

THẾ GIỚI THỂ

Bản tin nội bộ của MK Group

Số 159 | tháng 07.2024



TIN NỔI BẬT

- | | | | |
|----|--|----|--|
| 02 | MK SMART ĐẠT CHỨNG CHỈ ISO 14298 VÀ INTERGRAF 15374 | 07 | ENTRUST: GIAN LẬN DANH TÍNH KHÔNG PHÂN BIỆT ĐỐI XỬ |
| 03 | MK GROUP - MK SMART THAM GIA CASHLESS DAY 2024 | 12 | LUẬT CẢN CƯỚC: TẠO THUẬN LỢI TỐI ĐA CHO NGƯỜI DÂN |
| 04 | QUYẾT ĐỊNH 2345/QĐ-NHNN: CHỐT CHẶN QUAN TRỌNG GIÚP BẢO VỆ TÀI SẢN CỦA KHÁCH HÀNG | 13 | THỰC TRẠNG TẤN CÔNG RANSOMWARE NĂM 2024 |



MK Smart đạt chứng chỉ ISO 14298 và INTERGRAF 15374

Ngày 3/6/2024, MK Smart – thành viên của MK Group đã đạt chứng chỉ ISO 14298 – Government Level Quản lý quy trình in ấn bảo mật và chứng chỉ INTERGRAF 15374 – Secure Supplier về Hệ thống quản lý an ninh dành cho nhà cung cấp trong ngành in ấn bảo mật của Tổ chức INTERGRAF, EU.

Tiêu chuẩn quốc tế ISO 14298 là tiêu chuẩn cao nhất dành cho hoạt động Quản lý quy trình in ấn bảo mật để phân phối an toàn, đặc biệt là các tài liệu nhận dạng. Tiêu chuẩn INTERGRAF 15374 quy định cụ thể các yêu cầu đối với nhà cung cấp sản phẩm có tính năng bảo mật hoặc đối với nhà cung cấp dịch vụ đảm bảo tính bảo mật vật lý của ấn phẩm do công ty in bảo mật sản xuất.

Việc đạt được 2 chứng nhận ISO 14298 và INTERGRAF 15374 này góp phần đã khẳng định những nỗ lực và cam kết của MK Smart nói riêng và MK Group nói chung trong việc:

- **Nâng cao tính bảo mật:** Việc đạt được chứng chỉ thể hiện MK Smart đã thực hiện thành công những cải tiến và nâng cấp các quy trình sản xuất, quản lý thông tin và toàn bộ chuỗi cung ứng liên quan đến in ấn bảo mật. Điều này giúp ngăn chặn việc giả mạo, làm giả và thay đổi các tài liệu nhạy cảm như hộ chiếu, thẻ e-ID và các tài liệu bảo an khác.
- **Cải tiến chất lượng:** Các chứng chỉ cũng sẽ giúp thúc đẩy các hoạt động in ấn luôn được sắp xếp hợp lý và an toàn, giảm thiểu lỗi và đảm bảo chất lượng ổn định.
- **Tăng sự tin cậy của khách hàng:** Việc tuân thủ theo các quy định của hai chứng nhận giúp tăng tính xác thực, bảo mật và tính toàn vẹn cho các tài liệu của các khách hàng khi được sản xuất tại MK Smart.

Là đối tác sản xuất thẻ thông minh và tài liệu bảo an hàng đầu khu vực, MK Smart tự hào luôn không ngừng hoàn thiện và cải tiến các quy trình quản lý – sản xuất, tăng năng suất và chất lượng các sản phẩm giải pháp cung cấp cho thị trường, đảm bảo tuân thủ các tiêu chuẩn cao nhất về bảo mật của các tổ chức trong nước và quốc tế.

Về Intergraf:

Intergraf là Hiệp hội ngành in ấn châu Âu, đại diện cho các công ty hoạt động trong lĩnh vực đồ họa. Intergraf bao gồm 22 thành viên chính thức – là các hiệp hội in ấn quốc gia đến từ 21 quốc gia và 13 thành viên liên kết – là các công ty đến từ khắp Châu Âu. Intergraf có vai trò đại diện cho ngành in ấn Châu Âu, đảm bảo môi trường pháp lý tốt nhất ở cấp EU cho các công ty in ấn.



MK GROUP - MK SMART THAM GIA CASHLESS DAY 2024

Từ ngày 14 - 16.06.2024 tại Phố đi bộ Nguyễn Huệ, Quận 1, Tp. Hồ Chí Minh đã diễn ra Lễ hội Không tiền mặt 2024 với chủ đề “BẬT KHÓA AN TOÀN - MỞ ĐA TIỆN ÍCH” do Báo Tuổi Trẻ, Sở Công Thương TP. HCM, Cục Công nghệ Thông tin, Vụ Thanh toán và Vụ Truyền thông - Ngân hàng Nhà nước phối hợp tổ chức

Trong khuôn khổ sự kiện, MK Group đã mang đến một gian hàng trưng bày và giới thiệu các sản phẩm tại sự kiện năm nay với các giải pháp thanh toán tiên tiến như: Thiết bị đeo tích hợp tính năng thanh toán NFC (nhẫn, vòng tay...), thẻ thanh toán bằng vật liệu tái chế, các đầu đọc eID và sinh trắc học do MK nghiên cứu sản xuất. Đặc biệt, là combo “Thiết bị phát hành thẻ 1 trạm lưu động Entrust, Mỹ và phương thức e-KYC khách hàng với Giải pháp xác thực định danh khách hàng bằng Căn cước công dân gắn chip MK eID, đang là tâm điểm trong các sự kiện chuyển đổi số hiện nay. Ngoài ra, MK cũng tổ chức một ổ mini game dành cho khách hàng trải nghiệm giải pháp và chụp ảnh lưu niệm cùng các sản phẩm của MK Group.



Một số hình ảnh của MK Group - MK Smart tại sự kiện LỄ HỘI KHÔNG TIỀN MẶT - CASHLESS DAY 2024 tại Tp. Hồ Chí Minh

QUYẾT ĐỊNH 2345/QĐ-NHNN: CHỐT CHẶN QUAN TRỌNG GIÚP BẢO VỆ TÀI SẢN CỦA KHÁCH HÀNG

Từ ngày 1/7/2024, Quyết định 2345/QĐ-NHNN về việc triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng sẽ chính thức được áp dụng. Theo các chuyên gia, đây là bước tiến quan trọng của ngành Ngân hàng trong nỗ lực ngăn chặn tội phạm lừa đảo và bảo vệ tài sản của khách hàng.

Quyết định số 2345 được coi là một “cú hích” thúc đẩy toàn bộ hệ thống ngân hàng phải nghiêm túc hơn nữa trong việc xây dựng “tường lửa” bảo mật kiên cố bằng dữ liệu sinh trắc học.

Tại quyết định, Ngân hàng Nhà nước (NHNN) yêu cầu các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán căn cứ phân loại giao dịch để triển khai áp dụng các biện pháp triển khai áp dụng biện pháp xác thực sinh trắc học cho một số loại giao dịch trong thanh toán trực tuyến trên Internet (Internet Banking, Mobile Banking).

