CÁC VẤN ĐỀ BẢO MẬT THANH TOÁN BẰNG THẺ TÍN DỤNG TRONG GIAO DỊCH THƯƠNG MẠI ĐIỆN TỬ

ISSUES WITH CREDIT CARD PAYMENT SECURITY IN E-COMMERCE TRANSACTIONS

Lý Kiến Long, Trần Ngọc Tú, Phan Nhật Phi, Nguyễn Huy Hoàng, Phạm Việt Thiên Phúc

Trường Đại học Kinh tế - Tài chính TP. HCM

***Tóm tắt**: Với sự phát triển nhanh chóng của công nghệ và sự gia tăng của giao dịch thanh toán trực tuyến, việc sử dụng thẻ tín dụng để thanh toán thông qua các ứng dụng điện tử trở thành một trong những phương pháp phổ biến và tiện lợi nhất. Tuy nhiên, đi kèm với sự tiện ích đó là những mối đe dọa liên quan đến an toàn thông tin cá nhân và tài chính của người dùng. Mục tiêu chính của nghiên cứu này là làm rõ các vấn đề bảo mật khi sử dụng thẻ tín dụng trong quá trình thanh toán điện tử. Sau khi phân tích dựa trên tình hình mất an toàn trong thanh toán điện tử tại khu vực Đông Nam Á và ở Việt Nam, kết quả nghiên cứu đã chỉ ra các mối đe dọa khi thanh toán bằng thẻ trong giao dịch thương mại điện tử bao gồm: Lừa đảo thẻ tín dụng, Ứng dụng độc hại, Phishing, Mã độc tấn công. Từ đó, nghiên cứu đề ra một số giải pháp và đề xuất thuật toán nhằm tăng cường bảo mật an toàn thông tin sẽ giúp công ty thương mại điện tử tránh được các rủi ro bảo mật nguy hiểm có thể ảnh hưởng tới quá trình kinh doanh và cũng như trải nghiệm an toàn của khách hàng.*

***Từ khóa:** Vấn đề bảo mật, thẻ tín dụng, phương thức thanh toán, giao dịch, thương mại điện tử.*

***Abstract:** Credit card use for online payments has grown in popularity and convenience as a result of the quick development of technology and the increase in online payment transactions. But along with such ease come risks to the privacy of consumers' financial and personal information. This study's main goal is to explain security concerns with credit card use for online purchases. The research findings have highlighted risks while using a card in e-commerce transactions after assessing the risky scenario in Southeast Asia and Vietnam, including Phishing, malware attacks, malicious applications, and credit card fraud. From then, the report offers several recommendations and suggests algorithms to improve information security and safety, which will assist e-commerce businesses in avoiding risky security situations that might negatively impact their operational procedures and secure client experience.*

***Keywords**: E-commerce security concerns, credit cards, payment methods, transactions, e-commerce*

I. GIỚI THIỆU

Với sự phát triển nhanh chóng của công nghệ và sự gia tăng của giao dịch thanh toán trực tuyến, việc sử dụng thẻ tín dụng để thanh toán thông qua các ứng dụng điện tử trở thành một trong những phương pháp phổ biến và tiện lợi nhất. Hãy nói về Hoa Kỳ, một trong các nước sử dụng phương thức thanh toán bằng thẻ tín dụng nhiều nhất và hiện là thị trường thương mại điện tử lớn thứ hai trên thế giới.

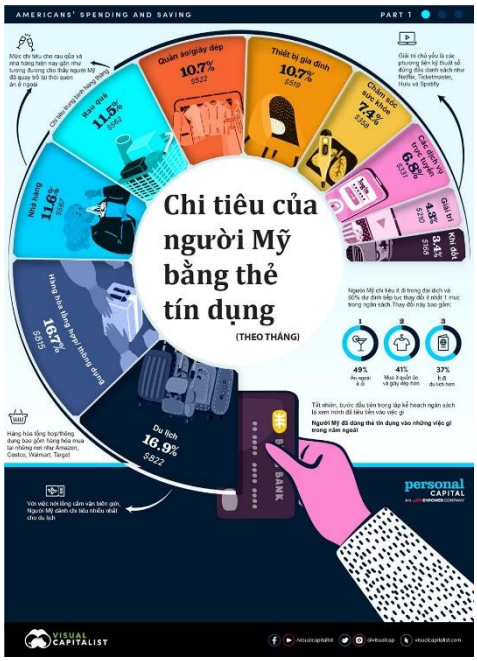
Nhà giàu Mỹ "quẹt" thẻ tín dụng hàng tháng thế nào?

Trong khi tiền mặt vẫn là vua, **86%** người Mỹ sử dụng thẻ cho ít nhất một số giao dịch mua hàng của họ. Người ta thường thấy người Mỹ sử dụng thẻ tín dụng cho tất cả mọi thứ, lớn và nhỏ. Các lý do cho điều này bao gồm sự tiện lợi, phần thưởng thẻ tín dụng, cộng với cơ hội tài trợ cho các giao dịch mua theo thời gian và xây dựng lịch sử tín dụng. Từ tháng 11 năm 2020 đến tháng 10 năm 2021 - khoảng thời gian đại dịch COVID-19 bao trùm không chỉ nước Mỹ mà trên toàn thế giới, Personal Capital đã thực hiện một khảo sát chi tiêu bằng thẻ tín dụng tại Hoa Kỳ.

