Bản tin điện tử nội bộ - Số 93 | Tháng 9 - 2019

THẾ GIỚI THẺ

Tổng biên tập: *Bà Phan Thị Quỳnh Hoa - Giám đốc Tập đoàn MK* | **Ý kiến đóng góp vui lòng gửi về:** *marketing@mkgroup.com.vn*

Lưu ý: *Toàn bộ thông tin/hình ảnh trong Bản tin điện tử nội bộ Thế Giới Thẻ MK Group được sưu tầm từ các nguồn tin khác nhau và chỉ sử dụng cho mục đích chia sẻ kiến thức.*

Ông Lê Minh Quốc đại diện Tập đoàn MK nhận giải thưởng "Sản phẩm, Giải pháp công nghệ số tiêu biểu" trong Lễ trao giải thưởng chuyển đổi số Việt Nam 2019.

Các tin bài chính

Thiết bị U2F Token của MK Group được Vinh danh tại Giải thưởng Chuyển đổi số 2019

Chiều 6/9, tại Nhà hát lớn Hà Nội đã diễn ra Lễ trao giải thưởng Chuyển đổi số lần II năm 2019, nhằm tôn vinh các tổ chức, cá nhân có những thành tựu, đóng góp quan trọng cho sự phát triển công nghệ số, công cuộc chuyển đổi số và phát triển kinh tế số quốc gia. Giải thưởng này do Hội Truyền thông số Việt Nam (VDCA) tổ chức với Hội đồng Giải thưởng gồm những chuyên gia, nhà quản lý, nhà báo trong các lĩnh vực khoa học và công nghệ, thông tin và truyền thông, kinh tế.

Tại Lễ trao giải thưởng Chuyển đổi số năm 2019, thiết bị bảo mật U2F Token của MK Group, có tên là FIDO® KeyPass S1, đã trở thành 1 trong 50 sản phẩm công nghệ thông tin tiêu biểu của Việt Nam được vinh danh.

Để được đón nhận vinh dự này, thiết bị KeyPass U2F Token của MK Group đã phải vượt qua những tiêu chí đánh giá khắt khe về: tính năng/chức năng của sản phẩm, dịch vụ, giải pháp, công nghệ, bảo mật và chất lượng sản phẩm, dịch vụ; sự nổi trội của sản phẩm, dịch vụ so với các sản phẩm khác cùng loại trên thị trường; sản phẩm, dịch vụ mới, có tiềm năng ứng dụng; lực lượng nhân sự, mức đầu tư dành cho ICT; quy trình quản lý, điều hành, sản xuất, kinh doanh; đánh giá hiệu quả của quá trình chuyển đổi bằng doanh thu, thị phần cũng như năng lực uy tín của đơn vị, chủ doanh nghiệp…

FIDO® KeyPass S1 tự hào là thiết bị đầu tiên của Việt Nam đạt được chứng chỉ U2F (Universal Second Factor) của Liên minh xác thực FIDO (FIDO Alliance), cho phép người sử dụng mạng (Internet, LAN,…) có thể truy cập một cách an toàn vào các dịch vụ trực tuyến hỗ trợ tính năng FIDO U2F mà không cần sử dụng bất kỳ phần mềm nào khác.

Bằng cách sử dụng nhân tố xác thực thứ hai bên cạnh tên đăng nhập và mật khẩu, thiết bị giúp người dùng ngăn chặn và loại bỏ những hành vi đánh cắp dữ liệu thông qua các website giả mạo (phishing) và chiếm quyền sử dụng tài khoản (man-in-the-middle) với thao tác sử dụng hết sức đơn giản gồm kết nối thiết bị và bấm nút vật lý. FIDO® KeyPass S1 hoạt động tốt trên hầu hết các hệ điều hành và trình duyệt. Bên cạnh đó, với tính năng lưu khóa cho nhiều trang web và ứng dụng, người dùng chỉ cần một thiết bị để bảo vệ an toàn cho tài khoản của nhiều dịch vụ khác nhau, từ Internet banking cho đến đăng nhập máy tính, Gamil, Facebook, Dropbox…

Việc thiết bị U2F Token của FIDO® KeyPass S1 trở thành 1 trong 50 sản phẩm công nghệ thông tin tiêu biểu của Giải thưởng Chuyển đổi số năm 2019 đã giúp khẳng định vị thế Chuyên gia hàng đầu trong lĩnh vực xác thực bảo mật và thẻ thông minh của MK Group, đồng thời góp phần chứng mình cho những giải pháp xác thực bảo mật "Made in Vietnam" - có đủ năng lực cạnh tranh về Chất lượng và Giá thành với các công ty toàn cầu bằng những sản phẩm như KeyPass U2F Token.

Với định hướng Smart Digital Secuirty – Bảo mật Số Thông minh, hiện MK Group đang nỗ lực để hoàn thiện thêm những sản phẩm xác thực bảo mật chất lượng cao để cung cấp cho thị trường trong thời gian tới" ./.

TIN VẮN THẺ NGÂN HÀNG

- **Từ ngày từ 18/9 đến 30/9/2019, Ngân hàng TMCP Quốc Dân (NCB) triển khai chương trình ưu đãi nhân dịp 24 năm thành lập.** Theo đó, chủ thẻ thanh toán hóa đơn bằng tính năng QRPay trên ứng dụng NCB Smart sẽ được hoàn tiền 100% cho giao dịch chi tiêu lần đầu. Và Khách hàng mở mới thẻ tín dụng NCB Visa sẽ nhận được 1 phần quà nhỏ từ ngân hàng .

