THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 115 | Tháng 12 - 2020

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

MK Group đạt giải thưởng THÀNH PHỐ THÔNG MINH VIỆT NAM 2020

Ngày 24/11, tại Nhà hát Ca múa nhạc Quân đội, Hà Nội, Công ty Cổ phần Tập đoàn MK (MK Group) đã được trao Giải thưởng THÀNH PHỐ THÔNG MINH VIỆT NAM 2020 dành cho Giải pháp "Thẻ thông minh đa ứng dụng và Hệ sinh thái thẻ thông minh" - Xếp hạng 5 sao tại Hạng mục "Giải pháp ứng dụng cho công dân/cộng đồng thông minh" trong khuôn khổ Giải thưởng do Hiệp hội phần mềm và Dịch vụ CNTT Việt Nam (VINASA) bình chọn. Ông Lê Minh Quốc - Giám đốc Kỹ thuật MK Smart, thành viên MK Group - đại diện cho Tập đoàn nhận vinh dự này.

Giải thưởng dành cho MK Group nằm trong nhóm Hạng mục 4 - Các giải pháp công nghệ cho các thành phố, dự án bất động sản, khu công nghiệp thông minh. Các đơn vị tham gia giải thưởng Thành phố Thông minh Việt Nam 2020 đã trải qua 3 vòng đánh giá, bình chọn gồm sơ tuyển, thuyết trình và thẩm định thực tế, bình chọn chung tuyển.

Trên thế giới và tại Việt Nam, việc sử dụng thẻ thông minh trong các hoạt động tài chính, ngân hàng, kiểm soát ra vào, giao dịch thanh toán, tích điểm, … ngày càng trở nên phổ biến. Tuy nhiên, tất cả những hình thái và ứng dụng đa dạng này của thẻ thông minh mặc dù hữu ích và thiết thực cho người sử dụng, song đặt riêng lẻ từng ứng dụng trên mỗi chiếc thẻ thông minh khác nhau thì không phải bao giờ cũng mang lại trải nghiệm người dùng tích cực và thân thiện. Đây chính là thách thức cho các nhà sản xuất thẻ lớn khi cần tạo được sự kết nối giữa "một chiếc thẻ thông minh – nhiều ứng dụng khác nhau" mà vẫn phải bảo mật an toàn dữ liệu cho chủ thẻ.

Chính từ yêu cầu này của thị trường, MK Group đã xây dựng nên sản phẩm Thẻ thông minh và Hệ sinh thái thẻ thông minh MK Group - là nơi kết nối các hoạt động "thanh toán – định danh – bảo mật – đa ứng dụng" để các đơn vị phát hành thẻ có thể hoàn toàn làm chủ các chương trình Thẻ thông minh của mình dựa trên xu hướng và nhu cầu thực tế của thị trường.

Sản phẩm thẻ thông minh đa ứng dụng do MK phát triển dựa trên hệ điều hành trên chip do MK sở hữu và làm chủ, cho phép tích hợp nhiều ứng dụng an toàn trên cùng một thẻ vật lý khi sử dụng lưu trữ hay xác thực theo yêu cầu như tích hợp với ứng dụng Chữ ký số, ứng dụng đối sánh sinh trắc học trên thẻ (Match on Card – MoC), ứng dụng FIDO để đảm bảo xác thực chính xác chủ thẻ khi truy cập vào các dịch vụ liên quan và chỉ có chủ thẻ mới có thể truy xuất được các dữ liệu đã lưu trên chip thẻ.

Có thể nói chính những điều này đã giúp giải pháp Thẻ thông minh đa ứng dụng và Hệ sinh thái thẻ thông minh của MK Group thực sự trở thành nền tảng số được thiết kế độc lập cho phép tích hợp linh hoạt với các hệ thống và cơ sở dữ liệu liên quan như hệ thống cơ sở dữ liệu liên quan như hệ thống cơ sở dữ liệu dân cư phục vụ cho Chính phủ điện tử, hệ thống ngân hàng trong các hoạt động tài chính, hệ thống quản lý y tế, bảo hiểm xã hội,…

Với 21 năm kinh nghiệm triển khai hàng triệu chương trình thẻ thông minh trong nước và quốc tế, MK Group tự hào đã thiết kế và xây dựng những kết nối cho các hoạt động "thanh toán - định danh - bảo mật - đa ứng dụng" một cách toàn diện và vững chắc, từ những thiết bị phần cứng, giải pháp phát hành thẻ chuyên biệt, tính năng bảo mật với nhiều cấp độ khác nhau trên thẻ thông minh… cho đến các dịch vụ hỗ trợ kỹ thuật khác. Những sản phẩm và giải pháp của Tập đoàn đã giúp các đơn vị phát hành thẻ hoàn toàn làm chủ những chương trình thẻ thông minh, phù hợp với mục tiêu góp phần xây dựng nên các thành phố của những tương tác kết nối mang hàm lượng công nghệ cao giữa người dân - doanh nghiệp - chính quyền, từ đó, cùng nhau kiến tạo nên những thành phố thông minh và văn minh hơn./.

