THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 103 | Tháng 4 - 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

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

MK Group tặng bảo hiểm sức khỏe Covid-19 cho cán bộ công nhân viên

Với mong muốn chủ động bảo vệ sức khỏe cho Cán bộ nhân viên (CBNV), góp phần đảm bảo chất lượng dịch vụ và phục vụ khách hàng được tốt nhất, Tập đoàn MK đã triển khai mua bảo hiểm Covid-19 cho toàn bộ CBNV của Tập đoàn.

Ngay khi đại dịch Covid-19 xuất hiện, MK Group cùng các thành viên đã lập tức triển khai các khuyến cáo của Bộ Y tế và các cơ quan chức năng như: trang bị khẩu trang y tế, dung dịch rửa tay sát khuẩn, dụng cụ đo thân nhiệt, tuyên truyền nâng cao nhận thức tới cán bộ công nhân viên … Ngoài ra, MK Group cũng thường xuyên trao đổi thông tin với các đối tác toàn cầu để chia sẻ thông tin và chủ động phối hợp xây dựng các kịch bản các phương án ứng phó nhằm bảo đảm hoạt động sản xuất kinh doanh và cung ứng sản phẩm – dịch vụ tới các khách hàng trong nước và quốc tế được diễn ra liên tục.

Bên cạnh đấy, MK Group cùng các công ty thành viên cũng đã có nhiều hoạt động hỗ trợ các Đối tác – Khách hàng trong nước vượt qua giai đoạn thách thức này, tiêu biểu như Công ty Cổ phần Thông minh MK (MK Smart), thành viên của MK Group đã triển khai Chương trình “Hỗ trợ dự phòng Phát hành – Cá thể hóa Thẻ tài chính ngân hàng” dành cho khối Tài chính – Ngân hàng với mong muốn giúp các Chương trình phát hành thẻ của các tổ chức này không bị gián đoạn.

Trong thời điểm đại dịch đang bùng phát hiện nay, ngoài việc đảm bảo hoạt động sản xuất kinh doanh ổn định, MK Group luôn chú trọng tới môi trường làm việc an toàn cũng như chăm lo sức khỏe của tất cả CBNV. Với việc mua bảo hiểm Covid-19 cho toàn bộ CBNV khối sản xuất và văn phòng trên cả nước, MK Group mong muốn tạo những điều kiện thuận lợi nhất để bảo vệ cán bộ nhân viên của mình, đồng thời góp phần chung tay cũng cộng đồng đẩy lùi dịch Covid-19.

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

Thanh toán không tiền mặt tăng mạnh mùa dịch

Theo thống kế từ NAPAS, từ Tết Nguyên đán đến giữa tháng 3/2020, tổng số lượng giao dịch thanh toán không dùng tiền mặt qua hệ thống này tăng 76%, tổng giá trị giao dịch tăng 124% so với cùng kỳ 2019.

Ngân hàng Nhà nước đưa ra nhiều khuyến nghị cùng với biện pháp "cách ly xã hội" của Chính phủ, người dân đang có xu hướng hạn chế sử dụng tiền mặt cho các giao dịch hàng ngày. Chính vì thế nên các hình thức thanh toán không tiền mặt như chuyển khoản, dùng thẻ tín dụng và ví điện tử đang lên ngôi.

Chia sẻ với VnExpress, một số đơn vị trung gian, công nghệ thanh toán cũng xác nhận sự gia tăng tích cực của số lượng thanh toán trực tuyến trong khoảng 2 tháng trở lại đây, tức thời điểm dịch bùng phát tại Việt Nam.

Tương tự, Visa cũng khẳng định, việc cách ly xã hội thời gian qua đã tạo ra sự thay đổi rõ rệt trong thói quen thanh toán của người dân. "Người tiêu dùng đã dần chuyển dịch nhiều hơn từ sử dụng tiền mặt sang các phương thức thanh toán điện tử khác để phục vụ cho nhu cầu mua sắm hàng ngày", bà Đặng Tuyết Dung, Giám đốc Visa tại Việt Nam và Lào, nhận xét.

Ngoài chuyển dịch chủ động từ người dùng, các thành phần trong hệ sinh thái thanh toán điện tử ở Việt Nam cũng rất nhanh nhạy chớp thời cơ để thổi bùng nhu cầu thanh toán trực tuyến. Cuối tháng 3, Visa đã công bố hợp tác cùng NextPay, đơn vị đang đặt mục tiêu sẽ phát triển 300.000 điểm chấp nhận thanh toán thẻ tại Việt Nam vào năm 2023.

Bà Đặng Tuyết Dung nhận định, Covid-19 đã mang lại cơ hội lớn cho các nền tảng thương mại điện tử. Các phương thức thanh toán mới cũng được thêm vào các nền tảng này để mang lại những trải nghiệm mua sắm tiện lợi nhất cho khách hàng.

"Tuy nhiên, sự tiện lợi này đôi khi cũng đi cùng những rủi ro giao dịch. Vì vậy, để đảm bảo an toàn khi thanh toán, người tiêu dùng nên nâng cao cảnh giác đối với tin tặc và các trang web độc hại để đề phòng các rủi ro liên quan đến bảo mật thông tin cá nhân", bà Dung khuyến cáo./.

(Vnexpress)

TIN VẮN THẺ NGÂN HÀNG

- **Từ đầu tháng 4 cho đến hết ngày 30/6/2020, Ngân hàng Standard Chartered** triển khai chương trình khuyến mại ưu đãi du lịch dành cho các chủ thẻ tín dụng Standard Chartered WorldMiles, bao gồm tặng quà khi mở thẻ lần đầu, hoàn tiền khi chi tiêu, bảo hiểm du lịch và bảo hiểm mua sắm giá trị cao cùng rất nhiều quà tặng ưu đãi khác.

