

THẾ GIỚI THỂ

Bản tin điện tử nội bộ - Số 121 | Tháng 4 - 2021



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

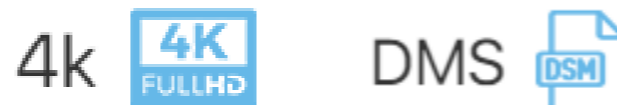
Lưu ý: Toàn bộ thông tin/hình ảnh trong Bản tin điện tử nội bộ Thế Giới Thể MK Group được sưu tầm từ các nguồn tin khác nhau và chỉ sử dụng cho mục đích chia sẻ kiến thức.

CÁC TIN BÀI CHÍNH



AUTOSECURE

Camera hành trình thông minh
đầu tiên tại Việt Nam
tích hợp trí tuệ nhân tạo (AI)



- [Camera hành trình thông minh AutoSecure xứng đáng nhận giải Sao Khuê 2021](#)
- [Lộ trình “chip hoá” gần hơn](#)
- [Thị trường thẻ sinh trắc học sẽ đạt mốc 55 tỷ USD vào năm 2025](#)
- [Thiết hại gian lận danh tính tăng lên 56 tỷ USD năm 2020](#)
- [Rò rỉ dữ liệu từ Accellion: “Từ tấn công đánh cắp dữ liệu và tổng tiền đến an toàn thông tin doanh nghiệp”](#)
- [Những xu hướng gian lận trong không gian thương mại điện tử năm 2021](#)

Camera hành trình thông minh AutoSecure xứng đáng nhận giải Sao Khuê 2021

Ngày 21/3, tại Trường Cao đẳng FPT Polytechnic, MK Vision đã thực hiện bài thuyết trình và giới thiệu sản phẩm camera hành trình thông minh AutoSecure trước Hội đồng Giám khảo - gồm TS. Nguyễn Việt Hải, Phó Viện trưởng Viện Khoa học Công nghệ VINASA, Giám đốc Công ty TNHH Phát triển Phần mềm và Đào tạo (eDT); bà Nguyễn Thị Thanh Thủy, Vụ trưởng Vụ Khoa học, Công nghệ và Môi trường, Bộ NN&PTNT; và ông Lưu Danh Anh Vũ, Giám đốc Đối tác, Amazon Web Services Việt Nam. Trải qua các vòng thẩm định và thuyết trình, AutoSecure đã được vinh danh bằng Giải thưởng Sao Khuê 2021 trong lĩnh vực “Nhóm các sản phẩm, phần mềm mới”.

Sự phát triển của công nghệ hiện đại đã và đang giúp cải thiện cuộc sống thường ngày của mỗi chúng ta, khiến cho mọi việc trở nên dễ dàng và thuận tiện hơn. Trong lĩnh vực giao thông, sự ra đời của các sản phẩm công nghệ mới đã tạo ra những ảnh hưởng tích cực, góp phần cải thiện ý thức của người dân khi tham gia giao thông, cũng như giảm thiểu nguy cơ gây tai nạn. Để giám sát và đảm bảo sự an toàn của các tài xế, không thể không kể đến các sản phẩm camera hành trình ô tô.

Thấu hiểu được tầm quan trọng của chiếc camera hành trình ô tô, cũng như những tính năng cần thiết của một sản phẩm công nghệ như vậy, MK Vision - công ty thành viên mới nhất của MK Group - đã nghiên cứu, phát triển và cho ra đời AutoSecure - camera hành trình thông minh đầu tiên tại Việt Nam được tích hợp trí tuệ nhân tạo (AI).

AutoSecure có khả năng ghi hình với độ phân giải lên tới 4K, mang đến sự tiện lợi cho người dùng khi xem lại các hành trình. Được trang bị cảm biến gia tốc, AutoSecure có thể cảnh báo trong thời gian thực những hành động lái xe bất thường như phanh gấp, va chạm hay chuyển hướng bất ngờ... Bên cạnh đó, sản phẩm của MK Vision còn giúp bảo vệ phương tiện khi đang đỗ trước những tình huống bất ngờ như va quệt, đánh cắp linh kiện hoặc phá hoại. Với camera góc rộng, mọi hành vi làm hư hại ô tô đều sẽ bị AutoSecure theo dõi, ghi lại và gửi cảnh báo đến chủ xe thông qua app trên điện thoại thông minh, tạo điều kiện để họ xử lý kịp thời trong những tình huống như vậy.

Điểm đặc biệt nhất của camera hành trình thông minh AutoSecure là thiết bị được tích hợp cảm biến DMS để quan sát và phân tích các hành vi của người lái xe. Với cảm biến DMS,



AutoSecure sẽ trở thành một “trợ thủ đắc lực” của các tài xế khi tham gia giao thông, cảnh báo họ khi có những biểu hiện nguy hiểm như mất tập trung, buồn ngủ, say xỉn... Giải pháp này vô cùng phù hợp để áp dụng cho các tài xế taxi, xe khách, xe dịch vụ, giao hàng, vận tải đường dài..., những người thường xuyên phải lái xe nhiều giờ liên tục.

Để nghiên cứu và phát triển sản phẩm camera hành trình thông minh AutoSecure, đội ngũ kỹ sư của MK Vision không chỉ sở hữu chuyên môn và kinh nghiệm vững vàng, mà còn luôn nỗ lực tối đa để mang đến cho người tiêu dùng những sản phẩm công nghệ “Make in Vietnam” đạt chuẩn quốc tế. Trong tương lai gần, chúng tôi sẽ không ngừng đưa ra thị trường những giải pháp camera thông minh chất lượng cao nhằm phục vụ nhu cầu giám sát và quản lý đặc thù của Việt Nam.

Lễ Công bố và Trao Giải thưởng Sao Khuê dự kiến sẽ diễn ra vào ngày 24/4 tại Nhà hát ca múa nhạc Quân đội, đường Hồ Tùng Mậu, Mai Dịch, Cầu Giấy và được truyền hình trực tiếp từ 09:00 - 11:30 trên kênh VTC2 của Đài TH Kỹ thuật số VTC, chia sẻ trên kênh YouTube, website của Giải thưởng Sao Khuê và trang fanpage của VINASA./.

Lộ trình “chip hoá” gần hơn

Kể từ ngày 31/3/2021, các ngân hàng sẽ buộc phải dừng phát hành thẻ ATM nội địa mới là thẻ từ, phải chuyển sang phát hành thẻ gắn chip. Đây là quy định được đặt ra tại Thông tư số 22/2020/TT-NHNN sửa đổi, bổ sung Thông tư số 19/2016/TT-NHNN của NHNN quy định về hoạt động thẻ ngân hàng.