(MK Group)

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

Thiết bị khóa bảo mật FIDO® KEYAPSS S3 của MK Group nhận danh hiệu Chìa khóa vàng 2020

Sáng 18/11, tại Cục Viễn Thông, Bộ Công nghệ Thông tin, MK Group đã vinh dự được trao tặng danh hiệu SẢN PHẨM AN TOÀN THÔNG TIN TRIỂN VỌNG XUẤT SẮC cho thiết bị KHOÁ BẢO MẬT FIDO® KEYPASS S3 trong khuôn khổ Lễ công bố và trao giải CHÌA KHOÁ VÀNG 2020 do Hiệp hội An toàn Thông tin Việt Nam (VNISA) bình chọn. Ông Lê Tuấn Khôi - Phó giám đốc MK Vision, thành viên của MK Group - đại diện cho Tập đoàn lên nhận Kỷ niệm chương và Giấy chứng nhận Danh hiệu.

Thông qua chương trình, nhiều sản phẩm và giải pháp ATTT - do các tổ chức, doanh nghiệp Việt Nam làm chủ về công nghệ - đã khẳng định được chất lượng, tính ưu việt và hiệu quả, góp phần thúc đẩy công cuộc chuyển đổi số của Việt Nam diễn ra một cách thành công. Đây cũng là hoạt động hưởng ứng Chương trình Chuyển đổi số Quốc gia và chiến lược "Make in Vietnam" của Chính phủ.

Tiếp nối thành công của Khóa bảo mật FIDO® KeyPass S1 đạt chứng chỉ FIDO U2F (FIDO Alliance) đã được MK Group giới thiệu ra thị trường, Thiết bị KHÓA BẢO MẬT FIDO® KEYPASS S3 hỗ trợ tính năng FIDO2 - được trang bị thêm màn hình hiển thị các dữ liệu cần xác thực nhằm gia tăng tính an toàn và chính xác trong quá trình thực hiện các hoạt động giao dịch trực tuyến. FIDO® KEYPASS S3 là công cụ hiệu quả giúp chống lại những hành vi phishing (lừa đảo bằng các trang web giả mạo), skimming (sao chép thông tin tài khoản), tấn công xen giữa (man-in-the-middle), từ đó giúp người tiêu dùng yên tâm thực hiện các hoạt động trực tuyến.

Thiết bị Khóa bảo mật FIDO® KeyPass là niềm tự hào đối với các sản phẩm công nghệ chất lượng cao "Make in Vietnam" do MK Group nghiên cứu và phát triển. Đặc biệt, danh hiệu Chìa khóa vàng 2020 chính là sự ghi nhận và đánh giá cao những nỗ lực của MK nhằm tạo ra những sản phẩm giải pháp an toàn thông tin "Make in Vietnam" chất lượng cao, ứng dụng thiết thực và hiệu quả vào đời sống kinh tế xã hội./.

(MK Group)

TIN VẮN THẺ NGÂN HÀNG

- **Công ty Cổ phần Thanh toán Quốc gia Việt Nam (Napas)** phối hợp với các ngân hàng thành viên công bố triển khai chương trình ưu đãi "Ngày mua sắm trực tuyến cùng Napas năm 2020" từ ngày 30/11 đến 6/12, nhằm tặng tiền tối đa lên đến 25 triệu đồng mỗi giải thưởng vào tài khoản thanh toán cho khách hàng khi thực mua sắm hàng hóa dịch vụ trực tuyến bằng thẻ nội địa Napas tại các website.

- **Từ ngày 13/11 đến hết ngày 15/12, Ngân Hàng Thương Mại Cổ Phần Sài Gòn Thương Tín (Sacombank)** thực hiện chương trình ưu đãi dành cho các chủ sở hữu thẻ thanh toán Plus và thẻ tín dụng Sacombank Family. Cụ thể, các chủ thẻ khi đổi từ thẻ từ sang thẻ chip sẽ được hưởng mức phí thay thế thẻ ưu đãi là 29.000đ thay vì 99.000đ và hoàn tối đa 100.000 đồng cho các giao dịch qua POS.

- **Từ 25/11/2020 đến hết 25/12/2020, Ngân hàng thương mại cổ phần Ngoại thương Việt Nam (Vietcombank)** áp dụng chương trình ưu đãi hoàn tiền tối đa 100.000 VNĐ khi thực hiện giao dịch tại POS có giá trị từ 500.000 VNĐ, dành cho các chủ thẻ nội địa Vietcombank Connect24 Chip contactless./.

(Tổng hợp từ Internet)

Discovery Bank ra mắt thẻ ảo và dịch vụ thanh toán không tiếp xúc Discovery Pay

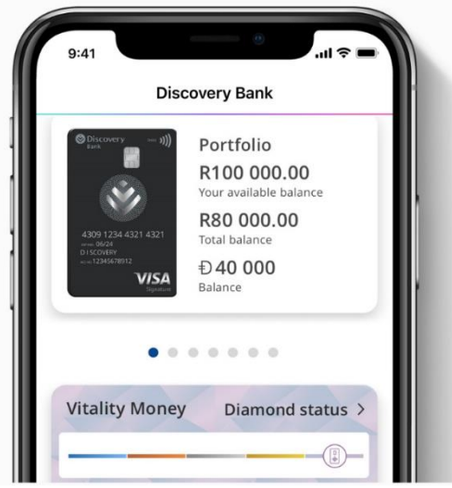
Discovery Bank tại Nam Phi mới đây đã cho ra mắt thẻ ảo và dịch vụ thanh toán không tiếp xúc Discovery Pay tại thị trường này.

