THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 131 | Tháng 9 - 2021

MK group
Smart Digital Security

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.*

CÁC TIN BÀI CHÍNH

Việt Nam: 67% người dùng tăng sử dụng thanh toán không tiếp xúc

Xu hướng thanh toán không tiền mặt tại Việt Nam tăng mạnh, trong đó, 67% tăng sử dụng thẻ tín dụng, chủ yếu chi tiêu cho thực phẩm, ăn uống, theo khảo sát của Visa.

"Khảo sát thái độ thanh toán của người tiêu dùng" do Visa vừa công bố cho biết, mức độ thanh toán không dùng tiền mặt của người Việt Nam tăng trưởng đáng kể qua tần suất sử dụng ví điện tử, thanh toán không tiếp xúc và mã QR.

Thế giới chứng kiến sự tăng trưởng vượt bậc của chuyển đổi số trong giai đoạn dịch bệnh. Theo nghiên cứu của Visa về thái độ thanh toán của người tiêu dùng, gần 2/3 người tiêu dùng ở Đông Nam Á tức là khoảng 64% đã trải nghiệm không dùng tiền mặt, đặc biệt là người tiêu dùng ở Việt Nam (84%), Thái Lan (82%) và Philippines (79%). Thái độ đón nhận tích cực của người tiêu dùng đã thúc đẩy sự phát triển của phương thức thanh toán không tiếp xúc (63%) và thanh toán thẻ (46%), cũng như việc mở rộng mạng lưới các điểm chấp nhận thanh toán số (41%) và gia tăng am hiểu của người tiêu dùng về tính an toàn của thanh toán điện tử (40%).

Tại Việt Nam, tăng trưởng thanh toán không dùng tiền mặt thể hiện qua tần suất sử dụng ví điện tử, thanh toán không tiếp xúc và mã QR. Thanh toán thẻ không tiếp xúc được dùng nhiều nhất trong danh mục thực phẩm và ăn uống, với 67% người tiêu dùng tăng cường sử dụng phương thức này trong năm 2020. Thanh toán qua mã QR cũng đã tăng vọt trong đại dịch, đặc biệt trong các giao dịch hàng ngày như thanh toán hóa đơn (71%), mua sắm trong lĩnh vực bán lẻ (58%) và tại siêu thị (57%).

“Chứng kiến đợt bùng phát lần thứ tư của dịch bệnh Covid-19 tại Việt Nam, người tiêu dùng tiếp tục duy trì các thói quen thanh toán được hình thành dưới tác động của đại dịch kéo dài trước đây. Hơn hết, sự phát triển của công nghệ đã tái định hình thương mại và thanh toán với những sáng kiến hỗ trợ tối ưu cho trải nghiệm của người tiêu dùng”, bà Tuyết Dung, Giám đốc Visa tại Việt Nam và Lào cho biết.

Theo khảo sát của Visa về thái độ thanh toán của người tiêu dùng, thanh toán bằng thẻ được sử dụng nhiều nhất trong danh mục thanh toán thực phẩm và ăn uống với tỷ lệ người dùng tăng cường sử dụng hơn 60%. Trong đó, thanh toán bằng thẻ không tiếp xúc chiếm ưu thế hơn với 89%, 31% người tiêu dùng thanh toán bằng thẻ không tiếp xúc ít nhất một lần một tuần và 23% sử dụng phương thức này lần đầu tiên kể từ khi đại dịch bùng phát./.

(Vnexpress)

TIN VẮN THẺ NGÂN HÀNG

- **Từ ngày 27/09/2021 cho đến hết ngày 31/01/2022, Ngân Hàng Thương Mại Cổ Phần Sài Gòn Thương Tín (Sacombank)** triển khai ưu đãi nhận quà gồm ví đựng thẻ, hoàn tối đa một triệu đồng phí thường niên khi đóng 100% phí năm đầu dành cho các khách hàng cá nhân mở mới thẻ tín dụng Visa Sacombank.

- **Trong tháng 9/2021, Ngân hàng Bản Việt (Viet Capital Bank)** triển khai chương trình ưu đãi dành cho khách hàng mở mới thẻ JCB Bản Việt từ xa với hàng loạt giảm giá mỗi khi khách mua sắm tại Shopee, Tiki, Lazada và đặt món qua Shopee Food, Grabfood.

- **Từ ngày 06/08 cho đến hết 15/12/2021, Ngân Hàng Thương Mại Cổ Phần Sài Gòn (SCB**) triển khai ưu đãi hoàn tiền hấp dẫn "Phát hành ngay – Quà trao tay" dành cho tất cả các khách hàng phát hành mới thẻ tín dụng SCB cá nhân./.

