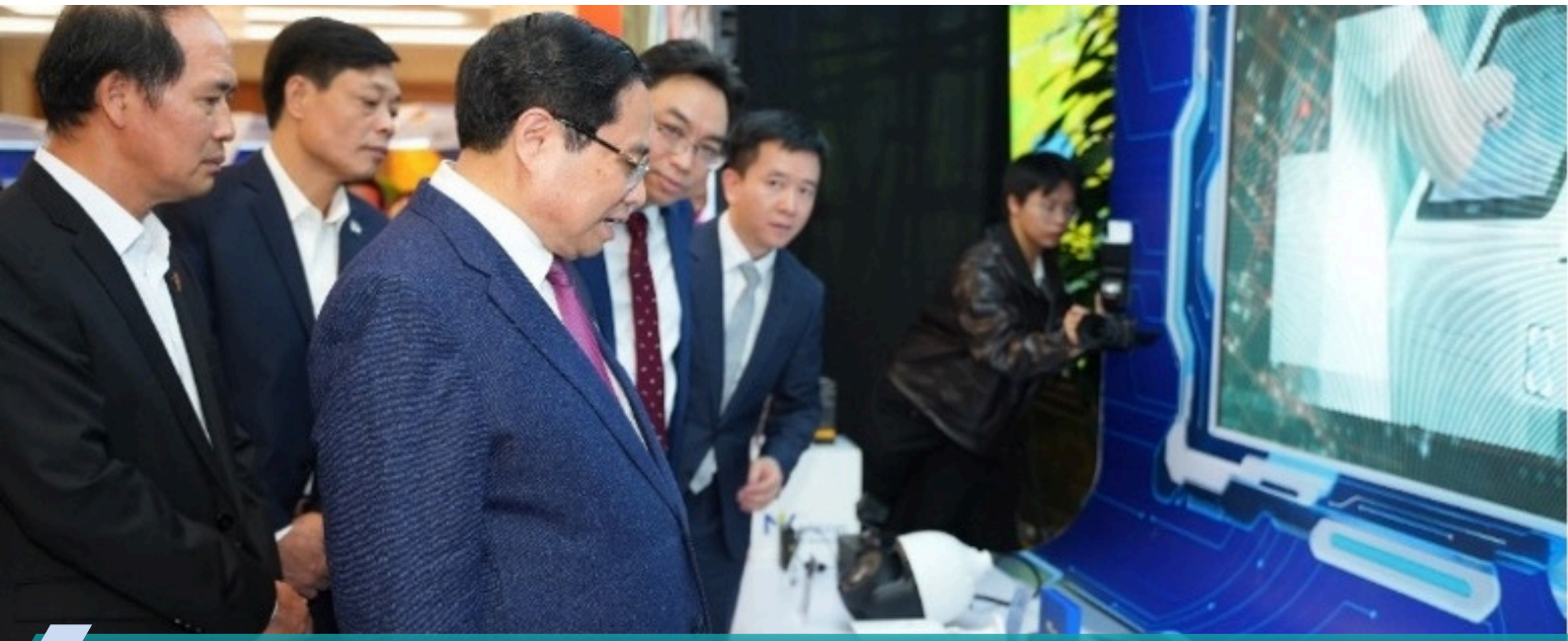
Số 179 | Tháng 1.2026

TIN NỔI BẬT

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

MK GROUP

THAM GIA TRIỂN LÃM SƠ KẾT ĐỀ ÁN 06 GIAI ĐOẠN 2022 - 2025: GÓP PHẦN KIẾN TẠO MẠCH SỐNG SỐ QUỐC GIA



Thủ Tướng Phạm Minh Chính đến tham quan khu trưng bày của MK Group

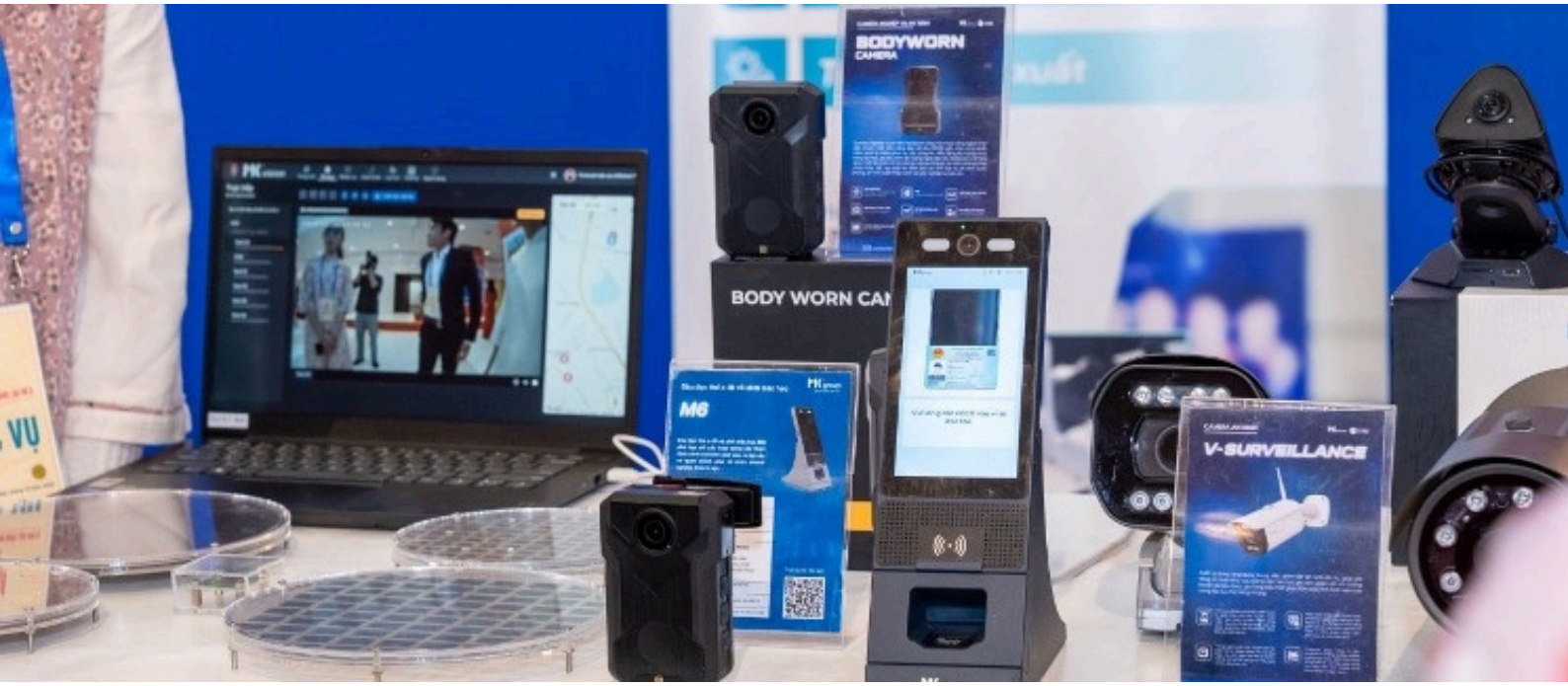
Ngày 18/12/2025, tại Văn phòng Chính phủ (số 1 Hoàng Hoa Thám, Hà Nội), Tập đoàn MK (MK Group) vinh dự tham gia Triển lãm Sơ kết Đề án 06 - Giai đoạn 2022-2025, sự kiện quan trọng nằm trong khuôn khổ Hội nghị sơ kết 1 năm triển khai Chương trình hành động của Chính phủ thực hiện Nghị quyết số 57-NQ/TW; 5 năm thực hiện chương trình tổng thể cải cách hành chính Nhà nước; 4 năm triển khai Đề án 06.