- **Từ ngày 17/9 đến 19/9/2019, nhân dịp sinh nhật, Ngân hàng Quốc tế (VIB)** triển khai ưu đãi với khách hàng khi mở mới gói tài khoản Saphire, thẻ tín dụng hay tham gia bảo hiểm tại tất cả các chi nhánh của Ngân hàng trên toàn quốc**.** Cụ thể, khách hàng đến chi nhánh VIB sẽ được tặng 200.000 đồng vào tài khoản khi mở mới gói Saphire với tài khoản thanh toán, e-banking và thẻ Thanh toán quốc tế (IDC).

- **Từ ngày 20/8 đến hết 10/10/2019, LienVietPostBank** triển khai chương trình hoàn tiền 50% đối với khách hàng mở thẻ tín dụng MasterCard Theo đó, khách hàng được hoàn tiền 50% (tối đa 500.000 đồng) khi đăng ký phát hành mới, kích hoạt thẻ và có chi tiêu trong trong thời gian khuyến mại./.

(Tổng hợp từ Internet)

Tiền mặt vẫn còn tương lai trên đất Mỹ

Tại Mỹ, tiền mặt vẫn là phương thức thanh toán phổ biến nhất trong các giao dịch như mua một ly cà phê, một gói kẹo cao su hay một cốc bia. Tại sao vậy? Bởi vì tiền mặt là phương thức thanh toán nhanh hơn và thường thuận tiện hơn, đặc biệt là trong các giao dịch có giá trị thấp.

Kết quả điều tra dư luận mới được CreditCards.com thực hiện trong tháng 7/2019 cho thấy, trong số hơn 2.500 người trưởng thành ở Mỹ, có tới gần 50% thích sử dụng tiền mặt trong các giao dịch mua hàng dưới 10 USD. Trong khi đó, “Thế hệ Millennials” (23-38 tuổi) có xu hướng ưa thích sử dụng phương thức thanh toán di động (m-payment) và thẻ không tiếp xúc.

Ngay cả đối với các chủ thẻ tín dụng tích lũy điểm thưởng, 43% trong số này nói rằng tiền mặt vẫn là phương thức thanh toán chính của họ, trong khi 31% ủng hộ thẻ ghi nợ và chỉ 26% ưa thích thẻ tín dụng.

Nguyên nhân chính khiến các chủ thẻ tín dụng tích lũy điểm thưởng ưa chuộng thanh toán bằng tiền mặt hoặc thẻ ghi nợ hơn là do chúng nhanh hơn và dễ dàng hơn. Những lý do khác khiến người Mỹ sử dụng tiền mặt hoặc thẻ ghi nợ trong các giao dịch mua hàng có giá trị thấp là: lo ngại về nợ thẻ tín dụng, các cửa hàng có hạn mức thẻ tín dụng tối thiểu hoặc phải trả phí cho các giao dịch có giá trị thấp.

Trong số các chủ thẻ tích lũy điểm thưởng, Thế hệ Millennials có tỷ lệ sử dụng thẻ tín dụng cao nhất trong các giao dịch mua hàng có giá trị thấp. Con số này giảm xuống còn 24% trong thế hệ “Xers” (39-54 tuổi) và 22% trong thế hệ “Baby Boomers” (55-73 tuổi). Theo nghiên cứu, những người có thu nhập và trình độ học vấn cao thường sử dụng thẻ tín dụng với tần suất cao hơn.

Mặc dù hạn chế lớn nhất trong hoạt động sử dụng thẻ tín dụng cho các giao dịch có giá trị thấp là tốc độ, song chỉ có 39% chủ thẻ tín dụng tích lũy điểm thưởng sử dụng dịch vụ m-payment và 14% sử dụng thẻ không tiếp xúc. Tuy nhiên, những người đã sử dụng một trong 2 phương thức thanh toán trên sẽ ít có khả năng thanh toán bằng tiền mặt hơn (38%) so với những người chưa từng sử dụng (46%).

Ông Ted Rossman, chuyên gia phân tích tại CreditCards.com nhận xét: “M-payment và thẻ không tiếp xúc là những phương thức tuyệt vời để tăng tốc quá trình thanh toán mà không phải hy sinh tính bảo mật. M-payment thậm chí còn an toàn hơn thẻ tín dụng gắn chip vì chúng thường yêu cầu xác thực sinh trắc, chẳng hạn như quét vân tay, khuôn mặt hoặc mống mắt."

Mặc dù m-payment và thẻ không tiếp xúc vẫn phổ biến ở nước ngoài và tiếp tục giành được động lực tăng trưởng ở Mỹ, nhưng có đến hơn một nửa số chủ thẻ tích lũy điểm thưởng ở “Xứ cờ hoa” cho biết họ không có thẻ không tiếp xúc và 22% không chắc chắn.

Một số phát hiện khác trong nghiên cứu:

• Chủ thẻ tín dụng tích lũy điểm thưởng là nam giới có tỷ lệ sử dụng loại thẻ này nhiều gấp đôi so với chủ thẻ nữ giới (20% so với 9%).
• 44 % chủ thẻ tín dụng tích lũy điểm thưởng là nam giới đã sử dụng m-payment, trong khi đó tỷ lệ này ở chủ thẻ nữ giới chỉ là 34%.
• Một phần tư Thế hệ Millennials sở hữu thẻ tín dụng tích lũy điểm thưởng đã sử dụng dịch vụ thanh toán không tiếp xúc, trong khi đó tỷ lệ này ở Thế hệ Xers là 15% và 8% ở thế hệ Baby Boomers.
• 61% Thế hệ Millennials sở hữu thẻ tín dụng tích lũy điểm thưởng đã sử dụng m-payment. Tỷ lệ này nhiều hơn so với Xers (44%) và Baby Boomers (24%)./.

(PYMNTS)

EMVCo công bố các thay đổi thông số kỹ thuật xác thực nhà phát hành thẻ

Tổ chức tiêu chuẩn thẻ thanh toán EMVCo mới đây đã công bố các thay đổi thông số kỹ thuật đề xuất dành cho các hệ thống thanh toán để phù hợp với số ký tự dài hơn trên thẻ tín dụng và ghi nợ phục vụ việc nhận dạng nhà phát hành thẻ.