(Tổng hợp từ Internet)

Nguồn: Internet

American Express ra mắt thiết kế "thẻ nghệ thuật" Centurion mới

Thẻ American Express Centurion độc quyền nổi tiếng, hay còn được biết đến với tên gọi thẻ tín dụng Amex Black, đang được kiến trúc sư(KTS) nổi tiếng Rem Koolhaas và họa sĩ Kehinde Wiley "tân trang".

Theo mạng Hypebeast, KTS Koolhaas đã giành được chiến thắng tại Giải thưởng Kiến trúc Pritzker và là nhà sáng lập Nhóm Thiết kế Kiến trúc Metropolitan.

Những nét vẽ tinh tế trên bề mặt tấm thẻ nhằm truyền tải ý tưởng về "tầm nhìn hướng tới cuộc sống tốt đẹp hơn"./.

(Maxim)

Entrust cập nhật tính năng quản lý vòng đời khóa mã hóa trên Amazon Web Services

Entrust - tập đoàn hàng đầu thế giới về các giải pháp nhận dạng, thanh toán và bảo vệ dữ liệu đáng tin cậy - mới đây đã công bố bản cập nhật tính năng quản lý vòng đời khóa mã hóa dành cho các khóa được khách hàng khởi tạo để sử dụng trong Amazon Web Services (AWS). Tính năng này cho phép các tổ chức tự động hóa và mở rộng quyền kiểm soát khóa mã hóa trên các đám mây công cộng, mang lại sự hỗ trợ dành cho BYOK và các khóa AWS gốc thông qua một giao diện trực quan.

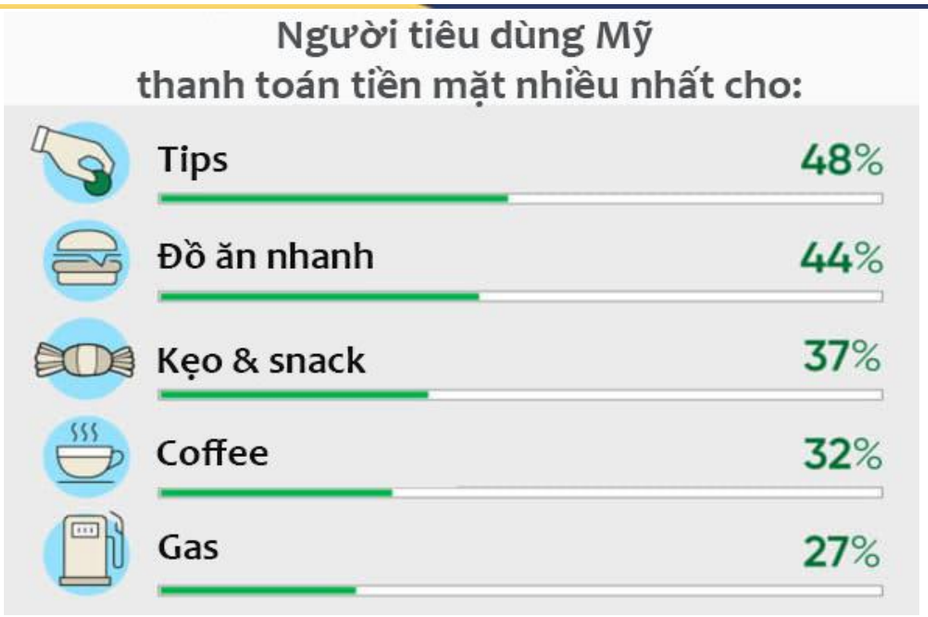
Ông Eric Chiu - Phó Chủ tịch Entrust phụ trách các giải pháp bảo vệ dữ liệu - chia sẻ: "Khi khách hàng chuyển đổi khối lượng công việc được ảo hóa sang các dịch vụ đám mây, họ muốn duy trì quyền kiểm soát các khóa mã hóa bảo vệ dữ liệu quan trọng. Entrust hiện cho phép khách hàng toàn quyền kiểm soát các khóa chính trong AWS, và chúng tôi có kế hoạch mở rộng phạm vi kiểm soát này trên nhiều nhà cung cấp dịch vụ đám mây công cộng. KeyControl sao lưu và tự động hóa các khóa chính trong hệ thống quản lý khóa (KMS), để đảm bảo toàn quyền kiểm soát các khóa từ khi được khởi tạo đến khi hết hạn. Khi khách hàng tiến vào 'vùng biển chưa được khai thác' để triển khai dịch vụ đa đám mây, họ có thể được hưởng lợi sự mau lẹ trong tiến trình xử lý khối lượng công việc trong AWS, đồng thời vẫn 'giữ vững tay lái' - đảm bảo quyền kiểm soát tài sản CNTT mà họ đang hướng tới".