Sau 4 năm triển khai, Đề án 06 đã khẳng định vai trò đầu tàu của Bộ Công an trong tiến trình chuyển đổi số quốc gia, tạo chuyển biến mạnh mẽ từ nhận thức đến hành động, đưa chuyển đổi số trở thành nhiệm vụ chung của toàn bộ hệ thống chính trị. Đề án lấy người dân và doanh nghiệp làm trung tâm, từng bước hình thành mạch sống số quốc gia thông qua dữ liệu dân cư, định danh và xác thực điện tử. Trong giai đoạn tiếp theo, Đề án 06 chuyển trọng tâm sang khai thác giá trị dữ liệu, với 4 định hướng chiến lược: hoàn thiện thể chế; phát triển hệ sinh thái công dân số; thúc đẩy kinh tế dữ liệu; và bảo đảm an ninh dữ liệu, chủ quyền số - qua đó cụ thể hóa các mục tiêu của Nghị quyết 57 về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia.

Trong khuôn khổ triển lãm "Đề án 06 - Kiến tạo mạch sống số quốc gia, thúc đẩy triển khai Nghị quyết 57", Thủ tướng Chính phủ cùng lãnh đạo các bộ, ngành đã tham quan khu trưng bày của các doanh nghiệp công nghệ chủ lực như Viettel, VNPT, FPT, CMC, các ngân hàng và MK Group, ghi nhận những giải pháp công nghệ đã và đang được triển khai hiệu quả trong thực tiễn. Tại sự kiện, MK Group đã giới thiệu hệ sinh thái các giải pháp bảo mật và định danh số "Make in Vietnam", phục vụ quản lý nhà nước, dịch vụ công và an ninh thông minh. Các giải pháp tiêu biểu bao gồm công nghệ thẻ chip, các nền tảng định danh số, xác thực đa lớp và bảo mật dữ liệu đáp ứng tiêu chuẩn an toàn cao.

Là doanh nghiệp công nghệ Việt Nam đồng hành xuyên suốt quá trình triển khai Đề án 06, MK Group tự hào góp phần xây dựng chính phủ số, xã hội số và công dân số an toàn, tin cậy, đồng thời khẳng định năng lực làm chủ công nghệ lõi và trách nhiệm của doanh nghiệp Việt trong công cuộc bảo vệ không gian số quốc gia.

TẬP ĐOÀN MK VINH DỰ ĐỒNG HÀNH CÙNG CÁC TRIỂN LÃM SẢN PHẨM CÔNG NGHỆ CHIẾN LƯỢC MAKE IN VIETNAM



Trong tháng 12/2025, MK Group và MK Vision (công ty thành viên của Tập đoàn MK) đã tham gia và đồng hành cùng nhiều triển lãm thành tựu công nghệ do các Bộ, Ban, Ngành tổ chức, giới thiệu các sản phẩm và giải pháp công nghệ lõi "Make in Vietnam" phục vụ chuyển đổi số chính phủ, quản lý nhà nước, gia tăng an ninh - an toàn, giao thông và đô thị thông minh.

Trong chuỗi sự kiện này, ngày 19/12/2025, MK Vision và Tập đoàn MK đã có vinh dự được trưng bày hệ sinh thái AI Camera xử lý tại biên (AI Camera on Edge) trong khuôn khổ triển lãm "Hào khí 80 năm - Hành trình vinh quang tiến vào kỷ nguyên mới" do Cục Cảnh sát Giao thông - Bộ Công an tổ chức. Ngay sau đó, Tập đoàn MK cũng đã được góp mặt trong gian hàng triển lãm công nghệ chiến lược của Bộ Khoa học và Công nghệ, tại Triển lãm thành tựu khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số sau 40 năm đổi mới đất nước diễn ra từ 26/12 đến 27/12/2025, Trung tâm Hội nghị Quốc gia, Hà Nội.

Tại các sự kiện, MK Group và Vision đã giới thiệu về hệ sinh thái Camera AI "Make in Vietnam" do Tập đoàn tự nghiên cứu, phát triển và sản xuất, thể hiện năng lực làm chủ toàn bộ chuỗi giá trị công nghệ. Đặc biệt, các giải pháp AI Camera on Edge - công nghệ xử lý AI trực tiếp tại thiết bị được xác định là công nghệ phát triển chủ lực và đã được phê duyệt trong chính sách công nghệ chiến lược ưu tiên, đáp ứng yêu cầu cao về bảo mật dữ liệu, độ trễ thấp và khả năng vận hành ổn định trong các hệ thống hạ tầng trọng yếu.

Bên cạnh đó, MK cũng đã giới thiệu các sản phẩm đầu đọc MK eID, phục vụ định danh điện tử và xác thực an toàn, có khả năng tích hợp linh hoạt với hệ thống Camera AI và các nền tảng quản lý. Sự kết hợp giữa AI Camera và MK eID góp phần hình thành chuỗi giải pháp đồng bộ, phục vụ hiệu quả cho quản lý nhà nước, dịch vụ công và đô thị thông minh.

Sự hiện diện của MK Group và MK Vision tại các triển lãm không chỉ khẳng định năng lực công nghệ và tinh thần đổi mới sáng tạo "Make in Vietnam", mà còn thể hiện cam kết đồng hành cùng các cơ quan quản lý trong phát triển các công nghệ chiến lược, góp phần xây dựng hạ tầng số an toàn, hiện đại và bền vững cho Việt Nam./.

BAN CƠ YẾU CHÍNH PHỦ VÀ MK GROUP HỢP TÁC PHÁT TRIỂN CÔNG NGHỆ LƯỢNG TỬ, MẬT MÃ VÀ AN TOÀN THÔNG TIN

Sáng 23/12, tại Hà Nội, Ban Cơ yếu Chính phủ và Công ty Cổ phần Tập đoàn MK (MK Group) đã ký kết Thỏa thuận hợp tác toàn diện trong các lĩnh vực công nghệ lượng tử, mật mã, bảo mật và an toàn thông tin. Thỏa thuận hướng tới xây dựng hệ sinh thái sản phẩm mật mã "Make in Vietnam", góp phần bảo đảm chủ quyền công nghệ, đặc biệt trong bối cảnh chuyển đổi số quốc gia và sự phát triển nhanh của các công nghệ chiến lược.