Số nhận dạng nhà phát hành (IIN) là phần đầu tiên của số tài khoản chính (PAN) gồm từ 10 đến 19 chữ số ở mặt trước của thẻ ghi nợ hoặc thẻ tín dụng nhằm xác định nhà phát hành thẻ. Hiện tại, IIN bao gồm 6 chữ số đầu tiên của PAN nhưng sẽ được chuyển sang 8 chữ số vào năm 2021.

Thông cáo báo chí của EMVCo cho biết, do những thay đổi sắp tới, các đơn vị chấp nhận thẻ cần phải cập nhật các đầu đọc thẻ để có thể xử lý những IIN dài hơn nhằm ngăn chặn tình trạng giao dịch bị hủy bỏ hoặc xử lý không chính xác.

Sự thay đổi này bắt nguồn từ Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) và Ủy ban Kỹ thuật điện Quốc tế (IEC) bởi 2 cơ quan này năm 2017 đã phát hành phiên bản mới của ISO / IEC 7812-1 - tiêu chuẩn quy định hệ thống đánh số để nhận dạng các tổ chức phát hành thẻ - nhằm đáp ứng số lượng ngày càng tăng của các tổ chức phát hành thẻ./.

(ATM Marketplace)

Vụ rò rỉ dữ liệu của MasterCard tại Đức ảnh hưởng tới 90.000 khách hàng

Vụ vi phạm đầu tiên, bị phát hiện vào hôm 19/8, đã làm rò rỉ khoảng 90.000 bộ dữ liệu về địa chỉ và số thẻ tín dụng của khách hàng, theo báo cáo từ Cơ quan bảo vệ dữ liệu Bỉ (BDPA).

MasterCard thông báo rằng, sự cố này "không liên quan tới toàn bộ mạng lưới thanh toán của MasterCard… đã xảy ra sự cố liên quan đến nền tảng khách hàng thân thiết đặc biệt ở Đức do một nhà cung cấp bên thứ ba quản lý, dẫn đến hành vi phát tán trái phép một số thông tin nhất định".

Tuyên bố của Chủ tịch BDPA David Stevens nhấn mạnh: "Chúng tôi đã nhận được rất nhiều câu hỏi và khiếu nại về sự cố này. Chúng tôi muốn cam kết lại một lần nữa với những người sử dụng rằng: chúng tôi đã liên hệ với MasterCard để có thêm thông tin, đang cùng với cơ quan bảo vệ dữ liệu Hessian và tất cả các cơ quan hữu quan khác theo dõi vụ việc này một cách chặt chẽ".

Chương trình khách hàng thân thiết Priceless Specials được một nhà cung cấp dịch vụ bên thứ ba điều hành và đã ngừng hoạt động sau khi MasterCard nắm được thông tin về vụ vi phạm đầu tiên.

Người phát ngôn của MasterCard cho biết: "Chúng tôi rất coi trọng công tác bảo vệ dữ liệu và bảo mật. Do đó, chúng tôi sẽ nỗ lực hết sức để điều tra và giải quyết vấn đề liên quan đến nhà điều hành hệ thống Priceless Specials ở Đức"./.

(PYMNTS)

Người Mỹ thích dùng thẻ tín dụng mua hàng dưới 10$

Theo dữ liệu khảo sát mới từ CreditCards.com, 16% trong số những người trưởng thành tại Mỹ cho biết họ thường dùng thẻ tín dụng cho các khoản mua hàng dưới 10 USD.

Tỷ lệ được tăng từ 12% của năm 2018. Đối với những người sử dụng thẻ tín dụng có ưu đãi như tiền hối, tích điểm hay dặm thì tỷ lệ là 26%, tăng so với 23% của năm ngoái.

Đây là kết quả từ cuộc khảo sát trực tuyến được thực hiện vào tháng 7 năm 2019 với hơn 2.500 người trưởng thành sống tại Mỹ. Từ năm 2014 đến 2017, khi cuộc thăm dò hàng năm xác định mức mua hàng dưới 5 USD, tỷ lệ người tiêu dùng sử dụng thẻ tín dụng cho những giao dịch này cũng tăng lên 17%, từ 11%.

Khoảng một nửa số người tham gia khảo sát (49%) thích tiền mặt khi mua dưới 10 USD. Với những người sử dụng thẻ tín dụng có ưu đãi thì tỷ lệ này là 43%. Khoảng 1/3 của cả hai nhóm khách hàng này- tương ứng 35% và 31% - báo cáo rằng sử dụng thẻ ghi nợ của họ để chi trả cho các giao dịch mua nhỏ này./.

(Thepaypers)

Visa công bố bộ dịch vụ và tính năng bảo mật mới

Nguồn: Internet

Visa vừa công bố một gói dịch vụ và tính năng bảo mật mới nhằm phát hiện và ngăn chặn những mối đe dọa gian lận nhằm vào các ngân hàng và đơn vị bán hàng.

Trong số các công cụ miễn phí có Visa Vital Signs với khả năng chủ động giám sát các giao dịch và cảnh báo các tổ chức tài chính về những hoạt động gian lận tiềm ẩn, có thể dẫn đến những hành vi rút tiền bất hợp pháp, xảy ra tại các ATM hay điểm bán hàng.

Một đặc tính khác có thể ứng dụng khả năng học sâu tới khối lượng lớn các giao dịch không sử dụng thẻ của Visa để xác định tổ chức tài chính và đơn vị bán hàng mà hacker có thể lợi dụng nhằm dự đoán số tài khoản, ngày hết hạn và mã bảo mật thông qua kiểm tra tự động. Công nghệ máy học có khả năng phát hiện những kiểu lừa đảo tinh vi, loại bỏ các kết quả xác thực giả mạo và cảnh báo các tổ chức tài chính và đơn vị bán hàng bị ảnh hưởng trước khi bắt đầu xảy ra những giao dịch gian lận.