Qua cuộc khảo sát của Personal Capital cho thấy, người dân chi tiêu cho du lịch nhiều nhất là 822 USD (16,9%), tiếp đến chi

tiêu hàng hóa tổng hợp/ thông dụng bao gồm hang hóa mua tại những nơi như Amazon, Costco, Walmart, Target là 815 USD (16,7%), chi tiêu ăn uống nhà hàng là 567 USD (11,6%), và chi tiêu cho giải trí (chú yếu là trực tuyến) là 331 USD (6,8%).

Đối tượng mà Personal Capital khảo sát chi tiêu bằng thẻ tín dụng dựa trên dữ liệu ẩn danh từ người dùng, là những người thu nhập cao hơn mức trung bình, có mức thu nhập ròng trung bình từ 405.000 - 1,3 triệu USD mỗi năm. Do đó, số tiền chi tiêu bằng thẻ tín dụng có thể cao hơn mức chi tiêu của dân số Mỹ nói chung.



Hình 1*. Đồ họa Việt hóa của cuộc khảo sát chi tiêu bằng thẻ tín dụng tại Mỹ của Personal Capital.*

Việc sử dụng phương thức thanh toán bằng thẻ tín dụng trong giao dịch thương mại điện tử ở nước Mỹ chiếm tỷ lệ phần trăm không hề nhỏ trong cuộc khảo sát. Vì vậy, việc tăng cường bảo mật là cần thiết với bất kỳ một doanh nghiệp hiện đại nào, không chỉ riêng e-commerce. Việc không ngừng cập nhật xu hướng an toàn thông tin sẽ giúp công ty thương mại điện tử tránh được các rủi ro bảo mật nguy hiểm có thể ảnh hưởng tới quá trình kinh doanh và cũng như trải nghiệm an toàn của khách hàng.

II. TỔNG QUAN

Có một số hành vi người tiêu dùng có thể dẫn đến rủi ro thanh toán bằng thẻ trong giao dịch thương mại điện tử. Những hành vi đó có thể là thói quen hằng ngày mà người dùng không thường xuyên để ý và gây ra hậu quả mất mát về tiền bạc:

- *Sử dụng mạng không an toàn:* Sử dụng mạng công cộng hoặc không bảo mật để thực hiện giao dịch online có thể làm cho thông tin thẻ của bạn dễ bị đánh cắp. Tin tặc có thể theo dõi hoặc giành quyền truy cập vào thông tin cá nhân và thông tin thanh toán của bạn. Hãy luôn sử dụng mạng an toàn, mã hóa (https) và kết nối VPN (mạng riêng ảo) để bảo vệ dữ liệu của bạn.
- *Mua sắm trên các trang web không đáng tin cậy:* Một số trang web không đáng tin cậy có thể giả mạo các trang web thương mại điện tử phổ biến để lừa đảo người mua hàng. Họ có thể yêu cầu bạn cung cấp thông tin thẻ tín dụng và sau đó sử dụng thông tin đó để tiến hành gian lận. Luôn luôn mua hàng trên các trang web có uy tín và được đánh giá tốt.
- *Mất kiểm soát thông tin thẻ:* Nếu bạn không kiểm soát thông tin thẻ của mình một cách cẩn thận, như lưu trữ thông tin trên các thiết bị không an toàn, như điện thoại di động không được bảo mật hoặc máy tính công cộng, có nguy cơ cao bị rò rỉ thông tin cá nhân. Điều này có thể dẫn đến việc sử dụng trái phép thông tin thẻ và gây thiệt hại tài chính.
- *Phản ứng không cẩn thận với các cuộc gọi, email lừa đảo:* Tin tặc có thể sử dụng các phương pháp xâm nhập như gửi email lừa đảo hoặc cuộc gọi điện thoại để lừa đảo bạn cung cấp thông tin cá nhân và thông tin thẻ tín dụng. Hãy luôn cảnh giác và không cung cấp thông tin nhạy cảm cho bất kỳ ai qua điện thoại hoặc email mà bạn không tin tưởng.

Tình hình mất an toàn trong thanh toán điện tử tại khu vực Đông Nam Á:

Nghiên cứu gần đây của Kaspersky vào năm 2020 cho thấy mối tương quan tích cực giữa việc áp dụng các phương thức thanh toán kỹ thuật số với nhận thức về các rủi ro và mối đe dọa liên quan ở Đông Nam Á. Kết

quả chỉ ra rằng nghiên cứu phát hiện rằng gần như tất cả những người được khảo sát ở Đông Nam Á (97%) đều nhận thức được ít nhất một loại đe dọa đối với các nền tảng thanh toán điện tử, trong khi gần 3/4 (72%) cá nhân đã gặp phải ít nhất một loại đe dọa liên quan đến công nghệ này. Đáng chú ý, lừa đảo phi kỹ thuật là mối đe dọa hàng đầu đối với hầu hết các quốc gia Đông Nam Á, bao gồm Indonesia (40%), Malaysia (45%), Philippines (42%), Singapore (32%) và Việt Nam (38%). Duy chỉ có Thái Lan có mối đe dọa hàng đầu là trang web giả mạo (31%).