Theo các chuyên gia, xác thực bằng sinh trắc học có thể hạn chế tối đa khả năng làm giả và có tính bảo mật cao nhất hiện nay. Giải pháp này cho phép cơ quan quản lý, tổ chức cung cấp dịch vụ xác định được chính xác chủ tài khoản, người thực hiện giao dịch, người thụ hưởng. Từ đó góp phần nâng cao hơn nữa hiệu quả công tác phòng chống tội phạm sử dụng công nghệ cao trên không gian mạng.

13.900 vụ tấn công gây thiệt hại 390.000 tỷ đồng

Tại Việt Nam, các đối tượng tội phạm mạng trong và ngoài nước liên tục thay đổi phương thức, thủ đoạn, triệt để lợi dụng công nghệ mới để tấn công, xâm nhập, lừa đảo quy mô lớn, gây thiệt hại lớn về kinh tế và ảnh hưởng xấu đến trật tự an toàn xã hội.

Đặc biệt, tội phạm tấn công vào hệ thống công nghệ thông tin và lừa đảo chiếm đoạt tài sản trên không gian mạng trong lĩnh vực tài chính, ngân hàng đang là mối nguy cơ tiềm ẩn nhiều rủi ro cho an ninh tài chính, tiền tệ; gây thiệt hại lớn về tài sản và bức xúc trong quần chúng nhân dân.

Những đối tượng này thường trú chân tại địa bàn các quốc gia láng giềng như Campuchia, Myanmar...; các đối tượng cầm đầu thường là người nước ngoài. Ngoài ra, việc người dùng mạng xã hội thiếu cảnh giác trước phương thức, thủ đoạn tinh vi trên không gian mạng cũng là nguyên nhân làm gia tăng các vụ lừa đảo qua mạng.

Trong năm 2023, Cổng cảnh báo an toàn thông tin Việt Nam ghi nhận khoảng 13.900 vụ tấn công mạng vào các cơ quan, tổ chức, doanh nghiệp; gần 16.000 phản ánh lừa đảo trực tuyến, gây thiệt hại hơn 390.000 tỷ đồng (tương đương 3,6% GDP); tổng số tiền người dân bị các đối tượng lừa đảo trên mạng khoảng 8.000 - 10.000 tỷ đồng, tăng gấp rưỡi so với năm 2022. Trong đó có 91% thông tin liên quan lĩnh vực tài chính. Tỷ lệ người dùng thiết bị di động, mạng xã hội... nhận tin nhắn, cuộc gọi lừa đảo trực tuyến là 73%.

Thiếu tướng Nguyễn Văn Giang
Phó Cục trưởng Cục An ninh mạng và phòng
chống tội phạm sử dụng công nghệ cao,
Bộ Công an (A05)

An ninh, an toàn thông tin là điều kiện trọng yếu của ngành Ngân hàng

Ngành Ngân hàng coi an ninh bảo mật là điều kiện trọng yếu. Ngân hàng Nhà nước (NHNN) xác định bảo đảm an ninh, an toàn thông tin là một trong những trụ cột chính trong chiến lược phát triển công nghệ thông tin, hiện đại hóa, thúc đẩy sự phát triển bền vững của ngành ngân hàng.

Trước thực trạng tội phạm mạng ngày càng gia tăng, ngành Ngân hàng đã tích cực thực hiện nhiều công tác phòng, chống lừa đảo trên không gian mạng. Trong những năm qua, NHNN đã ban hành nhiều văn bản quy phạm pháp luật, văn bản chỉ đạo, hướng dẫn về bảo đảm an toàn thông tin và hoạt động liên tục của các hệ thống thông tin. Đồng thời, NHNN cũng phối hợp với lực lượng công an tăng cường công tác kiểm tra chuyên đề về công tác bảo đảm an ninh, an toàn các hệ thống thông tin quan trọng tại các tổ chức tín dụng, trung gian thanh toán.

Đặc biệt, Quyết định 2345/QĐ-NHNN về việc triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng được các chuyên gia đánh giá là bước tiến lớn, có ý nghĩa thiết thực và bắt buộc phải làm.

Ông Phạm Tiến Dũng, Phó Thống đốc NHNN nhấn mạnh 3 ý nghĩa quan trọng của Quyết định 2345: *Thứ nhất, nếu chẳng may các đơn vị bị lấy mất thông tin của khách hàng, khi áp dụng quyết định 2345, kẻ gian không thể thực hiện được giao dịch, vì lúc này không chỉ yêu cầu về OTP mà còn bắt buộc phải xác thực khuôn mặt. Do kẻ gian không có xác thực khuôn mặt nên không thể so sánh với khuôn mặt trên hồ sơ gốc của ngân hàng, chính vì thế không thể thực hiện được lệnh chuyển tiền.*

Thứ hai, khi chiếm đoạt thông tin khách hàng, kẻ gian thường cài đặt sang một máy khác để thực hiện hành vi chiếm đoạt tài sản. Nhưng khi chúng thực hiện bước chuyển sang máy khác, các ngân hàng sẽ yêu cầu xác thực sinh trắc học để cài đặt ứng dụng, kẻ gian sẽ không thực hiện được.

Thứ ba, khi thực hiện giao dịch chủ tài khoản phải vào xác thực khuôn mặt, vì thế người đi thuê tài khoản không thể sử dụng được tài khoản cho thuê.

Nói về trải nghiệm khách hàng khi thực hiện Quyết định 2345, Phó Thống đốc Phạm Tiến Dũng khẳng định việc yêu cầu xác thực đối với giao dịch từ 10 triệu đồng trở lên sẽ không làm gián đoạn trải nghiệm của khách hàng khi giao dịch.

Theo thống kê của Ngân hàng Nhà nước, giao dịch 10 triệu đồng trở lên chỉ chiếm 11% giao dịch và nhiều trường hợp một người thực hiện nhiều giao dịch nên tổng số người giao dịch hạn mức này không đến 10%. Tổng số người có giao dịch trên 20 triệu trong 1 ngày chỉ 0,56%.

Đồng thời khi thực hiện giao dịch đến mức 20 triệu đồng đã xác thực sinh trắc học, thì các giao dịch từ 100.000 đồng tiếp theo sẽ không phải thực hiện bước này nữa, cho đến khi số tiền giao dịch lên đến 20 triệu đồng tiếp theo.



Các ngân hàng nhanh chóng và quyết liệt triển khai Quyết định 2345/QĐ- NHNN

Nhằm đáp ứng yêu cầu của Quyết định 2345, các tổ chức tín dụng và trung gian thanh toán đã nhanh chóng, khẩn trương thực hiện xây dựng cơ sở dữ liệu sinh trắc học được kiểm tra chéo với dữ liệu trong chip thẻ căn cước công dân của khách hàng do cơ quan Công an cấp.

Theo cập nhật của báo VnEconomy, dù là chủ nhật (30/6) nhưng nhiều ngân hàng vẫn huy động lực lượng cán bộ có mặt tại các quầy kệ, điểm giao dịch để cài đặt nhận diện sinh trắc học cho các khách hàng hạn chế tiếp cận công nghệ. Hoạt động này nhằm thực hiện Quyết định số 2345/QĐ-NHNN ngày 18/12/2023 (Quyết định 2345) về triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng có hiệu lực từ 1/7/2024.

Tiêu biểu có nhiều ngân hàng đã gần như áp dụng toàn bộ Quyết định 2345 cho tất cả khách hàng của mình trước ngày có hiệu lực hoặc chủ động triển khai đầy đủ các giải pháp đảm bảo an toàn bảo mật thông tin trong thanh toán trực tuyến và thanh toán thẻ ngân hàng như TPBank, Agribank, Vietcombank, MB, ACB, MSB, SHB...