Câu chuyện chuyển đổi thẻ từ sang thẻ chip được nhắc tới nhiều năm trở lại đây như một xu hướng tất yếu nhằm góp phần đảm bảo an ninh, an toàn, bảo mật thông tin, chống giả mạo, ngăn chặn các hành vi gian lận trong hoạt động phát hành và thanh toán thẻ. Thẻ chip phát hành hiện nay có hai dạng: thẻ có tiếp xúc và thẻ không tiếp xúc. Thẻ không tiếp xúc (contactless) vượt trội hơn về thời gian thanh toán khi chỉ mất 0,2 - 0,3 giây/giao dịch; đồng thời không yêu cầu mã PIN với giao dịch nhỏ, thanh toán một chạm (yêu cầu máy POS công nghệ liên kết tầm ngắn NFC). Với công nghệ chip Contactless, mỗi lần thanh toán, khách hàng chỉ cần chạm thẻ vào thiết bị chấp nhận thẻ (POS) chứ không cần cào thẻ như thông thường. Chuyển đổi sang thẻ chip cũng tạo ra cơ hội phát triển mới cho thẻ thanh toán, mở rộng các dịch vụ thẻ tại Việt Nam đồng thời tăng cường sự phát triển lành mạnh, an toàn, bền vững cho thị trường thẻ ngân hàng, bảo đảm cho việc các thành viên thị trường có thể liên kết, chia sẻ khai thác hiệu quả cơ sở hạ tầng công nghệ liên quan tới phát hành, thanh toán và sử dụng thẻ.

Ghi nhận cho thấy, thời gian qua các NHTM đã rất khẩn trương trong việc chuyển đổi sang thẻ chip cho khách hàng. Gần đây nhất, NCB cho biết kể từ 8/3/2021, 100% thẻ nội địa do ngân hàng này phát hành mới là thẻ chip, thẻ phát hành trước đó khách hàng vẫn sử dụng bình thường song nhà băng này khuyến khích khách hàng nên chuyển đổi sang thẻ chip để được miễn phí phát hành thẻ, phí sử dụng thường niên năm đầu. Còn Vietcombank từ tháng 2/2020 đã thông báo ngừng cung cấp dịch vụ cho các thẻ Connect24 có đầu số 686868 và đề nghị khách hàng tới quầy để đổi thẻ miễn phí. Tính đến hết tháng 2/2021, Vietcombank đã phát hành mới và chuyển đổi được 2,5 triệu thẻ gắn chip nội địa. Từ đầu năm 2020, tất cả thẻ thanh toán nội địa được mở mới tại VPBank đều là thẻ chip. Với Sacombank, ngay từ năm 2019, ngân hàng này cũng đã ngừng phát hành thẻ ATM mới là thẻ từ mà chuyển đổi sang phát hành ATM thẻ gắn chip, đến nay tỷ lệ chuyển đổi của Sacombank vào khoảng 60% thẻ; SCB cũng đang có tỷ lệ chuyển đổi sang thẻ chip khá cao là 81%...

Tuy nhiên vẫn còn một số khó khăn nhất định về phía các Ngân hàng khi chuyển đổi sang thẻ chip như: chi phí trang bị ATM/POS mới cũng như nâng cấp hệ thống thẻ, thiết bị đầu cuối, chi phí mua sắm phôi thẻ khá lớn nên các nhà băng sẽ phải có sự tính toán, hoạch định để cân bằng chi phí đầu tư nhưng vẫn phải đáp ứng được với yêu cầu chuyển đổi. Và đặc biệt, việc chuyển đổi sang thẻ chip này cũng sẽ gặp những vướng mắc ít nhiều từ phía khách hàng do tâm lý lâu nay của người Việt Nam rất “ngại” thay đổi.

TIN VẤN THẺ NGÂN HÀNG

- **Ngân hàng TMCP Quốc tế Việt Nam (VIB)** chính thức ra mắt Online Plus 2in1 - dòng thẻ đầu tiên tại Đông Nam Á tích hợp 2 số thẻ khác nhau cho thẻ tín dụng và thẻ thanh toán quốc tế trên một thẻ, với ưu đãi 43 triệu đồng khi khách hàng thanh toán và sử dụng dịch vụ Grab.
- **Từ ngày 07/04/2021 đến hết 30/06/2021, Ngân hàng Quân đội (MB)** triển khai chương trình “Đặc quyền ưu tiên - Hoàn tiền hấp dẫn”. hoàn 20% cho giao dịch chi tiêu đầu tiên với thẻ tín dụng MB Priority Visa Platinum phát hành mới trong thời diễn ra chương trình.
- **Trong khoảng thời gian từ ngày 01/04/2021 cho đến ngày 31/07/2021, Ngân hàng Sài Gòn Thương tín (Sacombank)** triển khai chương trình ưu đãi dành cho khách hàng thẻ tín dụng Sacombank Visa. Cụ thể, khi khách hàng phát sinh giao dịch thanh toán tối thiểu 1 triệu đồng trong vòng 30 ngày kể từ ngày kích hoạt thẻ có thể được hoàn phí thường niên lên tới 1 triệu đồng. Ngoài ra, khách hàng mở mới thẻ Sacombank Visa sẽ được nhận ngay 1 phần quà nhỏ đi kèm như ví đựng, túi thể thao,.../.



Nguồn: Internet

(ThoibaoNganhang)

(Tổng hợp từ Internet)

Ngân hàng Piraeus lựa chọn nền tảng thẻ số hóa của Antelop

Nguồn: Internet



Ngân hàng Piraeus - nhà phát hành thẻ lớn nhất tại Hy Lạp và nằm trong số 50 nhà phát hành thẻ ghi nợ hàng đầu châu Âu - đã chọn Antelop làm đối tác thanh toán số lâu dài, cho phép ngân hàng này cung cấp cho khách hàng một loạt giải pháp thanh toán di động và thẻ số hóa tiên tiến.

Ông Nikos Petrakis, Giám đốc Kinh doanh Thẻ của Ngân hàng Piraeus nhấn mạnh: “Chúng tôi là những người tiên phong trong lĩnh vực ngân hàng số tại Hy Lạp, vì chúng tôi là đơn vị đầu tiên thiết lập Winbank - giải pháp ngân hàng di động và Internet trên thị trường... Chúng tôi thấy rằng, các khách hàng đang tích cực sử dụng dịch vụ thanh toán di động NFC mà chúng tôi cung cấp thông qua Winbank Pay - dịch vụ mới do đối tác Antelop cung cấp. Vì vậy, chúng tôi đã quyết định triển khai Winbank Pay trực tiếp thông qua ứng dụng ngân hàng di động của chúng tôi để số hóa cả thẻ Visa và Mastercard”./.

(MailChimp)



Datacard® MX9100™ Card Issuance System

Hệ thống cá thể hóa độc đáo vượt trội cho thẻ phẳng nhằm gia tăng sự khác biệt

- Hiện đại hóa quy trình xử lý thẻ thông minh
- Hệ thống mô-đun hóa giúp việc cài đặt diễn ra nhanh chóng và dễ dàng
- Phần mềm quản lý bảo mật cho phép thiết lập và kiểm soát quá trình vận hành thiết bị một cách an toàn và hiệu quả
- Hệ thống quản lý chất lượng nội tuyến tự động giúp loại bỏ các nguy cơ sản phẩm không đạt chất lượng, từ đó giúp tăng năng suất và giảm chi phí sản xuất.