Tham dự lễ ký kết, về phía Ban Cơ yếu Chính phủ có Trung tướng Vũ Ngọc Thiềm – Trưởng ban, Thiếu tướng Hồ Văn Hương – Phó Trưởng ban, cùng đại diện lãnh đạo các cơ quan, đơn vị trực thuộc, trong đó có Viện Khoa học – Công nghệ mật mã, đơn vị đầu mối triển khai thỏa thuận. Về phía MK Group có ông Nguyễn Trọng Khang – Chủ tịch HĐQT kiêm Tổng Giám đốc, ông Đỗ Viết Hà – Giám đốc Công nghệ, ông Nguyễn Thanh Hoài – Giám đốc Phần mềm và bà Lê Việt Linh – Phó Giám đốc MK Hitek.

Lễ ký kết thoả thuận hợp tác giữa Ban Cơ yếu chính phủ và Công ty Cổ phần Tập đoàn MK

Phát biểu tại buổi lễ, Trung tướng Vũ Ngọc Thiềm nhấn mạnh, việc ký kết thỏa thuận hợp tác lần này có ý nghĩa quan trọng, đánh dấu bước phát triển mới trong mối quan hệ phối hợp giữa cơ quan quản lý nhà nước chuyên trách về mật mã và doanh nghiệp công nghệ trong nước. Mục tiêu chung là từng bước làm chủ khoa học – công nghệ chiến lược, bảo đảm an ninh mạng, an ninh dữ liệu và chủ quyền số, qua đó hiện thực hóa các định hướng lớn về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số đã được nêu trong Nghị quyết số 57-NQ/TW của Bộ Chính trị.

Theo Trung tướng Vũ Ngọc Thiềm, Ban Cơ yếu Chính phủ và MK Group đã có quá trình hợp tác từ trước với nhiều kết quả tích cực. Trên nền tảng đó, thỏa thuận hợp tác lần này tập trung vào ba mục tiêu trọng tâm. Thứ nhất, tăng cường quan hệ hợp tác chiến lược, lâu dài, phát huy thế mạnh của mỗi bên trong nghiên cứu, chuyển giao công nghệ và phát triển các sản phẩm an toàn thông tin phục vụ Chính phủ số, kinh tế số và xã hội số. Thứ hai, xây dựng khuôn khổ hợp tác toàn diện trong lĩnh vực công nghệ lượng tử, mật mã và bảo mật thông tin, hướng tới hình thành hệ sinh thái sản phẩm mật mã "Make in Vietnam", góp phần bảo đảm chủ quyền công nghệ lượng tử. Thứ ba, hỗ trợ lẫn nhau trong nghiên cứu, đổi mới sáng tạo, tăng cường liên kết giữa cơ quan quản lý nhà nước và doanh nghiệp công nghệ Việt Nam.

Với hơn 80 năm xây dựng và phát triển, Ban Cơ yếu Chính phủ là cơ quan đầu ngành trong công tác tham mưu cho Đảng, Nhà nước về bảo vệ bí mật nhà nước bằng mật mã; cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ; triển khai hệ thống giám sát an toàn thông tin trên các mạng CNTT trọng yếu và quản lý nhà nước về mật mã dân sự. Trưởng ban Vũ Ngọc Thiềm tin tưởng, thỏa thuận hợp tác sẽ được triển khai thực chất, hiệu quả, tạo ra các sản phẩm, giải pháp có giá trị cao, đóng góp thiết thực cho nhiệm vụ bảo vệ Tổ quốc trên không gian số và xây dựng hệ sinh thái đổi mới sáng tạo gắn kết Nhà nước – Nhà khoa học – Doanh nghiệp.

Cũng tại buổi lễ, ông Nguyễn Trọng Khang, Chủ tịch HĐQT kiêm Tổng Giám đốc MK Group cho biết, với định hướng phát triển các giải pháp xác thực và bảo mật số phục vụ an ninh, chính phủ điện tử và tài chính – ngân hàng, MK Group hiện đã làm chủ nhiều công nghệ lõi trong lĩnh vực bảo mật số thông minh, thẻ thông minh và sinh trắc học. Trong khuôn khổ hợp tác, MK Group cam kết triển khai các hoạt động đào tạo và phát triển nguồn nhân lực, bao gồm tổ chức chương trình thực tập, tham quan thực tế cho sinh viên Học viện Kỹ thuật mật mã, tài trợ học bổng và hỗ trợ các cuộc thi an toàn thông tin (CTF)./.

GIAO DỊCH THANH TOÁN DÙNG KHÔNG TIỀN MẶT TĂNG TIẾP CẢ VỀ SỐ LƯỢNG VÀ GIÁ TRỊ

Theo Ngân hàng Nhà nước, trong 11 tháng năm 2025, hoạt động thanh toán không dùng tiền mặt tăng trưởng khá so với cùng kỳ năm 2024, giao dịch thanh toán không dùng tiền mặt tăng 42,34% về số lượng và 22,59% về giá trị.

Thông tin từ Cổng thông tin điện tử Ngân hàng Nhà nước, hội nghị ngày 31/12 tại Hà Nội về triển khai nhiệm vụ ngân hàng năm 2026 có sự tham dự và phát triển chỉ đạo của Thủ tướng Phạm Minh Chính.

Báo cáo tổng kết năm 2025 và nhiệm kỳ 2021 - 2025 của Ngân hàng Nhà nước được trình bày tại hội nghị nêu rõ, ngành ngân hàng là một trong những ngành đi đầu trong chuyển đổi số, cải cách thủ tục hành chính, xây dựng cơ sở dữ liệu cũng như phát triển các tiện ích phục vụ người dân và doanh nghiệp.

Riêng trong hoạt động thanh toán, thời gian qua, Ngân hàng Nhà nước đã tham mưu, trình ban hành và ban hành nhiều chính sách quan trọng để thúc đẩy thanh toán không dùng tiền mặt, tạo thuận lợi cho chuyển đổi số hoạt động ngân hàng, đồng thời phát triển các sản phẩm, dịch vụ thanh toán mới, tiện ích, an toàn và có chi phí hợp lý.

TIN VẮN NGÂN HÀNG

- **Từ ngày 01/01/2026 đến hết ngày 31/03/2026 Ngân hàng Thương mại cổ phần Đầu tư và Phát triển Việt Nam (BIDV)** thực hiện chương trình "Thẻ mới trong tay - Lộc đầy mỗi ngày" với ưu đãi hoàn tiền từ 300.000 VNĐ lên tới 1.000.000 VNĐ dành cho các khách hàng khi mở mới các hạng thẻ tín dụng quốc tế cá nhân của BIDV và phát sinh giao dịch hợp lệ;

- **Từ tháng 12/2025 cho đến ngày 10/05/2026, Ngân hàng Thương mại Cổ phần Phát triển Thành phố Hồ Chí Minh (HDBank)** triển khai ưu đãi hoàn tiền từ 200.000 VNĐ dành cho các khách hàng mở mới và phát sinh giao dịch với thẻ tín dụng quốc tế HDBank;

- **Ngân hàng Thương mại Cổ phần Quốc tế Việt Nam (VIB) từ ngày 01/01/2026 đến hết 31/03/2026** triển khai chương trình khuyến mại quà tặng dành cho chủ thẻ tín dụng VIB, với tổng giá trị ưu đãi lên tới 2,5 triệu đồng, áp dụng cho các giao dịch chi tiêu mua sắm, ẩm thực, du lịch./.