Phòng Nghiên cứu các mối đe dọa của Visa sẽ tạo môi trường để kiểm tra quá trình xử lý khách hàng, logic kinh doanh và cài đặt cấu hình để xác định các lỗi dẫn đến những lỗ hổng tiềm ẩn. Chẳng hạn, Visa có thể xác minh được liệu một tổ chức tài chính có xác thực hiệu quả mật mã dành cho các giao dịch chip EMV hay không.

Và cuối cùng, công cụ Visa eCommerce Threat Disruption chủ động quét toàn bộ nội dung dữ liệu của các trang web thương mại điện tử để phát hiện những phần mềm độc hại có khả năng đánh cắp các dữ liệu thanh toán./.

(Finextra)

Google vượt qua thời đại mật khẩu nhờ công nghệ sinh trắc học

Giữa hàng loạt tuyên bố và những tên tuổi lớn trong lĩnh vực công nghệ, Google và Microsoft đã có các động thái mạnh mẽ nhằm loại bỏ những câu hỏi bảo mật tĩnh kiểu như tên thời con gái của mẹ bạn hoặc trường tiểu học của bạn.

Google vừa thông báo rằng người dùng sử dụng điện thoại Pixel sẽ có thể đăng nhập vào một số dịch vụ của cỗ máy tìm kiếm khổng lồ này thông qua trình duyệt Chrome bằng thông tin sinh trắc, chẳng hạn như dấu vân tay. Google khẳng định: "Tính năng mới này đánh dấu bước chuyển biến khác trong hành trình của chúng tôi nhằm đơn giản hóa và nâng cao mức độ an toàn cho hoạt động xác thực người dùng".

Tùy chọn sinh trắc trên sử dụng tiêu chuẩn được gọi là FIDO 2.0 (hoặc FIDO2), giúp các công ty có thể bỏ qua mật khẩu xác thực bằng cách sử dụng công nghệ xác thực vân tay hoặc khuôn mặt. Về mặt cơ học, công nghệ này sử dụng khóa mã hóa với 2 loại khóa: một khóa riêng và một khóa công khai. Người dùng có thể gửi tin nhắn kèm khóa công khai của họ tới ai đó, và khi người này nhận được tin nhắn, anh ta có thể dùng khóa riêng của mình để giải mã tin nhắn này.

Thông báo của Google được đưa ra vài tuần sau khi Microsoft hồi tháng tháng 5 tuyên bố rằng Windows Hello, hệ thống xác thực sinh trắc không mật khẩu đã đạt được chứng chỉ FIDO2. Cả 2 tuyên bố này đều xuất hiện sau thông tin hồi tháng 4 cho rằng bất kỳ chiếc điện thoại nào chạy hệ điều hành Android 7+ đều có thể hoạt động như một khóa bảo mật FIDO2. Được biết, Android đã đạt được chứng chỉ FIDO2 vào tháng 2.

Nguồn: Internet

Với tính năng mới, người dùng có thể tự xác thực bản thân trong toàn bộ hệ thống các dịch vụ Pixel thông qua chức năng mở khóa màn hình. Google nói rằng, đây là lần đầu tiên mà các dịch vụ được bảo mật với FIDO2 có thể được dùng cho những người sử dụng web, mặc dù hoạt động này, như đã nói ở trên, cho đến nay vẫn bị giới hạn trong phạm vi "thúc đẩy" các hoạt động xác thực, và chưa phải là các thao tác đăng nhập ban đầu.

Trong một cuộc phỏng vấn với PYMNTS, ông Andrew Shikiar, GĐĐH kiêm Giám đốc Marketing của Liên minh FIDO, cho biết động thái này của Google đã mở ra một cuộc đối thoại về việc loại bỏ mật khẩu.

Theo ông Shikiar, "đây là làn sóng thứ 2 trong hoạt động chấp nhận FIDO" bởi công nghệ xác thực này trước đó đã có mặt trên thị trường. Lần triển khai xác thực FIDO đầu tiên diễn ra vào năm 2014, khi PayPal và Samsung cho phép khách hàng xác thực bằng vân tay trên mẫu smartphone Galaxy S5. Tuy vậy, thông tin từ Google và Microsoft trong vài tháng qua cho thấy những điều mà ông Shikiar gọi là "sự triển khai nền tảng hóa" FIDO trên quy mô lớn, theo đó FIDO2 sẽ trở thành cốt lõi trong hoạt động bảo mật và xác thực người dùng của 2 "người khổng lồ" công nghệ trên.

Ông Shikiar nhấn mạnh, cần phải hiểu rằng có thể vẫn còn những mối lo ngại trong công chúng về công nghệ sinh trắc, và về các dữ liệu được lưu trữ trên đám mây, song phương pháp FIDO được chứng nhận - đang được Google, Microsoft và các tổ chức khác trong số 250 thành viên của Hiệp hội FIDO sử dụng - đồng nghĩa với việc toàn bộ dữ liệu sinh trắc chỉ được lưu trữ trên thiết bị. Thí dụ, Google sẽ không bao giờ thấy được các vân tay, và dữ liệu cũng không bao giờ được lưu trữ ở một nơi tập trung./.

(PYMNTS)

Nguồn: Internet

Mã QR: Đột phá trong nỗ lực phổ cập tài chính

Mã QR mang lại thay đổi căn bản để chấp nhận thanh toán, đặc biệt là ở các nền kinh tế đang phát triển. Các quốc gia như Trung Quốc và Ấn Độ chấp nhận phương thức này như một công cụ với chi phí thấp để hướng tới phổ cập tài chính. Thay vì sử dụng thiết bị chấp nhận thanh toán thông thường, các đơn vị kinh doanh/người bán hàng và người tiêu dùng có thể giao dịch trên một chiếc điện thoại di động (ĐTDĐ) không mấy đắt tiền.