Tình hình mất an toàn trong thanh toán điện tử tại Việt Nam:

Dưới đây là một số thông tin chung về tình hình mất an toàn trong thanh toán điện tử tại Việt Nam:

- Theo báo cáo của Công ty TNHH Bảo mật CNTT và Mạng Viettel (Viettel Cyber Security) năm 2020, Việt Nam đã ghi nhận 10.220 cuộc tấn công mạng vào hệ thống thanh toán điện tử. Trong số đó, có khoảng 7.920 cuộc tấn công liên quan đến lừa đảo thanh toán và 2.300 cuộc tấn công có mục tiêu là đánh cắp thông tin người dùng.
- Báo cáo của Công ty PwC (PricewaterhouseCoopers) năm 2020 cho thấy rằng 85% người dùng tại Việt Nam đã gặp ít nhất một lần rủi ro mất an toàn trong quá trình thanh toán điện tử, bao gồm lừa đảo thanh toán, tin tặc thẻ tín dụng và vi phạm bảo mật thông tin cá nhân.
- Theo Bộ Thông tin và Truyền thông Việt Nam, trong năm 2020, đã xảy ra 1.300 vụ vi phạm về an toàn thông tin, trong đó, một số vụ vi phạm liên quan đến mất an toàn trong thanh toán điện tử.

III. MỐI ĐE DỌA KHI THANH TOÁN BẰNG THẺ TRONG GIAO DỊCH THƯƠNG MẠI ĐIỆN TỬ

1. Lừa đảo thẻ tín dụng: Kẻ xấu có thể sử dụng thông tin thẻ tín dụng của bạn để thực hiện giao dịch trái phép. Điều này có thể xảy ra thông qua việc ăn cắp thông tin thẻ, gian lận trong quá trình thanh toán hoặc tấn công vào cơ sở dữ liệu của người bán.

Nguyên nhân: Kẻ lừa đảo có thể thu thập thông tin cá nhân của người khác, chẳng hạn như tên, địa chỉ, số điện thoại và ngày tháng năm sinh thông qua các phương tiện như email lừa đảo, điện thoại lừa đảo hoặc các trang web giả mạo.

2. Ứng dụng độc hại: Một số ứng dụng, tiện ích hoặc phần mềm độc hại có thể được cài đặt trên thiết bị của bạn khi bạn tải xuống từ các nguồn không đáng tin cậy. Những phần mềm này có thể giám sát và đánh cắp thông tin cá nhân, bao gồm thông tin thanh toán.

Nguyên nhân: Sự gia tăng của các ứng dụng và phần mềm độc hại đã tạo ra một môi trường nguy hiểm cho việc thanh toán trực tuyến. Kẻ tấn công thường sử dụng các kỹ thuật như phần mềm độc hại giả mạo, trojan[1], keyloggers[2] và man-in-the-browser[3] để đánh cắp thông tin cá nhân và thanh toán của người dùng.

3. Phishing: Kẻ tấn công có thể gửi email, tin nhắn hoặc trang web giả mạo nhằm lừa đảo bạn để tiết lộ thông tin thẻ tín dụng hoặc mật khẩu tài khoản. Những phương pháp này thường được thiết kế để trông giống như từ các tổ chức tin cậy như ngân hàng, người bán hoặc nhà cung cấp dịch vụ.

Nguyên nhân: Do sự thiếu hiểu biết và cảnh giác, người tiêu dùng không có đủ kiến

---

1 **Trojan:** là loại mã lây nhiễm máy tính ẩn trong các chương trình dường như vô hại hoặc sẽ cố lừa bạn cài đặt nó vào laptop

2 **Keyloggers:** thường là một phần mềm nhỏ gọn – hoặc đôi lúc nguy hiểm hơn thậm chí là một thiết bị phần cứng – với khả năng ghi lại mọi phím bấm mà người dùng đã nhấn trên bàn phím

3 **Man-in-the-browser:** là khi một Trojan được sử dụng để đánh chặn hoặc sửa đổi dữ liệu được gửi giữa trình duyệt và máy chủ web

thức về các phương thức tấn công trực tuyến như phishing, spoofing và keylogging. Họ có thể không nhận ra được các biểu hiện của các trang web giả mạo hoặc tin nhắn lừa đảo, và do đó dễ dàng rơi vào bẫy của tin tặc. Sử dụng mật khẩu dễ đoán hoặc yếu có thể dễ bị đoán được bởi tin tặc. Điều này làm cho tài khoản của bạn dễ bị xâm nhập và thông tin cá nhân bị lộ. Nếu người tiêu dùng sử dụng cùng một mật khẩu cho nhiều tài khoản, thì khi một tài khoản bị xâm nhập, tin tặc có thể truy cập vào các tài khoản khác.

4. Mã độc tấn công: Mã độc, chẳng hạn như mã độc đánh cắp thông tin (keyloggers) hoặc mã độc tạo ra các trang thanh toán giả (man-in-the-browser), có thể được sử dụng để lấy cắp thông tin thanh toán của bạn trong quá trình giao dịch trực tuyến.

Nguyên nhân: Kết nối không an toàn. Nếu người dùng thực hiện giao dịch thanh toán qua một kết nối mạng không an toàn, ví dụ như mạng Wi-Fi công cộng không được bảo mật, kẻ tấn công có thể theo dõi hoặc gián đoạn giao dịch để thu thập thông tin thanh toán. Kẻ tấn công tạo ra các trang web giả mạo của các trang thanh toán hoặc cửa hàng trực tuyến. Khi người dùng truy cập vào các trang web này và cung cấp thông tin thanh toán, thông tin này sẽ được kẻ tấn công thu thập và sử dụng để lừa đảo hoặc thực hiện giao dịch trái phép.

