

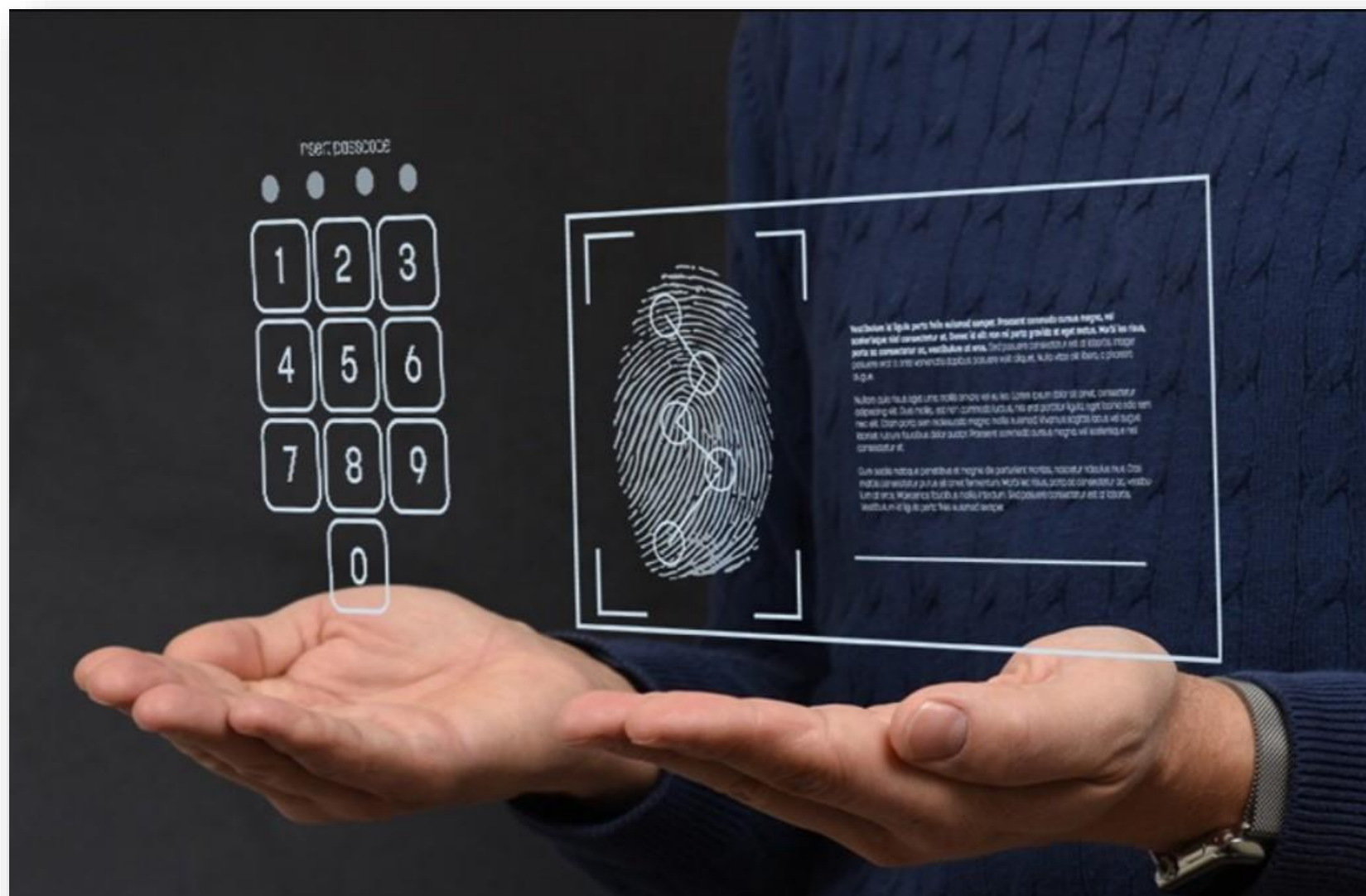
# THẾ GIỚI THẺ

Bản tin điện tử nội bộ - Số 132 | Tháng 10 - 2021

Tổng biên tập: Bà Phan Thị Quỳnh Hoa - Giám đốc Tập đoàn MK | Ý kiến đóng góp vui lòng gửi về: [marketing@mkgroup.com.vn](mailto: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 tài trợ “Hội nghị trực tuyến về xác thực: Sự cần thiết của các biện pháp xác thực mạnh mẽ cho các dịch vụ Chính phủ” do FIDO Alliance tổ chức](#)
- [Fingerprint Cards, Infineon chuyển xác thực sinh trắc vào phần tử bảo mật thẻ](#)
- [Cây ghép NFC sinh trắc học phục vụ thanh toán trên người tiêu dùng](#)
- [Năm 2023, thanh toán di động không tiếp xúc đạt mốc 49 tỷ giao dịch](#)
- [Mastercard hợp tác thu thập thông tin sinh trắc của 30 triệu dân châu Phi](#)
- [Tổng quan về nguy cơ gian lận trong nửa đầu năm 2021](#)

## MK Group tài trợ “Hội nghị trực tuyến về xác thực: Sự cần thiết của các biện pháp xác thực mạnh mẽ cho các dịch vụ Chính phủ” do FIDO Alliance tổ chức

Vào ngày 23/9/2021, sự kiện trực tuyến “Hội nghị trực tuyến về xác thực: Sự cần thiết của các biện pháp xác thực mạnh mẽ cho các dịch vụ Chính phủ” do Liên minh Xác thực FIDO (FIDO Alliance) tổ chức đã diễn ra với sự tham gia của người quan tâm, khách hàng và đối tác của FIDO Alliance đến từ nhiều quốc gia trên toàn thế giới.

Trong khuôn khổ sự kiện này, MK Group đã tham gia đồng hành với FIDO Alliance với cương vị là nhà tài trợ đóng góp cho sự kiện. Hiện MK Group cũng là doanh nghiệp công nghệ Việt sở hữu và sản xuất hai thiết bị Khóa xác thực bảo mật theo chuẩn FIDO gồm Khóa xác thực FIDO® KeyPass S1 đạt chuẩn FIDO U2F / hỗ trợ chuẩn FIDO2 – đây là thiết bị khóa xác thực đầu tiên của Việt Nam đạt chuẩn FIDO vào ngày 08/08/2018; và Khóa xác thực FIDO® KeyPass S2 đạt chuẩn FIDO2.

Tại sự kiện lần này, các chuyên gia và một số tổ chức như Dịch vụ Y tế Quốc gia Vương quốc Anh (NHS); Nền tảng đăng nhập một lần cho các dịch vụ của chính phủ Hoa Kỳ (login.gov) và Sở Thuế vụ (IRS) của Chính phủ Hoa Kỳ đã tập trung vào việc trình bày về các phương thức xác thực mạnh và cách các phương thức này giúp kích hoạt các dịch vụ của chính phủ bảo mật danh tính trực tuyến như thế nào.