Loại thẻ Ngân hàng này được ra mắt đồng thời với dịch vụ Discovery Pay, cho phép khách hàng được phép thực hiện thanh toán mà không cần thông tin chi tiết về ngân hàng. Khách hàng có thể thực hiện bất kỳ thanh toán này ngay trên điện thoại thông minh có kích hoạt dịch vụ.

Người dùng có thể tạo nhiều thẻ ảo để sử dụng và tùy chọn các loại giao dịch mà họ muốn sử dụng cho mỗi thẻ. Ngân hàng Discovery đã thông báo rằng khách hàng có thể thêm bao nhiêu thẻ ảo cũng được nếu họ cần.

Mỗi thẻ ảo đều có số thẻ duy nhất, ngày hết hạn và số xác minh thẻ. Nếu khách hàng chỉ sử dụng thẻ ảo cho thanh toán trực tuyến, họ có thể thiết lập giảm hạn mức mua hàng trực tuyến của thẻ vật lý xuống 0 để tăng cường bảo mật./.

Nguồn: Internet



(Paypers)

Entrust ra mắt máy phát hành thẻ ngay lập tức Sigma DS4

Entrust - tập đoàn hàng đầu thế giới trong lĩnh vực định danh đáng tin cậy, thanh toán và bảo vệ dữ liệu - vừa ra mắt máy in Sigma DS4 phục vụ giải pháp phát hành thẻ tài chính ngay lập tức. Với Sigma DS4, các ngân hàng, hiệp hội tín dụng và nhà bán lẻ có thể ngay lập tức phát hành thẻ tài chính phẳng và bảo mật. Sigma DS4 thiết lập tiêu chuẩn dành cho các đặc tính đơn giản, bảo mật và thông minh.

Sigma DS4 được thiết kế đặc biệt phù hợp với các môi trường đám mây ngày nay và có khả năng phát hành một cách dễ dàng những tấm thẻ tài chính bảo mật nhất thế giới. Với nhu cầu ngày càng lớn đối với các giải pháp công nghệ không tiếp xúc, hệ thống Sigma cho phép các ngân hàng và hiệp hội tín dụng dễ dàng phát hành và kích hoạt thẻ qua những dịch vụ "đến và mang đi", qua đó mang lại trải nghiệm người dùng tức thì và tiện lợi khi cần phát hành lại thẻ.

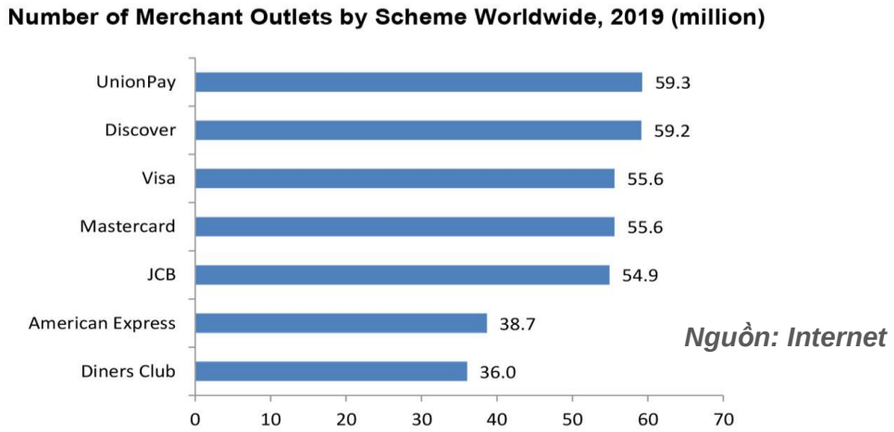
Sigma DS4 được xem là dòng máy in thẻ tài chính thân thiện nhất của Entrust với người dùng hiện nay. Với thiết kế bảng điều khiển trực quan, người dùng có thể xem trạng thái in, yêu cầu vật tư, kiểm tra trạng thái làm sạch, cập nhật firmware hoặc liên hệ trợ giúp hoàn toàn trên thiết bị di động.

Một số đặc điểm nổi bật của Sigma DS4:

- Đơn giản: Với mục tiêu hướng đến người dùng cuối, các giải pháp Sigma chú trọng đến trải nghiệm và khắc phục sự cố trực quan cho người dùng. Ngoài ra, máy in Sigma còn đi kèm với các thiết bị nâng cao như bộ vệ sinh và dụng cụ bảo vệ đầu in.
- Bảo mật: Máy in được xây dựng với các tính năng bảo mật hàng đầu như nền tảng module tin cậy, khởi động an toàn với khả năng mở rộng liền mạch đạt chứng chỉ PCI-CP.
- Thông minh: Thiết kế module hóa mang lại sự linh hoạt đặc biệt để đáp ứng mọi nhu cầu phát hành thẻ, trong đó có thiết kế nhiều khay đựng thẻ và các băng mực có thể tháo rời. Người dùng có thể dễ dàng truy cập và nâng cấp các module trong tương lai bởi Entrust liên tục nâng cấp công nghệ máy in thẻ để bàn./.

(AIThority)

RBR: 100 triệu người bán hàng chấp nhận thanh toán thẻ vào năm 2020



Nguồn: Internet

Source: Global Payment Cards Data and Forecasts to 2025 (RBR)

Nghiên cứu mới nhất từ RBR dự báo số lượng cửa hàng chấp nhận thanh toán thẻ trên toàn thế giới sẽ đạt gần 100 triệu vào cuối năm 2025.