- **Từ ngày 17/02/2020 đến hết ngày 30/04/2020, Ngân hàng Thương mại Cổ phần Quốc tế Việt Nam (VIB)** sẽ hoàn tiền lên đến 1,500,000 VNĐ dành cho các chủ thẻ mở mới thẻ tín dụng của VIB. Bên cạnh đó, VIB tặng kèm dung dịch rửa tay 500 ml cho tất cả các khách hàng đăng ký mở thẻ tín dụng trong suốt thời gian này.

- **Từ 21/03/2020 đến hết ngày 31/05/2020, Ngân hàng TMCP Kỹ thương Việt Nam (Techcombank)** sẽ triển khai gói ưu đãi “Cuối tuần siêu thị, hoàn tiền siêu vui” dành cho các chủ thẻ Techcombank Visa. Cụ thể vào thứ 7 cùng chủ nhật hàng tuần, các chủ thẻ khi mua sắm tại hệ thống Vinmart/Vinmart+ đều có thể nhận được ưu đãi hoàn tiền./.

(Tổng hợp từ Internet)

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

Người tiêu dùng Thổ Nhĩ Kỳ hạn chế sử dụng tiền mặt thời Covid-19

Sự bùng phát của đại dịch viêm đường hô hấp cấp COVID-19 đã khiến thêm nhiều người dân Thổ Nhĩ Kỳ tránh thanh toán bằng tiền mặt, và thay vào đó, họ lựa chọn sử dụng thẻ, đặc biệt là thẻ thanh toán không tiếp xúc (TTKTX), nhằm tránh nguy cơ lây lan virus SARS-CoV-2 trong cộng đồng, theo lãnh đạo Trung tâm thẻ InterBank (BKM).

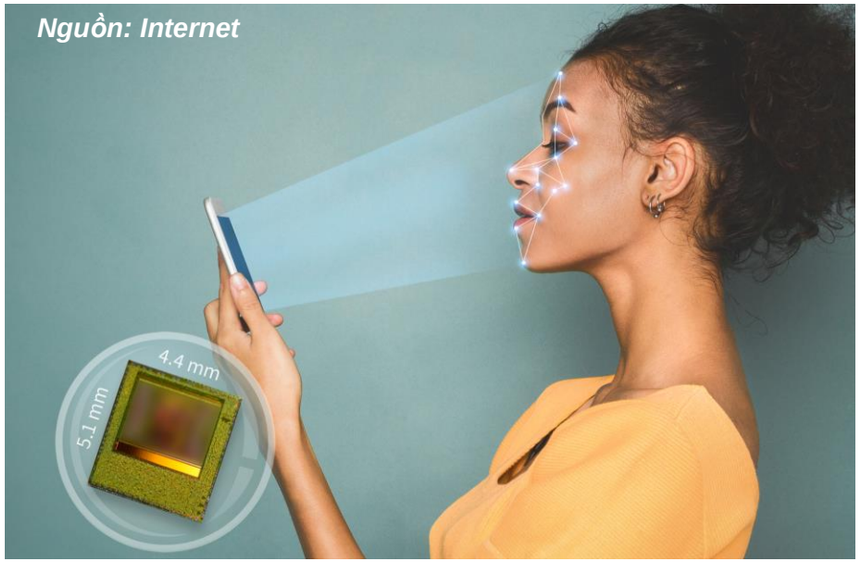
Nguồn: Internet

Soner Canko - Chủ tịch BKM - cho biết, tổ chức của ông đã nhận thấy sự thay đổi trong hành vi tiêu dùng của khách hàng sau khi phân tích dữ liệu giao dịch trong 11 ngày đầu tháng 3, khi mối lo ngại về tình trạng lây lan của virus SARS-CoV-2 tăng cao ở Thổ Nhĩ Kỳ. Theo ông Canko, khối lượng thanh toán thẻ được thực hiện trong khoảng thời gian này đã tăng 9% và tổng lượng TTKTX đạt 31 triệu giao dịch, cao hơn so với 30 triệu lượt trong cả năm 2015.

Trong khi đó, hoạt động mua sắm trực tuyến ở Thổ Nhĩ Kỳ cũng đang thực sự bùng nổ, bởi các cơ quan y tế nước này khuyến cáo người dân không đi đến những nơi công cộng tập trung đông người như các trung tâm thương mại. Cũng theo ông Canko, mua sắm trực tuyến tăng 4% trong 11 ngày đầu tháng 3 và chiếm gần 20% tổng lượng giao dịch thẻ./.

(Finextra)

Infineon và Qualcomm hợp tác ra mắt giải pháp tiêu chuẩn xác thực 3D



Infineon Technologies AG đã hợp tác với Qualcomm Technologies Inc. phát triển thiết kế tham chiếu dành cho xác thực 3D dựa trên Nền tảng Di động Qualcomm Snapdragon 865.

Theo đó, Infineon sẽ mở rộng danh mục ứng dụng công nghệ cảm biến 3D cho thiết bị di động. Mô hình tham chiếu sử dụng cảm biến 3D Time-of-Flight (ToF) REAL3 để mang lại một giải pháp hiệu quả về chi phí và dễ thiết kế dành cho các nhà sản xuất điện thoại thông minh (smartphone).

Công nghệ cảm biến 3D ToF của Infineon đã chứng minh được uy tín trên thị trường thiết bị di động trong suốt 4 năm qua. Tại sự kiện CES 2020 ở Las Vegas, công ty đã giới thiệu cảm biến hình ảnh 3D nhỏ nhất nhưng mạnh nhất thế giới (4,4 mm x 5,1 mm) với độ phân giải VGA. Cảm biến này đáp ứng những yêu cầu cao nhất về xác thực khuôn mặt, các tính năng ảnh nâng cao và trải nghiệm thực tế tăng cường.