Một số ngân hàng trung ương đã hoan nghênh việc sử dụng mã QR, và Indonesia là quốc gia gần đây nhất chuẩn hóa hoạt động chấp nhận mã QR. Theo báo cáo của Thế giới Di động:

- Ngân hàng Trung ương Indonesia (Bank Indonesia) đã thông qua hệ thống mã QR tiêu chuẩn. Theo đó, các nhà cung cấp dịch vụ thanh toán di động (m-payment) đến cuối năm nay phải nâng cấp nền tảng để chấp nhận những giao thức mới.
- Tuyên bố của Bank Indonesia khẳng định, việc đưa ra một tiêu chuẩn quốc gia về m-payment sẽ nâng cao hiệu quả giao dịch và thúc đẩy những nỗ lực phổ cập tài chính ở nước này.
- Sau khi triển khai, hệ thống mã QR sẽ được dùng cho những giao dịch thông qua các nhà cung cấp dịch vụ m-payment, ví điện tử và ứng dụng ngân hàng di động.

Tại Mỹ, mã QR đã giành được sự ủng hộ từ một số đơn vị bán lẻ hàng đầu. Mã QR ít liên quan hơn khi các đơn vị phát hành thẻ tín dụng chuyển sang NFC không tiếp xúc, một công nghệ cạnh tranh khác, mặc dù một số đơn vị bán lẻ lớn đã tích hợp tính năng này vào ví di động hoặc hệ thống POS.

Số báo gần đây của của tạp chí thương mại Chain Store Age đã đề cập đến việc chuỗi cửa hàng tiện ích 7-Eleven sẽ liên kết mã QR với hệ thống khách hàng thân thiết tại Mỹ:

- Để sử dụng tính năng thanh toán trên thiết bị di động, khách hàng cập nhật hoặc tải phiên bản mới nhất của ứng dụng 7-Eleven, mở ứng dụng trong cửa hàng tham gia và chạm vào nút "Bắt đầu" trên trang chủ, quét mã vạch sản phẩm để thêm vào giỏ hàng, với tính năng tự động áp dụng mã giảm giá hoặc khuyến mãi, và thanh toán bằng Apple Pay,
- Một mã QR xuất hiện trong ứng dụng khi bắt đầu thanh toán,
- Khách hàng sau đó quét mã QR tại bước xác nhận để khẳng định việc mua hàng. Một âm báo sẽ cho nhân viên thu ngân biết khách hàng đã sử dụng tính năng m-payment để mua hàng.

Nhưng tất cả mọi thứ không dễ dàng như vậy. Các tổ chức thanh toán đều đặt ra câu hỏi liệu đây có phải là một thay đổi thiết yếu. Thay vì cách tiếp cận an toàn, có thể kiểm soát được như thực hiện với NFC, mã QR chuyển quyền kiểm soát ra ngoài tầm của các mạng thanh toán. Ấn Độ là một thí dụ hoàn hảo về cách thức mà Ngân hàng Bưu điện nước này có thể phá vỡ cấu trúc ngân hàng truyền thống bằng mã QR. Theo FinTech News Singapore, như một phần của chiến lược phổ cập, New Delhi đang triển khai "các dịch vụ tài chính tại chỗ" ở khu vực xa xôi nhất của Ấn Độ. Mã QR là một yếu tố chính của quá trình:

- Mô hình sáng tạo này do Ngân hàng Thanh toán Bưu điện Ấn Độ (IPPB), một công ty TNHH 100% sở hữu của chính phủ trực thuộc Bộ Bưu chính, triển khai và Thủ tướng Ấn Độ Narendra Modi nhấn nút khởi động.
- Trên cả nước, hơn 350.000 bưu tá đang cung cấp dịch vụ tài chính tại chỗ cho những người dân ở cả những vùng hẻo lánh nhất của Ấn Độ.
- Các bưu tá được trang bị ĐTDĐ và máy quét sinh trắc cầm tay để thực hiện các nhiệm vụ của nhân viên ngân hàng, bao gồm mở tài khoản tiết kiệm, chuyển tiền, thanh toán hóa đơn tiện ích, nạp tiền ĐTDĐ, chấp nhận gửi tiền mặt và tạo điều kiện rút tiền.
- Những bưu tá này đã được đào tạo và chứng nhận để cung cấp các dịch vụ ngân hàng cũng như nâng cao hiểu biết về tài chính ở khu vực nông thôn. Họ đang được nhận được những khuyến khích bằng tiền cho cả 2 loại giao dịch được hỗ trợ và tự phục vụ.

Nhưng ngành công nghiệp thanh toán nên cẩn trọng! Theo India Times, Ấn Độ cũng đang cố gắng loại bỏ tỷ lệ chiết khấu cho phía đơn vị kinh doanh (MDR) tại điểm bán. Nếu nỗ lực này được nhân rộng, ngành công nghiệp thẻ thanh toán có thể đã tạo ra một "con quái vật"./.

(PaymentsJournal)

Tương lai của thanh toán đã được tìm thấy trên Bán đảo Scandinavia

Khi thế giới tiếp tục chuyển dịch theo xu hướng giảm thiểu sử dụng tiền mặt, thói quen trả tiền của người tiêu dùng ở Bán đảo Scandinavia mang lại những gợi ý về cách thức thanh toán trong tương lai. Bán đảo Scandinavia, gồm Đan Mạch, Na Uy và Thụy Điển, đang chứng kiến sự bùng nổ của thanh toán di động (m-payment), sự tiếp tục thống trị của thanh toán thẻ, và xu hướng sụt giảm nhanh chóng của hoạt động sử dụng tiền mặt.