Minh chứng thực tế:

Chiêu thức giả mạo nhân viên, nâng cao hạn mức thẻ tín dụng để chiếm đoạt tiền Tại Hà Nội, 4 đối tượng bị công an khởi tố về tội lừa đảo chiếm đoạt tài sản bằng hình thức giả danh nhân viên ngân hàng và gửi đường link trang web giả mạo ngân hàng nâng hạng mức thẻ tín dụng để chiếm đoạt tiền Vào khoảng tháng 9 năm 2022, các đối tượng này đã sử dụng tài khoản Zalo ảo để kết bạn với nạn nhân. Đã xác định khoảng 700 người bị hại và số tiền lên tới hàng chục tỷ đồng. Trong 3 tháng đầu năm 2023, dự án Chống lừa đảo đã phát hiện tới 3.271 trang web lừa đảo người dùng Việt Nam cho thấy các cuộc tấn công lừa đảo có xu hướng gia tăng. chiếm phần lớn là các website lừa đảo tài chính, với 3.076 trang từ giả mạo những thương hiệu, nhãn hãng lớn như Tiki, Shopee, Lazada đến các trang dụ đầu tư tài chính Forex, nhị phân Binary Option… để lừa đảo chiếm đoạt tài sản của người dân. Đại diện dự án Chống lừa đảo cũng cho biết, hiện nay, hình thức lừa đảo phổ biến nhất vẫn là lừa tuyển cộng tác viên "việc nhẹ lương cao", giả mạo các trang sàn thương mại điện tử như Tiki, Shopee, Lazada và các thương hiệu lớn để chiếm đoạt tài sản của các nạn nhân. Khoản tiền các đối tượng lừa chiếm đoạt được từ hình thức này thường từ vài triệu đến vài trăm triệu đồng.... Trong năm 2022, Cục An toàn thông tin đã chỉ đạo, điều phối, ngăn chặn, xử lý hơn 2.700 trang web lừa đảo trực tuyến, vi phạm pháp luật. Bảo vệ 4,87 triệu người dân, tương đương 6,96% người dùng Internet Việt Nam trước các tấn công lừa đảo trực tuyến, vi phạm pháp luật trên không gian mạng. Trong 2 tháng đầu năm 2023, số cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam được Cục An toàn thông tin phát hiện, hướng dẫn xử lý gần 3.000. Trong đó, riêng tháng 2/2023 là 1.687 sự cố tấn công mạng, tăng 33,9% so với cùng kỳ năm ngoái.

Hình 2. *Lực lượng chức năng thu giữ tang chứng, vật chứng.*

IV. GIẢI PHÁP VÀ DỊCH VỤ CÓ MẶT TRÊN THỊ TRƯỜNG VIỆT NAM HIỆN NAY.

Dưới đây là một số giải pháp chi tiết và các dịch vụ có mặt trên thị trường tại Việt Nam nhằm khắc phục các mối đe dọa khi thanh toán bằng thẻ trong giao dịch thương mại điện tử:

1. Xác thực hai yếu tố (Two-Factor Authentication - 2FA):

- *Sử dụng mã OTP (One-Time Password):* Đây là một mã số duy nhất và có hiệu lực một lần được gửi đến điện thoại di động của người dùng để xác thực giao dịch. Ngân hàng như Vietcombank, VietinBank và ACB cung cấp dịch vụ OTP thông qua ứng dụng di động hoặc tin nhắn SMS.
- *Sử dụng mã xác thực 3D-Secure:* Đây là một hình thức xác thực giao dịch trực tuyến thông qua một mật khẩu độc lập hoặc thông qua ứng dụng xác thực từ nhà cung cấp thẻ tín dụng/debit.

2. Mã hóa dữ liệu (Data Encryption):

- *Sử dụng SSL/TLS (Secure Sockets Layer/Transport Layer Security):* Đây là một giao thức bảo mật sử dụng mã hóa dữ liệu giữa người dùng và trang web. Sự kết hợp giữa người dùng và trang web thông qua SSL/TLS đảm bảo rằng thông tin thanh toán được truyền qua một kênh an toàn.
- *Tokenization:* Phương pháp này thay thế thông tin thẻ tín dụng bằng một "token" duy nhất, không thể đoán được. Những token này được sử dụng trong quá trình thanh toán, giúp bảo vệ thông tin thẻ tín dụng.

3. Giám sát giao dịch (Transaction Monitoring):

Hệ thống phát hiện gian lận: Các ngân hàng và dịch vụ thanh toán trực tuyến thường có hệ thống phát hiện gian lận để giám sát các giao dịch bất thường và đáng ngờ. Các giao dịch đáng ngờ có thể bị chặn hoặc yêu cầu xác nhận bổ sung từ người dùng.

4. Ứng dụng di động an toàn (Secure Mobile Applications):

Sử dụng ứng dụng di động được bảo mật: Các ngân hàng và dịch vụ thanh toán cung cấp ứng dụng di động có tích hợp các tính năng bảo mật cao như xác thực hai yếu tố, xác thực vân tay hoặc nhận dạng khuôn mặt để đảm bảo an toàn trong quá trình thanh toán trực tuyến.

5. Hợp tác và phối hợp:

Các đối tác liên kết: Các tổ chức ngân hàng và dịch vụ thanh toán có thể hợp tác với nhau để chia sẻ thông tin về các mối đe dọa và kỹ thuật bảo mật mới nhất, từ đó tăng cường khả năng phòng ngừa và phát hiện gian lận.

Trong trường hợp phát hiện các hành vi gian lận hoặc bất thường, người dùng nên báo cáo cho ngân hàng hoặc dịch vụ thanh toán liên quan để họ có thể thực hiện các biện pháp cần thiết và ngăn chặn các mối đe dọa tiềm ẩn.