Khách hàng chuyển đổi khóa mã hóa sang AWS có thể tận dụng phần mềm Entrust KeyControl, trước đây là HyTrust KeyControl, để khởi tạo và quản lý khóa một cách an toàn trong suốt vòng đời của chúng, dựa trên tiêu chuẩn mã hóa an toàn FIPS 140-2. Máy chủ quản lý khóa KeyControl tạo điều kiện thuận lợi cho công tác kiểm soát chặt chẽ quyền truy cập khóa, trong khi giao diện quản lý thống nhất cung cấp trải nghiệm người dùng nhất quán cho các khóa được lưu trữ trong KMS. Phiên bản KeyControl mới nhất đem đến khả năng quản lý các khóa được KeyControl khởi tạo, cũng như các khóa được khởi tạo nguyên bản trong AWS.

KeyControl cũng tích hợp các module bảo mật phần cứng Entrust nShield® HSM tại chỗ hoặc dưới dạng dịch vụ. Cơ cấu này giúp khách hàng có thêm sự bảo đảm và niềm vào tiến trình chuyển đổi đám mây bằng cách cung cấp nguồn xác thực dựa trên tiêu chuẩn FIPS 140-2 Cấp 3 phục vụ mục đích tạo khóa.

Được thiết kế để dễ dàng triển khai với khả năng mở rộng kinh doanh, tự động hóa và hiệu suất, KeyControl quản lý các khóa mã hóa toàn bộ hệ thống máy ảo và kho dữ liệu mã hóa, đồng thời có thể mở rộng quy mô để hỗ trợ hàng nghìn nhiệm vụ mã hóa trong những đợt triển khai lớn./.

(Entrust)



Tiền mặt vẫn là phương thức thanh toán ưa thích tại Mỹ

Khoảng 40% người tiêu dùng Mỹ vẫn thích sử dụng tiền mặt và chỉ 39% doanh nghiệp Mỹ duy trì chính sách chỉ sử dụng tiền mặt cho các giao dịch mua dưới 20 USD "mặc dù vẫn có sẵn các phương thức thanh toán không tiếp xúc như thẻ tín dụng, thẻ ghi nợ và ví điện thoại di động", theo một nghiên cứu từ Ngân hàng WSFS cho biết.

Cuộc khảo sát cũng cho thấy rằng hơn một nửa số người được hỏi (khoảng 51%) tin rằng "sử dụng tiền mặt giúp họ tiết kiệm được tiền", với tỷ lệ lên tới 58% trong Thế hệ Z (những người trẻ tuổi từ 18 đến 24), "52% trong số họ coi tiền mặt là phương thức thanh toán ưa thích của họ".

Các nhà nghiên cứu cho biết: "Tuy nhiên, nhiều người được hỏi cho biết họ giới hạn các giao dịch mua bằng tiền mặt tối đa ở mức 31 USD, vì 54% chỉ thường mang theo tiền mặt từ 1- 50 USD trong người. Khi được hỏi họ thường dùng tiền mặt để mua gì, câu trả lời phổ biến nhất nhất là: tiền tip (48%); mua thức ăn nhanh (44%); mua bánh và đồ ăn nhẹ (37%); mua cà phê (32%) và trả tiền gas (27%)."

Các nhà nghiên cứu cho biết thêm "Với nhiều giao dịch mua nhỏ được thanh toán bằng tiền mặt, phần lớn (71%) người bán hàng đồng ý rằng không có gì tệ hơn khi ai đó trả cho một giao dịch mua nhỏ với lượng tiền mặt lớn, chẳng hạn như 50 hay 100 USD."

Cuộc khảo sát được thực hiện với 1500 người tiêu dùng Mỹ từ 18 tuổi trở lên và 500 nhà bán hàng vào hồi tháng 6 năm 2021./.

(NFCW)

Dự báo: Tới năm 2026, thanh toán không tiếp xúc sẽ dẫn đầu thị trường giao dịch POS

Juniper Research dự báo thanh toán không tiếp xúc (TTKTX) sẽ chiếm hơn một nửa (57%) tổng giá trị toàn cầu của các giao dịch được thực hiện tại những thiết bị đầu cuối POS vào năm 2026, cao hơn gấp đôi so với mức dưới 25% trong năm 2021. Bên cạnh đó, số lượng smartphone trên toàn thế giới có thể chấp nhận TTKTX sử dụng công nghệ phần mềm POS (softPOS) sẽ tăng từ 3,2 triệu trong năm 2021 lên gần 24 triệu vào năm 2026.