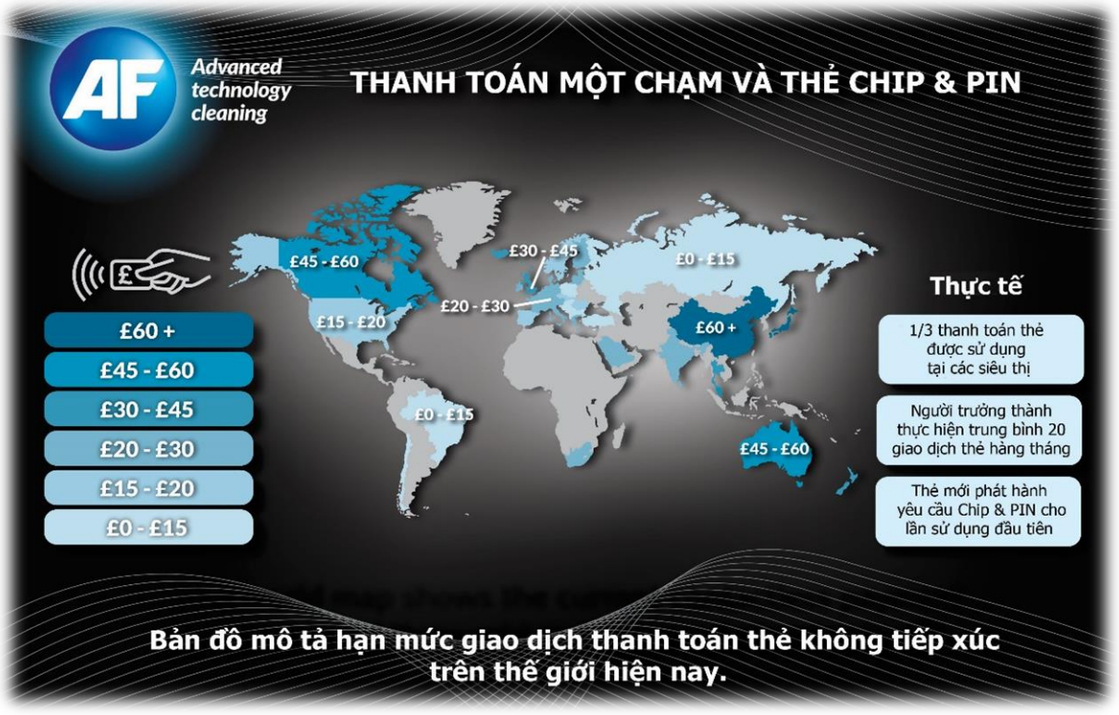
Ứng dụng 3D mới trên điện thoại thông minh 5G

Kể từ tháng 3/2020, cảm biến REAL3 ToF của Infineon đã cho phép quay video xóa phông lần đầu tiên trên smartphone 5G, tạo ra hiệu ứng hình ảnh tối ưu ngay cả với những hình ảnh chuyển động. Cảm biến hình ảnh 3D thu được ánh sáng hồng ngoại 940nm phản chiếu từ người dùng và các đối tượng được quét. Nó cũng sử dụng quy trình xử lý dữ liệu cấp cao để đạt được những phép đo độ sâu chính xác. Công nghệ SBI (Suppression of Background Illumination) được cấp bằng sáng chế giúp thiết bị hoạt động tốt trong hàng loạt môi trường ánh sáng khác nhau, từ ánh sáng mặt trời đến những căn phòng thiếu sáng. Khả năng này đảm bảo tốc độ xử lý mạnh mẽ nhất mà không làm giảm chất lượng xử lý dữ liệu./.

(Infineon)

29 quốc gia châu Âu nâng hạn mức giao dịch thanh toán không tiếp xúc

Các tổ chức thẻ lớn trong những tuần qua đã cam kết cho phép nâng hạn mức giao dịch thanh toán không tiếp xúc (TTKTX) trên toàn châu Âu.



Bản đồ mô tả hạn mức giao dịch thanh toán thẻ không tiếp xúc trên thế giới hiện nay.

Trên toàn Châu Âu, Mastercard đã ghi nhận sự gia tăng mạnh mẽ trong việc sử dụng thẻ TTKTX và thiết bị di động; 75% trong tổng khối lượng giao dịch Mastercard trên toàn châu Âu hiện là TTKTX. Chính sách nâng hạn mức trên sẽ cho phép các chủ thẻ và chủ cửa hàng sớm có thể thực hiện và nhận được thêm nhiều khoản thanh toán nhanh chóng và an toàn, mà không cần phải nhập mã PIN hay sử dụng tiền mặt.

Trong số 29 quốc gia châu Âu, Anh, Ireland, Estonia và Ba Lan đang dẫn đầu với những thay đổi lâu dài về hạn mức thanh toán, trong khi một số nước khác như Hà Lan và Hy Lạp lại chỉ điều chỉnh gia tăng tạm thời nhằm giúp người dân của họ mua sắm dễ dàng hơn trong khoảng thời gian khó khăn hiện nay./.

(Payments Cards & Mobile)

Phần Lan: Vận tải Helsinki bắt đầu triển khai thanh toán không tiếp xúc

Nguồn: Internet

Cơ quan quản lý giao thông vận tải khu vực Helsinki kể từ đầu tháng 3 đã bắt đầu triển khai phương thức thanh toán không tiếp xúc (TTKTX) EMV trong toàn mạng lưới đường sắt, xe buýt và phà của thành phố thủ đô Phần Lan.

Nhà cung cấp công nghệ LittlePay cho biết: "TTKTX sẽ được triển khai ngay lập tức, bắt đầu thử nghiệm cho tuyến phà của thành phố. Sau đó, chúng tôi sẽ áp dụng cho dịch vụ đường sắt và xe bus"./.

(NFCW)

New Zealand: Metlink không chấp nhận thanh toán tiền mặt trong giao thông công cộng do đại dịch COVID-19

Metlink, cơ quan vận tải tại khu vực Greater Wellington của New Zealand, đã ngừng chấp nhận thanh toán bằng tiền mặt trong toàn bộ hệ thống xe buýt, xe lửa, phà và nhà ga "để đi trước đại dịch COVID-19 một bước" và giúp hành khách và nhân viên cảm thấy yên tâm hơn. Động thái này là một phần của gói biện pháp mà Metlink đang giới thiệu.