Bên cạnh đó, các ngân hàng cũng nỗ lực và tích cực phối hợp với những tổ chức, doanh nghiệp được Bộ Công an (C06) cấp phép để triển khai các giải pháp giải pháp xác thực, định danh khách hàng qua căn cước công dân (CCCD) gắn chip, thu thập dữ liệu sinh trắc học của khách hàng theo Quyết định số 2345/QĐ-NHNN về triển khai các giải pháp an toàn, bảo mật trong thanh toán trực tuyến và thanh toán thẻ ngân hàng.

Ngoài ra, có một số ngân hàng cũng phối hợp với Trung tâm Nghiên cứu, ứng dụng dữ liệu dân cư và căn cước công dân (RAR) (trực thuộc Bộ Công an) cho phép khách hàng có thể cập nhật thông tin sinh trắc học trực tuyến thông qua giải pháp kết nối trực tiếp từ ứng dụng VNeID của Bộ Công an với ứng dụng mobile banking của ngân hàng.

Theo thống kê, tính đến 17 giờ ngày 3/7, có 16,6 triệu tài khoản khách hàng đã được các ngân hàng đối chiếu với dữ liệu sinh trắc học của Bộ Công an. Theo Phó Thống đốc, con số này tương đương bằng cả 1 năm ngành Ngân hàng mở tài khoản cho khách hàng.

Về cơ bản, đa số người có tài khoản có thể xác thực được qua điện thoại có NFC (viết tắt của Near-Field Communication - chuẩn kết nối không dây trong phạm vi tầm gần). Số ít có vướng mắc và được các ngân hàng hỗ trợ tại quầy. Hiện có ngân hàng đã làm xong xác thực 2,6 triệu tài khoản khách hàng.

Theo Thời báo Ngân hàng

Theo ý kiến của nhiều chuyên gia, Quyết định số 2345/QĐ-NHNN là giải pháp công nghệ đột phá đối với công tác an ninh, an toàn trong giao dịch trực tuyến, trong bối cảnh tội phạm công nghệ cao ngày càng diễn biến phức tạp với nhiều thủ đoạn lừa đảo tinh vi, đặc biệt là thao túng tâm lý.

Quyết định 2345: “Chiến dịch lớn” để bảo vệ khách hàng

Tại Hội thảo “Giải pháp bảo vệ khách hàng sử dụng dịch vụ ngân hàng” do Ngân hàng Nhà nước tổ chức sáng ngày 4/7, Phó Thống đốc NHNN Phạm Tiến Dũng khẳng định, xác thực sinh trắc học là thêm 1 lớp bảo vệ nữa, ngân hàng không bỏ một bước bảo mật nào, nên chỉ an toàn hơn cho khách hàng. Đây là một “chiến dịch lớn”, là điều bắt buộc phải làm, không thể khác được.

Bên cạnh đấy, Quyết định 2345 giải quyết 2 điểm quan trọng, đó là chấm dứt tình trạng mở tài khoản bằng giấy tờ giả; hai là xóa bỏ việc mở tài khoản bằng giấy tờ thật nhưng không phải chính chủ người đó mở. Việc xác thực sinh trắc học theo yêu cầu của Quyết định 2345 sẽ xác định đúng tài khoản, đúng người có căn cước công dân được Bộ Công an cấp.

“Bản chất của Quyết định 2345 là làm sạch tài khoản, loại bỏ các tài khoản sử dụng giấy tờ giả, loại bỏ tài khoản không chính chủ”, Phó Thống đốc khẳng định. Đồng thời, việc thực hiện xác thực sinh trắc học là cần thiết, thêm 1 lớp bảo vệ nên chắc chắn là an toàn hơn. Trường hợp khách hàng có làm mất giấy tờ, bị kẻ xấu mang đến ngân hàng giả mạo để lừa đảo tiền cũng khó thực hiện vì có sinh trắc học khuôn mặt để xác nhận chính chủ hay không.

Thời gian tới, nhằm thúc đẩy, tăng cường bảo đảm an ninh, an toàn, bảo mật cho dịch vụ ngân hàng trên không gian mạng theo chủ trương của Đảng và Chính phủ, góp phần bảo vệ khách hàng sử dụng dịch vụ tài chính - ngân hàng, NHNN tiếp tục nghiên cứu, hoàn thiện, ban hành kịp thời các văn bản, Thông tư thay thế, sửa đổi, bổ sung về quy định về an toàn, bảo mật cho việc cung cấp dịch vụ ngân hàng trên Internet ...; triển khai hiệu quả Quyết định số 2345/QĐ-NHNN nhằm đảm bảo an toàn, bảo mật trong giao dịch thanh toán nói riêng và sử dụng dịch vụ ngân hàng nói chung.

Bên cạnh đó, tiếp tục đầu tư hoàn thiện hạ tầng công nghệ thông tin của các tổ chức tín dụng, tổ chức trung gian thanh toán; đồng thời nâng cấp, phát triển các hạ tầng thanh toán đảm bảo hoạt động liên tục, thông suốt, an toàn, kết nối liền mạch, xuyên suốt với các ngành, lĩnh vực khác (như dịch vụ công, y tế, giáo dục, thương mại điện tử...) và kết nối thanh toán xuyên biên giới nhằm đáp ứng tốt nhu cầu sử dụng dịch vụ ngân hàng đa dạng, ngày càng tăng nhanh của các tổ chức, cá nhân trong nền kinh tế.

Đồng thời, tiếp tục phối hợp với Bộ Công an triển khai hiệu quả Đề án 06, trong đó chú trọng khai thác thông tin Căn cước công dân gắn chip và tài khoản VNeID để định danh, xác thực chính xác thông tin khách hàng và phối hợp, hỗ trợ trong quá trình cung ứng các sản phẩm, dịch vụ ngân hàng một cách tiện lợi, an toàn, đảm bảo phòng ngừa rủi ro, tội phạm lợi dụng dịch vụ thanh toán cho mục đích gian lận, lừa đảo...

(Theo tạp chí Tài chính Tiền tệ,
VnEconomy và VNBA)



CHƯƠNG TRÌNH THẺ

- **Từ nay đến hết 30/09/2024, TPBank** triển khai chương trình ưu đãi đặc quyền cho chủ thẻ tín dụng TPBank Signature với ưu đãi lên tới 50% tại các nhà hàng cao cấp.
- **Từ nay đến hết 31/12/2024 (hoặc hết ngân sách), BIDV** dành tặng ưu đãi Voucher 200.000đ chủ thẻ BIDV JCB Ultimate khi mua sắm tại Siêu thị & Trung tâm bách hóa tổng hợp AEON.
- **Từ nay đến hết 31/12/2024, Wooribank** triển khai chương trình quà tặng Dịch vụ Cao cấp dành cho chủ thẻ Woori VV Lux Point tại các phòng chờ và khách sạn khi đạt điều kiện chi tiêu.
- **Từ nay đến hết 30/09/2024, Agribank** giảm 15% (tối đa VNĐ 700.000 cho mỗi yêu cầu) khi đặt phòng khách sạn toàn cầu mỗi ngày cho các chủ thẻ thanh toán bằng thẻ Agribank Visa.
- **Từ nay đến hết 31/12/2024, VISA** triển khai chương trình ưu đãi lên đến 35% khi thuê xe với Avis và thanh toán bằng thẻ Visa Gold, Platinum, Signature và Infinite.