Nguồn: Internet

authenticate

AUTHENTICATE 2021

PAST EVENTS

SPONSORS

BLOG

MEDIA LIBRARY

Q

SIGN UP FOR UPDATES



### MK GROUP

Supporting

Established in 1999 in Vietnam, MK Group has over 22 years of experience in providing Digital Security solutions and Smart Card products.

MK Group has successfully provided and deployed our products and solutions for many customers in the government, finance – banking, enterprise, telecommunication and transportation sector. We always strive to be the leader in technology solutions and services through innovation and commitment to our dear customers.

Our core value is expressed via our own slogan which is: **Smart Digital Security**

- **Smart:** smart payment, identification and data exchange
- **Digital:** digitalize identification and transactions
- **Security:** secure data, identification and payment transactions

### CÔNG NGHỆ HIỆN ĐẠI GIÚP THỨC ĐẨY QUÁ TRÌNH XÁC THỰC CỦA FIDO

Các chuyên gia chia sẻ rằng các cuộc tấn công nhét thông tin xác thực mật khẩu đang ngày một trở nên phổ biến và việc trang bị xác thực đa yếu tố dựa trên các tiêu chuẩn của FIDO trở nên cần thiết hơn bao giờ hết. Nhận thức được điều này, nhiều cơ quan trực thuộc chính phủ Hoa Kỳ đã sử dụng thông tin xác thực Thẻ truy cập chung (CAC)/Xác minh danh tính cá nhân (PIV) thay vì chỉ sử dụng mật khẩu cơ bản.

Tại sự kiện, các thiết bị khóa bảo mật của MK Group đã nhận được nhiều sự quan tâm đến từ các khách hàng tiềm năng cũng như đối tác của FIDO Alliance trên toàn thế giới. Với các thiết bị của MK Group, các tổ chức, doanh nghiệp và người dân có thể chống lại các hành vi gian lận, ăn cắp thông tin truy cập tài khoản trên mạng như skimming (sao chép thông tin tài khoản), phishing (lừa đảo bằng các trang web giả mạo) cũng như man-in-the-middle (tấn công xen giữa)/.

(MK Group)

## Ngân hàng Nhà nước yêu cầu đẩy mạnh thanh toán không dùng tiền mặt lĩnh vực y tế, giáo dục

**Ngân hàng Nhà nước Việt Nam vừa có văn bản gửi các ngân hàng, chi nhánh ngân hàng nước ngoài, các tổ chức cung ứng dịch vụ trung gian thanh toán về việc đẩy mạnh thanh toán không dùng tiền mặt lĩnh vực y tế, giáo dục.**

Theo đó, triển khai chỉ đạo của Thủ tướng Chính phủ về các giải pháp cấp bách, hiệu quả nhằm tháo gỡ ách tắc, phục hồi kinh tế trong bối cảnh đại dịch COVID-19 còn diễn biến phức tạp và tiếp tục thực hiện Chỉ thị 22/CT-TTg về việc đẩy mạnh triển khai các giải pháp phát triển thanh toán không dùng tiền mặt tại Việt Nam, để góp phần thúc đẩy thanh toán không dùng tiền mặt trong lĩnh vực y tế và giáo dục, Ngân hàng Nhà nước Việt Nam đề nghị các ngân hàng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán trên cơ sở nhu cầu, năng lực và quy định pháp luật triển khai một số nội dung sau:

1. Tiếp tục phối hợp các cơ sở y tế, giáo dục nghiên cứu, triển khai các sản phẩm, dịch vụ thanh toán không dùng tiền mặt (như thanh toán thẻ, tài khoản, Ví điện tử, qua ATM, POS, Internet, thiết bị di động, QR Code,..) phù hợp với lĩnh vực y tế, giáo dục tạo điều kiện cho người dân thanh toán học phí, viện phí thuận tiện, nhanh chóng và an toàn.
2. Nghiên cứu, xem xét áp dụng chính sách ưu đãi, miễn, giảm phí dịch vụ thanh toán không dùng tiền mặt đối với học phí, viện phí trong thời gian tối thiểu 02 năm nhằm hỗ trợ người dân vượt qua đại dịch COVID-19.
3. Chủ tịch Hội đồng quản trị/Hội đồng thành viên, Tổng Giám đốc/Giám đốc của ngân hàng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán xây dựng chương trình, kế hoạch cụ thể về việc triển khai sản phẩm, dịch vụ, áp dụng chính sách ưu đãi, miễn, giảm phí đối với giao dịch thanh toán học phí, viện phí phù hợp với điều kiện và thực tiễn cung ứng dịch vụ thanh toán của tổ chức (loại phí, đối tượng, thời gian áp dụng...); tổ chức thực hiện và công bố công khai để khách hàng biết.
4. Trong quá trình triển khai thực hiện, nếu có khó khăn vướng mắc phản ánh kịp thời về Ngân hàng Nhà nước Việt Nam (qua Vụ Thanh toán) để nghiên cứu, xử lý./.

(TaichinhTiente.vn)

## TIN VẤN THẺ NGÂN HÀNG

- **Từ ngày 15/10/2021 đến 31/12/2021, Ngân Hàng Shinhan** triển khai chương trình “Ưu đãi toàn diện khi mở thẻ tín dụng Shinhan” dành cho mọi khách hàng mở mới thẻ tín dụng cá nhân Shinhan Visa Hi-Point, Shinhan Visa CashBack và Shinhan Visa Travel. Cụ thể, các khách hàng khi mở mới sẽ được miễn phí thường niên năm đầu tiên và có thể nhận được ưu đãi hoàn tiền lên tới 1 triệu đồng khi giao dịch trực tuyến.
- **Tham gia chương trình "Order thả ga - Nhận 175.000 đồng từ Napas" từ ngày 14/10 cho đến hết ngày 15/12/2021**, khách hàng nhận mã giảm trị giá 35.000 đồng khi thanh toán đơn hàng ứng dụng Beamin bằng thẻ Napas.
- **Từ ngày 25/09/2021 cho đến hết 31/01/2022, Ngân hàng TMCP Sài Gòn Thương Tín (Sacombank)** triển khai chương trình "Mở thẻ Visa – Nhận quà ưu đãi" dành cho tất cả các khách hàng cá nhân mở mới thẻ tín dụng Sacombank Visa. Khi mở mới thẻ Sacombank Visa, ngoài nhận được phần quà hấp dẫn là 1 ví đựng thẻ cao cấp, khách hàng còn có thể được nhận thêm ưu đãi hoàn phí thường niên tối đa 1 triệu đồng./.

(Tổng hợp từ Internet)



## Dự báo thị trường ATM toàn cầu sẽ đạt mức 27,7 tỷ USD vào năm 2026 trường

Theo báo cáo của *Global Industry Analysts Inc.* cho biết thị trường ATM toàn cầu dự kiến sẽ đạt 27,7 tỷ USD vào năm 2026, tăng trưởng với tốc độ tăng trưởng kép hàng năm ở mức 5,8%.