Nguồn: Internet

Metlink khẳng định: "Những tấm vé này sẽ có sẵn từ các trạm có nhân viên và cũng cần phải mua bằng Eftpos. Chúng tôi hiểu rằng, việc chuyển từ tiền mặt sang Snapper là mới mẻ đối với một số ít khách hàng và chúng tôi sẽ hỗ trợ họ hết sức có thể. Vì vậy, từ ngày 23-30/3, bất kỳ hành khách nào lên xe buýt, mà không có thẻ Snapper, sẽ được cấp thẻ mới với giá trị nạp trước là 5 NZD"./.

(NFCW)

Ngân hàng Trung Ương Brazil ra mắt tiêu chuẩn mã QR quốc gia

Ngân hàng Trung ương Brazil (BACEN) cuối tháng 3 đã đưa ra tiêu chuẩn mới về mã QR quốc gia nhằm mở rộng phạm vi phủ sóng của dịch vụ thanh toán di động.

BACEN tuyên bố, mục đích của tiêu chuẩn mã QR quốc gia - được gọi là Mã BR - nhằm tạo ra một phương thức thanh toán phổ thông. Sáng kiến thiết lập một sự tiêu chuẩn hóa có thể so sánh được với những gì hiện có tại các thiết bị thanh toán thông thường. Những thiết bị đó sẵn sàng chấp nhận nhiều loại hình công nghệ thanh toán khác nhau, bao gồm thẻ, chip và nhãn, và cả thiết bị cầm tay.

Tiêu chuẩn mã QR quốc gia cũng sẽ cho phép sử dụng cùng một mã vạch cho nhiều mục đích khác nhau.

Thông tin trên chỉ là tuyên bố mới nhất trong hàng loạt tuyên bố của BACEN trong thời gian gần đây. Bên cạnh các quy định về mã phản hồi nhanh, BACEN cũng đã ra mắt nền tảng thanh toán ngay lập tức vào tháng 2/2020. Tất cả những bước triển khai này đều nằm trong một chương trình đổi mới có phạm vi rộng lớn hơn nhằm nâng cấp và làm mới toàn bộ hệ thống tài chính hiện thời của Brazil./.

(Paypers)

Nguồn: Internet

Tấn công giả mạo leo thang trong đại dịch COVID-19

Trong bối cảnh dịch bệnh viêm đường hô hấp cấp COVID-19 ngày càng diễn biến nghiêm trọng, các công ty bảo mật và lực lượng thực thi pháp luật, trong đó có Cục Điều tra Liên bang Mỹ (FBI), đang đưa ra những cảnh báo về tình trạng leo thang của nạn tấn công giả mạo (phishing) và những hành vi lừa đảo khác của giới tội phạm mạng nhằm vào lực lượng lao động phần lớn làm việc tại nhà.

Trong khi đó, các nhà nghiên cứu cũng phát hiện ra những kẻ tội phạm đang liên tục mạo danh các tổ chức cung cấp những thông tin cập nhật về đại dịch COVID-19 cho người dân. Chẳng hạn, IBM X-Force đã lật tẩy những email giả mạo gần đây lấy danh nghĩa của Tổ chức Y tế Thế giới (WHO) và khẳng định được chuyển trực tiếp từ Tổng Giám đốc WHO - Tiến sĩ Tedros Adhanom Ghebreyesus.

FBI hôm 20/3 đã đưa cảnh báo sau khi các đặc vụ của cơ quan này báo cáo về việc phát hiện những chiến dịch thư rác và giả mạo, trong đó sử dụng các biện pháp kích thích kinh tế của chính phủ làm mồi nhử. FBI cũng cảnh báo về những tin nhắn mạo danh Trung tâm Kiểm soát và Phòng ngừa Dịch bệnh Mỹ (CDC), mà những kẻ gian lận xảo quyệt đã sử dụng trước đó.

Cảnh báo của FBI nhấn mạnh: “Hãy chú ý những email giả mạo yêu cầu bạn xác thực thông tin cá nhân để nhận được một tấm séc kích thích kinh tế từ chính phủ... Mặc dù cuộc thảo luận về những tấm séc kích thích kinh tế đã và đang được truyền thông đưa tin, nhưng các cơ quan chính phủ sẽ không gửi các email tìm kiếm thông tin cá nhân của bạn để phục vụ mục đích chuyển tiền cho bạn”.

Ngay sau FBI, Bộ Tư pháp Mỹ ngày 22/3 đã buộc tội những người sở hữu một trang web mà cơ quan này cho là đã hứa hẹn một cách gian trá về quyền tiếp cận với những bộ công cụ thử nghiệm vaccine. Bộ trưởng Tư pháp William Barr đã cam kết về một chiến dịch trấn áp trên phạm vi toàn quốc đối với những trang web như vậy.

Đáng buồn thay, điều tương tự không xảy ra với những hình thức định danh khác, chẳng hạn như GPLX và thẻ an sinh xã hội. Vụ tấn công 11/9 đã khiến chính quyền Mỹ phải thực hiện những biện pháp nâng cao tính bảo mật của GPLX do mỗi tiểu bang cấp phát (trong trường hợp không có thẻ căn cước, GPLX do tiểu bang cấp là thẻ ID trên thực tế ở Mỹ), song các tiểu bang đã đấu tranh thành công để tránh những đặc tính bảo mật chung vì họ muốn giữ quyền tự chủ.

Không khó để có được những tấm thẻ định danh giả mạo trên web, trong đó có GPLX ở Mỹ. Có lẽ, những loại giấy tờ này đủ để lừa được một nhân viên pha chế rằng, bạn đủ tuổi để mua đồ uống có cồn, song khó vượt qua được sự kiểm tra của cảnh sát giao thông hoặc nhân viên kiểm soát nhập cư.