**Vui lòng truy cập vào website
của các ngân hàng và tổ chức thẻ
để biết thêm chi tiết.**



ENTRUST: GIAN LẬN DANH TÍNH KHÔNG PHÂN BIỆT ĐỐI XỬ

Từ ngân hàng đến bất động sản, từ chăm sóc sức khỏe cho tới chia sẻ chuyến đi, v.v., rõ ràng chúng ta có thể thấy không có lĩnh vực nào là miễn nhiễm với gian lận danh tính. Trong báo cáo năm 2024 - Kỳ vọng của người dùng về danh tính kỹ thuật số của Onfido - một công ty Entrust, đã tiết lộ rằng 12% người dùng (khoảng 1 trên 10) dịch vụ kỹ thuật số đã trở thành nạn nhân của lừa đảo tăng cao hơn so với năm ngoái với tỷ lệ người tiêu dùng Mỹ là 15%, người tiêu dùng Pháp là 14% và Canada là 13%.

Từ hành vi đánh cắp danh tính và chiếm đoạt tài khoản cho đến sao chép danh tính và tạo tài khoản mới, hình thức lừa đảo nguy hiểm nhất hiện nay chính là “gian lận danh tính tổng hợp” - một sản phẩm do AI tạo ra một cách thực tế và ngày càng khó xác định.

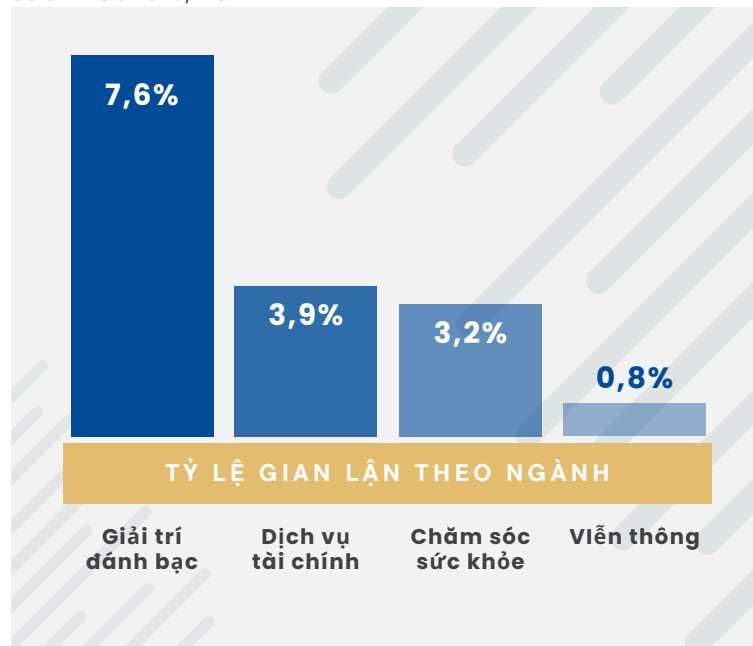
Theo một nghiên cứu gần đây của Hoa Kỳ tiết lộ rằng 72% người dùng mạng xã hội ở Mỹ cảm thấy khó phát hiện nội dung do AI tạo ra như tin tức giả mạo và lừa đảo; và chỉ 27% cảm thấy tự tin rằng họ có thể xác định được cuộc gọi từ bạn thân hoặc thành viên gia đình là cuộc gọi thực hay do AI tạo ra. Thêm vào đó, AI đã đồng thời tăng quy mô các cuộc tấn công được cá nhân hóa và giảm mức độ kỹ năng cần thiết để thực hiện chúng.

Các mối đe dọa gian lận trải dài qua nhiều thế hệ, ngành công nghiệp và khu vực địa lý

Cũng theo một thống kê về gian lận danh tính trong nghiên cứu của Onfido: thế hệ trẻ thường là nạn nhân của gian lận danh tính hơn những người từ 45 tuổi trở lên.

Kết quả này khá hợp lý trong bối cảnh những người trẻ tuổi dành nhiều thời gian trên mạng để chia sẻ thông tin cá nhân một cách công khai nhưng thường ít kinh nghiệm trong việc nhận biết các dấu hiệu lừa đảo. Thêm vào đó, họ có xu hướng đầu tư nhiều hơn vào các sản phẩm như tiền điện tử vốn là mục tiêu ưa thích của giới tội phạm.

Trong khi gian lận nói chung trong ngành tiếp tục gia tăng thì thứ hạng tương đối về gian lận trung bình theo ngành thay đổi từ năm này sang năm khác. Theo Báo cáo gian lận danh tính của Viện an ninh mạng Entrust, vào năm 2023, tỷ lệ gian lận trung bình trong ngành dao động từ mức cao 7,6% đối với ngành giải trí đánh bạc cho đến mức thấp 0,8% đối với ngành viễn thông. Trong số các ngành công nghiệp có tỷ lệ gian lận trung bình có thì ngành dịch vụ tài chính có tỷ lệ 3,9% và chăm sóc sức khỏe là 3,2%.



Các ngành như dịch vụ tài chính nhận thức rõ những rủi ro mà gian lận gây ra nên họ thường áp dụng mức độ bảo mật một cách nghiêm ngặt. Nhưng do họ cũng có mục tiêu tăng trưởng cao nên việc triển khai mà vẫn phải đảm bảo trải nghiệm khách hàng liên mạch cũng trở thành một điều tối quan trọng với các tổ chức này. Một điều đáng mừng là người dùng cuối coi việc ngăn chặn gian lận là lợi ích lớn nhất của việc xác minh danh tính rồi tiếp theo đó mới là tốc độ.

Còn dưới góc độ định vị địa lý, những kẻ lừa đảo hoạt động tích cực nhất ở châu Á, với tỷ lệ lừa đảo trung bình là 9%. Bắc Mỹ là 5,2%, Châu Âu là 3,1%. Vào năm 2023, những kẻ lừa đảo nhắm mục tiêu vào thẻ căn cước công dân nhiều hơn bất kỳ loại giấy tờ nào khác, chiếm 46,8% tổng số vụ gian lận giấy tờ, tiếp theo là hộ chiếu với 23,7% và giấy phép lái xe là 17,5%. Giấy phép lái xe của tỉnh Ontario của Canada có vinh dự bất ngờ khi trở thành tài liệu bị tấn công nhiều nhất ở Bắc Mỹ vào năm ngoái với tỷ lệ 10,4%.