Thị trường Mỹ hiện có giá trị 5,6 tỷ USD, nhưng thị trường Trung Quốc dự kiến sẽ đạt 5,7 tỷ USD vào năm 2026, với mức độ tăng trưởng kép hàng năm (CAGR) 8,8% trong thời điểm hiện tại. Nhật Bản và Canada cũng sẽ tăng trưởng lần lượt là 3,2% và 5,2%/.

(ATMmarketplace)



### Datacard® MX9100™ Card Issuance System

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

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

Hotline: 0903.481.456 • Email: [marrketing@mkgroup.com.vn](mailto:marrketing@mkgroup.com.vn)



# Fingerprint Cards, Infineon chuyển xác thực sinh trắc vào phần tử bảo mật thẻ



*Fingerprint Cards và Infineon đã phát triển một phương pháp xác thực sinh trắc học được thực hiện hoàn toàn trong phần tử bảo mật của Infineon, nhờ đó loại bỏ nhu cầu sử dụng bộ xử lý riêng biệt, đồng thời khiến quá trình phát triển và triển khai thẻ thanh toán sinh trắc học trở nên dễ dàng và tiết kiệm chi phí hơn.*

Fingerprint Cards và Infineon khẳng định khả năng thực hiện tiến trình xác thực trong phần tử bảo mật Infineon giúp duy trì hiệu suất sinh trắc học và tăng cường bảo mật.

Phương pháp xử lý mới được thực hiện thông qua bộ điều khiển bảo mật SLC38 40nm của Infineon, module cảm biến T-Shape 2 và phần mềm thanh toán sinh trắc học mới nhất của Fingerprint Card. Nhóm nghiên cứu và phát triển của Fingerprint Card đã tập trung vào nỗ lực giảm thiểu yêu cầu về bộ nhớ, flash và RAM của phần mềm đối với quá trình thực thi trong phần tử bảo mật Infineon.

Theo thông báo, gần một nửa số thẻ thanh toán gắn chip trên toàn thế giới hiện được tích hợp bộ điều khiển bảo mật Infineon.

Theo Fingerprint Card, quá trình xác thực sinh trắc học trong phần tử bảo mật Infineon được hoàn thành trong khoảng 250 mili giây, với tỷ lệ chấp nhận sai là 1 trên 20.000 và tỷ lệ từ chối sai ở dưới mức 3%./.

(Biometric Update)

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

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

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



Các thiết bị đi kèm giải pháp gồm:

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

MK Group là thành viên của:



HOTLINE

0903.481.456

www.contact@mkgroup.com.vn

Nguồn: Internet



## Santander ra mắt thẻ thanh toán thân thiện môi trường

Santander đã bắt đầu tung ra thẻ thanh toán "bền vững", thân thiện với môi trường được làm bằng các loại vật liệu tái chế tại Tây Ban Nha.

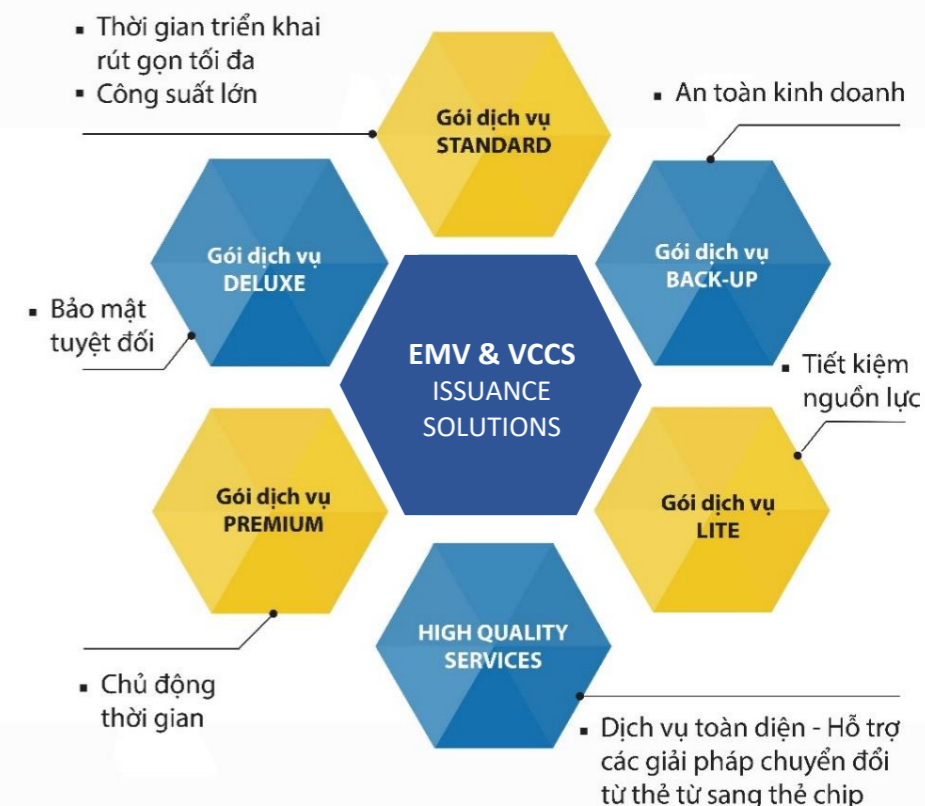
Ngân hàng đã cho ra mắt bản thiết kế thẻ "One Card" ở Ba Lan và Bồ Đào Nha. Họ đặt mục tiêu đến năm 2025, tất cả thẻ ghi nợ và thẻ tín dụng ở Tây Ban Nha, Bồ Đào Nha và Vương quốc Anh đều sẽ được làm bằng vật liệu tái chế.

Santander cho biết bằng việc cần ít năng lượng hơn để chế tạo một chiếc thẻ tái chế so với thẻ nhựa, việc chuyển đổi này sẽ giúp họ tránh phát thải hơn 1.000 tấn CO<sub>2</sub> mỗi năm. Và điều này sẽ giúp họ ngày càng tiến tới gần hơn mục tiêu đạt mức phát thải carbon ròng bằng 0 vào năm 2025.

Ngân hàng cũng đang áp dụng việc làm mới thương hiệu cho các dòng thẻ mới, bao gồm cả biểu tượng sinh thái, thiết kế độc đáo cho từng phân khúc khách hàng để dễ dàng nhận biết hơn và một vết cắt khuôn ở cuối thẻ để hỗ trợ người mù dễ dàng nhận biết loại thẻ này./.

(Finextra)

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



## Cấy ghép NFC sinh trắc học phục vụ thanh toán trên người tiêu dùng

**Người tiêu dùng ở Liên minh Châu Âu và Anh hiện có thể thực hiện thanh toán không tiếp xúc thông qua thiết bị cấy NFC sinh học ngay trên tay đảm bảo tuân thủ các tiêu chuẩn tương thích sinh học ISO 10993.**

Thiết bị cấy ghép NFC sinh học này không cần pin để hoạt động và được cấy ghép dưới da của người dùng, liên kết với một tài khoản thanh toán trực tuyến định trước. Nó cho phép chủ sở hữu thực hiện thanh toán không tiếp xúc ở bất cứ nơi nào chấp nhận thanh toán thẻ ghi nợ và thẻ tín dụng không tiếp xúc.