Theo Juniper Research, xu hướng tăng trưởng về giá trị của các giao dịch POS không tiếp xúc "phần lớn được hỗ trợ bằng cách nâng cao hạn mức giá trị giao dịch TTKTX" và "thể hiện sự thay đổi mạnh mẽ trong cách thanh toán của người tiêu dùng".

Nghiên cứu "Thiết bị đầu cuối POS: Đổi mới thiết bị, Bối cảnh cạnh tranh & Dự báo thị trường trong giai đoạn 2021-2026" nhận định "softPOS, khả năng sử dụng công nghệ NFC trên thiết bị di động để chấp nhận TTKTX, sẽ tăng tốc" vì "giải pháp mang lại lộ trình chấp nhận thẻ rẻ nhất từ trước đến nay dành các doanh nghiệp nhỏ nhất, có nghĩa là giải pháp đang tạo ra sức hấp dẫn đối với thị trường ngách này".

Tuy nhiên, nghiên cứu nhấn mạnh rằng do softPOS không phải là một thiết bị đầu cuối POS có thể nhận biết ngay lập tức, nên giải pháp này gặp phải hạn chế trong khả năng gây dựng niềm tin đối với người tiêu dùng xoay quanh vấn đề bảo mật, vì vậy "sẽ kìm hãm sức tăng trưởng"./.

(NFCW)

Nguồn: Internet

Tin tặc đánh cắp dữ liệu cá nhân của 7 triệu người Israel

Nguồn: Internet

Nhật báo Times of Israel ngày 7/9 cho hay tin tặc có nickname Sang Kancil tuyên bố đã đánh cắp thông tin cá nhân của 7 triệu người dân Israel. Sang Kancil đã công bố hình ảnh thẻ căn cước, giấy tờ tài chính của nhiều người Israel, đồng thời tiết lộ "bất ngờ" sẽ xuất hiện trong vài ngày tới.

Những dữ liệu bị tin tặc đánh cắp có nguồn gốc từ trang web CITY4U, được các cơ quan chức năng địa phương của Israel sử dụng để xử lý những thủ tục thanh toán như thuế đất, tiền phạt và các dịch vụ thiết yếu khác. Nếu thông tin do Sang Kancil đưa ra là chính xác, thì đây sẽ là vụ rò rỉ thông tin cá nhân nghiêm trọng nhất trong lịch sử Israel.

Sang Kancil hôm 5/9 đưa ra tuyên bố trên mạng Telegram khẳng định đã đột nhập vào hệ thống máy tính của chính quyền các địa phương ở Israel và từ ngày 6/9 bắt đầu công bố hình ảnh giấy tờ để chứng minh - gồm thẻ căn cước, giấy phép lái xe và hoá đơn thuế. Thông tin này được đưa lên Telegram và các diễn đàn tin tặc trực tuyến.

Đối tượng tấn công đã rao bán các dữ liệu đánh cắp được, song chưa đưa ra mức giá cụ thể. Một thông báo của Sang Kancil viết: "Đây là bất ngờ đầu tiên của tôi dành cho Năm Mới Do Thái. Hãy tận hưởng!".

Vụ tấn công mạng nói trên dường như tương tự vụ đột nhập vào công ty bảo hiểm Shirbit của Israel hồi năm 2020, trong bối cảnh ngày càng xảy ra nhiều vụ tấn công bằng mã độc tống tiền (ransomware) trên phạm vi toàn cầu./.

(TTXVN)

Liên minh FIDO cập nhật hệ thống hướng dẫn và tiêu chuẩn cải tiến mới

Ông Andrew Shikiar - CEO của Liên minh FIDO liên minh, tổ chức chịu trách nhiệm phát triển và thúc đẩy các tiêu chuẩn xác thực được thiết kế để góp phần giảm sự phụ thuộc vào mật khẩu - vừa công bố hệ thống hướng dẫn trải nghiệm người dùng và tiêu chuẩn cải tiến mới FIDO2.

CEO Shikiar nêu rõ: “Chúng tôi đã xem xét mọi khía cạnh, không chỉ về cách thức triển khai các thông số kỹ thuật FIDO, mà còn là thông điệp đúng đắn để khuyến khích người dùng lựa chọn xác thực FIDO và những dấu hiệu hình ảnh phù hợp”.