6. Tiêu chuẩn Giao dịch Điện tử An toàn (SET)

Các cấu phần tham gia vào giao dịch điện tử an toàn:

- Chủ thẻ
- Internet
- Doanh nghiệp
- Cổng thanh toán
- Ngân hàng thanh toán thẻ
- Mạng lưới thanh toán
- Ngân hàng phát hành thẻ
- Đơn vị cấp phép thanh toán.

Tiêu chuẩn Giao dịch Điện tử An toàn (SET) được phối hợp ban hành bởi MasterCard và VISA với mục tiêu đảm bảo an toàn và bảo mật thông tin cho các cá nhân, tổ chức tham gia vào việc thanh toán điện tử để thực hiện giao dịch mua bán online. SET đưa ra tiêu chuẩn và quy trình xử lý giao dịch như:

- Xác thực chủ thẻ và doanh nghiệp
- Bảo mật dữ liệu thanh toán
- Định nghĩa dịch vụ, nhà cung cấp dịch vụ bảo mật điện tử và giao thức bảo mật điện tử.

7. Công bố chương trình Bug Bounty

Bug Bounty (trao thưởng tìm lỗi) là giải pháp hiệu quả giúp bảo mật TMĐT nâng lên một tầm cao mới. Chương trình Bug Bounty khuyến khích các hacker mũ trắng và chuyên gia bảo mật tìm kiếm những lỗ hổng trên website/app TMĐT và báo cho doanh nghiệp. Bằng việc khắc phục những lỗ hổng bảo mật này, doanh nghiệp có thể hạn chế tối đa khả năng website, mobile app bị hack.

V. ĐỀ XUẤT GIẢI PHÁP

1. Theo dõi khối lượng lớn các đơn đặt hàng nhỏ

Một dấu hiệu thường xuyên của một cuộc tấn công thẻ là khối lượng lớn số lượng đặt hàng nhỏ. Những kẻ lừa đảo sử dụng bot thẻ tín dụng của họ để thử và mua các dịch vụ hoặc hàng hóa không đắt tiền với các chi tiết thẻ tín dụng khác nhau. Nếu một đơn đặt hàng thành công, kẻ lừa đảo sẽ chỉ bị tính một số tiền nhỏ. Vì vậy, hãy luôn theo dõi những đột biến bất thường trong nỗ lực mua hàng với giá rẻ.

2. Theo dõi các đơn hàng có chi phí vận chuyển cao

Tương tự, hãy theo dõi các đơn đặt hàng nhỏ từ những nơi nước ngoài, nơi chi phí vận chuyển cao hơn giá của chính sản phẩm. Hiếm khi có trường hợp ai đó có ý định tốt muốn trả nhiều tiền vận chuyển hơn cho sản phẩm thực tế. Ngay cả với khối lượng nhỏ, những đơn đặt hàng như vậy vẫn đáng để điều tra.

3. Đảm bảo IP khớp

Sử dụng kiểm tra vị trí địa lý IP để đảm bảo IP của người dùng khớp với địa chỉ thanh toán của họ trên trang thanh toán. Nếu không, người dùng có thể mua sắm từ một nơi nào đó khác ngoài địa chỉ trên thẻ tín dụng của họ. Mặc dù không phải là dấu hiệu gian lận ngay lập tức, vì nhiều người dùng duyệt qua VPN để có thêm quyền riêng tư, nhưng nó có thể được sử dụng kết hợp với các mẹo khác trong bài viết này để xác định xem đó có phải là một cuộc tấn công thẻ hay không.

4. Xây dựng một danh sách chặn khách hàng

Bất kỳ cá nhân nào được biết đến là người phạm tội gian lận nên được đưa vào danh sách chặn và không còn có thể mua sắm tại các cửa hàng trực tuyến của bạn nữa. Chính sách không khoan nhượng sẽ loại bỏ những người đã cố gắng tấn công cửa hàng của bạn và đóng vai trò cảnh báo cho bất kỳ ai khác đang nghĩ đến việc phát động một cuộc tấn công bẻ khóa thẻ.

5. Thẻ ủy quyền

Ủy quyền và nắm bắt là một cơ chế cho phép bạn ủy quyền trước tiên cho thẻ tín dụng của người dùng, kiểm tra xem chi tiết của thẻ có hợp lệ hay không và liệu thẻ có đủ tiền trước khi bạn thanh toán hay không. Điều này cho phép bạn xem xét bất kỳ giao dịch đáng ngờ nào có thể đã được thực hiện trong một cuộc tấn công thẻ trước khi thanh toán được thực hiện.

6. Kiểm tra tốc độ

Luôn theo dõi tốc độ người dùng đang cố gắng mua hàng hóa hoặc dịch vụ của bạn. Người dùng chính hãng thường không thực hiện nhiều giao dịch mỗi phút, nhưng bot thẻ tín dụng có thể thực hiện nhiều giao dịch mỗi giây. Vì vậy, hãy theo dõi tốc độ giao dịch của bạn, theo bất kỳ cách nào phù hợp nhất với bạn: Theo số tiền đô la, địa chỉ IP, địa chỉ thanh toán, thiết bị đã qua sử dụng, v.v.

7. Sử dụng AVS (Address Verification Service) và CVV (Card Verification Value)

Hệ thống xác minh địa chỉ (AVS) và Giá trị xác minh thẻ (CVV) là hai tính năng đơn giản để xác nhận rằng địa chỉ trên thẻ và CVV ba chữ số tại ngân hàng của thẻ phù hợp với những gì ngân hàng phát hành có trong hồ sơ. Sử dụng các tính năng này trong cổng thanh toán của bạn để khiến những kẻ lừa đảo khó thực hiện các cuộc tấn công thẻ hơn nhiều.