Công ty phát triển thiết bị này cho biết "Bộ cấy thanh toán Walletmor là một thiết bị nhỏ, có kích thước chỉ bằng một cái ghim cài nhỏ và dày khoảng nửa milimet, bao gồm một mạch tích hợp và một lớp bọc kim loại hoạt động như một ăng-ten, được thiết kế nằm gọn trong một vỏ bọc sinh học kín đáo và hoàn toàn an toàn với cơ thể người dùng".

"Thiết bị được tạo thành từ chất dẻo sinh học - vật liệu về mặt kỹ thuật được coi là một loại nhựa y tế để sản xuất các thiết bị y tế và có chứng chỉ tương thích sinh học hiện hành xác nhận sự phù hợp với tiêu chuẩn ISO 10993. Quan trọng nhất là thiết bị này không hề cần dùng điện để hoạt động."

"Thiết bị sẽ không tạo ra bất kỳ sóng vô tuyến nào và chỉ kích hoạt nhận diện thanh toán khi để gần một thiết bị đầu cuối thanh toán không tiếp xúc trong khoảng cách rất ngắn. Không thể theo dõi ai đó bằng thiết bị cấy ghép Walletmor. Đặc biệt, quá trình cấy ghép sẽ không gây đau đớn và chỉ mất 15 phút."

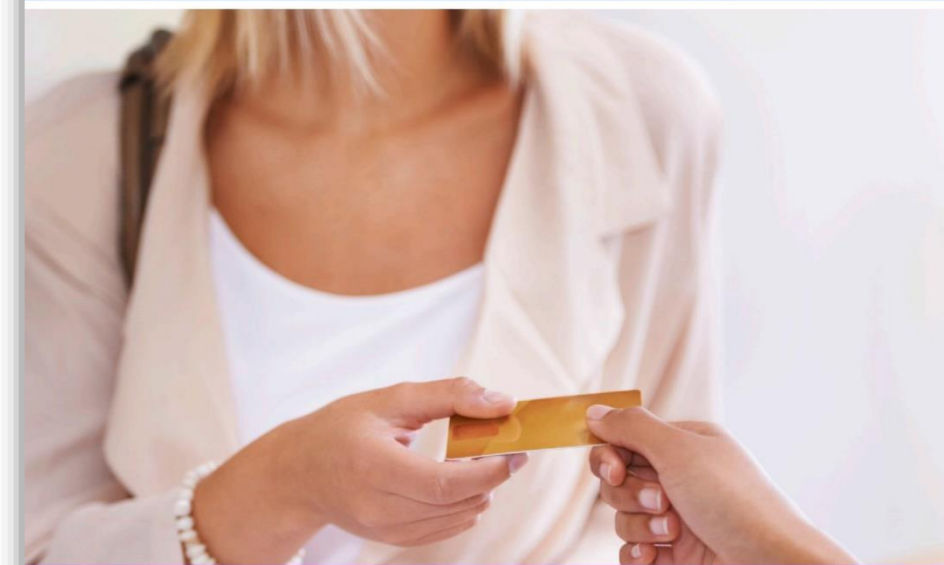
Sau khi người tiêu dùng đặt hàng thiết bị cấy ghép thanh toán NFC sinh học, người dùng mở tài khoản thanh toán trực tuyến và thêm chi phí vào tài khoản trên nền tảng iCard của Châu Âu trước khi tiến hành cấy ghép thiết bị tại bệnh viện, phòng khám hoặc phòng thí nghiệm y học thẩm mỹ có cung cấp dịch vụ.



Nguồn: Internet

(NFCW)

## GIẢI PHÁP PHÁT HÀNH THẺ NGAY LẬP TỨC CARDWIZARD



### TĂNG TÍNH GẮN KẾT - THỨC ĐẨY DOANH THU

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

### Giải pháp sẽ giúp các tổ chức phát hành thẻ:

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

HOTLINE  
0903.481.456

[www.contact@mkgroup.com.vn](mailto:www.contact@mkgroup.com.vn)

## Năm 2023, thanh toán di động không tiếp xúc đạt mốc 49 tỷ giao dịch



Nguồn: Internet

Theo dự báo của Juniper Research, tổng khối lượng giao dịch toàn cầu thông qua phương thức thanh toán không tiếp xúc (TTKTX) trên thiết bị di động sẽ tăng 92% - từ 26 tỷ lượt trong năm 2021 lên 49 tỷ lượt vào năm 2023.

Mức tăng trưởng trên sẽ “cao hơn đáng kể” so với khối lượng giao dịch thông qua thẻ TTKTX. Juniper Research dự báo khối lượng thanh toán di động không tiếp xúc sẽ tăng trưởng “nh nhanh gấp 2 lần so với khối lượng giao dịch thông qua thẻ TTKTX”.

Juniper Research nhận định: “Mức độ bảo mật được cải thiện và khả năng thanh toán đa kênh ngày càng mở rộng là những động lực thúc đẩy tăng trưởng chủ chốt”.

Cũng theo Juniper Research, Mỹ Latinh sẽ là khu vực bùng nổ mạnh mẽ nhất về khối lượng giao dịch thanh toán di động không tiếp xúc, với tốc độ tăng trưởng lên đến hơn 400% trong giai đoạn 2021-2023./.

(NFCW)

## SẢN PHẨM THẺ - THẺ THÔNG MINH

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

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



Các chứng chỉ đã đạt:



## Gian lận thanh toán trực tuyến - mối đe dọa nghiêm trọng đối với thị trường số

*Một nghiên cứu của Ravelin cho thấy gian lận thanh toán trực tuyến vẫn là mối quan ngại lớn nhất đối với các tổ chức tham gia thị trường số, khi hơn 3/4 tổng số doanh nghiệp xếp gian lận thanh toán trực tuyến vào danh sách những mối đe dọa nghiêm trọng nhất đối với họ.*

Theo kết quả nghiên cứu, gian lận thanh toán trực tuyến hiện là mối quan ngại đặc biệt đối với các thị trường kết nối người mua với người bán hàng hóa và dịch vụ bên thứ ba. 81% tổ chức tham gia thị trường hàng hóa và dịch vụ cho rằng gian lận thanh toán trực tuyến là một trong những mối đe dọa lớn nhất đối với họ, cao hơn so với 78% trong số các công ty phát triển ứng dụng đặt chỗ taxi và 68% trong số các công ty giao đồ ăn trực tuyến.

Tấn công chiếm đoạt tài khoản (ATO) là một mối đe dọa nghiêm trọng khác mà các doanh nghiệp trên đang phải đối mặt. 79% các công ty phát triển ứng dụng đặt chỗ taxi, 74% các công ty giao đồ ăn trực tuyến, 69% thị trường hàng hóa và dịch vụ đều khẳng định rằng ATO là một trong những mối đe dọa gian lận nghiêm trọng nhất đối với họ./.