Ông Shikiar hy vọng rằng phần lớn các dịch vụ tiêu dùng sẽ cho phép người dùng đăng nhập không cần mật khẩu trong vài năm tới. CEO của Liên minh FIDO nhấn mạnh: “Đó là một cuộc đua marathon, không phải chạy nước rút, và chúng tôi đang đạt được tiến bộ vượt bậc”.

Trong chương trình phỏng vấn trực tuyến của Information Security Media Group, ông Shikiar đã thảo luận về:

- Những sáng kiến mới nhất của FIDO;
- Các doanh nghiệp thay đổi cách tiếp cận đối với hoạt động giám sát và quản lý danh tính kể từ khi chuyển sang làm việc từ xa;
- Tiến triển của FIDO cho đến nay và những vấn đề cần giải quyết.

Ông Shikiar là CEO kiêm Giám đốc Makerting của Liên minh FIDO. Trước đó, quan chức này đã dẫn đầu các nỗ lực phát triển thị trường của Tizen Association, LiMo Foundation và Liberty Alliance Project./.

(BankInfoSecurity)

Pháp: Công dân có thể quét thẻ eID NFC để truy cập dịch vụ công

Công dân Pháp sẽ sớm có thể tự xác minh danh tính của mình khi truy cập vào các dịch vụ công trực tuyến an toàn, bao gồm mở tài khoản ngân hàng, khai thuế và thanh toán bảo hiểm y tế - bằng cách quét eID mới (CNIE) với điện thoại thông minh hỗ trợ NFC của họ.

Chính phủ Pháp giới thiệu chức năng nhằm cho phép chủ sở hữu CNIE mới sử dụng thẻ này trên thiết bị di động để đáp ứng yêu cầu xác thực được thực hiện bởi bất kỳ nhà cung cấp dịch vụ nào trong số 900 nhà cung cấp dịch vụ được kết nối với nền tảng FranceConnect.

Hiện tại, người dùng FranceConnect xác minh danh tính của họ bằng mã ID và mật khẩu cho tài khoản đã được đăng ký và xác thực an toàn với 6 đối tác dịch vụ công khác.

Thẻ eID điện tử CNIE chứa một con chip không tiếp xúc lưu trữ dữ liệu sinh trắc học của chủ sở hữu, bao gồm một bức ảnh và hai dấu vân tay, cũng như một con dấu xác thực ở dạng mã QR.

Bộ Nội vụ Pháp cho biết: "Theo các quy tắc bảo mật do quy định của Châu Âu áp đặt, Bộ muốn bổ sung một số yếu tố bảo mật nhất định để bảo vệ tốt hơn thẻ căn cước mới. Mục tiêu của họ là đảm bảo bảo vệ tối đa dữ liệu cá nhân được lưu trữ trong đó. Đặc biệt, dữ liệu sinh trắc học có trong thành phần điện tử của thẻ sẽ được lưu trữ trong một khoang bảo mật cao cấp và việc truy cập vào nó được kiểm soát đặc biệt."

Thẻ eID CNIE quốc gia mới của Pháp sẽ cho phép công dân Pháp hoàn tất các giao dịch trực tuyến bằng điện thoại thông minh. Công dân sẽ nhận được yêu cầu xác thực trên điện thoại thông minh của họ và sau đó, họ sẽ đặt CNIE ở mặt sau của điện thoại để nhận giao tiếp bằng công nghệ NFC. Ứng dụng dành cho thiết bị di động sẽ đọc và xác thực an toàn dữ liệu cá nhân được lưu trong chip của thẻ. Công dân sẽ cần phải xác nhận đồng ý trước khi thực hiện xác thực trên điện thoại.

Hệ thống eID mới này tuân thủ đầy đủ các quy định eIDAS của Liên minh Châu Âu, "bảo vệ an toàn danh tính công dân và sẽ đảm bảo rằng chỉ công dân có quyền hoặc được ủy quyền mới có quyền kiểm soát hệ thống đó". Chính phủ Pháp đã giới thiệu dịch vụ nhận dạng kỹ thuật số Alicem cho phép công dân sử dụng tính năng đọc hộ chiếu NFC để tự xác minh danh tính với hệ thống vào tháng 10 năm 2019./.

(NFCW)

62% người tiêu dùng Anh thích sử dụng thanh toán thẻ từ ví di động

Gần 2/3 người tiêu dùng ở Anh (62%) hiện thích sử dụng thẻ thanh toán qua ví di động, so với chỉ 31% vào năm ngoái, theo một cuộc khảo sát do Samsung Pay mới thực hiện.