Thụy Điển dẫn đầu trong việc loại bỏ tiền mặt

Năm 1661, Thụy Điển trở thành quốc gia đầu tiên ở châu Âu ra mắt tiền giấy và cũng gần như là quốc gia đầu tiên ở cựu lục địa ngừng sử dụng tiền mặt. Thụy Điển là tâm điểm cho dấu chấm hết của tiền mặt, chỉ 1% tổng giá trị thanh toán ở đất nước Bắc Âu này trong năm 2016 được thực hiện bằng tiền mặt. Các doanh nghiệp và ngân hàng đang thích ứng với sở thích của người tiêu dùng và các đơn vị bán hàng. Hiện nay, xu hướng chung của các doanh nghiệp Thụy Điển là không chấp nhận tiền mặt.

Có rất nhiều lợi ích khi không dùng tiền mặt, bao gồm:

- Tiết kiệm thời gian: Nhân viên tại cửa hàng IKEA ở Gavle, Thụy Điển cho biết, họ phải dành 15% thời gian để xử lý, đếm và cất giữ tiền, mặc dù những người mua hàng đã sử dụng tiền mặt trong chưa tới 1% tổng số lượt giao dịch.
- Tiết kiệm doanh thu: Các doanh nghiệp chịu rủi ro và chi phí cao khi dùng tiền mặt. Báo cáo “Thành phố không tiền mặt” của Visa cho hay: “Các doanh nghiệp thiệt hại tương đương 4% doanh thu mỗi tháng do nạn trộm cắp, tiền giả và máy đếm tiền”.
- An toàn: An toàn hơn cho người lao động và doanh nghiệp khi các công ty không dùng tiền mặt. Ngoài ra, không dùng tiền mặt cũng an toàn hơn cho các ngân hàng. Các ngân hàng Thụy Điển đã chứng kiến sự sụt giảm tới 99% các vụ cướp trong giai đoạn 2008 - 2017.

Điểm mạnh của thanh toán thẻ

M-payment tăng trưởng mạnh mẽ cũng không làm giảm sự ưa thích của những người Scandinavia đối với thanh toán thẻ. Xét theo bình quân đầu người, Scandinavia có tần suất sử dụng thanh toán thẻ cao nhất trên toàn cầu, trong đó Na Uy dẫn đầu với mức bình quân 475 lượt thanh toán thẻ/người tiêu dùng/năm.

Các tổ chức thẻ đã xây dựng một cơ sở hạ tầng chấp nhận thẻ vô cùng đáng tin cậy, cho phép người dân Scandinavia sử dụng thẻ trong khu vực và ở nước ngoài. Hơn nữa, các tổ chức thẻ đang chuyển dịch ra khỏi giới hạn ngoài việc quẹt và nhúng thẻ để thanh toán không tiếp xúc.

Thanh toán không tiếp xúc (TTKTX)

TTKTX cho phép người tiêu dùng thực hiện giao dịch thanh toán bằng cách chạm thẻ hoặc thiết bị vào đầu đọc thẻ. TTKTX an toàn, thuận tiện và cho phép người tiêu dùng nhanh chóng hoàn thành giao dịch. Mặc dù đang ở giai đoạn sơ khai, nhưng khi nhiều đơn vị chấp nhận thẻ áp dụng phương thức thanh toán này và người tiêu dùng tìm hiểu thêm, hoạt động sử dụng TTKTX sẽ tăng lên theo cấp số nhân.

TTKTX sẽ lý tưởng nhất trong các giao dịch thanh toán có giá trị thấp với yêu cầu thực hiện nhanh, trong đó có thẻ giao thông. Các đơn vị bán hàng sẽ ứng dụng công nghệ thanh toán này ở quy mô rộng hơn vì tỷ lệ chấp nhận cao hơn 10% so với quẹt dải từ truyền thống.

TTKTX không phải là lựa chọn duy nhất ở Scandinavia, nhưng người dân trong khu vực có thể sẽ nhanh chóng tận dụng phương thức thanh toán này. Năm 2018, người Na Uy sử dụng TTKTX trong 4,5% tổng lượng giao dịch tại các thiết bị đầu cuối vật lý; tuy vậy, tỷ lệ này có thể sẽ mở rộng đến hơn 50% trong 3 năm.

Sự bùng nổ của m-payment

Trên toàn Bán đảo Scandinavia, 3 tổ chức nội địa phổ biến đang dẫn đầu xu hướng tăng trưởng m-payment là Vipps ở Na Uy, Swish ở Thụy Điển, và Mobile Pay ở Đan Mạch. Chỉ tính riêng trong năm 2018, người dùng Vipps tại Na Uy đã thực hiện 141 triệu lượt giao dịch m-payment với giá trị 67 tỷ Kroner, tương đương với mức tăng trưởng 55% hàng năm. Các tổ chức m-payment của Scandinavia đang trải qua hiệu ứng mạng lưới, trong đó sự gia tăng số lượng người dùng làm tăng giá trị của tổ chức. Tỷ lệ thâm nhập thị trường của Vipps ở mức 75%, Mobile Pay ở mức 90% và Swish ở mức 69%.

Chính sách của các chính phủ

Người Scandinavi đã chấp nhận thanh toán điện tử một cách tự nhiên, song xét trên phương diện hành pháp, lực lượng dẫn dắt mạnh mẽ nhất tới một xã hội không tiền mặt lại là chính sách của chính phủ. Các doanh nghiệp sử dụng nhiều tiền mặt gây ra nguy cơ trốn thuế và rửa tiền cao hơn. Nhiều chính phủ đã ban hành các yêu cầu hạn chế tiền mặt để đẩy lùi nguy cơ do những hoạt động bất hợp pháp gây ra. Chính sách này đã thúc đẩy nhiều người tiêu dùng chấp nhận các phương thức thanh toán điện tử.