(Paypers)

## MÁY IN THẺ ĐỂ BÀN ENTRUST®

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



Sigma DS3



Sigma DS2



Sigma DS1



Sigma DS4



Ribbon - Phôi thẻ

HOTLINE  
0903.481.456

contact@mkgroup.com.vn

## Mastercard hợp tác thu thập thông tin sinh trắc của 30 triệu dân châu Phi

*Liên doanh giữa Community Pass (thành viên của Mastercard) và đối tác Paycode dự định thu thập thông tin sinh trắc học của 30 triệu cá nhân ở những vùng hẻo lánh của châu Phi trong vòng 3 năm tới. Kế hoạch này nhằm mục đích phát hành thẻ thông minh sinh trắc Mastercard Community Pass chạy các nền tảng của Paycode để cung cấp định danh sinh trắc số và tài khoản ngân hàng số.*

Thông tin sinh trắc học khuôn mặt và lòng bàn tay của người dùng được lưu trữ trong một con chip trên thẻ thông minh Community Pass của Mastercard. Paycode, một đối tác trong chương trình thúc đẩy kinh doanh của Mastercard, sẽ vận hành nền tảng cung cấp dịch vụ định danh sinh trắc học (không phải là căn cước công dân) và các dịch vụ tài chính như tài khoản ngân hàng kỹ thuật số cho chủ thẻ.

Các dịch vụ có thể được truy cập ngoại tuyến trong thời gian thực. Người dùng không cần sử dụng tài liệu định danh hiện có.

Năm 2014, Mastercard cũng đã tham gia vào một chương trình thử nghiệm ở Nigeria, với việc phát hành 13 triệu thẻ ID sinh trắc học mang thương hiệu Mastercard được tích hợp công nghệ trả trước của tổ chức thẻ này./.

*(Biometric Update)*



Nguồn: Internet



## DÒNG MÁY IN THẺ SIGMA DS

được thiết kế đặc biệt phù hợp với các môi trường đám mây, thiết bị cho phép các khách dễ dàng triển khai các chương trình phát hành thẻ tài chính ngay lập tức mà vẫn đảm bảo tính bảo mật.

- **Đơn giản:** Hướng dẫn thao tác trực quan sinh động giúp cải thiện trải nghiệm người dùng cuối cùng với các vật tư và phụ kiện hỗ trợ máy đầy đủ.
- **Bảo mật:** Máy in được xây dựng với các tính năng bảo mật hàng đầu như nền tảng mô đun tin cậy, khởi động an toàn với khả năng mở rộng liên mạch của Entrust đạt chứng chỉ PCI-CP.
- **Thông minh:** Thiết kế mô đun hóa mang lại sự linh hoạt đáp ứng mọi nhu cầu phát hành thẻ, bao gồm việc thiết kế nhiều khay đựng thẻ cùng với các băng mực có thể tháo rời, người dùng có thể dễ dàng truy cập và có thể nâng cấp các mô đun trong tương lai khi Entrust cập nhật các công nghệ cải tiến cho máy in thẻ để bàn.

MK Group – Entrust, đối tác tin cậy trong việc xây dựng và triển khai các chương trình Thẻ thành công – bảo mật và giúp tối ưu hóa chi phí đầu tư của mọi tổ chức



Nguồn: Internet

## HỆ THỐNG PHÁT HÀNH THẺ CÔNG SUẤT LỚN DATACARD® MX

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

## Giao dịch bán vé điện tử toàn cầu đạt mức 33,8 tỷ lượt vào năm 2023

Theo dự báo của Juniper Research, tổng khối lượng giao dịch mua vé điện tử trên toàn thế giới sẽ tăng 62% - từ 20,8 tỷ lượt trong năm 2021 lên 33,8 tỷ lượt vào năm 2023, trong đó, vé xe buýt và tàu điện ngầm chiếm 1/3 (tương đương 33%).

Juniper Research cũng dự đoán rằng tỷ lệ giao dịch bán vé điện tử không tiếp xúc trên toàn cầu sẽ đạt mức trên 23% vào năm 2026, so với 10% trong năm 2019.

Juniper Research nhận định: “Bán vé không tiếp xúc đang phát triển mạnh mẽ trong quá trình phục hồi sau đại dịch. Do nhiều hãng vận tải mở rộng triển khai chương trình bán vé không tiếp xúc giữa đại dịch, xu hướng này đã đẩy nhanh tiến trình áp dụng hình thức bán vé điện tử”.

Juniper Research viết tiếp: “Báo cáo dự đoán rằng thanh toán không tiếp xúc sẽ tăng tốc do sự thay đổi lâu dài trong hành vi của người tiêu dùng sau đại dịch, và trào lưu này sẽ được phản ánh trong lĩnh vực bán vé, khi hoạt động bán vé không tiếp xúc chiếm tỷ trọng ngày càng lớn tại các hãng vận tải”./.

(NFCW)



Hệ thống công suất tầm trung MX6100, MX2100, MX1100

Hệ thống công suất lớn MX9100, MX8100

HOTLINE  
0903.481.456

[www.contact@mkgroup.com.vn](mailto:www.contact@mkgroup.com.vn)

## Tổng quan về nguy cơ gian lận trong nửa đầu năm 2021

*Khi chúng ta bước vào giai đoạn mới của đại dịch, vaccine ngừa COVID-19 đã giúp một số khu vực mang lại cảm giác về trạng thái bình thường. Trong nửa đầu năm 2021, do độ phủ vaccine được mở rộng, nên số lượng những sự kiện trực tiếp, các cửa hiệu, nhà hàng và văn phòng được mở lại cũng tăng theo. Giai đoạn mới đã và đang mở ra những xu hướng số hóa khác biệt.*

Báo cáo này sử dụng những thông tin thu thập được từ mạng lưới NuData Security toàn cầu - một thành viên của Mastercard - trong nửa đầu năm 2021 để khám phá thế giới “lai”, là sự kết hợp giữa các hoạt động trực tuyến và ngoại tuyến, như mua hàng trực tuyến và nhận hàng tại cửa hiệu (BOPIS). Trong số hàng triệu sự kiện mà NuData Security theo dõi và ghi lại hàng ngày, chúng tôi nhận thấy giới gian lận đã ứng phó với sự phát triển của hệ sinh thái số phức tạp hiện nay bằng cách tinh chỉnh và chuyên biệt hóa những cuộc tấn công của chúng.