Mạo danh WHO

Trong những email mà các nhà nghiên cứu của IBM lật tẩy, kẻ gian đã sử dụng các thông điệp mạo danh từ WHO để phát tán phầm mềm độc hại (malware) HawkEye - một dạng keylogger phổ biến trong giới tội phạm mạng bởi những phiên bản mới hơn của loại malware này đã bị phát hiện hồi tháng 7/2019.

Trước đó, các nhà nghiên cứu của IBM hôm 19/3 đã bắt đầu nhận thấy những email giả mạo từ WHO với tên của Tiến sĩ Ghebreyesus. Những email này chứa một file đính kèm, có tên là Coronavirus Disease (Covid-19) CURE.exe - trong đó giấu một tập tin chạy ứng dụng “.NET”.

Theo báo cáo của IBM, file cài đặt đầu tiên tải về một tập tin chạy ứng dụng “.NET” thứ hai có khả năng tắt Windows Defender bằng cách thay đổi các khóa registry. Khi HawkEye được tải về, malware này cho phép những đối tượng tấn công chụp ảnh màn hình và thu thập dữ liệu từ các trình duyệt web và quản lý email như Mozilla, Postbox, Thunderbird, SeaMonkey, Flock, BlackHawk, CyberFox, KMeleon, IceCat, PaleMoon, IceDragon và WaterFox.

Đội ngũ nhân viên làm việc từ xa trở thành mục tiêu tấn công

Trong khi đó, công ty bảo mật AppRiver phát hiện, giới tội phạm mạng đang hướng mục tiêu vào các nhân viên làm việc tại nhà với những tin nhắn thông báo về các đồng nghiệp có kết quả xét nghiệm dương tính với virus SARS-CoV-2 trong tổ chức của họ. Các tin nhắn này chứa những tệp đính kèm độc hại, được ngụy trang như những giao thức mà tổ chức của họ đang sử dụng, cũng như một trang quảng cáo yêu cầu người nhận mở, đọc và in ra. Tuy nhiên, AppRiver không nêu rõ thông tin về thể loại malware mà kẻ gian sử dụng.

Những cảnh báo mới

Trước những rủi ro xuất phát từ các email giả mạo và những mối đe dọa trên không gian mạng khác nhằm vào đội ngũ nhân viên làm việc từ xa, các chuyên gia - trong đó có ông Tom Kellermann, người đứng đầu bộ phận chiến lược an ninh mạng của công ty VMWare Carbon Black - đã đưa ra những lời khuyên bổ ích.

Những lời khuyên của Kellermann đề cập đến điều mà ông gọi là “giữ khoảng cách số” - có nghĩa là các nhân viên cần phải duy trì máy tính làm việc của họ gắn chặt với một bộ định tuyến và hệ thống riêng biệt với bộ định tuyến trong nhà riêng của họ. Theo ông Kellermann, bộ định tuyến dành riêng cho công việc này cần được cập nhật và bảo vệ.

Bộ Quốc phòng Mỹ giữa tháng Ba đã cảnh báo các nhân viên quân sự và dân sự của cơ quan này cần phải thực hiện những biện pháp bảo mật nâ***ng cao để ngăn*** chặn những đối tượng tin tặc tiềm tàng./.

(*BankInfoSecurity)*

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

Làm việc từ xa và mối lo bảo mật dữ liệu

Làm việc từ xa(Remote working, teleworking, telecommuting) là tổ chức thực hiện công việc từ một địa điểm khác không phải là văn phòng công ty. Từ đó phát sinh ra các vấn đề bảo mật dữ liệu thông tin và hệ thống. Ba hạng mục cần được lên kế hoạch ngay là:

1. Đảm bảo an toàn máy móc thiết bị:

Làm việc tại nhà mang lại khả năng cơ động cao.Nhân viên có thể sử dụng nhiều thiết bị khác nhau như Desktop, Laptop, Smartphone, Tablet do công ty trang cấp. Nhân viên IT sẽ thực hiện cài đặt, cấu hình, bảo trì thường xuyên, trong khi Security manager có thể cài đặt các phần mềm bảo vệ ổ cứng(như Cryhod của Prim'X) một cách dễ dàng. Tuy nhiên nếu nhân viên sử dụng máy tính cá nhân, việc quản trị này sẽ gặp khó khăn hơn. Trong trường hợp này, bộ phận IT có thể cài đặt Mobile Device Management (MDM) giúp phân tách từ xa dữ liệu công ty cần bảo mật khỏi dữ liệu cá nhân, đồng thời quản lý dữ liệu này. Tuy nhiên việc cài đặt trên nhiều máy cùng một lúc sẽ đặt ra một số khó khăn. Một giải pháp là sử dụng các công cụ bảo vệ thiết bị End point trên nền tảng Cloud, cho phép hỗ trợ và quản lý của máy công ty và cá nhân. Thông qua một Dashboard, IT có thể cài đặt phần mềm An toàn thông tin trên các máy từ xa, đồng thời Security Manager triển khai Chính sách an ninh giúp tiết kiệm thời gian cho doanh nghiệp.

8 mẹo giúp bảo vệ Desktop và Laptop:

- Sử dụng đồng thời các phần mềm An ninh như Antivirus, Firewall cá nhân, lọc Spam và Web content, khóa Popup. và Cryhod (Prim'X) khóa ổ cứng chống đánh cắp.
- Hạn chế, cấp quyền truy cập vào thiết bị cho người dùng thông qua mật khẩu, khóa PKI. Nếu máy kết nối DC, có thể dùng ZoneCentral để truy cập và mã hóa dữ liệu.
- Đảm bảo cập nhật thường xuyên hệ điều hành và các ứng dụng cơ bản như Web browser, Email, Instant message client và các phần mềm an ninh khác.
- Dỡ các tính năng mạng không cần thiết trên PC và cài đặt mạng wireless một cách an toàn.
- Cấu hình các ứng dụng cơ bản nhằm lọc content và chặn các hoạt động khác vốn là nơi dễ bị tấn công.
- Chỉ cài đặt và sử dụng các phần mềm tin cậy
- Cấu hình từ xa các phần mềm theo yêu cầu và khuyến cáo của doanh nghiệp
- Duy trì an toàn cho PC bằng cách thay đổi mật khẩu thường xuyên và kiểm tra tình trạng phần mềm theo định kỳ.