Hotline: 0903.481.456 • Email: marrketing@mkgroup.com.vn



Châu Âu: Nhu cầu dùng tiền mặt tăng trong thời kỳ COVID



Nguồn: Internet

Theo báo cáo từ Ngân hàng Trung ương Châu Âu (ECB) cho biết tổng giá trị tiền mặt đang lưu thông tại Châu Âu đã tăng từ 1,3 tỷ EURO (1,5 tỷ USD) vào cuối năm 2019 lên 1,4 tỷ EURO (1,7 tỷ USD) vào cuối năm 2020.

Năm ngoài mức tăng "đặc biệt cao" tới 11% qua từng năm so với mức tăng trung bình chỉ 5% trong 10 năm qua, bất chấp xu hướng giảm tỷ lệ giao dịch tiền mặt do hạn chế tiếp xúc trong đại dịch cùng sự gia tăng liên tục sử dụng thẻ không tiếp xúc, thanh toán di động và mua sắm trực tuyến.

Theo phát hiện của ECB, lý do chính cho sự tăng trưởng nhu cầu này là việc sử dụng tiền mặt trong khu vực Châu Âu cho "mục đích phòng ngừa (tức là trữ tiền mặt)" của các hộ gia đình, tổ chức tài chính tiền tệ và doanh nghiệp trong đại dịch Covid-19.

Trong một bản tin nghiên cứu từ ECB cho biết: "Một hiện tượng được gọi là 'nghịch lý tiền mặt' đã xuất hiện ở khu vực đồng EURO, trong khi thực tế việc sử dụng tiền mặt để giao dịch bán lẻ đã giảm xuống đáng kể nhưng ngược lại, nhu cầu tiền mặt trong thị trường vẫn không ngừng tăng."

"Các cuộc khảo sát thanh toán gần đây cũng chỉ ra rằng tỷ lệ giao dịch tiền mặt trong khu vực đồng EURO đã giảm. Cùng với việc số hóa đang diễn ra mạnh mẽ trong thanh toán bán lẻ, có thể dự kiến nhu cầu về tiền mặt vẫn sẽ có xu hướng giảm dần. Tuy nhiên thực tế việc này lại không hề diễn ra và số lượng tiền giấy euro được lưu hành đã tăng lên kể từ năm 2007"./.

(NFCW)

GIẢI PHÁP XÁC THỰC BẰNG MẬT KHẨU MỘT LẦN KEYPASS™ OTP

Giải pháp xác thực bằng mật khẩu một lần KeyPass™ OTP giúp đảm bảo an toàn thông tin cho các hoạt động:

- Ngân hàng điện tử | Thương mại điện tử
- Giao dịch trực tuyến | Trò chơi trực tuyến



Các thiết bị đi kèm giải pháp gồm:

- Thẻ OTP Display (PIN Pad) – OTP Hardware Token (PIN Pad) –
- OTP SIM Sticker – OTP Software Token (on Mobile) –
- SMS OTP (on Mobile)

MK Group là thành viên của:



HOTLINE

0903.481.456

www.contact@mkgroup.com.vn



Nguồn: Internet

Thị trường thẻ sinh trắc học sẽ đạt mốc 55 tỷ USD vào năm 2025

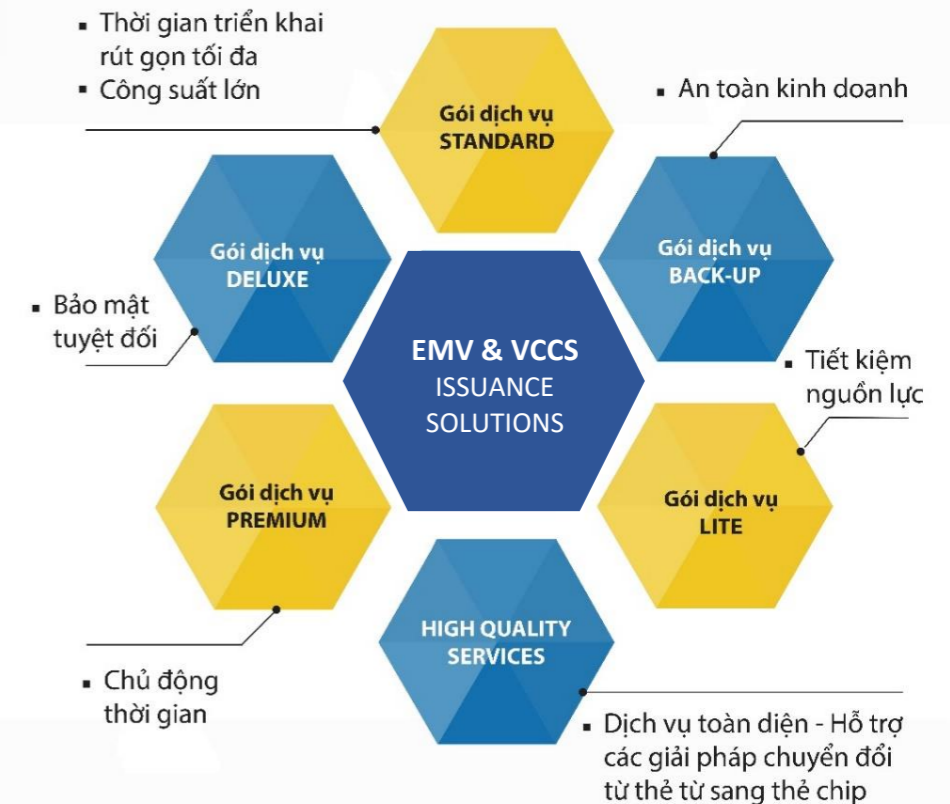
Frost & Sullivan mới đây đã công bố một báo cáo cho thấy COVID-19 đã thay đổi hành vi tiếp cận của con người với máy móc. Tổ chức cũng lưu ý rằng các tổ chức trong hầu hết các lĩnh vực đang ngày càng sử dụng các công nghệ như sinh trắc học và thực tế ảo nhiều hơn nhằm mang lại trải nghiệm cá nhân hóa cho khách hàng của họ và xu hướng này cũng tăng nhanh khi mọi người chuyển dần sang hệ sinh thái tiêu dùng từ xa trong thời kỳ đại dịch.

Với xu hướng thay đổi này, Frost & Sullivan dự đoán rằng thị trường công nghệ thực tế ảo và thực tế tăng cường toàn cầu sẽ tăng lên 661,40 tỷ USD vào năm 2025, với tốc độ tăng trưởng CAGR là 86,3% trong giai đoạn từ 2019 đến 2025. Phần lớn doanh thu trong đó (161,29 tỷ USD) sẽ đến từ lĩnh vực sản xuất, nơi công nghệ AR và VR sẽ được kết hợp với robot để trợ giúp hoạt động, sửa chữa chuỗi cung ứng kỹ thuật và quy trình sản xuất rộng lớn hơn.