### Tóm lược những xu thế lớn trên toàn cầu:

- **Trải nghiệm “lai” ngày càng đóng vai trò quan trọng trong mọi lĩnh vực:** Ngay cả khi nhiều người tiêu dùng (NTD) quay trở lại mua sắm trực tiếp, lưu lượng mua hàng thông qua kênh thương mại điện tử trong nửa đầu năm 2021 đã tăng 51% so với cùng kỳ năm 2020, qua đó cho thấy tầm quan trọng ngày càng cao của sự kết hợp liền mạch giữa trải nghiệm bán lẻ trực tuyến và ngoại tuyến. Lưu lượng truy cập tại các tổ chức tài chính (FI) cũng tăng 16%, và khối lượng giao dịch chuyển tiền tăng 23%, qua đó phản ánh mong muốn của NTD về khả năng duy trì tính tiện lợi của kênh ngân hàng trực tuyến, ngay cả khi các chi nhánh truyền thống mở cửa trở lại.
- **Doanh số bán vé sự kiện tăng cao, đi kèm với tình trạng bùng phát số vụ tấn công:** Khi những sự kiện lớn như hòa nhạc và lễ hội được phép tổ chức trở lại, các công ty bán vé sự kiện đã chứng kiến lưu lượng truy cập vào các dịch vụ tăng hơn gấp đôi trong nửa đầu năm 2021. Thật không may, số vụ tấn công cũng tăng tới 2,4 lần trong cùng kỳ, và 59% trong đó được thực hiện một cách tinh vi. Vì vậy, các công ty bán vé sự kiện cần trang bị những công cụ phù hợp để khắc chế những mối đe dọa này.
- **Những cuộc tấn công tinh vi tiếp diễn với trình độ ngày càng cao:** Những cuộc tấn công tự động tinh vi chiếm phần lớn tổng số vụ tấn công nhằm vào các sự kiện, kênh bán lẻ và thương mại điện tử, streaming và du lịch. Thông qua thủ đoạn mô phỏng hành vi của con người, những cuộc tấn công này có thể tránh được sự phát hiện của các công cụ bảo mật tiêu chuẩn. Khi những cuộc tấn công “trình độ cao” trở nên phổ biến, các công ty sẽ cần phải có nhiều biện pháp bảo vệ tiên tiến hơn để đối phó với chúng.
- **Hàng loạt thông tin đăng nhập bị đánh cắp dẫn đến xu hướng nở rộ “card cycling”:** Do nhiều hoạt động phải chuyển qua kênh trực tuyến trong đại dịch, giới gian lận đã tăng gấp đôi nỗ lực đánh lừa người dùng tiết lộ thông tin cá nhân. Mức tăng 54% của “card cycling” (tạm dịch là “kiểm tra thẻ bằng hình thức xoay vòng”) - một phương pháp dùng để kiểm tra tính hợp lệ của thông tin xác thực bị đánh cắp - là một dấu hiệu cho thấy sự thành công của những chiêu trò gian lận này.

## MÁY IN THẺ TÀI CHÍNH SIGMA DS4

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



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

HOTLINE  
0903.481.456

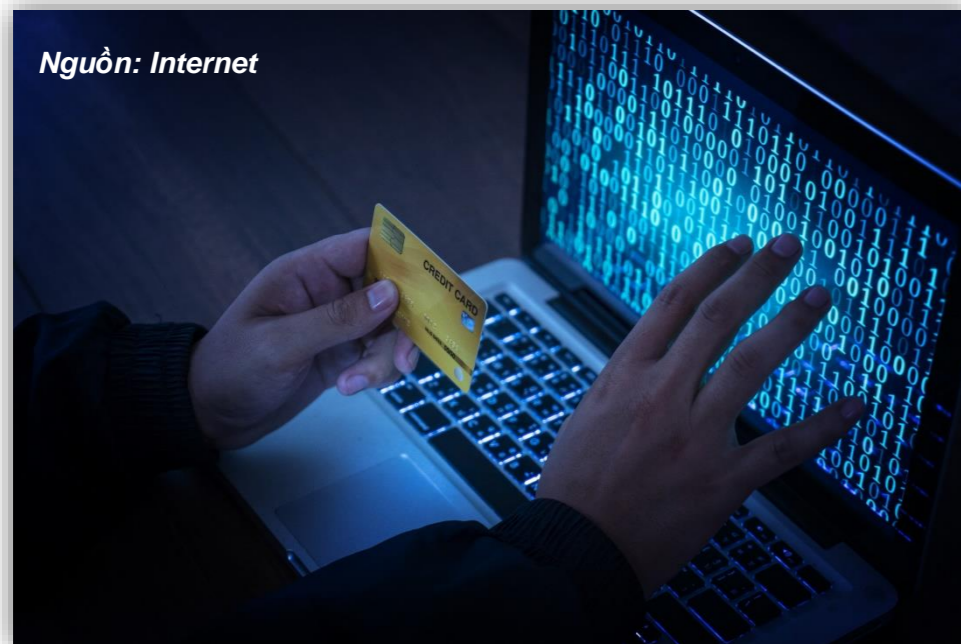
[www.contact@mkgroup.com.vn](http://www.contact@mkgroup.com.vn)

- **Giới gian lận nâng cao tỷ lệ thông tin đăng nhập thành công:** Tỷ lệ bình quân của thông tin đăng nhập hợp lệ được sử dụng trong một cuộc tấn công đã tăng vọt lên mức 9,9%, so với mức khoảng 1,9% của năm 2020. Đây có thể là dấu hiệu cho thấy những đối tượng tấn công đã tiếp cận được thông tin đăng nhập chất lượng cao thông qua các vụ lừa đảo hoặc xâm phạm dữ liệu - hoặc đóng vai trò là dấu hiệu cho thấy những cuộc tấn công tinh vi cố ý nâng cao tỷ lệ thông tin đăng nhập thành công một cách giả tạo để trốn tránh các biện pháp bảo mật dựa trên quy tắc.

### Chiều hướng gian lận trên thế giới: Mức độ nguy hiểm ngày càng cao của những cuộc tấn công tinh vi

#### Tiếp diễn những cuộc tấn công tinh vi

Mức độ phổ biến của những cuộc tấn công tự động tinh vi - trong đó mô phỏng hành vi của con người để tránh bị phát hiện - là mối quan ngại lớn trong nửa đầu năm 2021. Bằng cách bắt chước thao tác nhấn phím và di chuyển chuột của con người, cùng một số hành vi khác, và thậm chí mô phỏng hành vi của con người khi xử lý CAPTCHAS hoặc vượt qua các thách thức bảo mật khác, những bot này có thể đánh lừa các công cụ phát hiện bot tiêu chuẩn thông qua đội ngũ nhân viên. Nếu một công ty không triển khai sẵn sàng các biện pháp bảo mật mạnh mẽ, những cuộc tấn công tinh vi có thể gây ra thiệt hại nghiêm trọng.



Nguồn: Internet

Smart Digital Security

MAKE ENCRYPTION HAPPEN

## MÃ HÓA DỮ LIỆU EMAIL DOANH NGHIỆP

# ZED!

- Mã hóa các tệp tin trong quá trình truyền.
- Các file dữ liệu sẽ được đóng gói trước khi gửi ra ngoài, Prim'X gọi dữ liệu được đóng gói này với cái tên "vali ngoại giao". Vali này được bảo mật bất kể người dùng sử dụng phương tiện gì để trao đổi dữ liệu (email, các thiết bị lưu trữ ngoại vi, qua các giao thức truyền file, ...), chỉ người nhận mới có quyền mở vali bằng mật khẩu, chứng thực PKI, smart card, ...