Nghiên cứu cũng nhận định rằng số lượng các cửa hàng được thúc đẩy bởi các chính sách từ Chính phủ nhằm thúc đẩy thanh toán không dùng tiền mặt và chuyển sang thanh toán không tiếp xúc trong đại dịch Covid-19.

Thống kê "Dữ liệu thẻ thanh toán toàn cầu và dự báo đến năm 2025" do RBR thực hiện cho thấy số lượng cửa hàng bán lẻ chấp nhận thanh toán bằng thẻ trên toàn thế giới đã tăng 4% trong năm 2019, đạt 74,5 triệu và trong đó số lượng cửa hàng chấp nhận thanh toán bằng thẻ chỉ riêng ở Ấn Độ đã tăng 959.000, mở rộng thêm 40% so với trước đây.

“RBR dự báo số lượng cửa hàng chấp nhận thẻ trên toàn thế giới sẽ vẫn tiếp tục tăng trưởng mạnh, tăng từ 74,5 triệu vào cuối năm 2019 lên 95,9 triệu vào cuối năm 2025. Và phần lớn được thúc đẩy bởi các chính sách của chính phủ nhằm thúc đẩy thanh toán không dùng tiền mặt,” báo cáo cho biết.

Báo cáo cũng cho biết UnionPay đã vượt qua Discover với tư cách là chương trình thẻ được chấp nhận rộng rãi nhất trên toàn cầu, với 59,3 triệu đại lý chấp nhận thẻ UnionPay và 59,2 triệu chấp nhận thẻ Discover.

Visa và Mastercard đều được chấp nhận bởi 55,6 triệu cửa hàng trên toàn thế giới và vẫn là những chương trình thẻ được chấp nhận rộng rãi nhất bên ngoài Trung Quốc, chiếm 95% trên tổng số ở các quốc gia khác ngoài Trung Quốc./.

(NFCWord)

Europol phát hiện và ngăn chặn các cuộc tấn công gian lận thẻ trị giá 40 triệu EURO

Cơ quan điều tra Europol tuyên bố họ mới ngăn chặn được một vụ gian lận thất thoát trị giá khoảng 40 triệu EURO nhờ một cuộc theo dõi kéo dài 3 tháng nhằm vào các diễn đàn web đen.

Hoạt động điều tra này được Europol tổ chức dưới tên gọi Carding Action 2020, phối hợp giữa các cơ quan thực thi pháp luật từ Ý, Hungary, hỗ trợ cùng các cơ quan điều tra Anh và công ty tình báo về các mối đe dọa Group-IB.

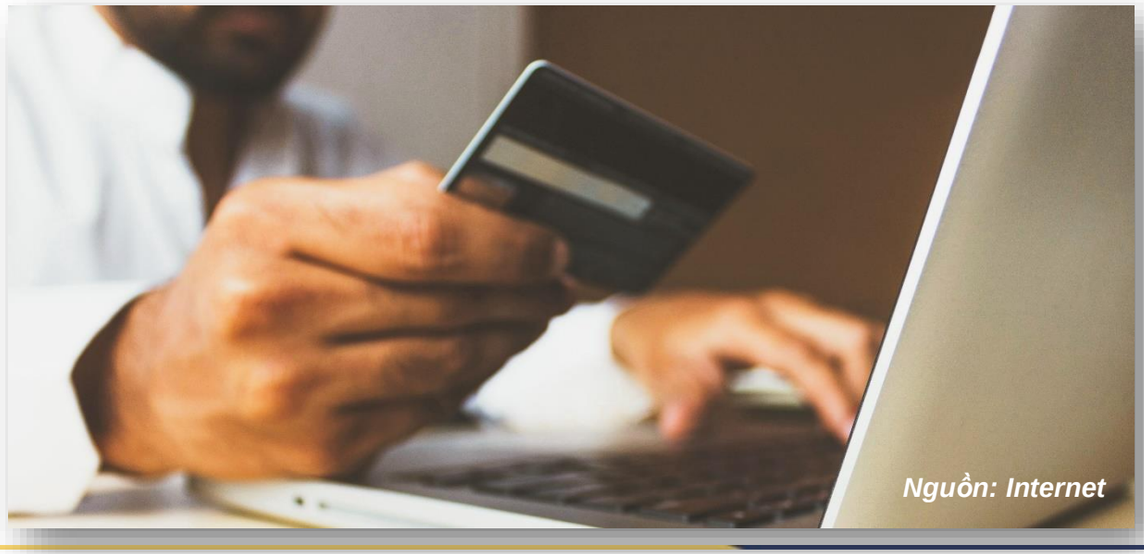
Group-IB đã cung cấp 90.000 dữ liệu thanh toán bị xâm phạm gần đây mà họ thu thập từ các nguồn không công khai, như tại cơ sở hạ tầng các bên cung cấp, cũng như các diễn đàn hay các khu chợ bán thẻ ngầm.

Tất cả các dữ liệu được thu thập này bao gồm dữ liệu thẻ bị xâm phạm thông qua các trang web lừa đảo, các thiết bị đầu cuối bị nhiễm trojan cũng như các trang web bị xâm phạm.