Trong khi đó, thị trường sinh trắc học được dự kiến sẽ tăng lên 54,97 tỷ USD trong cùng thời gian này. Nhu cầu về nhận dạng an toàn hơn sẽ thúc đẩy phần lớn xu hướng tăng trưởng này. Frost & Sullivan tin rằng mối quan tâm đến công nghệ sinh trắc học hành vi và tĩnh mạch lòng bàn tay sẽ đặc biệt được tăng cao trong thời gian này, trong khi nhận dạng vân tay, mống mắt, khuôn mặt và giọng nói vẫn sẽ được triển khai trên nhiều ứng dụng công cộng và thương mại./.

(Findbiometrics)

MK SMART CUNG CẤP CÁC GÓI DỊCH VỤ PHÁT HÀNH THẺ THEO CHUẨN EMV & VCCS



NCR ra mắt ATM không dùng thẻ đầu tiên tại Ấn Độ

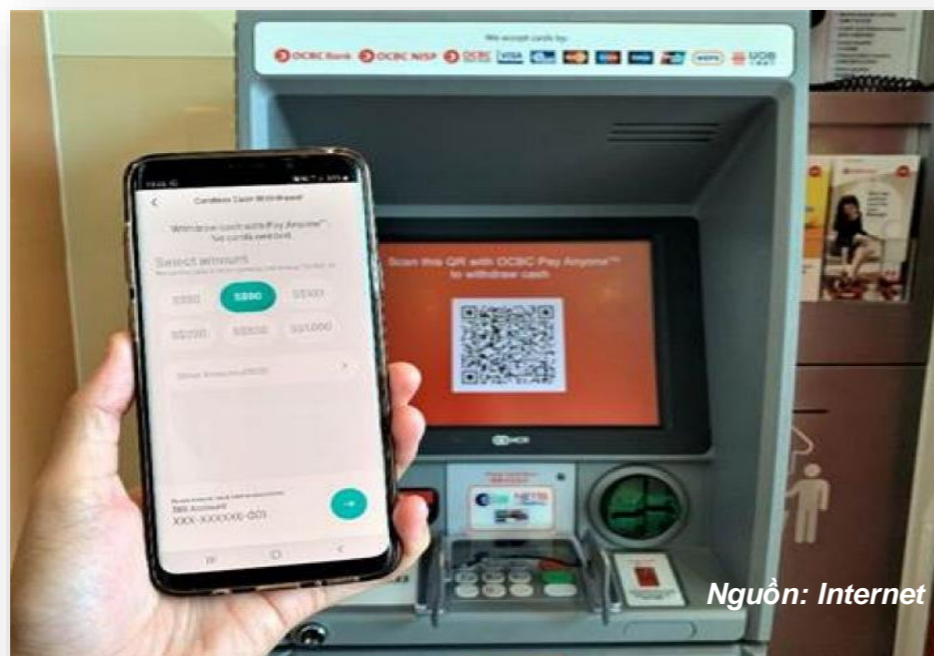
Đã đến lúc người tiêu dùng không cần thẻ, không cần quẹt mà vẫn có thể rút tiền ATM tại Ấn Độ, nhờ nhà sản xuất ATM, NCR Corporation.

Theo một báo cáo trên LiveMint, NCR Corporation đã phát triển máy ATM rút tiền mặt không cần thẻ có thể tương tác với UPI đầu tiên, được liên kết với Công ty thanh toán Quốc gia và Ngân hàng City Union.

Giải pháp đã được cài đặt thêm cho 1500 máy ATM của Ngân hàng City Union, cho phép khách hàng của họ có thể rút tiền mặt không dùng thẻ mà dùng mã QR. Khách hàng có thể rút tiền mặt bằng thiết bị di động với bất kỳ ứng dụng hỗ trợ UPI nào như GPay, BHIM hoặc Paytm. Thực sự không hề cần dùng thẻ. Người dùng chỉ cần quét mã QR động trên màn hình bằng thiết bị di động là đã có thể rút tiền mặt từ ATM ngay lập tức. Để giúp các giao dịch an toàn và bảo mật hơn, mã QR động sẽ liên tục được thay đổi.

Hiện tại, giới hạn rút tiền được giới hạn ở ₹ 5.000 (khoảng 68,23 USD). NCR đã nâng cấp phần mềm hiện có để cho phép thực hiện phương thức giao dịch này trên các máy ATM hiện có của Ngân hàng City Union. Không hề cần nâng cấp hoặc thay đổi phần cứng và từ góc độ bảo mật, những kẻ gian lận không có cơ hội "đọc lướt thẻ" vì giao dịch hoàn toàn dựa trên mã QR động. Không thể sao chép mã QR vì chúng thay đổi theo từng giao dịch, đó là lý do nó được gọi là mã QR "động".

Với tiện ích rút tiền mặt không cần thẻ dựa trên mã QR động này, người tiêu dùng có thể rút tiền từ bất kỳ máy ATM nào của bất kỳ ngân hàng nào, nếu máy ATM đó đã được nâng cấp./.



Nguồn: Internet

(ATMmarketplace)

GIẢI PHÁP PHÁT HÀNH THẺ NGAY LẬP TỨC CARDWIZARD



TĂNG TÍNH GẮN KẾT - THỨC ĐẨY DOANH THU

**Giải pháp phát hành thẻ ngay lập tức
Entrust Datacard® CardWizard giúp thẻ
trong trạng thái sẵn sàng sử dụng trong
tầm tay của khách hàng chỉ trong vài**

Giải pháp sẽ giúp các tổ chức phát hành thẻ:

- Khác biệt hóa thương hiệu
- Tối ưu hóa trải nghiệm của khách hàng
- Tiết kiệm chi phí và giảm thẻ lưu kho
- Bảo mật phát hành ngay lập tức
- Giúp các chương trình Thẻ được triển khai nhanh chóng

**HOTLINE
0903.481.456**

www.contact@mkgroup.com.vn

TietoEVERY: Đã đến lúc tích hợp công nghệ sinh trắc học vào thẻ thanh toán không tiếp xúc

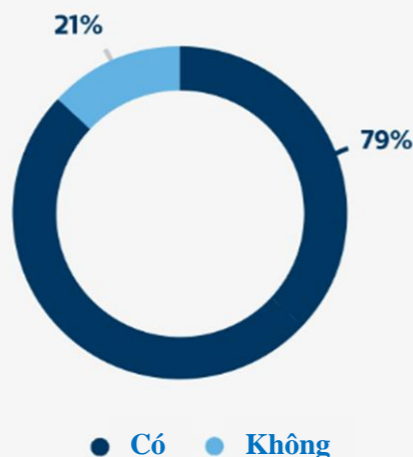
Nghiên cứu thị trường mới nhất về thẻ không tiếp xúc do TietoEVERY thực hiện cho thấy, người tiêu dùng (NTD) ở Anh và châu Âu lo ngại về những nguy cơ lây nhiễm dịch bệnh khi thanh toán tại cửa hàng, cùng với mối e ngại trước tình trạng đánh cắp và gian lận ngày càng nghiêm trọng khi hạn mức giao dịch được nâng lên.

Trong sách trắng “Bảo vệ cuộc cách mạng: Bước tiếp theo trong giao dịch không tiếp xúc”, TietoEVERY cho rằng hiện nay là thời điểm thích hợp để tích hợp công nghệ bảo mật sinh trắc học vào thẻ thanh toán không tiếp xúc (TTKTX).