Chứng chỉ

www.mk.com.vn - contact@mkgroup.com.vn HN: (84-24) 7100 6781 - HCMC: (84-28) 3930 5023

Năm 2019, số vụ tấn công tinh vi lần đầu tiên tăng đột biến trong lĩnh vực dịch vụ tài chính, trước khi lan sang các ngành dọc khác như bán lẻ vào năm 2020. Trong nửa đầu năm 2021, chúng chiếm phần lớn trong tổng số vụ việc tại 4 trong 6 lĩnh vực mà NuData Security khảo sát - gồm hàng hóa số, bán vé sự kiện, tổ chức tài chính, bán lẻ và thương mại điện tử, streaming và du lịch. Đặc biệt, trong lĩnh vực bán vé sự kiện, những cuộc tấn công tinh vi tăng theo cấp số nhân, do tình trạng gian lận vé tồn kho - trong đó, các đối tượng gian lận sử dụng bot để mua số lượng vé lớn nhằm phục vụ cho ý đồ bán lại. Mặc dù xu hướng tấn công tinh vi trong mọi lĩnh vực được khảo sát đều không cho thấy dấu hiệu hạ nhiệt, song các công ty có định hướng cách tân hơn đang nỗ lực cải thiện hàng rào bảo mật, triển khai những công cụ phân tích hành vi để sẵn sàng đối phó.

#### Nở rộ "Card cycling"

Trong nửa đầu năm 2021, NuData Security đã ghi nhận "card cycling" tăng 54% so với cùng kỳ năm ngoái. Trong một cuộc tấn công nhồi thông tin xác thực, "card cycling" đóng vai trò là một phương pháp kiểm tra tính hợp lệ của thông tin thanh toán bị đánh cắp.

Khi bot tự động của kẻ gian "xoay tua" danh sách các số thẻ tín dụng bị đánh cắp hoặc dữ liệu khác, nó sẽ ghi lại tài khoản thẻ nào bị từ chối và tài khoản thẻ nào được chấp nhận. Vào cuối chu trình, đối tượng lừa đảo sẽ có được bản danh sách các số thẻ tín dụng hợp lệ mà chúng có thể sử dụng để tự mua hàng hoặc bán lại trên thị trường chợ đen với giá cao.

Tình trạng nở rộ “card cycling” là một dấu hiệu tiêu cực về xu hướng gia tăng tổng thể của vấn nạn gian lận tài chính trực tuyến trong thời kỳ đại dịch. Do có nhiều NTD giao dịch trực tuyến hơn, giới gian lận đang cố gắng tìm ra những chiêu trò mới để đánh lừa họ chia sẻ thông tin cá nhân. Một số chiêu trò trong đó sở hữu trình độ kỹ thuật rất cao - chẳng hạn như những cuộc tấn công sử dụng lớp phủ để đánh cắp thông tin bằng cách phủ một cửa sổ trong suốt, vô hình lên bàn phím cảm ứng trên màn hình thiết bị di động của người dùng.

### *Biện pháp khắc chế “card cycling”*

“Card cycling” gây ra những rủi ro cả về tiền của và uy tín cho các doanh nghiệp. Nếu kẻ xấu thử nghiệm thành công thông tin thanh toán bị đánh cắp trên ứng dụng hoặc trang web của bạn, chúng cũng có thể sẽ thử tiến hành giao dịch mua hàng gian lận - dẫn đến những khoản bồi hoàn và nguy cơ gây thiệt hại cho lợi nhuận của doanh nghiệp. Triển khai hành động để khắc chế “card cycling” cũng tránh được thiệt hại đối với thương hiệu.

Nếu ứng dụng các giải pháp bảo mật thích hợp trên trang web hoặc ứng dụng thương mại điện tử, bạn sẽ dễ dàng phát hiện ra những thủ đoạn “card cycling”. Bất kỳ người dùng nào nhập nhiều số thẻ tín dụng khác nhau một cách liên tiếp và nhanh chóng từ cùng một địa chỉ IP đều có thể là một “card cyclist”. Giám sát những dấu hiệu mang tính hành vi như nhấp gõ phím cũng có thể giúp xác định hoạt động được tự động hóa, trong đó có các tập lệnh “card cycling”.

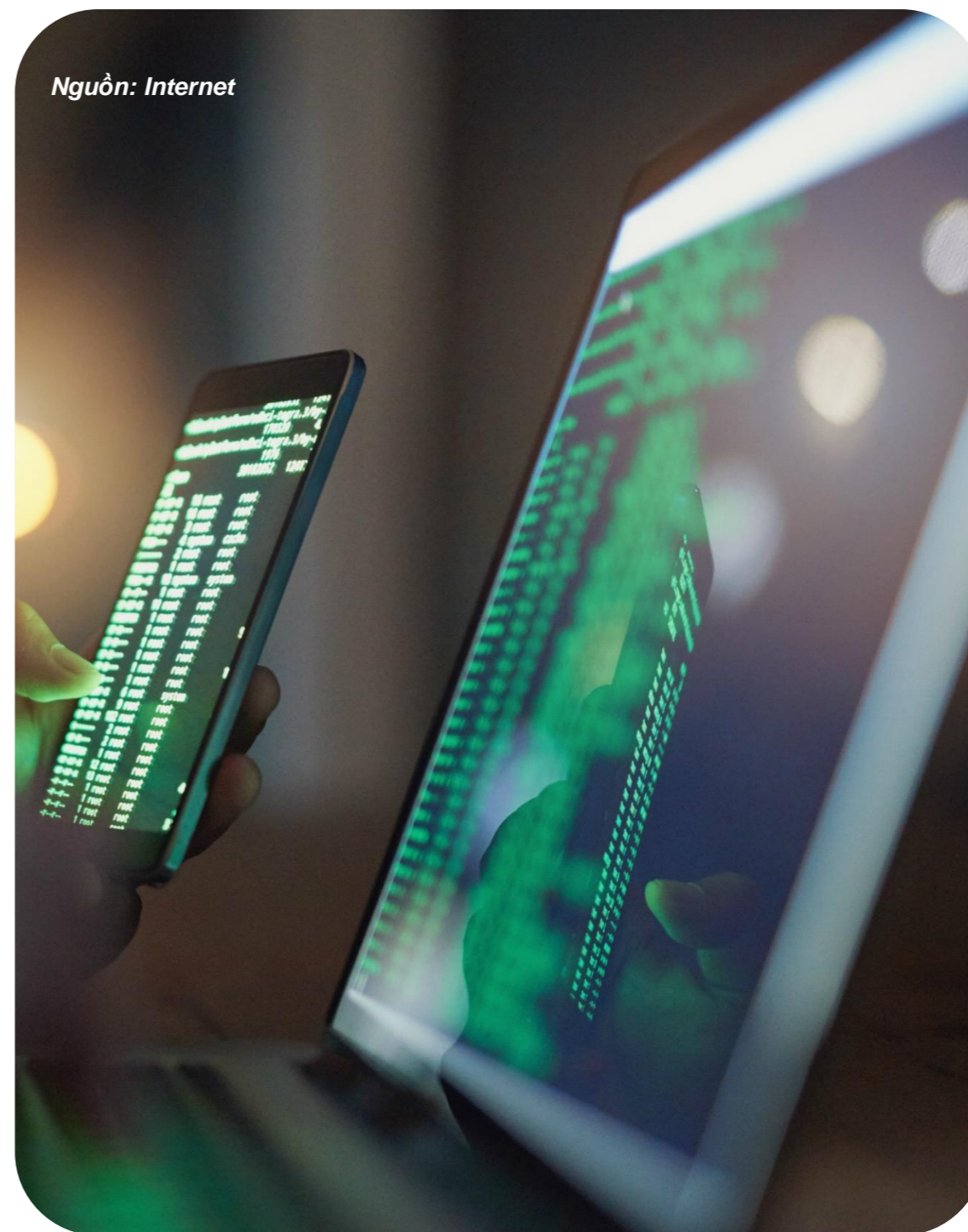
### **Mức độ thành công của những cuộc tấn công đăng nhập gia tăng đột biến**