8 mẹo an toàn cho thiết bị di động

- Hạn chế quyền truy cập vào thiết bị như cài mật khẩu, PIN, và tự động khóa thiết bị khi ở chế độ chờ.
- Bỏ các chế độ kết nối như Bluetooth, NFC(near field communication) trừ trường hợp khi cần thiết.
- Đảm bảo cập nhật thường xuyên các phần mềm An ninh theo tuần hoặc theo ngày
- Cài đặt các ứng dụng giúp bảo vệ thiết bị chống Malware
- Chỉ tải và chạy các ứng dụng bản quyền.
- Không bẻ khóa hoặc root thiết bị
- Không kết nối thiết bị với các điểm sạc lạ không an toàn
- Sử dụng môi trường làm việc riêng biệt, an toàn và được mã hóa do doanh nghiệp hỗ trợ và quản lý để truy cập dữ liệu và dịch vụ nhằm tối đa hóa khả năng bảo mật dữ liệu.
- Theo mẹo của NIST, kể cả bạn làm việc bằng máy tính cá nhân hay công ty, cần MÃ HÓA TOÀN BỘ Ổ CỨNG, giúp bảo vệ toàn bộ file, data, phần mềm và hệ điều hành.

Do tất cả các thiết bị đều sử dụng xác thực đa nhân tố (Multi factor authentication), nếu cài đặt phần mềm này sẽ giảm thiểu được kẻ tấn công đánh cắp dữ liệu.

2. An toàn truy cập từ xa:

Trước hết các nhân viên phải duy trì được khả năng truy cập từ xa khi làm việc tại nhà thông qua các kênh như Email, cũng như truy cập vào dữ liệu công ty và dữ liệu chia sẻ. Tìm giải pháp cho yêu cầu này không phải là việc dễ dàng. Một số biện pháp truyền thống có thể là đường truyền riêng VPNs, Desktop ảo hoặc truy cập Web cá nhân(Webmail). Dù vậy, các biện pháp này cũng đã tăng độ rủi ro lên một cấp độ mới. Dữ liệu tài chính, khách hàng và nhân viên có thể bị đánh cắp gây tổn hại uy tín và kinh doanh của doanh nghiệp. Tuy nhiên, việc mất dữ liệu không phải là vấn đề duy nhất mà quan trọng là toàn bộ hệ thống thông tin có thể gặp nguy hiểm nếu thiết bị không được bảo vệ an toàn. Ví dụ một User làm việc từ xa trên một máy ảo bị tấn công, virus có thể lây nhiễm lên Server tổng của doanh nghiệp. VPN's cũng không thực sự an toàn nếu từ End point sử dụng phương pháp truy cập không hợp lý sẽ tạo điều kiện cho Hacker tấn công thông qua conn đường này. Chúng ta nên sử dụng Remote Access Penetration Testing để đánh giá yếu điểm để sửa chữa.

3. Hướng dẫn bảo mật dữ liệu an toàn khi làm việc:

Nếu bạn chưa có Chính sách làm việc từ xa thì bạn cần phải xây dựng ngay Bản Qui định hướng dẫn các bước nhằm Bảo mật dữ liệu và hệ thống. Một vài hướng dẫn gợi ý như sau:

Bảo vệ thiết bị:

Chống mất cắp, không để thất lạc khi không làm việc ở nhà, màn hình phải luôn được khóa khi rời đi, các thành viên khác trong gia đình không nên sử dụng máy. Nhân viên phải chịu trách nhiệm đền bù thiệt hại nếu để mất thiết bị.

Bảo vệ dữ liệu trên máy:

Đảm bảo rằng nhân viên truyền dữ liệu an toàn. Nhân viên có khả năng sử dụng mạng wifi kém an toàn sẽ dễ bị tấn công hơn. Mạng công ty thường được bảo mật tốt hơn mạng gia đình. Các biện pháp đã triển khai cho công ty như Filter Proxy đến kiểm soat mạng cũng cần triển khai tại nhà.

Một lưu ý nữa là thông tin hệ thống có thể được lưu trên Cloud và truy cập xác thực đa nhân tố. Nếu cài đặt sử DLP(chống mất cắp dữ liệu), nhân viên của bạn có thể bị khóa không thể gửi các dữ liệu bảo mật tới một địa chỉ mail bên ngoài domain của công ty hoặc lên dịch vụ Cloud như Dropbox hay Google drive

Bảo vệ Email:

Luôn nhắc nhở nhân viên ý thức về việc đánh cắp thông tin và sai sót của con người chính là kẽ hở cho tấn công mạng. Nhân viên cần kiểm tra kỹ nội dung, địa chỉ trước khi ấn vào link hoặc bất cứ file đính kèm nào.

Kết luân: Việc ứng dụng tất cả các lưu ý nói trên vào Qui định làm việc từ xa (Remote work policy) sẽ giúp nhân viên bảo mật an toàn dữ liệu, hệ thống và hệ thống mạng của doanh nghiệp khi làm việc tại nhà. Đây có thể là một trở ngại đối với những tổ chức lần đầu áp dụng chính sách này. MK group có thể hỗ trợ doanh nghiệp của bạn với một số giải pháp bảo mật và mã hóa hệ thống cấp cao của Prim'X.

PRIMX

MAKE ENCRYPTION HAPPEN

CHỨNG CHỈ

Chúng tôi mong sẽ có cơ hội được trao đổi cụ thể nhằm xây dựng giải pháp hỗ trợ phù hợp với doanh nghiệp.