Song song đó, hạ tầng thanh toán không dùng tiền mặt, chuyển đổi số ngành ngân hàng cũng luôn được chú trọng đầu tư, nâng cấp. Công tác đảm bảo an ninh, an toàn trong hoạt động thanh toán và các hệ thống thông tin ứng dụng, nghiệp vụ ngân hàng được đặc biệt chú trọng. Hệ sinh thái số, thanh toán số đã được thiết lập kết nối giữa dịch vụ ngân hàng với nhiều dịch vụ khác trong nền kinh tế để cung ứng trải nghiệm liền mạch cho người dùng.

Đáng chú ý, thanh toán không dùng tiền mặt tiếp tục tăng trưởng, chuyển đổi số ngân hàng đạt nhiều thành tựu quan trọng, từ đó, góp phần thúc đẩy phát triển Chính phủ số, kinh tế số và xã hội số. Theo thống kê, đến nay, 87% người trưởng thành tại Việt Nam đã có tài khoản ngân hàng. Nhiều nghiệp vụ cơ bản của ngân hàng đã được số hóa hoàn toàn. Nhiều tổ chức tín dụng tại Việt Nam có tỷ lệ trên 95% giao dịch được thực hiện trên kênh số.

Trong 11 tháng năm 2025, hoạt động thanh toán không dùng tiền mặt tăng trưởng khá so với cùng kỳ năm ngoái. Cụ thể, giao dịch thanh toán không dùng tiền mặt trong 11 tháng của năm 2025 đã tăng 42,34% về số lượng và 22,59% về giá trị. Trong đó, giao dịch thanh toán qua kênh Internet tăng tương ứng 52,91% về số lượng và 36,25% về giá trị; giao dịch qua kênh điện thoại di động tăng tương ứng 36,48% và 20,48%; giao dịch qua QR Code tăng 54,45% về số lượng và 141,02% về giá trị.

Thời gian vừa qua, Ngân hàng Nhà nước cũng đã phối hợp chặt chẽ với Bộ Công an triển khai nhiệm vụ được giao tại "Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022 - 2025, tầm nhìn đến năm 2030" (gọi tắt là Đề án 06 để làm sạch dữ liệu, xác minh thông tin và đối chiếu thông tin sinh trắc học của khách hàng, hỗ trợ các hoạt động nghiệp vụ, qua đó góp phần giảm số lượng vụ việc lừa đảo mất tiền của khách hàng./.

(Vietnamnet)

VÍ ĐIỆN TỬ TRỞ THÀNH "CỬA NGÕ" MẶC ĐỊNH CHO THANH TOÁN TOÀN CẦU

Trong năm 2025, ví điện tử đã tiến ra khỏi vai trò là công cụ tiện lợi để thanh toán, chuyển mình thành giao diện trung tâm cho việc lưu chuyển tiền tệ trên toàn thế giới. Ban đầu được xem như phương thức thanh toán nhanh cho mua sắm trực tuyến và tại cửa hàng, ví điện tử đang đảm nhiệm vai trò sâu rộng hơn, và trở thành kênh tiếp cận các nguồn tài chính hiện có như thẻ, tài khoản ngân hàng, mà không cần thay thế chúng.

Theo dữ liệu của PYMNTS, ví di động hiện chiếm 35% giao dịch trực tuyến và 21% thanh toán tại cửa hàng trên 11 quốc gia đại diện cho hơn một nửa GDP toàn cầu. Điều này phản ánh sự thay đổi quan trọng: người tiêu dùng không từ bỏ thẻ hay tài khoản, mà đơn giản là thay đổi cách họ tiếp cận chúng thông qua ví điện tử.

Ở những thị trường như Nhật Bản và Singapore, ví đã trở thành phần tất yếu của giao dịch hàng ngày, nhờ sự phổ biến của mã QR, phương thức thanh toán thời gian thực và hành vi "ưu tiên di động". Ở nhiều thị trường châu Âu và Hoa Kỳ, ví điện tử tăng trưởng chậm hơn nhưng vẫn củng cố vị thế như một lựa chọn thanh toán an toàn hơn với sự kết hợp cùng bảo mật sinh trắc học, tiện dụng cho các thao tác thanh toán hàng ngày.

Các chuyên gia nhấn mạnh rằng ví không chỉ là "đích đến" thanh toán: chúng chính là cổng mở ra nhiều lựa chọn cho người dùng - chuyển đổi linh hoạt giữa thẻ, chuyển khoản và số dư trong ví, và giúp mang lại khả năng thanh toán linh hoạt hơn.

Sự phát triển của ví điện tử đang thúc đẩy kỳ vọng về giao dịch nhanh hơn, an toàn hơn và minh bạch hơn, đặt nền tảng cho một hệ sinh thái thanh toán toàn cầu với ví số ở trung tâm của mọi chuyển động tài chính.

(PYMNTS)

NATIONWIDE: RÚT TIỀN MẶT TẠI ATM TIẾP TỤC GIA TĂNG

Theo dữ liệu từ Nationwide, tổng giá trị tiền mặt được rút từ các máy ATM tại Vương quốc Anh đã đạt 4,2 tỷ bảng trong năm 2025, vượt qua mức kỷ lục trước đó là 4 tỷ bảng vào năm 2017.

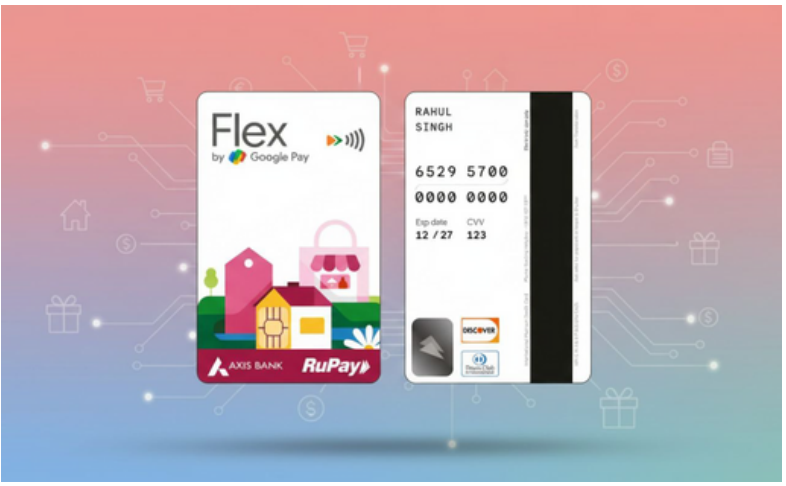
Số liệu kỷ lục mới này củng cố luận điểm rằng việc rút tiền mặt tại các ATM đã tăng trưởng liên tục trong bốn năm liền trên toàn hệ thống chi nhánh của Nationwide.