Theo thời gian, NTD đóng tài khoản email, thay đổi mật khẩu và hủy thẻ tín dụng, vì vậy, phần lớn thông tin cá nhân bị đánh cắp được kẻ gian sử dụng đều đã lỗi thời hoặc không chính xác, buộc chúng phải kiểm tra xoay vòng (card cycling) số lượng lớn thông tin xác thực chỉ nhằm mục tiêu có được một lần truy cập thành công.

Trên thực tế, chỉ có từ 0,5% đến 2% tổng số vụ tấn công đăng nhập (trong tất cả các lĩnh vực được khảo sát) sử dụng thông tin đăng nhập chính xác. Kết quả đó có vẻ thấp, nhưng khi một cuộc tấn công tự động duy nhất có thể nhập vào 1 triệu thông tin đăng nhập, thì 0,5%-2% trong tổng số nỗ lực tấn công đăng nhập thành công sẽ dẫn đến hàng nghìn tài khoản bị xâm nhập và có thể gây ra nhiều thiệt hại nếu các biện pháp bảo vệ khác không được triển khai để ngăn chặn hành vi này.

Trong nửa đầu năm 2021, tỷ lệ sử dụng thành công thông tin đăng nhập bình quân mà chúng tôi ghi nhận được trên mạng lưới NuData Security toàn cầu đã gia tăng đột biến lên mức 9,9%, so với mức khoảng 1,9% của năm 2020. Bước nhảy vọt này phần lớn xảy ra trên các kênh bán lẻ, streaming và bán vé sự kiện, trong khi lĩnh vực tài chính vẫn duy trì mức độ ổn định cao nhất.

*Nguồn: Internet*



Mặc dù không thể lý giải chính xác về nguyên nhân dẫn đến tình trạng gia tăng tỷ lệ sử dụng thành công thông tin đăng nhập - đặc biệt là tại sao tình trạng này lại diễn biến phức tạp trong nhiều lĩnh vực, song chúng tôi xin được liệt kê ra 4 căn nguyên tiềm tàng như sau:

### 1. Những vụ xâm phạm dữ liệu chưa bị phát hiện

Theo IBM, phải mất bình quân 287 ngày trước khi một vụ xâm phạm dữ liệu bị phát hiện và ngăn chặn. Tỷ lệ sử dụng thành công thông tin đăng nhập cao trong một lĩnh vực nhất định có thể là dấu hiệu cho thấy một công ty trong lĩnh vực đó đã phải hứng chịu một vụ xâm phạm dữ liệu chưa xác định được, dẫn đến việc rò rỉ một lượng lớn thông tin cá nhân.

### 2. Kẻ gian ưu tiên tấn công những lĩnh vực đang phát triển nhanh chóng

Quá trình chuyển đổi số trong thời kỳ đại dịch diễn ra cực kỳ nhanh chóng, khiến nhiều đơn vị kinh doanh phải xử lý lượng lớn dữ liệu khách hàng trực tuyến trong lúc không có nhiều kinh nghiệm bảo vệ dữ liệu. Kẻ gian, vốn biết được thực trạng này, có thể đang nhắm mục tiêu vào những lĩnh vực bắt đầu phát triển theo hướng số hóa trong 18 tháng qua, bởi vì các lĩnh vực này có thể được coi là có ít kinh nghiệm ứng dụng các biện pháp kiểm soát bảo mật và gian lận.

### 3. Tấn công gian lận (phishing) gia tăng

Kẻ gian đang có được nhiều thông tin xác thực hợp lệ thông qua những vụ tấn công gian lận, vốn gia tăng đột biến trong thời kỳ đại dịch. Năm 2020, Google đã ghi nhận kỷ lục 2 triệu trang web lừa đảo, tăng gần 20% so với năm 2019.

### 4. Tài khoản giả (được tạo ra để đóng vai trò) là một phần của những cuộc tấn công tinh vi

Nhiều công cụ bảo mật dựa trên quy tắc tự động gắn cờ người dùng có tỷ lệ sử dụng thành công thông tin đăng nhập thấp là bot tiềm tàng. Để tránh bị phát hiện, một số đối tượng gian lận đã nghĩ ra thủ đoạn nâng cao tỷ lệ thành công một cách giả tạo bằng cách tạo ra nhiều tài khoản giả.

### Kết luận

Hiện nay, các công ty vẫn cảm nhận được tác động từ tình trạng bùng phát vấn nạn lừa đảo và những hình thức gian lận khác trong thời kỳ đại dịch. Số lượng lớn thông tin xác thực bị đánh cắp trong các vụ việc như vậy có thể đã góp phần nâng tỷ lệ sử dụng thành công thông tin đăng nhập lên mức cao kỷ lục, cũng như thúc đẩy tần suất sử dụng “card cycling”. Những xu hướng này có thể sẽ tiếp diễn đến hết năm 2021, vì vậy, yêu cầu xây dựng các biện pháp bảo mật mạnh mẽ nhằm đối phó với những cuộc tấn công vừa đề cập (ngay cả khi chúng cung cấp thông tin xác thực phù hợp) ngày càng trở nên quan trọng hơn đối với các tổ chức./.

(NuData Security)



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



**Công ty thành viên**



**Copyright© 2021 by MK Group**

[www.mkgroup.com.vn](http://www.mkgroup.com.vn) | [contact@mkgroup.com.vn](mailto:contact@mkgroup.com.vn)

[www.facebook.com.vn/mkgroup1999](https://www.facebook.com.vn/mkgroup1999)

**Headquarters in Hanoi:**

2<sup>nd</sup> floor, The Vista Building, No. 4, 15  
Lane Duy Tan Str., Cau Giay Dist.

**Tel:** (+84-24) 7100 6781

**Ho Chi Minh City:**

7<sup>th</sup> floor, Thien Son Building, 5 Nguyen  
Gia Thieu St., Ward 6, District 3

**Tel:** (+84-28) 3930 5023