Tận dụng các giải pháp nhận dạng được hỗ trợ bởi AI để ngăn chặn gian lận

Tin tốt về việc chống gian lận chính là tất cả các ngành dọc đều có thể rút ra những bài học từ các mục tiêu ban đầu bị ảnh hưởng nặng nề – chẳng hạn như ngân hàng – về cách tận dụng các giải pháp lấy danh tính làm trung tâm do AI cung cấp để:

- Xác thực bảo mật tài liệu và dữ liệu
- Tăng cường xác thực người dùng và xác minh sinh trắc học
- Tích hợp kỹ thuật số và cấp thông tin xác thực
- Bảo vệ và mã hóa dữ liệu
- Phân tích thiết bị và hành vi
- Cải thiện trải nghiệm người dùng

(Theo Entrust Blog)

MK[®]group
Smart Digital Security

ENTRUST



MÁY IN THẺ ENTRUST SIGMA DS

LỰA CHỌN SỐ 1 CHO CÁC
CHƯƠNG TRÌNH THẺ THÀNH CÔNG

- ✓ ĐƠN GIẢN
- ✓ THÔNG MINH
- ✓ BẢO MẬT



HOTLINE: 0903.481.456



contact@mkgroup.com.vn

VISA RA MẮT DỊCH VỤ CUNG CẤP THẺ ẢO KHẨN CẤP CHO KHÁCH DU LỊCH

Dịch vụ mới này của Visa giúp cho những khách du lịch bị mất ví trong khi đang du lịch có thể đề xuất và nhận được thẻ kỹ thuật số thay thế qua tin nhắn hoặc email ngay lập tức.

Theo báo cáo của Visa, ví kỹ thuật số hiện được 74% du khách Mỹ sử dụng trong các chuyến hành trình của họ.

Dịch vụ thay thế thẻ khẩn cấp kỹ thuật số được cung cấp nhằm giúp xử lý các trường hợp bất ngờ, để các tổ chức tài chính vẫn giúp đảm bảo cho chủ thẻ có được những chuyển đi liền mạch, thoải mái trên khắp thế giới.

Mỗi khi khách hàng thực hiện yêu cầu, một thẻ kỹ thuật số mới sẽ được tạo ra và các tổ chức phát hành thẻ có thể gửi đi để chủ thẻ xác thực và thêm vào ví kỹ thuật số của họ, sử dụng thay thế cho thẻ vật lý thông thường.

Kathleen Pierce-Gilmore, người đứng đầu toàn cầu về các giải pháp phát hành của Visa, cho biết: "Chúng ta đều có thể hiểu được cảm giác hoảng loạn, bế tắc mỗi khi đang đi du lịch và chẳng may bị mất thẻ hay mất ví. Giải pháp thẻ khẩn cấp kỹ thuật số mới của chúng tôi được tạo ra nhằm giải quyết chính những vấn đề này. Nó cung cấp quyền truy cập tức thời, an toàn vào nguồn tiền cho khách du lịch, đồng thời cho phép các nhà phát hành thẻ cung cấp dịch vụ khách hàng vượt hơn mong đợi."

(Theo Finextra)



JUNIPER: GIÁ TRỊ THANH TOÁN KHÔNG TIẾP XÚC SẼ TĂNG GẤP ĐÔI VÀO 2029

Juniper Research dự đoán việc áp dụng các giải pháp thanh toán softPOS của các doanh nghiệp nhỏ sẽ giúp thúc đẩy tổng giá trị giao dịch thanh toán không tiếp xúc tăng 113% vào năm 2029.

Trong dự báo, Juniper nhận định sự tăng trưởng này sẽ giúp giá trị giao dịch toàn cầu tăng từ 7,4 nghìn tỷ USD vào năm 2024 lên tới mức 15,7 nghìn tỷ USD vào năm 2029.

Các nhà phân tích cho biết "Sự góp mặt của hệ thống SoftPOS - nơi thanh toán không tiếp xúc có thể được chấp nhận bằng cách sử dụng điện thoại thông minh tương thích, đang tạo điều kiện thuận lợi cho các nhà bán hàng nhỏ lẻ hơn trong việc giúp phá vỡ rào cản chi phí áp dụng thanh toán không tiếp xúc tại, và giúp gia tăng tỷ lệ chấp nhận thanh toán chung."

"Bên cạnh đó, nghiên cứu còn dự đoán rằng thông báo triển khai Tap to Cash của Apple gần đây dành cho thanh toán cá nhân và việc triển khai rộng rãi Tap to Pay trên iPhone sẽ giúp đẩy nhanh hơn nữa tốc độ tăng trưởng giao dịch."

(Theo Finextra)



PAY.UK: THÍ ĐIỂM GIÚP GIA TĂNG CHỖNG GIAN LẬN LÊN 40%

Nhà điều hành hệ thống thanh toán Pay.UK đã thông báo rằng chương trình thí điểm phát hiện và ngăn chặn gian lận của họ đã giúp tăng khả năng phát hiện thêm 40%, và giảm thiệt hại gian lận 112 triệu bảng

Chương trình thí điểm được Pay.UK phối hợp cùng với Visa, Synectics Solutions và Featurespace bắt đầu khởi động thực hiện từ tháng 6 năm 2023. Chương trình đã giúp các Ngân hàng và các Nhà cung cấp dịch vụ thanh toán (PSP) cùng tham gia quá trình chia sẻ dữ liệu chung để phân tích các giao dịch tài chính, sử dụng thông tin dự đoán để phát hiện trước và ngăn chặn các hoạt động gian lận một cách an toàn.

Mỗi đối tác tham gia nhận được dữ liệu giao dịch Thanh toán từ các ngân hàng và PSP theo thỏa thuận chia sẻ dữ liệu. Mỗi đối tác xây dựng các mô hình máy học độc lập để xác định hoạt động đáng ngờ và so sánh hoạt động đó với các hành vi gian lận đã biết.

Kết quả thí điểm cho thấy chương trình mới này đã thành công trong việc phát hiện hoạt động lừa đảo trước khi nó xảy ra, cho thấy tiềm năng giúp ngăn chặn việc người dân và doanh nghiệp trở thành nạn nhân của lừa đảo.

Các quan chức của Pay.Uk cho biết kết quả tích cực từ thí điểm này chứng tỏ tầm quan trọng của sự đổi mới và hợp tác giữa các ngành trong việc phát triển các giải pháp hiệu quả để vượt qua những kẻ lừa đảo và bảo vệ mọi người trong bối cảnh thanh toán luôn thay đổi.

(Theo ThePaypers)

Gen Z ưa dùng các công cụ thanh toán mới

Theo kết quả nghiên cứu và phân tích của EY, các khách hàng thuộc Thế hệ Gen Z sẽ từ bỏ giao dịch nếu phương thức thanh toán ưa thích của họ không được đơn vị bán hàng cung cấp sẵn.

Các khách hàng Gen Z - những người trong độ tuổi từ 12 đến 27 - có sở thích riêng về cách sử dụng và lựa chọn phương thức thanh toán.

Rõ ràng, Gen Z ưa thích mọi vấn đề liên quan số hóa, và điều tương tự cũng xảy ra với các phương thức thanh toán. Tuy vậy, theo một chuyên gia thanh toán nghiên cứu thói quen của Gen Z cho EY, một số lựa chọn và hành vi thanh toán của thế hệ người tiêu dùng này ẩn chứa khá nhiều bất ngờ.

(Payments Dive)

UniCredit ra mắt thẻ thanh toán dành cho người khiếm thị

UniCredit sẽ nâng cấp thẻ ghi nợ, tín dụng và thẻ trả trước với các tính năng được Mastercard thiết kế dành riêng cho những khiếm thị một phần hoặc toàn phần.

UniCredit Italy là ngân hàng mới nhất đăng ký thiết kế "Thẻ cảm ứng Mastercard", dựa trên hệ thống các điểm nổi cạnh bên được thiết kế nhằm giúp khách hàng nhận biết đúng thẻ bằng cách chạm trên bề mặt.