Xu hướng thanh toán ở Scandinavia sẽ không được sao chép một cách máy móc trên toàn thế giới. Sẽ có những sắc thái khác, trong đó có một số động lực hành pháp hướng tới việc áp dụng các phương thức thanh toán thay thế. Tuy nhiên, quy tắc chung là chúng ta đang hướng tới một xã hội không tiền mặt./.

(PaymentsJournal)

5 mối đe dọa nghiêm trọng nhất về bảo mật thanh toán di động

Thanh toán di động (m-payment) liệu có an toàn ? Câu hỏi này thường nảy ra trong tâm trí mọi người khi các dịch vụ mua sắm trực tuyến và m-payment xuất hiện trên thị trường. Sự linh hoạt và tiện lợi khiến cho m-payment trở nên thời thượng hơn đối với những người dùng di động.

Hiện có khoảng 55 triệu người đang sử dụng các tùy chọn m-payment ở Mỹ, tương đương 20,2% dân số của nền kinh tế lớn nhất thế giới. M-payment, đang nhanh achóng thay thế các tùy chọn thanh toán lỗi thời, cho phép khách hàng thực hiện thanh toán hoặc hoàn thành giao dịch chuyển khoản thông qua các công nghệ như Android Pay, Samsung Pay, Apple Pay, ví Paytm và nhiều công nghệ khác. Tuy nhiên, khi nói đến khả năng bảo mật trong quá trình thực hiện các giao dịch m-payment, hiện vẫn tồn tại một số vấn đề đáng quan ngại.

Kết quả của một khảo sát vừa được công bố cho thấy, tỷ lệ các vụ phạm tội liên quan đến m-payment đã chạm mức 71% trong năm 2019. Theo các chuyên gia, tỷ lệ này chắc chắn sẽ tăng lên tới mức khó tin trong những năm tới. Do vậy, đối với những người sử dụng điện thoại di động (ĐTDĐ) để thanh toán, dưới đây là 5 mối đe dọa bảo mật nghiêm trọng nhất cần được chú ý để tránh mọi hình thức gian lận.

1. **Sử dụng nhiều tùy chọn phần mềm**

Tương tự máy tính xách tay và máy tính để bàn, ĐTDĐ cũng đang hoạt động trên các hệ thống phần cứng và phần mềm khác nhau. Tuy nhiên, trên thế giới hiện vẫn còn một số người đang sử dụng các phiên bản hệ điều hành iOS và Android cũ. Và hành động này có thể dẫn đến những nguy cơ bảo mật khác nhau. Các thiết bị không được hỗ trợ tốt bởi những công nghệ bảo mật di động mới nhất sẽ là mục tiêu hấp dẫn để các tin tặc và kẻ lừa đảo khai thác và tấn công.

Trong trường hợp các ứng dụng di động được bảo mật nhưng thiết bị có thể không đáp ứng các tiêu chuẩn, song chúng vẫn cung cấp cho bạn mức độ bảo mật di động cơ bản. Các thiết bị di động cũng cần được bảo mật đầy đủ với những đặc tính nâng cao để bảo vệ bạn khỏi mọi hình thức lừa đảo. Một số thí dụ về thiết bị di động bảo mật bao gồm mã xác minh đối với ĐTDĐ hoặc email, cảm biến quét khuôn mặt, cảm biến vân tay, định vị, nhận dạng giọng nói, v.v. Do đó, khách hàng nên chọn cho mình một chiếc điện thoại thông minh (smartphone) có các đặc tính nâng cao về phần mềm và phần cứng để bảo vệ tài khoản và thanh toán đầu cuối.

2. Mất điện thoại

Ngày nay, smartphone có chức năng giống như những tấm thẻ tín dụng. Nó chứa tất cả các dữ liệu cần thiết như thông tin liên lạc, tên, bộ sưu tập ảnh cá nhân, kết nối phương tiện truyền thông xã hội, và nhiều thứ khác nữa. Tương tự, nó cũng cung cấp quyền truy cập đầy đủ vào tài khoản ngân hàng, thẻ ghi nợ và thẻ tín dụng thông qua các ứng dụng thanh toán khác nhau, ví di động, ứng dụng ngân hàng trực tuyến và hơn thế nữa. Nhưng điều gì sẽ xảy ra nếu bạn thất lạc chiếc ĐTDĐ của mình tại bất kỳ cửa hàng, nhà hàng hoặc nơi đông người nào khác? Liệu mọi dữ liệu

cá nhân của bạn chắc chắn sẽ bị rò rỉ? Những dữ liệu này bao gồm tất cả các thông tin ngân hàng và m-payment, và điều đó có thể dẫn đến các hành vi gian lận.

Không phải người nào tìm thấy chiếc điện thoại cũng sẽ trả lại nó cho bạn. Do đó, bạn nên tìm kiếm những chiếc smartphone được tích hợp khả năng bảo mật tốt để bảo vệ điện thoại, ví di động của bạn, và ngăn chặn các hoạt động lừa đảo khác. Thay vì sử dụng một phương thức xác thực duy nhất, bạn nên sử dụng phương thức xác thực 2 nhân tố để mở khóa smartphone thông qua các tùy chọn nhận dạng khuôn mặt, vân tay và mống mắt cùng mã PIN.

3. **Những thói quen sử dụng không phù hợp**

Ngay cả khi bạn sở hữu một chiếc ĐTDĐ có khả năng bảo mật cao, bạn vẫn có thể gặp vấn đề về bảo mật thanh toán bởi cách mà bạn sử dụng nó. Những kẻ lừa đảo có thể lợi dụng trình duyệt web trên ĐTDĐ mà bạn thực hiện các giao dịch mua hàng hoặc thanh toán. Nên nhớ rằng các trình duyệt như Chrome và Safari luôn có độ rủi ro cao khi bạn sử dụng chúng để thực hiện các giao dịch thanh toán.