Hiệp hội này ghi nhận đã có khoảng 34,7 triệu lượt rút tiền mặt tại 1.270 máy ATM, đặt ở 605 chi nhánh trong năm vừa qua, tăng khoảng 6% so với năm 2024. Số tiền rút trung bình mỗi giao dịch cũng tăng từ 113 bảng năm 2024, lên mức 120 bảng trong năm 2025.

Bên cạnh đó, các dữ liệu tổng hợp cũng cho thấy lượng rút tiền từ khách hàng không thuộc Nationwide tăng 6%, đồng thời lượng rút tiền từ chính khách hàng Nationwide cũng tăng 6%.

(Finextra)

GOOGLE RA MẮT THẺ TÍN DỤNG LIÊN KẾT UPI TẠI ẤN ĐỘ



Dưới sự hợp tác cùng Ngân hàng Axis, Google đã cho ra mắt dòng thẻ tín dụng kỹ thuật số đồng thương hiệu Flex by Google Pay có tích hợp công nghệ UPI (hệ thống thanh toán đồng nhất), dựa trên mạng lưới RuPay tại Ấn Độ.

Người dân Ấn Độ có thể đăng ký thẻ ảo trực tiếp trong ứng dụng Google Pay chỉ trong vài phút. Sau đó, người dùng có thể sử dụng thẻ để quét và thanh toán tại hàng triệu cửa hàng bán lẻ cũng như trực tuyến.

Hiện tại, Google Pay đã trở nên cực phổ biến với người dân Ấn Độ, chiếm hơn 32% trên tổng số lượng các thanh toán UPI, chỉ đứng sau PhonePe thuộc sở hữu của Walmart.

(Finextra)

VISA XÂY DỰNG HỆ SINH THÁI THANH TOÁN HIỆN ĐẠI TẠI SYRIA

Sau hơn thập kỷ bất ổn chính trị, Visa sẽ bắt đầu hợp tác chính thức với Ngân hàng Trung ương Syria để giúp thiết lập một hệ thống thanh toán hiện đại hóa dành cho người dân tại đây.

Visa cho biết những nỗ lực ban đầu của họ sẽ bao gồm mở rộng hợp tác với các tổ chức tài chính được cấp phép để phát triển nền tảng thanh toán an toàn. Điều này bao gồm việc giới thiệu thẻ thanh toán với các tiêu chuẩn cao cấp toàn cầu như chip EMV, xây dựng hệ thống thanh toán ví điện tử và hỗ trợ mã hóa token.

Đối với các nhà bán lẻ, Visa sẽ hỗ trợ kích hoạt các phương thức chấp nhận thanh toán hiện đại như thanh toán một chạm và quét mã QR. Mục tiêu là phát triển một mạng lưới thanh toán dễ tiếp cận thông qua Nền tảng Chấp nhận thanh toán Visa,

duy trì chi phí thấp và phù hợp với lượng lớn các doanh nghiệp siêu nhỏ, nhỏ và vừa tại Syria.

Visa cũng có kế hoạch hỗ trợ các chương trình cụ thể dành cho các doanh nhân địa phương đang nỗ lực xây dựng và mở rộng các quy trình thanh toán mới.

(PaymentJournal)

FBI CẢNH BÁO CÔNG CHÚNG VỀ CHIÊU TRÒ MẠO DANH NHÂN VIÊN NGÂN HÀNG

Trung Tâm Khiếu Nại Tội Phạm Internet (IC3) thuộc Cục Điều tra Liên bang Mỹ (FBI) đã đưa ra cảnh báo về việc tội phạm mạng giả danh các tổ chức tài chính để đánh cắp tiền hoặc thông tin từ cá nhân, doanh nghiệp và các tổ chức.

IC3 đã tiếp nhận hơn 5.100 báo cáo về gian lận chiếm đoạt tài khoản (Account Takeover - ATO) kể từ tháng 1/2025. Các báo cáo này ghi nhận tổng thiệt hại hơn 262 triệu USD.

Trong loại hình gian lận kể trên, tội phạm mạng mạo danh nhân viên hỗ trợ hoặc website của một tổ chức tài chính để lừa nạn nhân cung cấp thông tin. Từ đó, chúng có thể truy cập và chiếm quyền kiểm soát tài khoản ngân hàng, tài khoản trả lương hoặc tài khoản y tế trực tuyến.

Trong một số trường hợp, gian lận ATO bắt đầu bằng thủ đoạn tấn công phi kỹ thuật (social engineering). Ví dụ, đối tượng tội phạm lừa chủ tài khoản cung cấp thông tin đăng nhập bằng cách giả danh nhân viên của tổ chức tài chính, nhân viên hỗ trợ khách hàng hoặc kỹ thuật; sử dụng tin nhắn, cuộc gọi hoặc email với nội dung giả mạo rằng tài khoản đang phát sinh giao dịch gian lận và hướng nạn nhân đến một trang web lừa đảo (phishing) để "ngăn chặn thêm rủi ro"; hoặc chuyển nạn nhân sang một kẻ gian khác đang giả danh cơ quan thực thi pháp luật.

Trong các trường hợp khác, gian lận ATO được thực hiện qua các trang phishing. Kẻ gian có thể tạo ra một trang web có giao diện giống với trang mạng của tổ chức hợp pháp và lừa chủ tài khoản nhập thông tin đăng nhập. Một số nhóm còn mua quảng cáo trên công cụ tìm kiếm, giả dạng quảng cáo của doanh nghiệp uy tín để dẫn dắt nạn nhân đến trang web giả mạo.

Khi đã có thông tin đăng nhập, các đối tượng tội phạm thường ngay lập tức khóa quyền truy cập của chủ tài khoản và chuyển tiền đến các tài khoản do chúng kiểm soát.

Báo cáo PYMNTS Intelligence ghi nhận mức bình quân gần 4 trong 10 hộ gia đình tại Mỹ từng là nạn nhân của lừa đảo trong 5 năm qua. Báo cáo cũng cho thấy trong 81% trường hợp, kẻ gian thường mạo danh người có thẩm quyền, người lạ thân thiện hoặc người quen để tạo lòng tin và thực hiện hành vi lừa đảo.

(PYMNTS)

TRUY TỐ 54 NGƯỜI TRONG VỤ TẤN CÔNG RÚT TIỀN ATM Ở NEBRASKA

Bồi thẩm đoàn ở Nebraska đã truy tố 54 người vì cáo buộc tham gia vào một vụ tấn công rút tiền hàng loạt tại ATM.

Theo báo chí địa phương đưa tin, các cáo buộc cho rằng một số bị cáo này đã âm mưu thực hiện hành vi gian lận ngân hàng, trộm cắp ngân hàng và cung cấp hỗ trợ vật liệu cháy nổ nguy hiểm.