Cuộc khảo sát cho thấy rằng mặc dù 56% người tiêu dùng được phỏng vấn vẫn đang sử dụng thẻ thanh toán vật lý, nhưng 90% trong họ lại tin rằng trong bối cảnh đại dịch Covid-19 phức tạp, việc thanh toán không tiếp xúc bằng điện thoại thông minh hoặc đồng hồ thông minh trở nên thuận tiện hơn và 86% nói rằng việc sử dụng các phương thức thanh toán di động này khiến họ cảm thấy an toàn.

Mặc dù đại dịch Covid-19 đang là nguyên nhân chính khiến thói quen thanh toán chuyển dịch sang di động và cuộc khảo sát cũng cho thấy rằng trong thời gian "đóng cửa" bởi dịch năm 2020, gần một nửa người tiêu dùng Anh (46%) sẵn sàng thực hiện thanh toán kỹ thuật số và gần 20% trong họ cho rằng việc thanh toán di động từ điện thoại thông minh lẫn các thiết bị di động khác sẽ tốt hơn cho môi trường.

42% người được hỏi cho biết rằng cảm thấy bất tiện nếu phải mang cùng lúc nhiều loại thẻ thanh toán và hơn một nửa (53%) cho biết họ sẽ rất vui khi không còn nhận được thẻ thanh toán vật lý từ ngân hàng của mình.

Teg Dosanjh của Samsung cho biết: “Sự thay đổi này cho thấy khách hàng đang chuyển sang sử dụng thanh toán di động thường xuyên hơn khi họ nhận thấy sự an toàn và tiện lợi mà chúng đem lại. Thực tế ngày nay các phương thức bán lẻ cũng đã thay đổi và khách hàng cũng hiểu rõ về cách để giữ an toàn cho bản thân trong khi mua sắm mà vẫn đảm bảo tăng tốc độ giao dịch."/.

(NFCW)

FIDO: Công nghệ hữu hiệu bảo vệ người dùng trước nạn tấn công lừa đảo

Thông báo này có thể đã quen thuộc với bạn: “Tài khoản ngân hàng của bạn đã bị xâm phạm. Vui lòng nhập thông tin chi tiết để kích hoạt lại tài khoản của bạn”.

Nếu bạn gật đầu đồng ý, bạn có thể là một trong số rất nhiều người đã bị tội phạm mạng nhắm tới. Tấn công lừa đảo (phishing) vẫn là thủ đoạn nguy hiểm nhất để đánh lừa người tiêu dùng (NTD) hòng đánh cắp tài khoản và tài sản.

Trên đây chỉ là một thí dụ về e-mail lừa đảo được gửi từ những đối tượng có vẻ đáng tin cậy. Các e-mail tấn công lừa đảo được thiết kế chuyên nghiệp là nguồn cơn gây ra 91% trong tổng số những cuộc tấn công mạng, qua đó chứng tỏ mức độ nguy hiểm của những mối đe dọa này.

Tuy vậy, phishing không chỉ gây ra rủi ro đối với NTD, mà còn là một trong những thách thức bảo mật lớn nhất mà các doanh nghiệp phải đối mặt trong công tác bảo mật thông tin. Trên thực tế, trong năm 2020, đã có gần 3 triệu nỗ lực phishing nhằm vào các doanh nghiệp vừa và nhỏ có trụ sở tại khu vực Đông Nam Á.

Nhu cầu cấp thiết là các doanh nghiệp phải tự bảo vệ mình một cách thỏa đáng trước những cuộc tấn công như vậy, và nhiều doanh nghiệp đang chuyển sang lựa chọn chiến lược đào tạo an ninh mạng nhằm nâng cao nhận thức cho đội ngũ nhân viên về các nguy cơ trên không gian mạng. Câu hỏi đặt ra là: Đào tạo mang lại hiệu quả ra sao trong nỗ lực xóa sổ vấn nạn phishing?

Sơ hở trong công tác đào tạo phòng, chống phishing

Các doanh nghiệp thường chủ yếu dựa vào hoạt động đào tạo người dùng cuối về cách phát hiện những cuộc tấn công phishing. Hiện có vô số tài liệu để đội ngũ nhân viên tìm hiểu về các chiến thuật phòng/chống phishing, từ kiểm tra kỹ lỗi chính tả trong e-mail đến gọi điện cho ai đó mà bạn thường xuyên liên lạc khi xảy ra điều gì đó có vẻ không ổn mà bạn nhận được từ họ.