Nếu bạn đang sử dụng ĐTDĐ để thanh toán, nhằm nâng cao khả năng bảo mật, bạn cần sử dụng các công cụ phát hiện trình duyệt, bởi các công cụ này sẽ bảo vệ người dùng khỏi các hành vi gian lận được thực hiện thông qua những trình duyệt di động không an toàn. Thay vì sử dụng các trình duyệt như vậy, bạn hãy tìm kiếm các ứng dụng di động an toàn và tiên tiến đi kèm với phiên bản cập nhật.

Cuối cùng, đối với trường hợp người dùng di động không sử dụng bất kỳ loại khóa PIN nào hoặc các tùy chọn bảo mật khác trên ĐTDĐ, có nghĩa là họ đã tạo điều kiện vô cùng thuận lợi để những kẻ lừa đảo thực hiện các hành vi gian lận khi thiết bị bị mất. Vì vậy, khách hàng nên tìm kiếm một ứng dụng thanh toán và trình duyệt được cập nhật để bổ sung khả năng bảo mật cho ĐTDĐ.

4. Bảo vệ ví di động của bạn

Với sự ra đời của các tùy chọn m-payment, một số ứng dụng thanh toán đã ra đời. Paytm, Google Pay, Apple Pay, PayPal và các loại ví thanh toán tương tự khác đã nhanh chóng trở nên phổ biến với những ưu đãi tuyệt vời, hoàn tiền, giảm giá... Tất cả những ứng dụng như vậy đều hoạt động khi liên kết thẻ ghi nợ hoặc thẻ tín dụng với ví di động. Các thông tin như

Hiện nay, các nhà cung cấp ví di động sử dụng mã thông báo token được tạo ngẫu nhiên để thực hiện thanh toán mà các đơn vị bán hàng không thể thấy được trong khi thực hiện giao dịch.

Tội phạm mạng có thể lạm dụng số tài khoản của bạn, nhưng khi bạn kết nối mạng với Wifi công cộng không được bảo vệ để bổ sung bất kỳ thẻ tín dụng hoặc thẻ ghi nợ nào vào các ứng dụng thanh toán, rủi ro sẽ tăng lên rất cao. Kẻ gian có thể dễ dàng giả mạo tất cả các dữ liệu thực hiện giao dịch khi chúng được sử dụng trong lúc đăng ký. Để bảo vệ bạn khỏi những gian lận như vậy, hãy sử dụng thẻ với ví di động khi ở nhà hoặc bảo vệ mạng cá nhân bằng mật khẩu. Sử dụng Mạng riêng ảo (VPN) cũng là cách tốt nhất để nâng cao mức độ bảo mật trong khi sử dụng ví di động.

5. Cẩn thận với những bản sao ứng dụng

Bạn có chắc chắn đã cài đặt ứng dụng chính xác trên ĐTDĐ của mình hay không? Hoặc nó là một trong những bản sao ứng dụng? Hiện nay, có nhiều bản sao ứng dụng khác nhau được thiết kế tương tự các ứng dụng gốc cung cấp tùy chọn thanh toán an toàn. Khi bất kỳ người dùng nào sử dụng bản sao ứng dụng và đăng ký thông tin ngân hàng của họ trong đó, bọn tội phạm sẽ gặp nhiều thuận lợi hơn trong việc thực hiện các hoạt động lừa đảo thông qua thẻ tín dụng, thẻ ghi nợ và các thông tin cá nhân khác. Những bản sao ứng dụng như vậy thường đi kèm với các tùy chọn bảo mật yếu có thể bị những kẻ xấu truy cập một cách dễ dàng.

Cả Google và Apple đều dựng các hàng rào bảo vệ bắt buộc khi bạn tải ứng dụng xuống để sử dụng. Song tội phạm mạng vẫn có những thủ đoạn khác nhau để cài đặt các bản sao ứng dụng có chứa virus vào thiết bị của bạn. Đối với các thiết bị iOS, những kẻ lừa đảo lợi dụng những thiết bị bị bẻ khóa để thực hiện thanh toán gian lận. Và cách tốt nhất để giữ điện thoại của bạn tránh xa các bản sao ứng dụng như vậy là sử dụng công cụ chống phần mềm độc hại.

Các hệ thống có chứa các công cụ hoặc phần mềm chống phần mềm độc hại sẽ bảo vệ ĐTDĐ của bạn khỏi hành vi cài đặt bất kỳ bản sao ứng dụng nào. Công tác nghiên cứu vẫn được thực hiện để tìm ra những giải pháp thích hợp nhằm đối phó với các bản sao độc hại. Một thí dụ điển hình về sự thành công, Klara - ứng dụng thanh toán của Thụy Điển - gần đây đã huy động được nguồn hỗ trợ tài chính của 3 đối tác chiến lược đầy sức mạnh.

Có nhiều biện pháp khác nhau có thể giúp người dùng smartphone tránh khỏi các hành vi gian lận hoặc tội phạm mạng. Bạn có thể tăng cường độ mạnh của mật khẩu, cài đặt ứng dụng tìm điện thoại, sử dụng mạng được cá nhân hóa, tránh thanh toán với mạng công cộng, phổ biến tới người thân các quy trình m-payment an toàn./.

(PaymentsJournal)

MK® group
Smart Digital Security

www.mkgroup.com.vn | contact@mkgroup.com.vn | www.facebook.com.vn/mkgroup1999

Hà Nội: Tầng 11, tòa nhà TTC, 19 Duy Tân, Cầu Giấy | Tel: (+84-24) 6266 2703
Tp. Hồ Chí Minh: Tầng 7 Thiên Sơn Building, 5 Nguyễn Gia Thiều, Quận 3 | Tel: (+84-28) 3930 5023