Trong đó, một bị cáo đã bị cáo buộc đánh cắp hàng triệu USD và chuyển giao tiền cho nhiều đồng phạm hòng che giấu thông tin vụ tấn công này. Nếu bị kết tội, các bị cáo có thể phải đối mặt với mức án từ 20 đến 335 năm tù.

Bản cáo trạng đã nêu rõ các bị cáo đã thực hiện hành vi tấn công mở trái phép máy ATM để tiến hành xâm nhập máy móc bên trong. Sau đó, họ sẽ cài đặt phần mềm độc hại để thực hiện hành vi tước quyền điều khiển ATM và cho rút tiền hàng loạt trái phép.

(ATMmarketplace)

TENCENT HỢP TÁC CÙNG MASTERCARD THÚC ĐẨY THANH TOÁN SINH TRẮC HỌC XUYÊN QUỐC GIA

Dịch vụ Click to Pay của Mastercard, dựa trên xác thực sinh trắc học và mã hóa giao dịch, sẽ được tích hợp vào hệ thống thanh toán xuyên biên giới MIDAS của Tencent, được sử dụng cho toàn bộ danh mục dịch vụ giải trí trực tuyến của doanh nghiệp.

Tencent dự định sử dụng công nghệ này cho hệ sinh thái MIDAS (Dịch vụ thu hút khách hàng quốc tế di động), phục vụ các doanh nghiệp giải trí kỹ thuật số và người dùng của họ.

Gã khổng lồ công nghệ Trung Quốc cũng cho biết thêm rằng dịch vụ thanh toán quốc tế này sẽ được hàng chục triệu người chơi sử dụng để thanh toán cho các trò chơi do 30 công ty game khác nhau sản xuất.

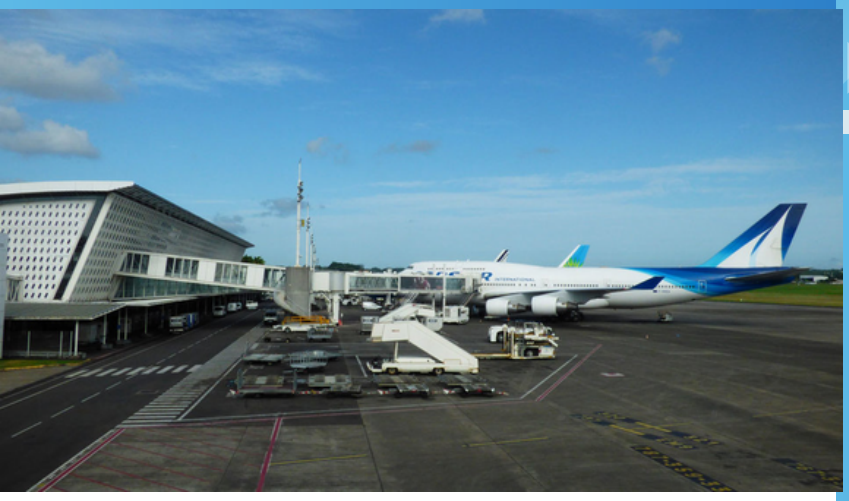
Click to Pay được thiết kế để đơn giản hóa việc mua sắm trực tuyến bằng cách cho phép khách hàng bỏ qua các bước nhập thông tin thanh toán thủ công. Thay vào đó, Mastercard sử dụng công nghệ mã hóa token, thay thế mật khẩu và số thẻ bằng các số tự thay đổi ngẫu nhiên, hay còn gọi là token, cho mỗi giao dịch, cũng như kết hợp xác minh sinh trắc học trên các thiết bị di động.

Mastercard tiết lộ họ đang đặt mục tiêu thay thế hoàn toàn việc nhập thông tin thanh toán thủ công bằng sinh trắc học và mã hóa token cho các giao dịch mua sắm trực tuyến trong vài năm tới.

Người mua sắm trực tuyến có thể chọn thanh toán bằng Click to Pay của Mastercard hoặc thẻ được lưu trữ trong hệ thống của người bán, sau đó xác nhận thanh toán bằng xác thực sinh trắc học thông qua dấu vân tay hoặc quét khuôn mặt trên thiết bị.

(BiometricUpdate)

MK group
Smart Digital Security



SÂN BAY GUADELOUPE TRIỂN KHAI CỔNG SINH TRẮC HỌC TỰ ĐỘNG

Hành khách đi qua Sân bay Guadeloupe - Maryse Condé sẽ được trải nghiệm thế hệ cổng điện tử tự động kết hợp sinh trắc học mới, được thiết kế để giúp quá trình làm thủ tục tại sân bay nhanh hơn và an toàn hơn.

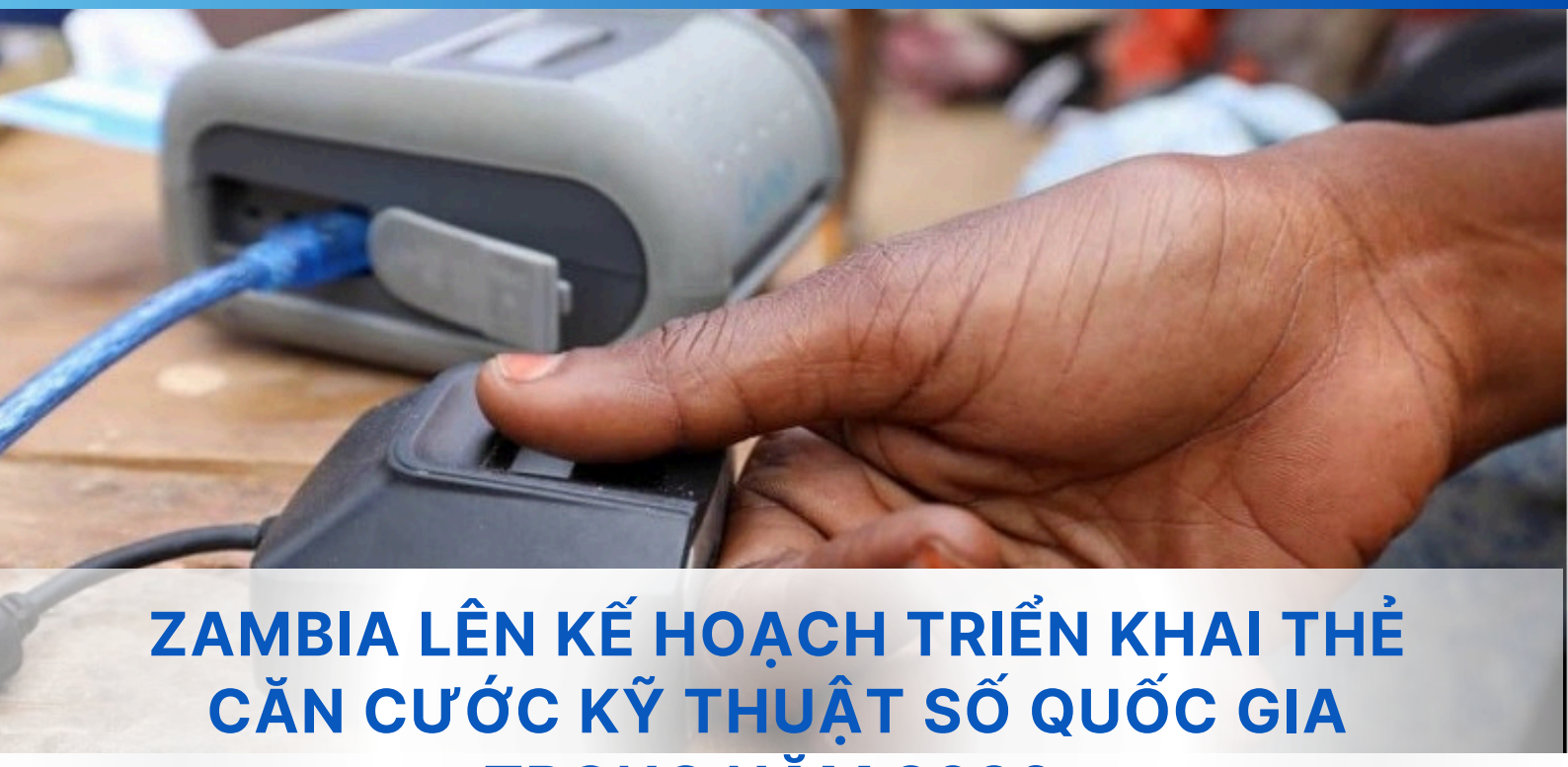
Hệ thống cổng điện tử mới cho phép hành khách tiếp cận khu vực an ninh và cổng lên máy bay thông qua xác thực tự động, tự phục vụ. Bằng cách sử dụng xác minh thời gian thực, hệ thống mới này sẽ giúp giảm thời gian xếp hàng và thời gian chờ đợi của hành khách.