Europol sau đó đã tạo điều kiện phối hợp trao đổi giữa các cơ quan thực thi pháp luật từ Ý, Hungary, Anh và các chương trình thẻ. Tiếp đến, các Ngân hàng đã được cảnh báo từ các cơ quan chức năng và tiến hành ngăn chặn những vụ tấn công có ước tính trị giá khoảng 40 triệu EURO.

Edvardas Šileris, người đứng đầu Trung tâm tội phạm mạng châu Âu Europol, cho biết: "Với hơn 40 triệu EURO thiệt hại đã được ngăn chặn, Carding Action 2020 là một chuỗi hành động tuyệt vời thể hiện được giá trị khi chia sẻ dữ liệu giữa các ngành công nghiệp tư nhân và các cơ quan thực thi pháp luật là chìa khóa để chống lại các hành động gian lận điện tử và ngăn chặn hành vi đe dọa tới công dân EU"./.

(Finextra)



Nguồn: Internet

Doanh thu toàn cầu năm 2020 của công nghệ sinh trắc học vân tay giảm 22%

Theo một báo cáo mới đây của công ty tư vấn thị trường công nghệ ABI Research, doanh thu từ các thiết bị sinh trắc học trên toàn cầu dự kiến sụt giảm 22%, xuống còn 6,6 tỷ USD trước cuối năm nay.

Mức độ sụt giảm trên tương đương với 1,8 tỷ USD, song dữ liệu mới nhấn mạnh rằng kết quả này chỉ là tạm thời. Trên thực tế, báo cáo của ABI Research dự báo, thị trường sinh trắc học toàn cầu sẽ lấy lại đà tăng trưởng trong năm 2021, với doanh thu dự kiến đạt mức 40 tỷ USD vào năm 2025.

Chuyên gia phân tích an ninh số Dimitrios Pavlakis cho rằng, tình trạng suy giảm hiện tại của thị trường sinh trắc học có thể liên quan đến 3 vấn đề khác nhau, gồm: chính phủ, thương mại và công nghệ.

Ông Pavlakis nhận định: “Thứ nhất, các vấn đề này chủ yếu xuất phát từ những chương trình cải cách kinh tế trong thời kỳ khủng hoảng - buộc các chính phủ phải hạn chế ngân sách và tập trung vào công tác kiểm soát thiệt hại, phúc lợi xã hội và hiệu quả vận hành”. Nói cách khác, các chính phủ trên thế giới đã phải trì hoãn hoặc hủy bỏ nhiều ứng dụng dựa trên vân tay.

Lý do thứ hai liên quan đến các ứng dụng thương mại tại chỗ và kiểm soát truy cập, bởi số lượng nhân viên làm việc từ xa đã tăng lên đáng kể từ hồi đầu năm 2020.

“Cuối cùng, những lo ngại về vệ sinh do các công nghệ vân tay dựa trên tiếp xúc đã tác động đến doanh thu của lĩnh vực sinh trắc học, dẫn đến tình trạng sụt giảm đột ngột số lượng đơn hàng trên toàn thế giới”, ông Pavlakis bình luận thêm.

Tuy nhiên, nhà phân tích này khẳng định, đại dịch COVID-19 cũng đã thúc đẩy nhu cầu về các ứng dụng sinh trắc học mới. Trong đó, khả năng di động và kiểm soát truy cập - vốn sử dụng công nghệ sinh trắc học như một phần của xác thực đa yếu tố (MFA) dành cho đội ngũ nhân viên làm việc từ xa - có thể trở những thành biện pháp xác thực công nghệ thông tin thường xuyên trong thời gian dài.

Báo cáo dữ liệu thị trường “Công nghệ và Ứng dụng Sinh trắc học” của ABI Research cũng đề cập đến những ứng dụng sinh trắc học dành cho các thành phố thông minh.

Ông Pavlakis giải thích: “Các khoản đầu tư vào cơ sở hạ tầng thành phố thông minh trong tương lai sẽ tính đến hoạt động giám sát bổ sung, cũng như phân tích hành vi theo thời gian thực và nhận dạng khuôn mặt để phục vụ các nỗ lực nghiên cứu dịch tễ học, theo dõi và ứng phó khẩn cấp”./.

(Biometric Update)

PCI SSC chuẩn bị phát hành tiêu chuẩn bảo mật thanh toán nâng cao PCI DSS 4.0

Khi các xu hướng thanh toán mới nổi lên, chẳng hạn như sự tăng trưởng đột biến của thương mại điện tử trong đại dịch COVID-19, các tiêu chuẩn thẻ thanh toán cũng phải thay đổi.