Theo kết quả nghiên cứu được thực hiện trong làn sóng COVID-19 thứ hai ở châu Âu hồi tháng 1/2021, 83% NTD Anh lo ngại về nguy cơ lây nhiễm virus SARS-CoV-2 khi mua sắm và thanh toán tại cửa hàng. Bên cạnh đó, cũng có tới 55,3% lo ngại về sự an toàn của thẻ thanh toán khi hạn mức giao dịch được nâng lên thành 100 Bảng (GBP) từ ngày 6/4 năm nay.

Nghiên cứu chỉ ra rằng, TTKTX đã trở thành lựa chọn quen thuộc của 78,3% NTD Anh, trong đó có 90% đã sử dụng lựa chọn này trong 3 tháng gần nhất.

Bạn có muốn thẻ thanh toán tiếp theo của mình có chức năng sinh trắc học không?



Sự chuyển biến tương tự cũng diễn ra ở những thị trường hàng đầu châu Âu, với 72% NTD Thụy Điển và 77% NTD Na Uy sử dụng thẻ TTKTX tính đến tháng 1/2021.

Những cuộc khảo sát gần đây cho thấy, ước tính sẽ có 1/5 NTD Anh sẽ chuyển ngân hàng để được cung cấp các dịch vụ tốt hơn, và đã đến lúc các ngân hàng khẳng định lợi thế cạnh tranh bằng cách cung cấp thẻ sinh trắc học.

Nghiên cứu cũng dự báo, gần một nửa NTD Anh (49%) sẽ chuyển ngân hàng để có được thẻ thanh toán sinh trắc học, trong khi khoảng một nửa NTD ở Thụy Điển và Na Uy sẵn sàng thực hiện quyết định thay đổi tương tự./.

(Payments Cards & Mobile)

SẢN PHẨM THẺ - THẺ THÔNG MINH

MK cung cấp các sản phẩm Thẻ - Thẻ thông minh, giải pháp Phát hành – Cá thể hóa thẻ toàn diện và các ứng dụng thẻ, góp phần tạo nên những chương trình thẻ chất lượng cao và hiệu quả.

- Công nghệ in ấn được chứng nhận bởi các tổ chức quốc tế Visa, MasterCard, JCB, UPI, NAPAS, GSMA, ISO 9001, ISO 14000;
- Sản phẩm phát hành và cá thể hóa trên dây chuyền tiến tiến - hiện đại;
- Cung cấp toàn diện các giải pháp Phát hành – Cá thể hóa - Ứng dụng Thẻ toàn diện và đồng bộ;
- Công suất lớn, đáp ứng nhanh chóng các yêu cầu về tiến độ và thời gian giao hàng;
- Đội ngũ kỹ sư và công nhân chất lượng cao, được đào tạo theo chuẩn quốc tế;



Các chứng chỉ đã đạt:



HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

Thiệt hại gian lận danh tính tăng lên 56 tỷ USD năm 2020

Báo cáo nghiên cứu về gian lận danh tính năm 2021, do Javelin Strategy & Research phát hành, đã tiết lộ rằng tổng thiệt hại do gian lận danh tính kết hợp đã tăng lên 56 tỷ USD trong năm 2020 vừa qua.

Gần 1/3 nạn nhân của vấn nạn gian lận danh tính này đã cho biết các nhà cung cấp dịch vụ tài chính của họ đã không thể giải quyết thỏa đáng vấn đề gian lận mà họ gặp phải và 38% nạn nhân đã buộc phải đóng tài khoản của họ vì không còn tin tưởng vào giải pháp tại tổ chức tài chính nơi hành vi gian lận của họ xảy ra.

Khi người tiêu dùng đang ngày càng phụ thuộc vào các sản phẩm thanh toán kỹ thuật số trong bối cảnh năm 2020, các âm mưu gian lận danh tính cũng ngày càng thay đổi tinh vi hơn để bắt kịp xu thế tiêu dùng khách hàng. Các thiệt hại liên quan đến việc thanh toán kỹ thuật số và chuyển khoản ngang hàng (P2P) cũng đều tăng đột biến./.

(Paypers)



MÁY IN THẺ ĐỂ BÀN DATACARD®

- Lý tưởng cho các Chương trình Thẻ nhận diện của mọi tổ chức trong các lĩnh vực: Doanh nghiệp, Chính phủ, Trường học, Bệnh viện và các Tổ chức bán lẻ - dịch vụ.
- Các máy in thẻ là sự kết hợp hoàn hảo giữa khả năng in thẻ chất lượng cao và chi phí hợp lý
- Thêm cá tính năng in ấn bảo mật: in mực UV bảo mật, phủ lớp bảo mật, dập dấu nổi giúp các chương trình thẻ trở nên an toàn.
- Phần mềm thân thiện dễ sử dụng
- Vật tư – Phụ tùng chính hãng
- Dịch vụ hỗ trợ kỹ thuật nhanh chóng



Máy in thẻ SD260



Máy in thẻ SD460



Máy in thẻ CR805



Máy in thẻ SD360



Máy in thẻ CD119

HOTLINE

0903.481.456

www.contact@mkgroup.com.vn

Rò rỉ dữ liệu từ Accellion: “Từ tấn công đánh cắp dữ liệu và tổng tiền đến an toàn thông tin doanh nghiệp”

Công ty phần mềm Accellion và Mandiant đã thông báo đến khách hàng và truyền thông rằng họ vá thành công 4 lỗ hổng bảo mật sau sự cố rò rỉ dữ liệu nghiêm trọng.

Một số nạn nhân của Accellion sau khi bị đánh cắp dữ liệu đã bị đe dọa tổng tiền, và do không trả tiền chuộc nên những dữ liệu này đã bị một tổ chức có tên là Clop phát tán trên website của chúng. Công ty phần mềm Accellion đã công bố những cơ sở đầu tiên liên quan đến sự cố an toàn thông tin là do một số khách hàng đang sử dụng các thiết bị truyền dữ liệu lạc hậu đến 20 năm. Gần 100 khách hàng bị tấn công từ 4 lỗ hổng trong FTA, trong đó 25 doanh nghiệp đã phải gánh chịu hậu quả nặng nề từ việc mất mát dữ liệu.

Joel York, giám đốc Marketing của Accellion chia sẻ với ISMG rằng, sau khi đối tượng tấn công tìm được một lỗ hổng trong FTA hồi tháng 12/2020, nhiều lỗ hổng khác đã xuất hiện vào tháng 1/2021.

Một vài khách hàng của Accellion phải nhận liên tiếp 2 trái đắng: đầu tiên là họ bị mất dữ liệu, và sau đó nhận được email của các đối tượng từ nhóm Clop yêu cầu trả tiền chuộc để thông tin không bị phát tán lên mạng. Singtel, tập đoàn viễn thông lớn nhất của Singapore và Hãng luật Jones Day không chấp nhận trả tiền chuộc nên đã bị phát tán dữ liệu nhạy cảm lên mạng.