Giải pháp hỗ trợ cả nhận dạng sinh trắc học và mã vạch, cho phép xác minh hành khách liền mạch trong khi vẫn duy trì các tiêu chuẩn an ninh cao. Ngoài ra, các đội ngũ vận hành sân bay có quyền truy cập vào giám sát và phân tích thời gian thực, cung cấp khả năng hiển thị tốt hơn về lưu lượng hành khách và hiệu suất hoạt động.

Các cơ quan quản lý cho biết hệ thống đã được thiết kế để đảm bảo tuân thủ đầy đủ các quy định về an ninh và bảo vệ dữ liệu, củng cố niềm tin và độ tin cậy cùng với việc tăng hiệu quả.

Việc đưa vào sử dụng các cổng điện tử này nhấn mạnh cam kết của Sân bay Guadeloupe trong việc nâng cao trải nghiệm của hành khách thông qua đổi mới công nghệ nhằm đáp ứng tiêu chuẩn an toàn tiện lợi và nhu cầu du lịch ngày càng tăng.

(Identity Week)



ZAMBIA LÊN KẾ HOẠCH TRIỂN KHAI THẺ CĂN CƯỚC KỸ THUẬT SỐ QUỐC GIA TRONG NĂM 2026

Chính quyền Zambia đang lên kế hoạch để đảm bảo rằng người dân quốc gia này sẽ được nhận thẻ căn cước kỹ thuật số quốc gia vào cuối năm 2026.

Việc triển khai thẻ căn cước kỹ thuật số sẽ là một cột mốc quan trọng trong việc thực hiện Dự án Tăng tốc Số hóa Zambia (DZAP).

Quá trình chuyển đổi số của Zambia theo DZAP là một phần của giai đoạn thứ hai của Chương trình Số hóa Toàn diện ở Đông và Nam Phi (IDEA), được Ngân hàng Thế giới phê duyệt vào tháng 6 năm 2024.

(BiometricUpdate)

GOOGLE: NĂM 2026, TỘI PHẠM MẠNG TĂNG TỐC NHỜ AI

Các nhà lãnh đạo an ninh đang đứng trước một năm với nhiều biến động lớn. Trong báo cáo "Dự báo An ninh mạng năm 2026", Google đã phác họa bức tranh về bối cảnh hiểm họa thay đổi hoàn toàn dưới sự tác động của Trí tuệ nhân tạo (AI), khi các nhóm tội phạm mạng được tiếp thêm năng lượng và các chiến dịch tấn công mang yếu tố quốc gia-nhà nước ngày càng trở nên hung hăng. Các đối tượng tấn công sẽ hành động nhanh hơn, đồng thời mở rộng quy mô hoạt động bằng cách tự động hóa mọi việc.

Bước sang năm 2026, AI sẽ là một phần bình thường trong các hoạt động tấn công và phòng thủ hàng ngày. Kẻ xấu đã và đang sử dụng công nghệ này để tự động hóa các hành vi lừa đảo, nhân bản giọng nói và định hình thông tin sai lệch. Một trong những mối đe dọa phát triển nhanh nhất là Tấn công chèn lệnh (Prompt Injection). Đây là cách thao túng hệ thống AI để chúng bỏ qua các lớp bảo vệ và thực thi các lệnh ẩn. Khi ngày càng nhiều công ty triển khai Mô hình ngôn ngữ lớn (LLM) vào các quy trình kinh doanh, những cuộc tấn công này lại càng dễ thực hiện và khó bị phát hiện hơn.

AI cũng đang làm thay đổi thủ đoạn tấn công phi kỹ thuật (social engineering). Các nhóm tội phạm như ShinyHunters đã sử dụng giọng nói giả mạo và các kịch bản lừa đảo cực kỳ chân thực để dụ dỗ nạn nhân, thay vì cố gắng qua mặt công nghệ. Thủ đoạn nhân bản giọng nói giờ đây có chi phí thấp và đủ sức thuyết phục để giả mạo giám đốc điều hành hoặc nhân viên CNTT trong những cuộc gọi lừa đảo qua điện thoại (vishing).

Báo cáo cũng lưu ý về sự phụ thuộc ngày càng nhiều vào "Tác nhân AI" (AI Agent) - tức là các hệ thống tự động hành động để hoàn thành nhiệm vụ. Những tác nhân này sẽ cần có danh tính số riêng biệt và cơ chế kiểm soát truy cập nghiêm ngặt. Các chương trình bảo mật, vốn được xây dựng cho người dùng là con người, sẽ không còn đủ sức bảo vệ. Quản lý danh tính sẽ phải tính đến khả năng ra quyết định dựa trên AI và các đặc quyền tạm thời dựa trên từng nhiệm vụ cụ thể.

Mặt khác, AI cũng đang định hình lại các hoạt động bảo mật. Thay vì tự mình rà soát thủ công các cảnh báo, đội ngũ chuyên gia phân tích sẽ sớm chỉ đạo các công cụ AI thực hiện công việc đó. Thay vì xem xét các tệp nhật ký, họ sẽ xem xét các bản tóm tắt vụ việc và xác nhận những bước ngăn chặn đã được tự động thực hiện. Sự thay đổi này cho phép phản ứng nhanh hơn, song cũng đặt ra những thách thức giám sát mới.