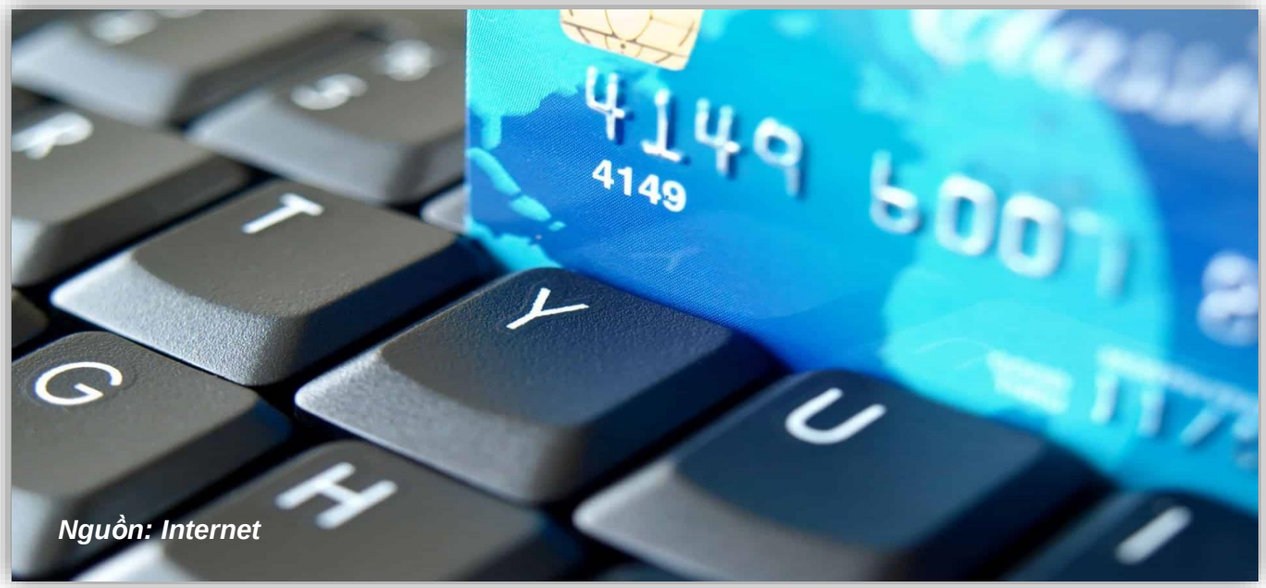
Hiện nay, Hội đồng Tiêu chuẩn Bảo mật PCI (PCI SSC) đang chuẩn bị phát hành phiên bản cập nhật quan trọng của Tiêu chuẩn Bảo mật Dữ liệu Lĩnh vực Thẻ thanh toán (PCI DSS) và sẽ bổ sung phiên bản này vào Khung Bảo mật Phần mềm - tài liệu được thiết kế để bảo vệ dữ liệu thẻ thanh toán một cách tốt hơn - của tổ chức.

Ông Jeremy King - Giám đốc quốc tế của PCI SSC - nhận định: “Các giao dịch thanh toán đang thay đổi nhanh chóng hơn bao giờ hết. Vì vậy, các chương trình của chúng tôi cũng thực sự cần phải thay đổi. Các tiêu chuẩn PCI không ngừng được nâng cao ngay cả trong đại dịch COVID-19 Do vậy, chúng tôi đã đưa ra một tiêu chuẩn mới với tên gọi là Khung Bảo mật Phần mềm”.

Theo ông King, PCI SSC đang chuẩn bị hoàn thiện PCI DSS phiên bản 4.0. Tài liệu chính hỗ trợ PCI DSS 4.0 dự kiến sẽ được phát hành vào giữa năm 2021, trong khi các tài liệu hỗ trợ khác sẽ được công bố trong năm 2022.

Tiêu chuẩn mới sẽ giải quyết hàng loạt vấn đề từ mã hóa dữ liệu chủ thẻ trên những hệ thống đáng tin cậy đến mở rộng sử dụng xác thực để phù hợp với các tiêu chuẩn do Viện Khoa học và Công nghệ Quốc gia Mỹ phát triển./.

(GovInfoSecurity)



Nguồn: Internet

Gian lận thẻ tín dụng Châu Âu gây thiệt hại 1,83 tỷ USD

Theo nghiên cứu của Buy Shares, tổng thiệt hại do gian lận thẻ gây ra ở châu Âu đã lên tới hơn 1,83 tỷ USD, trong đó, Anh chiếm 45,36% - tương đương với 706,9 triệu Euro (khoảng 833 triệu USD), đứng thứ 2 là Pháp với 440,9 triệu Euro (519 triệu USD).

Trong phần còn lại, Đức xếp ở vị trí thứ 3 với tổng mức thiệt hại 91,5 triệu Euro (108 triệu USD), trong khi Tây Ban Nha đứng sau với 90,6 triệu Euro (107 triệu USD), Italy đứng thứ 5 với 67,1 triệu Euro (79 triệu USD), và Romania chịu thiệt hại ít nhất với 2,9 triệu Euro (4 triệu USD).

Tại thị trường Anh, tính đến năm 2019, thẻ ghi nợ và thẻ tín dụng chịu thiệt hại lớn nhất, với tỷ lệ 76%; tiếp đến là thẻ bị đánh cắp hoặc bị mất chiếm 15%; đánh cắp thẻ định danh (ID) chiếm 6%; thẻ giả chiếm 2%; thẻ không được chuyển đến tay người nhận chiếm 1%.

Nghiên cứu của Buy Shares cũng chỉ rõ vai trò của các tổ chức thanh toán trong công tác kiềm chế vấn nạn gian lận thẻ./.

(ATMmarketplace)

12 chiến thuật và xu hướng phổ biến của tội phạm mạng trong năm 2020

Nguồn: Internet

Các cơ quan thực thi pháp luật vẫn coi những cuộc tấn công bằng phầm mềm đòi tiền chuộc (ransomware) là mối đe dọa nghiêm trọng nhất trên không gian mạng. Tuy vậy, phishing (lừa đảo bằng các trang web giả mạo), tấn công email doanh nghiệp và những hình thức gian lận khác - vốn có thể lợi dụng chủ đề đại dịch COVID-19 - cũng đang hiện hữu.