Mọi thông tin chi tiết xin vui lòng liên hệ đến email:
contact@mkgroup.com.vn

Từ giấy tờ đến số hóa:
Cuộc cách mạng trong lĩnh vực bảo mật tài liệu (Kỳ 2)

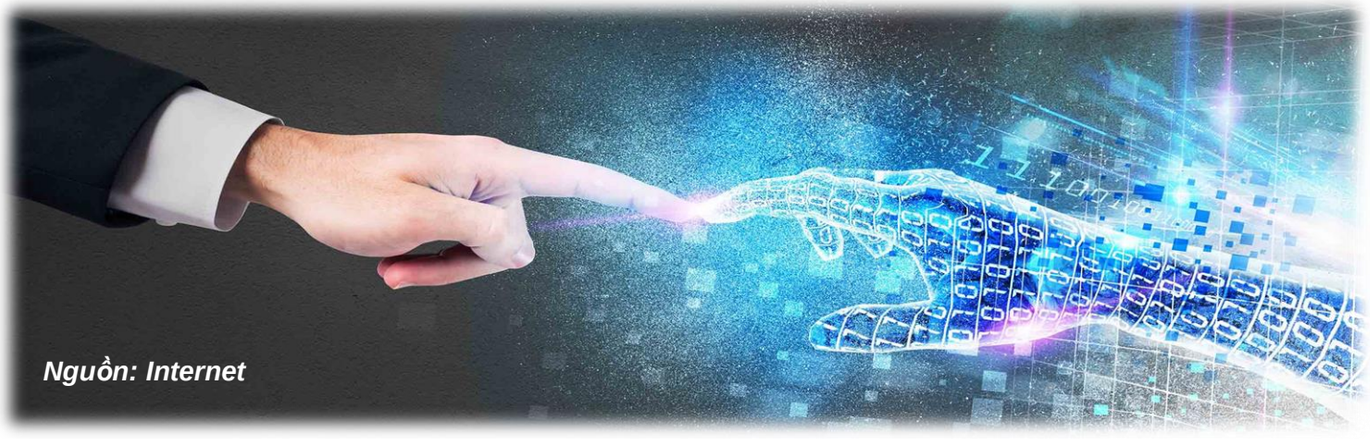
Phần 2: Hệ thống số và bảo mật dữ liệu

Liệu mức độ bảo mật mà những phương thức số hóa mang lại cho các giao dịch tài chính và xác thực danh tính có tương ứng với các phương pháp truyền thống có uy tín từ lâu dành cho giấy tờ truyền thống hay không? Nếu không, liệu có thể cải thiện những phương thức số hóa này không? Đây là những câu hỏi quan trọng trong xu hướng chuyển dịch từ thế giới vật lý sang thế giới số hiện nay.

Công nghệ - yếu tố thúc đẩy hệ thống số và định danh số

Động lực lớn nhất thúc đẩy sự phát triển của các hệ thống số chính là "công nghệ". Chẳng hạn, Apple mỗi năm đều ra mắt iPhone phiên bản mới; động thái tương tự cũng đến từ Samsung và các nhà sản xuất smartphone Android khác. Định luật Moore cho rằng, sức mạnh của bộ xử lý sẽ tăng gấp đôi sau mỗi năm, vì vậy, những chiếc smartphone mới được ra mắt vì chúng tốt hơn thế hệ tiền nhiệm. "Tốt hơn" có nghĩa là năng lực tính toán mạnh mẽ hơn, bộ nhớ lớn hơn, camera có độ phân giải cao hơn, màn hình có độ phân giải lớn hơn và cao hơn, cùng các tính năng và ứng dụng mới để tận dụng tất cả những cải tiến này. Chưa kể tốc độ của các mạng di động càng cao và độ phủ sóng wifi ngày càng rộng.

Lĩnh vực định danh số thậm chí còn non trẻ hơn. Sự phát triển của máy ảnh, bộ nhớ và tốc độ tốt hơn cho phép sử dụng smartphone để xác nhận danh tính của người mang giấy phép lái xe (GPLX) và thông tin định danh của công dân. Một số quốc gia và tiểu bang ở Mỹ đang phát triển và thử nghiệm GPLX và thẻ căn cước dựa trên ĐTDĐ, trong khi luật pháp Estonia cho phép sử dụng chữ ký số được mã hóa để thay thế cho chữ ký viết tay ngay từ tháng 12/2000.



Nguồn: Internet

Phân cấp bảo vệ hệ thống số

Trên thực tế, đã có nhiều minh chứng về những vụ trộm cắp tài chính và thông tin định danh trực tuyến. Những vụ việc này thường nghiêm trọng đến mức chúng được đưa tin trên các phương tiện truyền thông đại chúng, thay vì chỉ thông tin trong giới chuyên môn.

Điều đáng nói đây là các vụ đánh cắp hoặc tấn công lại nhằm vào những nơi lưu trữ dữ liệu của chúng ta. Những hệ thống trực tuyến nâng cao do liên quan đến hoạt động lưu trữ trong "đám mây", có nghĩa là một thực thể vô hình, không thể chạm được, và vì vậy không thể bị xâm nhập một cách bất hợp pháp. Tuy vậy, trên thực tế, dữ liệu của chúng ta được truyền tải qua Internet (thông qua những tuyến cáp và vệ tinh) đến các trung tâm máy chủ khổng lồ, các tòa nhà chứa hàng nghìn hoặc thậm chí hàng trăm nghìn máy chủ thực hiện và ghi lại các giao dịch hoặc danh tính của chúng ta. Những nguồn tài nguyên mang đậm tính vật lý này được bảo vệ tốt, với các bản sao lưu và dự phòng tích hợp, song những thí dụ trên cho thấy, chúng đã bị tấn công do các kết nối mạng Internet.