8. Sử dụng các công cụ phòng chống gian lận tự động và bảo vệ bot

Các giải pháp bảo mật truyền thống có xu hướng phụ thuộc nhiều vào danh tiếng IP, dựa trên giả định rằng bất kỳ hoạt động độc hại nào từ địa chỉ IP có nghĩa là tất cả các hoạt động từ IP đó có khả năng thù địch. Ngày nay, các tác nhân đe dọa phân phối bot thông qua IP dân cư, được hưởng lợi từ danh tiếng xuất sắc. Các yêu cầu họ gửi thường không thể phân biệt được với những yêu cầu do người dùng thông thường tạo ra. Do đó, các phương pháp tiếp cận dựa trên IP không còn hiệu quả nữa.

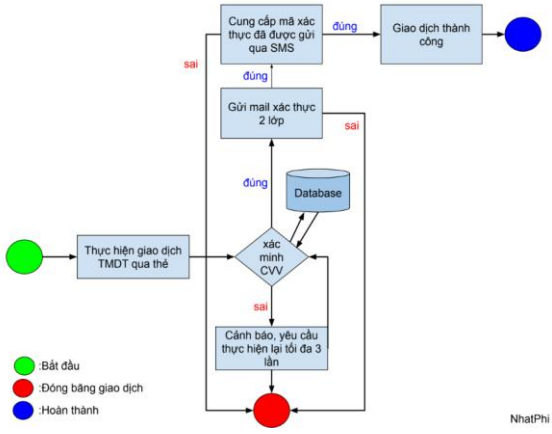
Để ngăn chặn việc bẻ khóa thẻ và đánh cắp thẻ, cộng với các cuộc tấn công bot tự động khác, một giải pháp bảo vệ bot với khả năng phát hiện hành vi theo thời gian thực là rất quan trọng.

Hình 3. *Sơ đồ hoạt động của công cụ ngăn chặn, phòng chống gian lận tự động và bảo vệ bot.*

Một giải pháp phát hiện bot tốt sẽ có thể nhanh chóng xác định chính xác hành vi bất thường của khách truy cập có dấu hiệu của các nỗ lực bẻ khóa thẻ và thẻ. Nó cũng sẽ tự động chặn các bot độc hại trước khi chúng có thể thực hiện bất kỳ giao dịch gian lận nào. Trong khi tất cả các hành động phòng ngừa và phòng thủ này xảy ra, trải nghiệm người dùng cho khách truy cập con người chính hãng được duy trì.

VI. ĐỀ XUẤT THUẬT TOÁN

Các cuộc tấn công bẻ khóa thẻ và thẻ chủ yếu là các cuộc tấn công do bot điều khiển để kiểm tra tính hợp lệ của dữ liệu thẻ hoặc chứng từ bị đánh cắp. Chúng tiêu tốn của các nhà bán lẻ hàng tỷ doanh thu mỗi năm



và có thể gây ra thiệt hại nghiêm trọng về danh tiếng cho thương hiệu của bạn. Cách tốt nhất để ngăn chặn các cuộc tấn công bẻ khóa thẻ (và tất cả các hình thức đe dọa bot khác) là với giải pháp bảo vệ bot nâng cao ngăn chặn các bot tinh vi nhất truy cập vào trang web, ứng dụng và API của bạn.

Nếu các bot xấu hiện đang sử dụng các công nghệ và thiết bị giống như con người, đến từ cùng một địa chỉ IP và hoạt động giống hệt như chúng ta, thì cần những loại kỹ thuật phát hiện bot nào để phân biệt bot với con người một cách hiệu quả?

Hãy chia nhỏ cách hoạt động của công cụ phát hiện mối đe doạ khi thanh toán bằng thẻ. Đây là tổng quan các yếu tố và quá trình hoạt động:

- *Tín hiệu yêu cầu:* Chúng tôi trích xuất hàng trăm tín hiệu khác nhau từ mỗi yêu cầu và thêm thông tin bổ sung vào dữ liệu được thu thập.
- *Bot đã được xác minh & Quy tắc tùy chỉnh:* Nếu chúng tôi nhận ra khách truy cập là một bot được liệt kê tốt hoặc được cho phép, nó được phép tiếp tục.
- *Phát hiện bot dựa trên chữ ký*: Nếu yêu cầu mang chữ ký bot xấu vốn đã quen thuộc, nó sẽ bị chặn.
- *Phát hiện bot học máy:* Chúng tôi sử dụng cả học máy có giám sát và không giám sát để xác định các mẫu bot mới trong thời gian thực, bao gồm các tín hiệu phát hiện hành vi.
- *Phản hồi:* Cho phép con người, chặn bot hoặc hiển thị cho người dùng - chỉ khi vẫn còn bất kỳ nghi ngờ nào về hoạt động của bot.

Lược đồ có thể trông giống như một quá trình tuyến tính, nhưng quá trình phát hiện thực tế thì không: mọi thứ xảy ra trong thời gian thực. Khi một yêu cầu đi vào điểm cuối của khách hàng, quyết định phản hồi được đưa ra và áp dụng.

Thuật toán tổng hợp xếp chồng lên nhau ("mô hình chính" của chúng tôi) sau đó kết hợp các dự đoán từ các mô hình cơ sở và đưa ra quyết định cuối cùng: con người hoặc bot, và nếu là bot, loại nào?