Theo kế hoạch triển khai ở Italy, khoảng 20 triệu thẻ sẽ từng bước được phát hành trong năm 2024 tới các khách hàng tại 12 thành phố mà UniCredit đặt chi nhánh. Dòng thẻ này cũng sẽ được làm từ PVC tái chế./

(Finextra)

Australia, Ticketmaster hợp tác giải quyết vụ lộ lọt thông tin của nửa tỷ khách hàng

Chính phủ Australia ngày 30/5 xác nhận Văn phòng An ninh mạng Quốc gia đang “hợp tác” với công ty phân phối và bán vé Ticketmaster (Mỹ) sau khi nhóm tin tặc khét tiếng ShinyHunters tuyên bố đã truy cập thông tin chi tiết của 560 triệu khách hàng toàn cầu.

ShinyHunters đã tung ra bằng chứng về vụ việc trên web đen - trong đó tuyên bố đánh cắp thông tin cá nhân của hơn 500 triệu khách hàng - và yêu cầu khoản tiền chuộc 500.000 USD, mô tả đây là khoản “bán một lần”.

Dữ liệu bị đánh cắp chủ yếu bao gồm tên, địa chỉ, email, số điện thoại và 4 chữ số cuối trên số thẻ tín dụng của khách hàng cùng với ngày hết hạn. Người phát ngôn Chính phủ Australia ra tuyên bố cho biết: “Văn phòng An ninh mạng Quốc gia đang hợp tác với Ticketmaster để tìm hiểu vụ việc”. Cơ quan này cũng kêu gọi những người có “thắc mắc cụ thể” liên hệ trực tiếp với Ticketmaster.

Tháng 1/2024, một tòa án ở thành phố Seattle (bang Washington, Mỹ) đã phạt tù Sebastien Raoult - hacker máy tính người Pháp, thành viên của ShinyHunters. Đối tượng này bị kết án 3 năm tù giam và phải nộp hơn 5 triệu USD tiền bồi thường sau khi thừa nhận lên kế hoạch lừa đảo qua điện thoại và đánh cắp danh tính.

Các công tố viên Mỹ ước tính vụ hack trên diện rộng đã gây thiệt hại hàng triệu USD cho các công ty nạn nhân và “nhiều tổn thất khác không thể đo lường được” đối với hàng trăm triệu cá nhân có dữ liệu bị bán cho các đối tượng tội phạm khác.

Giáo sư an ninh mạng Katina Michael của Đại học Wollongong (Australia) đánh giá những cuộc tấn công đang ảnh hưởng đến nhiều người hơn với những hậu quả ngày càng nghiêm trọng. Theo bà, số lượng nạn nhân bị hack “sẽ gia tăng, có thể lên tới một tỷ người trong tương lai”. Giáo sư Michael cảnh báo các chính phủ, công ty và người tiêu dùng chưa làm đủ để tự vệ hoặc đầu tư vào các cơ chế bảo vệ cơ bản như xác thực 2 yếu tố.

Ticketmaster, có trụ sở tại California, vận hành một trong những nền tảng bán vé trực tuyến lớn nhất thế giới.

(AFP)



Hàn Quốc điều tra vụ rò rỉ dữ liệu cá nhân của đội ngũ nhân viên công vụ

quan Cảnh sát quốc gia Hàn Quốc ngày 20/6 xác nhận đã mở cuộc điều tra sơ bộ sau khi thông tin cá nhân của hàng chục quan chức tòa án, công tố và cảnh sát bị rò rỉ trên Internet.

Cuộc điều tra nội bộ được tiến hành hồi tháng 5, sau khi thông tin cá nhân của các quan chức tòa án, văn phòng công tố và cơ quan cảnh sát Hàn Quốc bị một cá nhân có nickname “Warfare” chia sẻ trên một trang web ở nước ngoài, nơi thường xuyên bị tin tặc truy cập vào tháng 3.

Cơ quan Cảnh sát quốc gia Hàn Quốc cho biết thông tin bị rò rỉ bao gồm tên cũng như những gì được cho là tài khoản mạng nội bộ và mật khẩu của 40 quan chức, trong đó có một thẩm phán cấp cao. Cảnh sát có kế hoạch mở cuộc điều tra chính thức ngay sau khi tìm được thêm thông tin chi tiết.

Hồi tháng 4, “Warfare” cũng đăng tải thông tin tương tự của hàng chục người được cho là nhân viên 2 tập đoàn lớn của Hàn Quốc là Samsung Electronics và Hyundai Motor.

(TTXVN)

LUẬT CĂN CƯỚC: TẠO THUẬN LỢI TỐI ĐA CHO NGƯỜI DÂN

Luật Căn cước được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XV, kỳ họp thứ 6 thông qua ngày 27/11/2023, chính thức có hiệu lực thi hành từ ngày 1/7/2024. Luật gồm 7 chương, 46 Điều. Khi được thông qua, Luật Căn cước sẽ mang lại những tác động tích cực đến các cơ quan, tổ chức và cá nhân.



Cụ thể, Luật Căn cước được xây dựng, ban hành nhằm mục đích phục vụ giải quyết thủ tục hành chính và cung cấp dịch vụ công trực tuyến. Các dịch vụ công trực tuyến thiết yếu được cung cấp như lĩnh vực cư trú, hộ tịch, bảo hiểm xã hội, giáo dục, y tế, đất đai, lao động... để phục vụ người dân, doanh nghiệp trên cơ sở sử dụng xác thực, chia sẻ thông tin trong Cơ sở dữ liệu quốc gia về dân cư để cắt giảm, đơn giản hóa thủ tục hành chính.

Đối với mục tiêu phục vụ phát triển kinh tế, xã hội, thông qua việc nghiên cứu, triển khai ứng dụng các tính năng của chip điện tử trên thẻ căn cước đối với các lĩnh vực tài chính, ngân hàng và một số lĩnh vực phát triển kinh tế, xã hội khác; tích hợp, phát triển các ứng dụng trên nền tảng hệ thống định danh điện tử với các ứng dụng cốt lõi như:

Ví điện tử, thanh toán không dùng tiền mặt, chứng khoán, điện, nước... lên ứng dụng VNeID, mã QR của thẻ căn cước công dân gắn chip điện tử. Trên cơ sở đó tập trung phát triển, hoàn thiện và triển khai hiệu quả ứng dụng di động công dân số từ ứng dụng VNeID trên cơ sở mở rộng tích hợp các thông tin, dịch vụ như: y tế, bảo hiểm, giấy phép lái xe, ngân hàng, thanh toán điện tử, ứng cứu khẩn cấp, phản ánh hiện trường, tố giác tội phạm...

Mặt khác, Luật Căn cước được xây dựng, ban hành nhằm mục đích phục vụ công dân số. Hiện nay, người dân có rất nhiều loại giấy tờ khác nhau, như căn cước, thẻ bảo hiểm y tế, bảo hiểm xã hội, giấy phép lái xe, giấy đăng ký xe, các loại bằng cấp, chứng chỉ... Nhằm tạo điều kiện cho công dân, cần phải xác thực 100% các thông tin thiết yếu, quan trọng trên ứng dụng VNeID hoặc qua thẻ căn cước công dân gắn chip điện tử như:

Thông tin tiêm chủng, xét nghiệm, giấy phép lái xe, đăng ký xe... Từ đó, từng bước thay thế các giấy tờ của người dân trong một số các giao dịch theo quy định pháp luật. Cung cấp các dịch vụ công, dịch vụ thương mại phục vụ tiện ích số của công dân trên ứng dụng VNeID như: Dịch vụ cư trú, căn cước, thương mại điện tử, thanh toán điện tử và các dịch vụ khác.