Từ tháng 12, một số nạn nhân khác của Accellion FTA đã thông báo sự cố tương tự như Ngân hàng Dự trữ New Zealand, Asic, Cục Điều phối Tài chính Australia, Văn phòng Kiểm toán liên bang Washington, Đại học Colorado, Viện Nghiên cứu QIMR Berghofer Australia, và gần đây nhất là chuỗi bán buôn Kroger.

Đơn vị tư pháp FireEye's Mandiant, sau khi được Accellion cảnh báo, đã thực hiện nhiều bài kiểm tra xâm nhập và đánh giá coding của FTA, song không còn phát hiện các lỗ hổng nguy hại.

Do có nhiều cuộc tấn công xảy ra, Accellions đã đẩy nhanh tiến độ chấm dứt vòng đời sản phẩm cũ vào tháng 4 và khuyến khích các khách hàng FTA từ bỏ sản phẩm này để chuyển sang sản phẩm mới mang tên Kiteworks an toàn hơn.

CÁCH THỨC XÂM NHẬP CỦA KẼ GIAN?

Mandiant đã công bố blog post mô tả những sự cố ghi nhận được. Accellion cho biết sẽ công bố toàn bộ báo cáo do Mandiant thực hiện trong các tuần tiếp theo. Mandiant gọi nhóm tấn công Accellion là UNC2546 - được xếp vào danh sách “tội phạm chưa xếp loại” do không thuộc nhóm tội phạm thông thường. Theo Mandiant, vào giữa tháng 12, UNC2546 đã bắt đầu khai thác lỗ hổng SQL injection trong FTA của Accellion. UNC2546 lợi dụng lỗ hổng này để cài đặt một mã độc lên web mà Mandiant gọi là DEWMODE.

HỆ THỐNG PHÁT HÀNH THẺ CÔNG SUẤT LỚN DATACARD® MX

- Lý tưởng cho các tổ chức Phát hành thẻ tầm trung và cao;
- Tính năng toàn diện: Mã hóa thẻ thông minh/dải từ, dập nổi, in chìm, in khắc laser;
- Tùy chọn mô-đun linh hoạt theo yêu cầu đặc thù của từng chương trình thẻ;
- Dịch vụ bảo hành – bảo trì toàn diện

Hệ thống công suất tầm trung MX6100, MX2100, MX1100



Hệ thống công suất lớn MX9100, MX8100



HOTLINE
0903.481.456

www.contact@mkgroup.com.vn



Chưa rõ bằng cách nào mà đối tượng tấn công có thể ghi được DEWMODE lên ổ đĩa, song mã độc đã trích xuất danh mục file dữ liệu và nội dung toàn bộ các file này từ kho dữ liệu MySQL của FTA. Khi đối tượng tấn công đánh cắp thông tin, những yêu cầu phản hồi và lưu trên log, tuy nhiên, Mandiant cho hay hầu hết các lệnh đều được mã hóa và việc giải mã là khá phức tạp.

HỒI TIẾP THEO: TỔNG TIỀN!

Cuộc tấn công bên trên mới chỉ là phần đầu. Vài tuần sau đó, một số tổ chức đã trở thành mục tiêu của cuộc tấn công thứ hai của nhóm UNC2582 và đã nhận được tin nhắn tổng tiền đòi tiền chuộc dữ liệu.

Vào tháng 3, Clop đã lập ra website, trên đó chúng tung ra thông tin của các nạn nhân từ chối trả tiền. Dường như có sự trùng lặp giữa Clop, UNC2582 và một nhóm khác tên là FIN11 - chuyên thực hiện những chiến dịch giả mạo. UNC2582 theo sát diễn tiến để tung dữ liệu lên website của Clop. Mandiant cũng xác nhận một số email tổng tiền của UNC2582 đến từ địa chỉ IP hoặc tài khoản được FIN11 khởi tạo trước đó.

Tuy vậy, Mandiant cho rằng vẫn còn khó có thể đưa ra được kết luận cuối cùng. Sự chông chéo giữa FIN11, UNC2546 và UNC2582 là khá thuyết phục, nhưng chúng ta cần tiếp tục truy vết các bằng chứng một cách riêng biệt, song song với tiến trình đánh giá bản chất của mối liên hệ giữa chúng.

BƯỚC TƯỜNG THÀNH CUỐI CÙNG: MÃ HÓA DỮ LIỆU

Những báo cáo trên cho thấy, nhiều doanh nghiệp đang triển khai các biện pháp phòng vệ chủ động thông qua phân tích, thiết lập các hàng rào bảo vệ chống lại những cuộc tấn công từ bên ngoài. Tuy nhiên, khi các chiến tuyến này bị xuyên thủng, tin tặc sẽ dễ dàng đánh cắp thông tin hoặc dùng mã độc phá hoại rồi đòi tiền chuộc. Một giải pháp hữu hiệu được nhiều tổ chức doanh nghiệp quốc tế ưa dùng là xây dựng một môi trường làm việc an toàn thông qua phương pháp Mã hóa. Mặc dù đối tượng tấn công lấy được dữ liệu hoặc thông tin vô tình lộ lọt do lỗi nhân viên thì dữ liệu đó cũng không thể đọc được. Tất cả file dữ liệu trên máy người dùng, lưu trữ trên các thiết bị, trên Cloud, lưu chuyển qua thư điện tử hoặc các thiết bị lưu trữ rồi đều được tự động mã hóa, qua đó nâng cao cấp độ bảo mật.

Xuất phát từ nhu cầu thực tế, MK Group mang tới giải pháp Prim'X của Pháp, cùng sự hỗ trợ của đội ngũ kỹ sư nhiều kinh nghiệm. Điều này sẽ giúp các tổ chức và doanh nghiệp Việt Nam làm việc trong một môi trường an toàn, đảm bảo sự sống còn và uy tín của họ./.

(MK Group tổng hợp)

MÁY IN THẺ TÀI CHÍNH SIGMA DS4

GIẢI PHÁP THÔNG MINH – HIỆU QUẢ
CHO MỌI CHƯƠNG TRÌNH THẺ TẠI CHI NHÁNH THÀNH CÔNG



- Khả năng phát hành bao gồm:
 - In đơn màu và/hoặc đủ màu truyền nhiệt trực tiếp
 - Mã hóa thẻ thông minh tiếp xúc/không tiếp xúc/ dải từ
- Quyền truy cập kiểm soát kép với bảo mật ổ khóa bảo vệ kho thẻ, nguồn cung cấp, và thẻ bị từ chối, đáp ứng yêu cầu bảo mật của Visa và Mastercard.
- Phát hành tức thì được lưu trữ trên đám mây là giải pháp duy nhất trong ngành được chứng nhận PCI-CP.
- Dễ dàng mở rộng các chương trình phát hành thẻ theo nhu cầu thực:
 - Thêm các hộp đựng thẻ cho từng thiết kế được lựa chọn
 - Thêm mô đun dập nổi phủ nhũ bạc để tăng chất lượng và hiệu ứng hình ảnh cho thẻ
- Dữ liệu được mã hóa khi kết nối – gửi giữa Phần mềm phát hành tương ứng Datacard® và máy in và không được lưu trữ trong máy in sau khi in.
- Giải pháp tổng thể với các dịch vụ đi kèm, luôn sẵn sàng đồng hành cùng các tổ chức xây dựng các chương trình phát hành thẻ tại chi nhánh thành công.

HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

Những xu hướng gian lận trong không gian thương mại điện tử năm 2021

Dưới đây là một số xu hướng mà các đối tượng gian lận đang khai thác và các đơn vị kinh doanh nên cảnh giác trong năm 2021.

Những biến thể mới của các hình thức gian lận cũ

Tấn công chiếm đoạt tài khoản (ATO)

Gian lận ATO tăng 282% trong khoảng thời gian giữa năm 2019 và 2020. Dự báo cho năm 2021 là giới tin tặc sẽ sử dụng các phương pháp tự động hóa như tạo script và nhồi thông tin danh tính để thực hiện những vụ tấn công và khiến gian lận ATO trở nên dễ dàng hơn bao giờ hết. Hậu quả sẽ như thế nào? Chúng ta sẽ chứng kiến nhiều vụ rò rỉ dữ liệu hơn, song chúng ta cũng phải tự vấn: khả năng này đồng nghĩa với việc lĩnh vực dịch tài chính cuối cùng sẽ không còn tin tưởng vào username và password? Hay là chấp nhận đăng nhập không sử dụng mật khẩu, dựa vào thông tin sinh trắc học, và xác thực liên tục để ngăn chặn ATO? Nhận dạng BOT trong khâu tạo tài khoản trực tuyến sẽ dễ dàng phát hiện ra một người nào đó không tạo mới hoặc chỉnh sửa thông tin tài khoản trực tuyến. Ý tưởng này, cùng với quyết định không sử dụng username và password làm rào cản chính đối với kẻ gian, sẽ nhanh chóng mang lại lợi ích cho các nhà bán lẻ.

Một mối quan ngại khác là ATO đang phát tán rộng rãi trong không gian thương mại điện tử (TMĐT), đặc biệt nghiêm trọng trên thị trường game trực tuyến. Mức độ rủi ro cao hơn khi nhà cung cấp phải duy trì sự tham gia và hoạt động của người chơi, đồng thời đảm bảo tính thông suốt của các giao dịch trong thời gian thực. Khó khăn ở đây là liệu nhà cung cấp game có các giải pháp ngăn chặn gian lận hiệu quả để phân biệt dữ liệu giao dịch hợp pháp hoặc gian lận hay không. Bên cạnh nhận dạng BOT, các giải pháp xác thực di động và định danh số sẽ mang lại sự chắc chắn về thông tin định danh và khả năng xác thực khách hàng một cách thuận lợi.



Nguồn: Internet

GIẢI PHÁP XÁC THỰC GIAO DỊCH THẺ TRỰC TUYẾN EMV 3D SECURE

- Là phương thức bảo mật tiên tiến, giúp bảo vệ chủ thẻ và các đơn vị chấp nhận thẻ tránh các rủi ro trong thanh toán trực tuyến.
- Có thể tích hợp với các phương thức xác thực bằng sinh trắc học, OOB hay OTP.
- Hỗ trợ khả năng xác thực dựa trên mức độ rủi ro (RBA).
- Được chứng nhận bởi EMV Co., Visa, Amex, Mastercard, JCB và UPI.



HOTLINE
0903.481.456

www.contact@mkgroup.com.vn

Hoàn trả chi phiếu (Chargeback)/ Gian lận thân thiện

Chargeback là hình thức gian lận TMĐT phổ biến nhất và là một trong những thách thức gây thiệt hại lớn nhất mà các nhà bán lẻ trực tuyến phải trải qua. Mặc dù chúng ta phân biệt được gian lận cố ý và gian lận thân thiện - có chủ đích hay vô tình, song hậu quả là như nhau: Chargeback thường khiến chúng ta phải gánh thêm các khoản phí, mất hàng hóa hoặc dịch vụ. Các thói quen mua sắm mới - như mua trực tuyến và nhận tại cửa hàng (BOPIS), thẻ quà tặng số hóa hoặc curbside pick-up (soạn sẵn túi hàng) - cũng dẫn đến nhiều tình huống hoàn trả chi phiếu hơn. Vì vậy, mọi người không nên bất ngờ khi gian lận chargeback có thể chiếm từ 40% đến 80% tổng thiệt hại do gian lận gây ra trong năm 2021.

Gian lận giao dịch/phishing

Thông qua hình thức gian lận này, những đối tượng xấu thực hiện các giao dịch mua hàng bằng cách sử dụng thông tin thanh toán bị đánh cắp, thường có được thông qua những cuộc tấn công phishing (lừa đảo bằng các trang web giả mạo). Kẻ gian mạo nhận là đại diện của một công ty đáng tin cậy, và nạn nhân bị lừa tự nguyện chia sẻ các thông tin cá nhân. Năm 2020, do hình thức làm việc từ nhà riêng trở nên phổ biến, những người không thành thạo về công nghệ dễ có nguy cơ nhấp chuột vào các phishing email hơn. Bên cạnh đó, các nhóm gian lận còn hợp tác với những thực thể khác nhau (chẳng hạn như trung tâm chăm sóc khách hàng, công ty giao nhận...) - vốn có đội ngũ nhân viên làm việc từ xa trong vai trò là các nhà thầu. Vì vậy, đôi khi rất khó biết chắc được một người gửi email có thực sự liên kết với một trong những mắt xích khác trong chuỗi TMĐT hay không. Liệu chúng ta sẽ chứng kiến nhiều vụ tấn công phishing hơn, hoặc các doanh nghiệp đã học được từ năm 2020 và hiện sẵn sàng đấu tranh với gian lận hơn hay không?



Nguồn: Internet




GIẢI PHÁP MÃ HÓA DỮ LIỆU CẤP CAO PRIM'X

CRYHOD

Mã hóa dữ liệu chống bị đánh cắp dành cho máy tính

Giải pháp Cryhod sẽ mã hóa hoàn toàn đĩa dữ liệu trong toàn bộ máy trạm di động của công ty bạn. Với Cryhod, dữ liệu chỉ có thể truy cập bởi người dùng được phân quyền và cần được xác thực hợp lệ trước khi khởi động.





Chứng chỉ



www.mk.com.vn - contact@mkgroup.com.vn HN: (84-24) 6266 2703 - HCMC: (84-28) 3930 5023

Danh tính giả

Được coi là hình thức tội phạm tài chính phát triển nhanh nhất ở Mỹ, gian lận danh tính giả hư cấu nên một con người, khi kẻ xấu kết hợp thông tin cá nhân từ một con người có thật với những chi tiết bịa đặt nhằm mục đích mở tài khoản hoặc giao dịch trực tuyến. Kẻ gian sử dụng danh tính giả để mua hàng trực tuyến, và hành vi này có thể dẫn đến tổn thất doanh thu khổng lồ. Khi đơn vị bán hàng không có hệ thống trí tuệ nhân tạo (AI) chống gian lận có độ chính xác cao, họ thậm chí còn có thể xác thực sai.