Ông Billy Leonard - Trưởng nhóm công nghệ của Google Threat Intelligence Group - phân tích: "Trong khi kẻ xấu chắc chắn đang cố gắng sử dụng các nền tảng AI chính thống, các rào cản bảo vệ đã hướng nhiều đối tượng tấn công tìm đến những mô hình sẵn có trong thế giới ngầm tội phạm. Những công cụ này không bị hạn chế và có thể mang lại lợi thế đáng kể cho những kẻ yếu kém

hơn về mặt công nghệ. Hiện có một số công cụ như vậy, và chúng tôi dự báo chúng sẽ kéo thấp rào cản gia nhập đối với nhiều đối tượng tội phạm".

Một mối lo ngại khác là sự trỗi dậy của "Tác nhân bóng tối" (Shadow Agent). Đội ngũ nhân viên có thể sử dụng các công cụ AI không được phê duyệt để xử lý công việc, và thường không nhận ra những rủi ro về dữ liệu. Quy định cấm tuyệt đối các công cụ này sẽ chỉ đẩy vấn đề vào hoạt động ngầm. Báo cáo khuyến nghị các tổ chức nên thiết lập mạng lưới rào cản bảo vệ, giám sát và quản trị đối với cách thức sử dụng các hệ thống AI trong nội bộ.

Tội phạm mạng tiếp tục bành trướng

Mã độc tống tiền (Ransomware) và đánh cắp dữ liệu vẫn là những mối đe dọa gây hỗn loạn nhất trên toàn thế giới. Các cuộc tấn công kết hợp - vừa mã hóa hệ thống, vừa đánh cắp dữ liệu và gây áp lực lên nạn nhân thông qua hành vi công khai các vụ rò rỉ - tiếp tục lan rộng.

Trong Quý I/2025, hơn 2.300 nạn nhân đã được công bố tên trên các trang rò rỉ, và đây là con số cao nhất kể từ khi công việc theo dõi bắt đầu vào năm 2020. Các đối tượng tấn công đang khai thác các chuỗi cung ứng phần mềm và các lỗ hổng zero-day để cùng lúc tiếp cận hàng trăm mục tiêu.

Tấn công phi kỹ thuật vẫn là điểm đột nhập phổ biến. Lừa đảo qua điện thoại và các tin nhắn được thiết kế riêng vẫn vượt qua được cơ chế Xác thực Đa yếu tố (MFA) và những biện pháp phòng thủ khác. Các kế hoạch tống tiền đang phát triển vượt ra ngoài phạm vi dữ liệu bị đánh cắp, trong đó có những mối đe dọa ngừng hoạt động hoặc công khai hồ sơ về các giám đốc điều hành.

Khi ngày càng nhiều hoạt động tài chính chuyển sang nền tảng blockchain, kẻ gian sẽ lợi dụng chính các hệ thống này để che giấu tung tích và tẩu tán tài sản phi pháp. Tình trạng này buộc các nhà điều tra hiện nay phải có khả năng đọc hiểu hợp đồng thông minh, truy vết ví điện tử và liên kết các giao dịch trên sổ cái công khai. Tính minh bạch của Blockchain là con dao hai lưỡi: một mặt nó giúp tội phạm né tránh các chiến dịch truy quét, mặt khác cũng để lại hồ sơ vĩnh viễn có thể được dùng làm bằng chứng truy tố sau này.

Với các biện pháp phòng vệ ở điểm cuối ngày càng mạnh mẽ, kẻ xấu đang chuyển hướng sang các nền tảng ảo hóa. Bằng cách nhắm mục tiêu vào chương trình giám sát máy ảo (hypervisor) - nơi lưu trữ máy ảo, đối tượng tấn công có thể vô hiệu hóa hàng trăm tác vụ chỉ trong vài giờ. Vì vậy, báo cáo khuyến nghị các doanh nghiệp trực tiếp đầu tư cho nhiệm vụ bảo vệ cơ sở hạ tầng này, chứ không chỉ các ứng dụng đang chạy trên đó.

Môi trường công nghiệp cũng vẫn là những mục tiêu lớn. Tội phạm sẽ tấn công phần mềm doanh nghiệp hỗ trợ công nghệ vận hành, gây áp lực buộc phải trả tiền chuộc nhanh chóng khi sản xuất bị ngưng trệ.

Các hoạt động mang yếu tố quốc gia-nhà nước ngày càng mở rộng

Các chiến dịch trên không gian mạng liên quan đến chính phủ các nước được dự đoán sẽ tiếp tục hoành hành trong năm 2026, mỗi chiến dịch đều được thúc đẩy bởi những mục tiêu riêng. Dự báo, Nga sẽ chuyển từ các hoạt động thời chiến ngắn hạn ở Ukraine sang những mục tiêu toàn cầu mang tính dài hạn hơn. Các chiến dịch thông tin và các nhóm tin tặc hành động (hacktivist) sẽ tiếp tục tập trung vào châu Âu và Bắc Mỹ, bao gồm can thiệp bầu cử và phá hoại cơ sở hạ tầng.

Trung Quốc có khả năng vẫn là tác nhân nhà nước hoạt động tích cực nhất. Các chiến dịch của Bắc Kinh tập trung vào lĩnh vực gián điệp và những hành động lén lút, nhắm mục tiêu vào các nhà cung cấp dịch vụ bên thứ ba và thiết bị biên (edge device) thường thiếu sự giám sát. Ngành công nghiệp bán dẫn là trọng tâm chính khi sự cạnh tranh về công nghệ AI ngày càng gay gắt.

Iran sẽ tiếp tục kết hợp các hoạt động gián điệp, phá hoại và gây ảnh hưởng gắn liền với những cuộc xung đột khu vực. Dự báo, các trang tuyên truyền và tin tức giả mạo sẽ sử dụng nội dung do AI tạo ra để khuếch trương các thông điệp ủng hộ Tehran. Triều Tiên sẽ vẫn tập trung đánh cắp tiền điện tử và thu thập tin tức tình báo. Năm 2025, các nhóm tin tặc Triều Tiên đã dính líu đến vụ trộm khoảng 1,5 tỷ USD, và các hoạt động đó dự kiến sẽ tiếp diễn. Một số nhân viên CNTT Triều Tiên đang nhận công việc từ xa ở nước ngoài để tìm cách giành quyền truy cập các hệ thống doanh nghiệp và ví điện tử./

(Help Net Security)

MK® group

Smart Digital Security

ĐỐI TÁC TIN CẬY TRONG CÁC LĨNH VỰC THẺ THÔNG MINH, TÀI LIỆU BẢO AN, XÁC THỰC BẢO MẬT, CAMERA AI & CÔNG NGHIỆP QUỐC PHÒNG

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.