Nhận định trên được đưa ra trong báo cáo hàng năm lần thứ 7 mang tên "Đánh giá về mối đe dọa từ tội phạm có tổ chức trên mạng Internet" (IOCTA) do Trung tâm phòng, chống Tội phạm mạng châu Âu (EC3) - một đơn vị thuộc Cơ quan Cảnh sát châu Âu (Europol).

Báo cáo của EC3 đã liệt kê 12 chiến thuật và xu hướng phổ biến của tội phạm mạng trong năm 2020. Cụ thể như sau:

1. Tấn công email doanh nghiệp (BEC)

Hình thức tấn công này tiếp tục diễn biến phức tạp. Europol cảnh báo: "Giới tội phạm đang lựa chọn các mục tiêu một cách kỹ lưỡng hơn, chúng cho thấy sự hiểu biết sâu sắc về các quy trình hoạt động nội bộ và những điểm yếu của các hệ thống".

2. Chủ đề COVID-19

COVID-19 là chủ đề lớn nhất trong năm nay, vì vậy, giới lừa đảo, gian lận và những đối tượng khác chắc chắn không từ bỏ cơ hội này để kiếm chác.

Báo cáo viết: "Kẻ gian điều chỉnh những hình thức tội phạm mạng sẵn có để phù hợp với chủ đề đại dịch COVID-19, lợi dụng sự không rõ ràng của tình hình và nhu cầu của người dân về những thông tin đáng tin cậy. Trong nhiều trường hợp, COVID-19 đã gây ra sự thổi phồng về những vấn đề hiện tại, vốn trở nên phức tạp hơn bởi số lượng người làm việc ở nhà tăng lên đáng kể".

3. Hợp tác phạm tội

Một trong những mối lo ngại lớn nhất của các các cơ quan thực thi pháp luật về malware là những băng nhóm tội phạm sử dụng mã độc để liên kết với nhau.

EC3 cho biết: "Cả các quốc gia thành viên và khối tư nhân đều thông báo về sự gia tăng trong hoạt động trao đổi và hợp tác giữa các đối tượng tội phạm... Những điểm tương đồng trong cách thức hoạt động của 3 malware - gồm Ryuk ransomware, Trickbot và Emotet - cho thấy, giới tội phạm với nhiều phương thức tiếp cập tấn công khác nhau có thể thuộc về cùng một cấu trúc tổng thể hoặc chúng đang trở nên sáng suốt hơn khi hợp tác cùng nhau".

Một xu hướng tương tự cũng bị phát giác trong những băng nhóm sử dụng ransomware bởi chúng ngày càng "hợp tác với nhau trong lĩnh vực malware, cơ sở hạ tầng và các hoạt động rửa tiền".

Nguồn: Internet

4. Giới tội phạm vẫn ưa chuộng tiền ảo

Báo cáo IOCTA nhấn mạnh: "Các loại tiền ảo tiếp tục tạo điều kiện thuận lợi cho hoạt động thanh toán của các hình thức tội phạm mạng khác nhau, bởi các đồng tiền ảo đang tăng giá và bảo vệ cho họ sự riêng tư, bí mật".

Trái lại, các hoạt động trao đổi và các loại ví, nơi người dùng lưu trữ tiền ảo một cách hợp pháp, vẫn tiếp tục là những mục tiêu hàng đầu của kẻ gian.

5. Tấn công từ chối dịch vụ (DDoS)

Trong khi số lượng tổng thể của những cuộc tấn công DDoS đã giảm xuống trong thời gian gần đây, song một số cuộc tấn công cá nhân vẫn gây ra những sự gián đoạn trên diện rộng. Báo cáo của EC3 cho hay: "Các cơ quan thực thi pháp luật cũng điều tra hàng loạt vụ việc, khi các đối tượng tội phạm dính líu đến những cuộc tấn công có quy mô nhỏ nhằm vào các các tổ chức, tống tiền họ bằng cách đe dọa thực hiện những cuộc tấn công có quy mô lớn hơn".

Một xu hướng tấn công DDoS khác là nhằm vào các tổ chức nhỏ hơn, vốn ít có khả năng triển khai những hàng rào phòng thủ DDoS. Đây là những mục tiêu tương đối "dễ xơi" của các đối tượng tội phạm.

6. Malware "module hóa"

Trong những năm qua, các loại Trojan ngân hàng là công cụ yêu thích dành cho các đối tượng tội phạm muốn đánh cắp thông tin ngân hàng của người dùng cá nhân và vét sạch tài khoản của họ. Tuy nhiên, theo báo cáo IOCTA, "malware tinh vi hơn và được module hóa" - được thiết kế để mang lại cho kẻ gian nhiều khả năng lợi hại hơn - hiện được sử dụng phổ biến hơn. Đáng chú ý, malware Emotet hiện là kẻ thù số 1 đối với công chúng bởi những thiệt hại mà nó tiếp tục gây ra.

7. Gian lận trong các giao dịch thẻ vật lý không hiện diện (Card-not-present - CNP)

Báo cáo IOCTA nhận xét: "Gian lận CNP tiếp tục gia tăng bởi giới tội phạm đa dạng hóa các mục tiêu tấn công và hình thức skimming (sao chép thông tin tài khoản) điện tử - e-skimming. Nhờ nguồn dữ liệu phong phú luôn sẵn có và cộng đồng tội phạm mạng hoạt động dưới vỏ bọc hợp pháp, giới tội phạm hiện có điều kiện thuận lợi hơn để thực hiện những vụ tấn công có chủ đích ở mức độ cao", cũng như kiếm tiền tiền từ dữ liệu đánh cắp được, trong đó có thông tin thẻ thanh toán.