Thậm chí có những hình mẫu về các doanh nghiệp sáng tạo thông qua cách thức triển khai những khóa đào tạo này. Tháng 12 năm ngoái, GoDaddy.com đã tiến hành một bài kiểm tra về phishing bằng cách gửi tới 500 nhân viên 1 e-mail đề nghị khoản thưởng 650 USD cho kỳ nghỉ. Điểm đáng chú ý là những nhân viên nhấp vào liên kết trong email đã không được thưởng tiền, mà còn phải tham gia khóa đào tạo bổ sung về an ninh mạng.
Mặc dù người dùng cuối đã có được nhận thức rõ ràng hơn sau quá trình đào tạo, song mọi việc chỉ có thể dừng lại ở đó. Tin tặc ngày càng trở nên tinh vi hơn khi thực hiện những cuộc tấn công, sử dụng cơ sở hạ tầng phức tạp trên các trang web phishing. Người dùng cuối có thể cảm thấy khó khăn khi xác định các trang web bất hợp pháp hoặc phân biệt chúng với những trang web hợp pháp. Một số chiến thuật tấn công bao gồm hành vi sử dụng các liên kết chia sẻ có vẻ đáng tin cậy, chẳng hạn như Dropbox, và đặt những sự kiện trên lịch với các liên kết hội nghị trực tuyến có vẻ đúng chuẩn trong các e-mail lừa đảo.

Nguồn: Internet

Trên thực tế, một nghiên cứu tâm lý học cho thấy khi đề cập đến những cuộc tấn công phishing, mọi người có xu hướng tin rằng họ ít có khả năng phạm phải các hành vi rủi ro và ít có nguy cơ bị lừa đảo hơn so với những người khác ở xung quanh. Tâm lý này gây ra cảm giác sai lầm về sự an toàn trước những cuộc tấn công như vậy.

Để khiến cho mọi việc trở nên tồi tệ hơn, những chiêu trò gian lận này thường liên quan đến các thủ đoạn tấn công phi kỹ thuật nhằm đánh lừa và điều khiển các nạn nhân nhân thực hiện hành động mà kẻ gian mong muốn - thường là nhấp vào liên kết hoặc tải xuống tệp đính kèm. Chúng cũng lợi dụng bản chất của những người lao động tham gia lĩnh vực kinh doanh trực tuyến, vì những hoạt động này thường phải được thực hiện một cách nhanh chóng. Được thiết kế để thúc đẩy tương tác mang tính cảm xúc và tức thời, phần nhiều trong số những email lừa đảo khiến các cá nhân bỏ qua lô-gíc và không lưu tâm đến những dấu hiệu cảnh báo đỏ, cho đến khi quá muộn.

Công nghệ mang đến trải nghiệm người dùng an toàn, thuận tiện hơn

Nếu người dùng không thể được tin tưởng với những hành động của họ, thì cách duy nhất là nâng cao năng lực của phương pháp xác thực những hành động này để đảm bảo ngăn chặn các tác nhân độc hại. Cách thức tiếp cận vừa đề cập sẽ giảm bớt gánh nặng xác thực của người dùng nhờ vào công nghệ.

Hiện có sẵn các tùy chọn công nghệ mà doanh nghiệp có thể áp dụng để tự bảo vệ trước những cuộc tấn công phishing và khiến cuộc sống của người dùng trở nên thuận tiện, an toàn hơn. Chẳng hạn, xác thực an toàn bằng công nghệ mã hóa giúp lưu giữ thông tin đăng nhập một cách an toàn và riêng tư, giúp các doanh nghiệp mang đến trải nghiệm người dùng an toàn hơn.