Cùng với đó, Luật Căn cước được xây dựng, ban hành nhằm hoàn thiện hệ sinh thái phục vụ kết nối, khai thác, bổ sung làm giàu dữ liệu dân cư, triển khai hiệu quả việc kết nối, chia sẻ giữa Cơ sở dữ liệu quốc gia về dân cư với các Cơ sở dữ liệu quốc gia khác, cơ sở dữ liệu chuyên ngành, bảo đảm giải quyết các thủ tục phục vụ người dân được chính xác và thuận lợi. Đồng thời phục vụ công tác chỉ đạo, điều hành của lãnh đạo các cấp.

Trên nền Cơ sở dữ liệu quốc gia về dân cư và các thông tin đã được tích hợp, sử dụng ứng dụng trí tuệ nhân tạo để tổng hợp, phân tích, dự báo các thông tin để phục vụ việc điều hành của Chính phủ, Thủ tướng Chính phủ, hoạch định chính sách kinh tế, xã hội.

(Theo <https://congan.haiphong.gov.vn/>)

THỰC TRẠNG TẤN CÔNG RANSOMWARE NĂM 2024



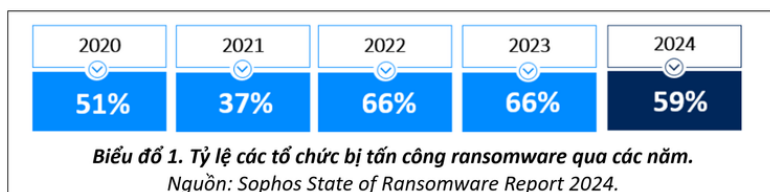
Báo cáo tình trạng mã độc tống tiền (ransomware) thường niên lần thứ 5 của Sophos cho thấy bức tranh toàn cảnh của vấn nạn này trong thế giới thực của 5.000 tổ chức trên toàn cầu, chỉ ra nguyên nhân cốt lõi cho đến mức độ nghiêm trọng của những vụ tấn công, tác động tài chính và thời gian phục hồi.

Dựa trên kết quả của cuộc khảo sát được tiến hành trong khoảng thời gian từ tháng 1-2/2024 đối với những người đứng đầu bộ phận CNTT/An ninh mạng tại 14 quốc gia ở châu Mỹ, EMEA (châu Âu, Trung Đông, châu Phi) và châu Á-Thái Bình Dương, báo cáo lần này kết hợp những đánh giá sâu sắc hàng năm với các lĩnh vực nghiên cứu hoàn toàn mới. Báo cáo đi sâu vào những yếu sách tống tiền và các khoản tiền chuộc, đồng thời làm sáng tỏ vai trò mới của cơ quan thực thi pháp luật trong quá trình khắc phục hậu quả từ ransomware.

Dưới đây là một số nội dung đáng chú ý trong báo cáo của Sophos

Tỷ lệ tấn công giảm nhưng chi phí khôi phục tăng cao

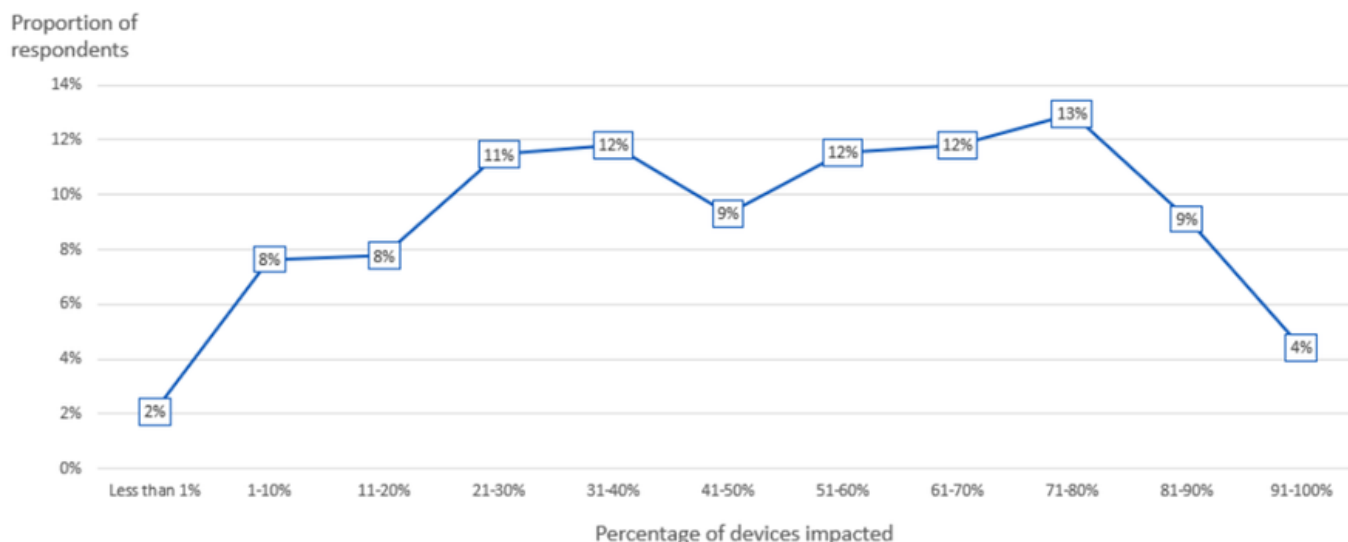
Theo những người được khảo sát, 59% tổ chức đã bị ransomware tấn công trong năm ngoái. Đây là mức giảm đáng mừng so với tỷ lệ 66% được báo cáo trong cả hai năm trước. Tuy vậy, hơn 50% số tổ chức bị tấn công cho rằng hiện không phải là lúc hạ thấp tinh thần cảnh giác.



Mặc dù tỷ lệ tấn công đã giảm trong năm qua, song tổng chi phí khắc phục - không bao gồm các khoản tiền chuộc - đã tăng vọt lên 2,73 triệu USD, tăng 50% so với mức 1,82 triệu USD được báo cáo vào năm 2023.

Hiếm khi xảy ra hành vi mã hóa toàn bộ dữ liệu tổ chức

Trung bình, chỉ khoảng 49% số máy tính của các tổ chức bị ảnh hưởng bởi những vụ tấn công bằng ransomware. Hành vi mã hóa toàn bộ môi trường của bạn hiếm khi xảy ra. Chỉ 4% tổ chức cho biết hơn 91% tổng số thiết bị của họ bị ảnh hưởng.