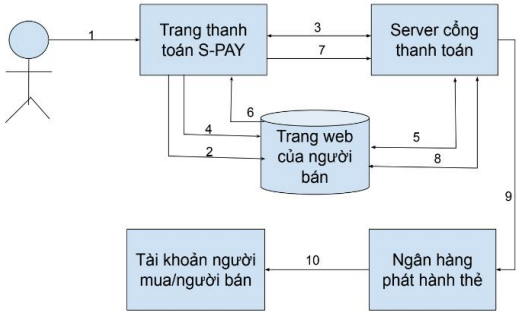
Hình 4. *Mô phỏng thuật toán của quá trình xác thực truy cập.*

Để có độ chính xác dự đoán tối đa, chúng tôi phân tích các bộ dữ liệu với các chi tiết khác nhau:

- Thông qua IP
- Xác thực CVV
- Email và lớp bảo mật
- SMS
- Chữ kí điện tử
- Database CVV khách hàng.

Quá trình thực hiện giao dịch được chúng tôi mô tả một cách chi tiết thông qua giải thích hoạt động của phần mềm dựa trên thuật toán chủ yếu bao gồm hai phần là trình duyệt S-PAY (trang thanh toán) và mô-đun xác thực.

Quá trình giao dịch chỉ có thể được truy cập bởi người dùng hợp pháp có mã CVV hoặc mật khẩu một lần dùng (OTP) được người dùng xác định.



Hình 5. *Mô phỏng quá trình giao dịch trực tuyến qua Spay.*

1. Khách hàng được yêu cầu nhập CVV của thẻ và mã OTP để truy cập hệ thống.

2. Sau khi đăng nhập thành công, khách hàng mở trình duyệt S-Pay để truy cập trang web của người bán và đặt hàng.

3. Hệ thống OTP trong mô-đun Xác thực của Pripay tự đồng bộ hóa với máy chủ cổng thanh toán.

4. Dự thảo yêu cầu ban đầu, ReqDraft được tạo tự động bởi S-pay và được mã hóa bằng khóa công khai (PublicKey) của cổng thanh toán.

5. Người bán gửi ReqDraft nhận được cho máy chủ cổng thanh toán, sau khi xác minh khách hàng sẽ thông báo cho người bán về tính xác thực của khách hang.

6. Sau đó, Người bán tạo hóa đơn giao dịch, TransBill là: TransBill = EnCrypt[(Merchant ID,Merchant's Acc.No.,Payment details),PRMER.

7. Khách hàng xác minh thông tin đơn đặt hàng và sau đó Mô-đun xác thực của S-pay gửi T_ID nhận được từ người bán tới cổng máy chủ thanh toán để xác thực người bán.

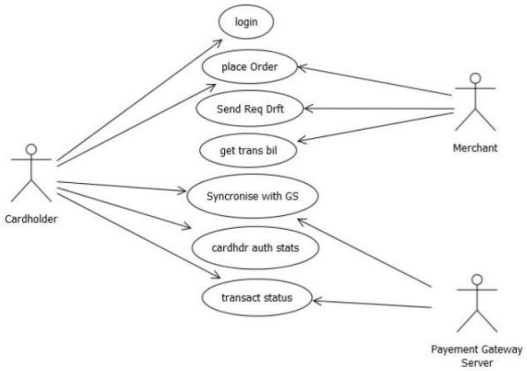
8. Máy chủ cổng thanh toán gửi T_ID cho người bán tương ứng và người bán lần lượt gửi TransBill cho máy chủ cổng thanh toán, sau đó sẽ giải mã TransBill bằng khóa công khai của người bán và ủy quyền cho người bán cũng như thông báo cho khách hàng rằng người bán đã được xác thực.

9. Máy chủ cổng thanh toán sau đó gửi chi tiết thanh toán và chi tiết của khách hàng (số thẻ tín dụng) cho ngân hàng phát hành.

10. Ngân hàng phát hành sau khi xác minh thanh toán sẽ chuyển khoản tiền được yêu cầu vào tài khoản/người mua của người bán và cả khách hàng và người bán đều được thông báo về trạng thái giao dịch.

Các tính năng bảo mật của S-pay

Chúng tôi đã mô tả S-pay hoạt động của phần mềm và bây giờ, chúng tôi xây dựng cấu trúc của Spayal cùng với các tính năng bảo mật của nó. Usecase diagram sử dụng của phần mềm Spay được hiển thị trong hình.



Hình 6. *Usecase diagram: Vai trò và chức năng giữa các bên tham gia.*

Xác thực sinh trắc học

Một khái niệm khác về bảo mật giao dịch điện tử trực tuyến là sử dụng sinh trắc học. Hoạt động sinh trắc học là ứng dụng rất phổ

biến để nhận dạng. Trên khắp thế giới, nhiều nhà nghiên cứu đã làm việc trong lĩnh vực tương tự. Sinh trắc học xác định con người bằng cách đo lường một số khía cạnh của các đặc điểm cá nhân như:

- Hình học bàn tay hoặc dấu vân tay.
- Các đặc điểm hành vi khác như chữ ký viết tay của bạn.
- Chẳng hạn như giọng nói của bạn.

Các công nghệ xác thực sinh trắc học như nhận dạng khuôn mặt, ngón tay, bàn tay, mống mắt và loa được sử dụng rộng rãi ngày nay và đã được sử dụng. Hệ thống sinh trắc học chủ yếu là hệ thống nhận dạng mẫu hoạt động bằng cách lấy dữ liệu sinh trắc học từ một người, trích xuất một tính năng từ dữ liệu và so sánh các tính năng được trích xuất với dữ liệu được lưu trữ trong cơ sở dữ liệu. Hệ thống sinh trắc học hoạt động ở hai chế độ chế độ xác minh hoặc chế độ nhận dạng.