Trong báo cáo “Dự đoán về tương lai của gian lận năm 2021”, Experian cho rằng, giới gian lận có thể sử dụng những khuôn mặt giả cho mục đích xác thực sinh trắc học - hiện tượng được đặt tên là “Frankenstein ID”. Experian tin rằng, giới tội phạm sẽ dựa vào AI để tạo ra những danh tính mới bằng cách kết hợp các đặc điểm của khuôn mặt từ nhiều người khác nhau, hay còn gọi là “deepfake”. Nếu thủ đoạn này thực sự xảy ra, liệu các doanh nghiệp đang sử dụng công nghệ nhận dạng khuôn mặt trong vai trò của chiến lược ngăn chặn gian lận số 1 có sẵn sàng đối đầu với những cuộc tấn công như vậy hay không? Để ngăn chặn hình thức tấn công này, việc sử dụng tính năng phát hiện sự sống trên khuôn mặt và đảm bảo sự hiện diện có thật sẽ đảm bảo rằng danh tính giả không thể được dùng để đăng ký hoặc xác thực.

Mua sắm bằng giọng nói và deepfake

Mua sắm bằng giọng nói là trào lưu mới nhất trong thương mại di động. Những người khổng lồ như Amazon, Apple, Google, và Facebook đều đang cung cấp cho thị trường các sản phẩm loa thông minh. Đi kèm với trào lưu này là những mối quan ngại khi có đến 39% tổng số vụ tấn công nhằm vào các công ty truyền thông được thực hiện trên không gian mạng sử dụng các giao dịch di động. Các nền tảng, giao diện, và thiết bị phục vụ công nghệ mua sắm bằng giọng nói còn tương đối mới và khiến kênh này dễ mắc phải những tổn thương bảo mật như các vụ xâm phạm quyền riêng tư và lừa đảo bằng giọng nói deepfake.

Tấn công deepfake có thể được sử dụng cho những mục đích xấu, chẳng hạn như những nỗ lực qua mặt các hệ thống xác thực. Nhà bán lẻ nên triển khai tính năng nhận dạng sự sống trong giọng nói trên toàn bộ hoạt động của trung tâm chăm sóc khách hàng và tổng đài trả lời tự động (IVR) để phát hiện định danh giọng nói giả mạo trong quá trình đăng ký và xác thực.

Những hình thức gian lận tương lai

Gian lận hoàn tiền

Những khó khăn kinh tế trong năm 2020 đã gây ra tình trạng khủng hoảng cả về thất nghiệp và kinh doanh bán lẻ. Vì vậy, nhà cung cấp công nghệ chống gian lận Ravelin cho rằng, tình trạng này sẽ thúc đẩy nhiều người lợi dụng mọi chương trình khuyến mãi và hoàn tiền mà họ có thể có được. Một số đối tượng cơ hội hơn thậm chí có thể sử dụng thủ đoạn vừa đề cập hơn một lần, do đó, lợi nhuận của công ty có thể bị ảnh hưởng nghiêm trọng, bởi nguồn tài chính dành cho hoạt động tiếp thị của đơn vị bán hàng có thể bị chi tiêu quá mức và lãng phí. Không có gì ngạc nhiên khi những đơn vị này công bố số vụ lạm dụng khuyến mãi và gian lận hoàn tiền tăng lần lượt 49% và 51%.

Đáng chú ý, gian lận hoàn tiền khó bị phát hiện, phần lớn bởi vì không có sự hoàn trả chi phiếu liên quan. Kẻ gian lợi dụng khía cạnh này: cái gọi là “những người hoàn tiền” quảng cáo các dịch vụ của chúng trên những diễn đàn trực tuyến hợp pháp hoặc mạng truyền thông xã hội. Chúng cung cấp cho người tiêu dùng (NTD) những hướng dẫn “phải tuân thủ” để có được một khoản hoàn tiền. Chúng liệt kê danh sách các công ty “đảm bảo” hoàn tiền. Khi các

nhà bán lẻ hoàn tiền cho chủ thẻ, NTD phải trả cho “người hoàn tiền” từ 15% đến 30% khoản tiền có được. Tuy vậy, kẻ gian có thể sử dụng hình thức tấn công phi kỹ thuật để thay mặt NTD đưa ra các yêu cầu hoàn tiền.

Mua trước, trả sau (BNPL – Buy Now, Pay Later)

Với BNPL, các nhà bán lẻ cho phép NTD lựa chọn mua sản phẩm với mức tín dụng 0%. NTD không phải thanh toán ngay toàn bộ số tiền cho BNPL - một cơ hội để những đối tượng gian lận có thể khai thác. So với những hình thức gian lận ATO, gian lận BNPL có thể lợi dụng khoảng thời gian kéo dài hơn từ lúc bắt đầu hành vi gian lận cho tới khi bị phát hiện. Mặt khác, để đánh bại hệ thống, kẻ gian có thể thuê những “con la chuyển tiền” (những tài khoản được tội phạm sử dụng để đánh cắp tiền mà không nhất thiết phải kiểm soát một cách trực tiếp) và thiết lập các cửa hàng để mua tài liệu định danh hợp pháp tại những quốc gia đang phát triển.

Kết luận

Gian lận thương mại điện tử là một nguy cơ lớn đối với kinh doanh và phải được ngăn chặn bằng một hệ thống phát hiện gian lận được thiết kế và triển khai hợp lý. Các nhà bán lẻ cần phân tích mọi giao dịch liên quan để kiểm tra và giám sát các công tác quản lý nội bộ một cách hiệu quả. Một doanh nghiệp có thể tiến hành hoạt động kiểm tra và giám sát liên tục để cải thiện các công tác quản lý gian lận, đồng thời ngay lập tức sửa chữa mọi quy định không phù hợp. Cuối cùng, toàn bộ các nhân viên nên kiểm thử hệ thống để đảm bảo tạo điều kiện thuận lợi cho trải nghiệm tiêu dùng.

Công tác phòng, chống và phát hiện gian lận đang trở nên phức tạp hơn bao giờ hết. Hãy đánh giá về mọi yếu tố trong đại dịch COVID-19 như điều kiện kinh tế, yêu cầu quản lý, tình trạng thiếu hụt tài nguyên CNTT. Triển khai một số chiến thuật này sẽ giúp chiến thắng kẻ gian, đẩy lùi nguy cơ, và duy trì trải nghiệm tiêu dùng tích cực mà NTD mong muốn./.

(Paypers)



**ĐỐI TÁC TIN CẬY VỀ CÁC GIẢI PHÁP XÁC THỰC
BẢO MẬT, CÁ THỂ HÓA THẺ & SẢN PHẨM THẺ THÔNG MINH**



Copyright© 2021 by MK Group

www.mkgroup.com.vn | contact@mkgroup.com.vn

www.facebook.com.vn/mkgroup1999

Headquarters in Hanoi:

2nd floor, The Vista Building, No. 4, 15

Lane Duy Tan Str., Cau Giay Dist.

Tel: (+84-24) 6266 2703

Ho Chi Minh City:

7th floor, Thien Son Building, 5 Nguyen

Gia Thieu St., Ward 6, District 3

Tel: (+84-28) 3930 5023