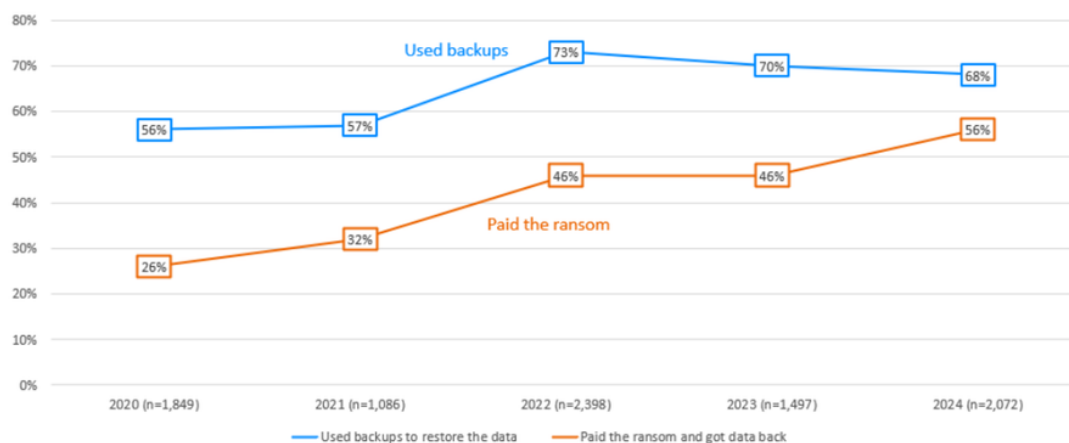
Biểu đồ 2. Tỷ lệ thiết bị hứng chịu tác động từ những vụ tấn công bằng ransomware.

Nguồn: Sophos State of Ransomware Report 2024.

Hơn một nửa số nạn nhân đã trả tiền chuộc

Lần đầu tiên có tới 56% tổ chức bị mã hóa dữ liệu thừa nhận đã trả tiền chuộc để khôi phục dữ liệu. Việc sử dụng các bản sao lưu (backup) giảm xuống mức 68%, thấp hơn so với tỷ lệ 70% của năm ngoái. Trong khi đó, 26% dùng thêm “các phương tiện khác” để lấy lại dữ liệu, bao gồm phối hợp với các cơ quan thực thi pháp luật hoặc sử dụng khóa giải mã đã được công khai.

Hơn một nửa số nạn nhân đã trả tiền chuộc Lần đầu tiên có tới 56% tổ chức bị mã hóa dữ liệu thừa nhận đã trả tiền chuộc để khôi phục dữ liệu. Việc sử dụng các bản sao lưu (backup) giảm xuống mức 68%, thấp hơn so với tỷ lệ 70% của năm ngoái. Trong khi đó, 26% dùng thêm “các phương tiện khác” để lấy lại dữ liệu, bao gồm phối hợp với các cơ quan thực thi pháp luật hoặc sử dụng khóa giải mã đã được công khai.

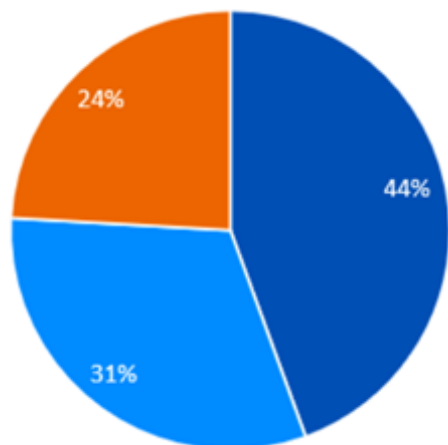


Biểu đồ 3. Phương thức khôi phục dữ liệu bị mã hóa trong giai đoạn 2020-2024.

Nguồn: Sophos State of Ransomware Report 2024.

Một thay đổi đáng chú ý trong năm qua là xu hướng các nạn nhân sử dụng nhiều phương pháp khác nhau để khôi phục dữ liệu bị mã hóa như trả tiền chuộc và sử dụng bản sao lưu. Gần một nửa số tổ chức bị mã hóa dữ liệu (47%) đã sử dụng nhiều phương pháp cùng một lúc - cao hơn gấp đôi tỷ lệ được báo cáo vào năm 2023 (21%).

Số tiền chuộc tăng vọt nhưng nạn nhân hiếm khi trả số tiền như yêu sách ban đầu



RANSOM DEMAND VS. RANSOM PAYMENT

Biểu đồ 4. Yêu sách tiền chuộc so với tiền chuộc được chi trả.

Nguồn: Sophos State of Ransomware Report 2024.

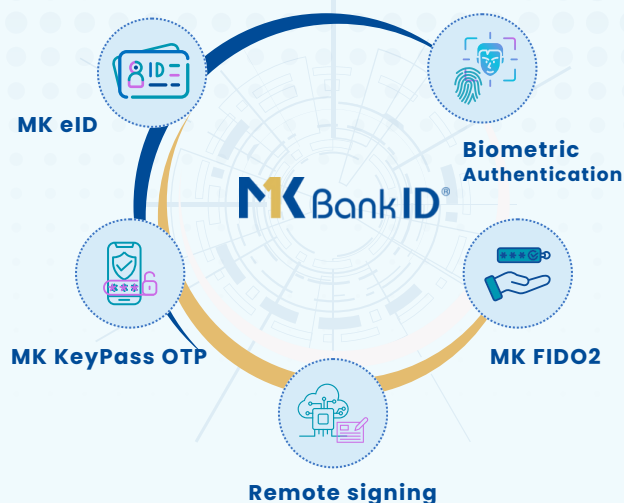
Trong số các đối tượng được khảo sát, 1.097 người (tại các tổ chức đã trả tiền chuộc) tiết lộ số tiền được trả trên thực tế, thừa nhận khoản thanh toán bình quân đã tăng gấp 5 lần so với năm ngoái, từ 400.000 USD lên 2 triệu USD. Mặc dù tỷ lệ trả tiền chuộc tăng lên, nhưng chỉ 24% số người được hỏi xác nhận khoản thanh toán của họ tương ứng với yêu sách ban đầu, trong khi 44% trả ít hơn, và 31% trả nhiều hơn./.

(Theo BankInfoSecurity)

MK[®]group
Smart Digital Security

HỆ SINH THÁI MK BANKID

Các giải pháp xác thực bảo mật trên không gian số



MK eID

Giải pháp định danh, xác thực khách hàng sử dụng thẻ CCCD gắn chip

Xác thực sinh trắc học

Giải pháp thực hiện đối sánh, xác thực sinh trắc học khuôn mặt, vân tay của khách hàng dựa trên các đặc điểm sinh trắc học duy nhất

MK KeyPass OTP

Giải pháp xác thực mạnh KeyPass™ OTP với các phương thức xác thực từ OTP cơ bản, OTP nâng cao có chức năng ký giao dịch

MK FIDO2

Giải pháp xác thực mạnh tuân thủ chuẩn FIDO2, phương pháp chống phishing hiệu quả

MK SmartCA - Remote signing

Dịch vụ chứng thực chữ ký số theo mô hình ký số từ xa ứng dụng công nghệ đám mây (cloud-based)

Hà Nội: (024) 7100 6781

Tp. Hồ Chí Minh: (028) 3930 1055



ĐỐI TÁC TIN CẬY VỀ THẺ THÔNG MINH | XÁC THỰC BẢO MẬT TÀI LIỆU BẢO AN | AI CAMERA

 <https://mkgroup.com.vn>

 contact@mkgroup.com.vn

Trong trường hợp Quý độc giả không muốn nhận bản tin, hãy phản hồi cho chúng tôi theo địa chỉ:

- **Email:** contact@mkgroup.com.vn
- **Tiêu đề thư:** Không nhận bản tin Thế Giới Thẻ MK



Xin vui lòng truy cập vào website MK Group để hiểu rõ hơn về **Chính sách bảo mật và xử lý dữ liệu cá nhân** của chúng tôi.