Chế độ xác minh:

Trong chế độ xác minh, hệ thống xác thực danh tính của một người bằng cách so sánh dữ liệu sinh trắc học được thu thập với cơ sở dữ liệu hệ thống được lưu trữ. Trong một hệ thống như vậy, một cá nhân muốn được công nhận sẽ yêu cầu nhận dạng, thường thông qua Mã số nhận dạng cá nhân PIN), tên người dùng, thẻ thông minh, v.v. và hệ thống tiến hành so sánh 1-1 để xác định xem người đó có đúng hay không… Mục đích là để ngăn chặn nhiều người sử dụng cùng một danh tính và do đó đạt được tính bảo mật của hệ thống.

Chế độ nhận dạng:

Trong chế độ nhận dạng, hệ thống nhận dạng một cá nhân bằng cách tìm kiếm các mẫu của tất cả người dùng trong cơ sở dữ liệu cho phù hợp. Do đó, hệ thống tiến hành so sánh một-nhiều để tìm kiếm danh tính của một cá nhân mà người đó không cần phải xác nhận danh tính.

VII. KẾT LUẬN

Tương lai quyền riêng tư và bảo mật là hai yếu tố chính ảnh hưởng đến niềm tin của khách hàng vào giao dịch điện tử. Do đó, các công ty hoặc trang web hoặc tổ chức cung cấp và bán sản phẩm hoặc dịch vụ của họ trực tuyến nên nỗ lực nhiều hơn trong việc tác động tích cực đến nhận thức của khách hàng về quyền riêng tư và bảo mật. Bảo mật hệ thống máy tính là một vấn đề toàn cầu đang ảnh hưởng đến người dùng TMĐT cá nhân cũng như doanh nghiệp. Người dùng cần được thông báo và phải chịu trách nhiệm về tính bảo mật của các tài nguyên mà họ đang sử dụng và xây dựng. Theo đó, họ nên đóng vai trò tích cực trong việc bảo vệ quyền riêng tư của mình. Tất cả các hệ thống bảo mật khác thường dựa trên xác thực chủ thẻ nhưng bỏ qua xác minh của người bán khiến hệ thống giao dịch dễ bị tấn công đối với các cuộc tấn công của người bán cần được quan tâm và các hành vi gian lận liên quan đến Internet như sao chép trang web, thông đồng với người bán, v.v.

Trong thời gian chạy sinh trắc học, dấu vân tay sẽ được ghi lại cho giao dịch di động và nó không được lưu trữ sẵn trong thiết bị di động để nó cung cấp bảo mật cao hơn và không bị bên thứ ba đánh cắp. Yêu cầu xác thực và trả lời phải ở dạng được mã hóa.

VIII. TÀI LIỆU THAM KHẢO

[1] Greg Mahnken (2021), *Tiền mặt hay tín dụng? Văn hóa thẻ tín dụng ở Hoa Kỳ*, Bài viết của Study in the USA, 05/04/2021.

[2] Bảo Đăng (2022), *(Infographic) Nhà giàu Mỹ 'quẹt' thẻ tín dụng hàng tháng như thế nào?,* Tạp chí Thị trường Tài chính Tiền tệ, Hà Nội.

[3] Đỗ Như (2023), *Chiêu thức giả mạo nhân viên, nâng hạn mức thẻ tín dụng để chiếm đoạt tiền*, Tạp chí Điện tử, Hà Nội.

[4] Thái Thanh Sơn và Thái Thanh Tùng (2018), *Thương mại điện tử trong thời đại số*, NXB Thông tin và Truyền thông, Hồ Chí Minh.

[5] PricewaterhouseCoopers (2020), *Báo cáo của Công ty PwC*, Việt Nam.

[6] Security, V. C. (2020), *Báo cáo của Công ty TNHH Bảo mật CNTT và Mạng Viettel*, Việt Nam.

[7] Kaspersky (05/4/2022), *Tình trạng mất an toàn trong thanh toán điện tử tại khu vực Đông Nam Á*, Tạp chí Điện tử, Hà Nội.

Link tham khảo:

[Infographic] Nhà giàu Mỹ 'quẹt' thẻ tín dụng hàng tháng thế nào? (thitruongtaichinhtiente.vn)

Kaspersky ghi nhận số lượng mối đe dọa trực tuyến và ngoại tuyến tại Việt Nam giảm đáng kể trong năm 2020 - Kaspersky Lab | Antivirus Protection | Internet Security (nts.com.vn)

Tình hình mất an toàn trong thanh toán điện tử tại khu vực Đông Nam Á (mic.gov.vn)

Gần 72% người dùng bị tấn công mạng khi thanh toán điện tử - Tuổi Trẻ Online (tuoitre.vn)

Phát hiện hàng triệu cảnh báo tấn công mạng, 90% thuộc hệ thống tài chính, ngân hàng – Viettel Cyber Security

Gần 1.300GB dữ liệu cá nhân, tổ chức bị mua bán và đề xuất hoàn thiện quy định (mic.gov.vn)

Chiêu thức giả mạo nhân viên, nâng hạn mức thẻ tín dụng để chiếm đoạt tiền - Nhịp sống kinh tế Việt Nam & Thế giới (vneconomy.vn)