8. Lạm dụng trẻ em trên mạng trực tuyến

Đáng buồn là hoạt động phán tán trên mạng trực tuyến các thông tin lạm dụng tình dục trẻ em (CSAM), cũng như hoạt động sử dụng những thông tin này, đang tiếp tục gia tăng.

Europol nhấn mạnh: "Tương tự năm ngoái, số lượng CSAM trực tuyến bị phát hiện tiếp tục gia tăng, và tình trạng này diễn biến trầm trọng hơn do - cuộc khủng hoảng COVID-19 đã gây ra những hậu quả nghiêm trọng đối với năng lực điều tra của các cơ quan thực thi pháp luật".

Báo cáo IOCTA cho biết: "Philippines tiếp tục là nơi diễn ra tình trạng lạm dụng trẻ em từ xa trực tiếp (LDCA) nghiêm trọng nhất", số vụ việc LDCA tăng vọt do "các gia đình nghèo phải vật lộn mưu sinh và trẻ em không được tới trường". Bên cạnh đó, tình trạng LDCA phổ biến ở Romania cho thấy "mức độ livestream rất cao ở đất nước này, qua đó chứng tỏ EU cũng không thoát khỏi mối đe dọa đó".

9. Ransomware

Theo báo cáo IOCTA, ransomware vẫn là mối đe dọa phổ biến nhất khi giới tội phạm gia tăng sức ép bằng cách đe dọa công khai dữ liệu nếu các nạn nhân từ chối trả tiền. Mối đe dọa này đang được mở rộng trên toàn cầu. Những cuộc tấn công ransomware dường như ngày càng trở nên có chủ đích hơn và có thể nhanh chóng mở rộng tới các thành phố và thiết bị thông minh.

Tuy vậy, các nạn nhân cũng là một thách thức liên quan đến hình thức phạm tội này. Ông Philipp Amann - người đứng đầu bộ phận chiến lược của EC3 nhận định: "Khi đánh giá mức độ thiệt hại mà ransomware có thể gây ra, các nạn nhân dường như cũng ngần ngại thông báo cho các cơ quan thực thi pháp luật hoặc công luận khi họ gặp nạn, thực tế này gây ra khó khăn đối với nỗ lực xác định và điều tra về những vụ việc như vậy".

10. Tráo SIM (SIM Swapping)

Báo cáo IOCTA lần đầu tiên cho rằng SIM Swapping là một trong những xu hướng lớn, bởi vì thủ đoạn này đã gây ra "những thiệt hại nghiêm trọng" và cũng thu hút sự quan tâm lớn hơn của các cơ quan thực thi pháp luật.

Báo cáo của EC3 viết: "Tương tự hình thức tấn công phi kỹ thuật (social engineering attack) có chủ đích cao, SIM swapping có nguy cơ gây ra những hậu quả nghiêm trọng đối với các nạn nhân, bằng cách cho phép các đối tượng phạm tội qua mặt những biện pháp xác thực 2 nhân tố (2FA) dựa trên tin nhắn văn bản SMS để kiểm soát hoàn toàn những tài khoản nhạy cảm của các nạn nhân".

11. Tấn công theo kiểu SmiShing (kết hợp giữa SMS và phishing)

SMiShing - thuật ngữ được kết hợp giữa SMS và phishing - là thủ đoạn gửi các tin nhắn SMS lừa đảo, thường sao chép phương pháp của các ngân hàng. SmiShing là hình thức gian lận đang phát triển nhanh chóng, tương tự phishing, song người nhận có thể không nghi ngờ.

Báo cáo IOCTA nhận định: "Do phần lớn khách hàng của các ngân hàng luôn được khuyên nhủ đề cao cảnh giác trước email, nên mức độ nghi ngờ của họ đối với những tin nhắn lừa đảo không ở mức tương đương. Bên cạnh đó, các ngân hàng khó hoặc không có thể bảo vệ khách hàng trước những cuộc tấn công SmiShing, bởi giới tội phạm lợi dụng những lỗ hổng của Alpha Tag trong SMS và Signaling System 7 (SS7)".

12. Tấn công phi kỹ thuật và phishing

Báo cáo cho rằng, social engineering vẫn là một trong những mối đe dọa lớn nhất, đặc biệt là khi xảy ra những cuộc tấn công phishing. "Hiện nay, giới tội phạm mạng đang triển khai một chiến lược toàn diện hơn bằng cách chứng tỏ năng lực cao khi lợi dụng các công cụ, hệ thống và điểm yếu, sử dụng thông tin định danh giả mạo và hợp tác chặt chẽ với các tối tượng tội phạm mạng khác".

Báo cáo khẳng định: "Mặc dù xu hướng này cho thấy sự tinh vi ngày càng cao của một số đối tượng tội phạm, song phần lớn những cuộc tấn công social engineering và phishing được thực hiện một cách trót lọt do các biện pháp bảo mật yếu kém hoặc nhận thức không đầy đủ của người dùng"./.

(IronDefenseSecurity)

(84-24) 6266 2703 - 513 thegioithe@mkgroup.com.vn www.facebook.com/mkgroup1999

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