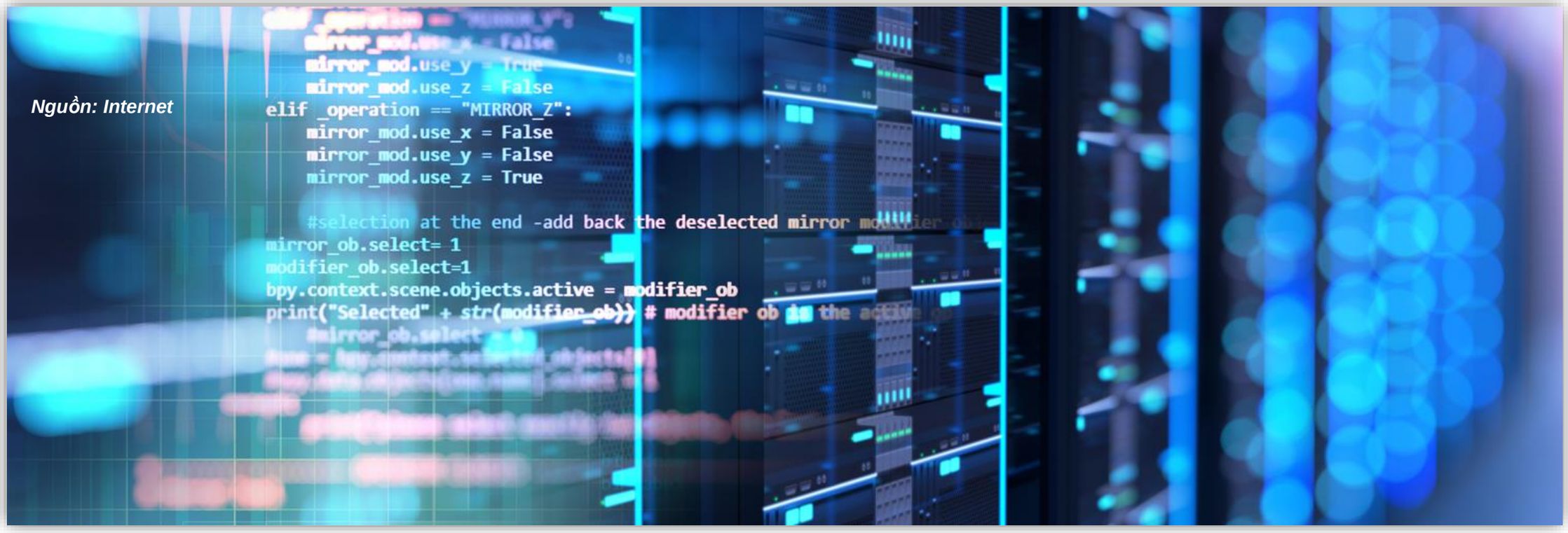
Những giải pháp như vậy sử dụng các biện pháp chống phishing thông tin xác thực mang tính kỹ thuật, tương tự những biện pháp đã được xác định trong hệ thống tiêu chuẩn ngành - như các tiêu chuẩn của FIDO Alliance và W3C. Với những cách tiếp cận này, thiết bị và trình duyệt sẽ âm thầm hoạt động để đảm bảo rằng trang web đang được truy cập là xác thực, mà không phải là trang web phishing ẩn đằng sau một tên miền tương tự. Khả năng này ngăn ngừa những sai lầm phổ biến, chẳng hạn như nhầm số '0' thành chữ 'O'. Do đó, người dùng không còn phải lo lắng về việc phải đề phòng những cuộc tấn công như vậy, và thay vào đó sẽ có thể để thiết bị xử lý những tiểu tiết này.

Chúng ta không biết rõ hơn, nhưng chúng ta có thể hành động tốt hơn

Hiện nay, chính sách ngăn chặn những cuộc tấn công lừa đảo khai thác thông tin xác thực nên tập trung ít hơn vào công tác đào tạo người dùng và thay vào đó, nên chú trọng hơn vào việc áp dụng giải pháp công nghệ xác thực, vốn thực sự có hiệu quả trong nỗ lực ngăn chặn những cuộc tấn công phishing. Mặc dù công tác đào tạo người dùng góp phần hạn chế rủi ro, song sẽ không bao giờ loại bỏ được hoàn toàn rủi ro. Biện pháp tự vệ trước vấn nạn tấn công phishing đòi hỏi cách tiếp cận bảo mật kết hợp và phân lớp. Bằng cách tạo ra một chuỗi rào cản, mỗi lớp rào cản bổ sung sẽ làm giảm khả năng "vượt rào" của những cuộc tấn công phishing.

Khi các doanh nghiệp lập chiến lược cho tiến trình tái thiết và phục hồi, cũng như chuẩn bị cho trạng thái "bình thường" mới sau đại dịch, họ phải tiếp tục tập trung vào mọi khía cạnh của an ninh mạng và nên ưu tiên sử dụng những công nghệ xác thực sẵn có nhằm ngăn chặn mối đe dọa phishing hiện hữu./.

(BusinessMirror)



Nguồn: Internet

(84-24) 7100 6781 - 133 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

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

MK® group
Smart Digital Security

Công ty thành viên

MK® smart Smart Digital Security

MK® Hi-tek Smart Digital Security

MK® vision Smart Secure Style

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) 7100 6781

Ho Chi Minh City:
7th floor, Thien Son Building, 5 Nguyen Gia Thieu St., Ward 6, District 3
Tel: (+84-28) 3930 5023