Các máy tính, kho lưu trữ dữ liệu và mạng kết nối trên cần được bảo vệ tương tự hệ thống phân cấp bảo vệ trong thế giới tài liệu vật lý, do đó, có rất nhiều lớp bảo vệ trong thế giới số. Mã băm, PKI (cơ sở hạ tầng khóa công khai), đăng nhập 2 yếu tố, SSI (nhận dạng tự chủ), các ứng dụng được mã hóa và trung tâm máy chủ được bảo vệ - tất cả những biện pháp này và nhiều biện pháp khác đều được triển khai để bảo vệ dữ liệu tài chính và danh tính của chúng ta trong lĩnh vực số.

Nguồn: Internet

Nguồn: Internet

Tuy nhiên, cần lưu ý rằng, tất cả các quy trình bảo mật trên đều hoạt động trong miền số, mà không có bất cứ sự tương tác nào với con người.

Có rất nhiều dự án hợp tác đang được triển khai nhằm thiết lập các tiêu chuẩn và hệ thống cải tiến để phục vụ mục đích bảo vệ dữ liệu, trong đó có dự án Olympus do Liên minh châu Âu (EU) tài trợ và tiêu chuẩn GPLX di động mới của ISO. Tất cả những dự án này cho thấy nhu cầu bảo mật trong miền số là thiết yếu, mặc dù động lực ban đầu có thể - và về mặt phần cứng, vẫn là - do công nghệ thúc đẩy.

Thế nhưng các hệ thống vẫn rất dễ bị tấn công và sai lệch, nguy cơ khiến các cơ quan kiểm soát biên giới sẽ phải cảnh giác. Các cơ quan này dự định sẽ đưa vào sử dụng lối đi nhận dạng bằng khuôn mặt, thay vì giấy tờ, từ lề đường đến máy bay dành cho những hành khách khởi hành, chẳng hạn như tại sân bay Changi của Singapore, sân bay Đại Hưng mới của Bắc Kinh và chương trình thí điểm của JetBlue tại sân bay Boston Logan. Tuy nhiên, không có sân bay nào trong số này sở hữu một hệ thống không dùng giấy tờ tương tự dành cho hành khách quốc tế đến, cũng như không có bất cứ kế hoạch nào để triển khai công nghệ vừa đề cập.

Trên thực tế, các cơ quan kiểm soát biên giới vẫn yêu cầu kiểm tra thông tin định danh đối với hành khách đến, để đảm bảo giấy tờ khớp với người mang, mặc dù hoạt động này thường được kiểm tra bằng máy thay vì kiểm tra bằng con người. Tuy vậy, ngay cả khi xác minh hộ chiếu và thẻ căn cước bằng máy tại sân bay, nếu xảy ra bất kỳ vấn đề nào, nhân viên kiểm soát nhập cư sẽ kiểm tra giấy tờ và khuôn mặt của người mang để đảm bảo những yếu tố này là trùng khớp và hợp pháp.

Giác quan của con người

Trong những hệ thống số đang được sử dụng để phục vụ các giao dịch tài chính hoặc thông tin nhận dạng, không có phạm vi kiểm tra bảo mật bằng con người; khi cảnh sát giao thông kiểm tra GPLX trên smartphone của tài xế, họ sẽ không thẩm vấn tính hợp pháp của giấy tờ đó - mà chỉ đơn giản xác nhận rằng tài xế có giấy phép hợp lệ hay không. Tương tự, khi một khách hàng sử dụng smartphone để thanh toán một món hàng nào đó trong cửa hàng, anh ta/chị ta, nhà bán lẻ hoặc ngân hàng đều không thể kiểm tra giao dịch; họ chỉ đơn giản là chứng kiến giao dịch đó được thực hiện.

Liệu chúng ta nên có một số tương tác của con người trong những hệ thống nói trên hay không? Có phải chúng ta thực sự quá tin tưởng, quá miễn cưỡng khi "nghi ngờ về sức mạnh của những thuật toán" xử lý các giao dịch và xác nhận danh tính này hay không?

Khi một người có kinh nghiệm kiểm tra một giấy tờ vật lý mà anh ta quen thuộc, anh ta sẽ thực hiện công tác đó không chỉ bằng giác quan mà còn bằng bộ não và trí nhớ của mình; anh ta rất thành thạo với giấy tờ và những đặc tính bảo mật của nó. Có lẽ, đây là một yếu tố góp phần chứng minh cho thực tế rằng: tỷ lệ USD giả cao hơn nhiều so với Euro giả, bởi có quá nhiều tờ USD được giao dịch bên ngoài nước Mỹ.

Có một chuỗi sinh lý thần kinh quan trọng thiết lập mối liên kết giữa mắt (nhìn) và bộ não (tâm trí) để dẫn đến nhận thức của chúng ta. Hermann von Helmholtz (1821-1894) là người đầu tiên nghiên cứu thực nghiệm về sinh lý học của nhận thức; ông được nhắc đến trong cuốn sách nổi tiếng "Eye and Brain" (Mắt và Não) của Richard L Gregory (1923-2010). Cuốn sách mô tả cách chúng ta cảm nhận khi sử dụng 2 cơ quan này. Trong khi đó, Magdelen D Vernon (1901-1991) đã khẳng định rõ ràng trong cuốn "Tâm lý học về Nhận thức" rằng, "nhìn không giống như nhận thức; cần có sự tham gia của tâm trí để nhìn rồi sau đó mới nhận thức được."

Điều ngược lại xảy ra khi chúng ta sử dụng smartphone làm "giấy tờ bảo mật"; chúng ta tin tưởng, chúng ta thảnh thơi, chúng ta không chú ý đến những gì đang diễn ra "ở phía sau". Do đó, chúng ta khiến bản thân dễ bị tổn thương trước những kẻ sẽ làm hại chúng ta bằng cách đánh cắp danh tính hoặc tiền của chúng ta./.

Mời Quý Độc giả đón đọc "Phần cuối: Bảo mật tài chính và xác thực" tại eTGT #104 tháng 4.

Nguồn: Internet

(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