# **1.5 NGHIÊN CỨU TÀI LIỆU VỀ BẢO MẬT THANH TOÁN DI ĐỘNG**

NGHIÊN CỨU TÀI LIỆU VÈ BẢO MẬT THANH TOÁN DI ĐỘNG

[**1.5 NGHIÊN CỨU TÀI LIỆU VỀ BẢO MẬT THANH TOÁN DI ĐỘNG** 1](#_Toc171026568)

[**1.** **Bảo mật thanh toán là gì** 1](#_Toc171026569)

[**2.** **Các hình thức bảo mật thanh toán** 2](#_Toc171026570)

[**3.** **5 nguyên tắc bảo mật khi thanh toán trên thiết bị di động** 3](#_Toc171026571)

[**4.** **Cách cải thiện việc bảo mật thanh toán** 4](#_Toc171026572)

[**5.** **Những thách thức và xu hướng tương lai của bảo mật thanh toán di động** 5](#_Toc171026573)

[**6.** **Kết luận** 8](#_Toc171026574)

[**7.** **Tài liệu tham khảo** 9](#_Toc171026575)

1. **Bảo mật thanh toán là gì**

Bảo mật thanh toán là các hệ thống và giải pháp để bảo vệ thông tin tài chính của khách hàng, bao gồm số thẻ tín dụng, số tài khoản ngân hàng, mật khẩu khỏi sự truy cập trái phép từ người khác.



Điều này giúp ngăn chặn các hành vi gian lận, trộm cắp thông tin và các vấn đề khác có thể gây tổn thất tài chính cho khách hàng. Luôn đảm bảo an ninh thanh toán là điều quan trọng giúp duy trì niềm tin của khách hàng khi thanh toán trực tuyến trên website hoặc ứng dụng của doanh nghiệp.

1. **Các hình thức bảo mật thanh toán**



Có nhiều loại công nghệ bảo mật thanh toán khác nhau, mỗi loại đều có ưu và nhược điểm riêng. Dưới đây là một số hình thức bảo mật thanh toán phổ biến nhất:

**Mã hóa:** Mã hóa là quá trình biến đổi thông tin thành dạng không thể đọc được bằng mắt thường. Đây là một trong những phương pháp bảo mật thanh toán hiệu quả nhất.

**Mã thông báo:** Mã thông báo là một chuỗi ký tự ngắn, được tạo ra ngẫu nhiên và chỉ được sử dụng một lần. Mã thông báo được sử dụng để xác thực danh tính của khách hàng khi thanh toán trực tuyến.

**Xác thực:** Xác thực là quá trình xác minh danh tính của người dùng trước khi họ được phép truy cập vào một hệ thống hoặc tài khoản. Có nhiều phương pháp xác thực khác nhau, bạn có thể tìm hiểu các phương pháp ở ngay dưới đây.

**Xác thực một yếu tố (SFA):** Yêu cầu một hình thức nhận dạng, thường là mật khẩu hoặc mã PIN

**Xác thực hai yếu tố (2FA):** Yêu cầu hai hình thức nhận dạng, chẳng hạn như mật khẩu và mã OTP được gửi đến thiết bị hoặc số di động đã đăng ký

**Xác thực đa yếu tố (MFA):** Yêu cầu ba hình thức nhận dạng trở lên, có thể bao gồm dữ liệu sinh trắc học, câu hỏi bảo mật hoặc mã thông báo vật lý.

**Phát hiện và ngăn chặn gian lận:** Các hệ thống phát hiện và ngăn chặn gian lận được sử dụng để xác định các giao dịch đáng ngờ và ngăn chặn việc gian lận trong thanh toán.

**Tuân thủ tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán:** Tiêu chuẩn bảo mật dữ liệu ngành thẻ thanh toán (PCI DSS) là một bộ quy tắc quy định các yêu cầu bảo mật cho các doanh nghiệp xử lý thẻ thanh toán.

**Cổng thanh toán:** Cổng thanh toán là một dịch vụ trung gian giúp khách hàng có thể thực hiện các giao dịch được tích hợp cổng thanh toán trực tiếp trên website doanh nghiệp một cách an toàn.

1. **5 nguyên tắc bảo mật khi thanh toán trên thiết bị di động**

**An toàn cho thiết bị di động khi giao dịch**

Thiết bị di động của bạn giống như chìa khóa két tiền, tức tài khoản ngân hàng. Nếu để rơi vào tay kẻ gian, bạn có thể mất sạch tiền. Vì vậy, dù thiết bị không cần cấu hình mạnh, nhưng phải luôn sạch.

**Tránh truy cập trang web lạ để ngăn cài đặt phần mềm gián điệp thu thập thông tin cá nhân.**

Cài đặt phần mềm bảo mật: Thường xuyên cập nhật phần mềm diệt virus và chống gián điệp. Sử dụng tường lửa, mật khẩu, vân tay, sinh trắc học để bảo mật.

**Môi trường mạng giao dịch an toàn**

Bạn có thể giao dịch ở bất cứ đâu có kết nối internet, nhưng tuyệt đối không sử dụng mạng công cộng kém bảo mật như nhà hàng, quán cà phê.

**Luôn cập nhật App thanh toán**

Ngân hàng thường nâng cấp tính năng và bảo mật cho các app thanh toán. Bạn cần cập nhật các app này thường xuyên và bảo mật thông tin cá nhân, mật khẩu.

**Không giao dịch với những trang thanh toán lạ**

Chỉ giao dịch với các trang web uy tín, được cấp phép chính thống để tránh mất tiền vì lừa đảo.

**Khóa chức năng giao dịch khi không sử dụng**

Sau khi giao dịch, đăng xuất ngay và khóa chức năng thanh toán online. Đặt hạn mức giao dịch tối thiểu để hạn chế rủi ro nếu tài khoản bị kiểm soát.

1. **Cách cải thiện việc bảo mật thanh toán**

**Để cải thiện bảo mật thanh toán hiệu quả, doanh nghiệp cần thực hiện các bước sau:**

**Đánh giá rủi ro:** Doanh nghiệp cần đánh giá các rủi ro bảo mật có thể xảy ra đối với hệ thống thanh toán của mình.

**Áp dụng các biện pháp bảo mật:** Doanh nghiệp cần áp dụng các biện pháp bảo mật phù hợp để giảm thiểu các rủi ro đã được xác định.

**Theo dõi và kiểm tra:** Doanh nghiệp cần theo dõi và kiểm tra hệ thống bảo mật thanh toán của mình để đảm bảo hiệu quả vận hành trơn tru.

**Sử dụng giao thức SSL/TLS:** Giao thức SSL/TLS giúp mã hóa thông tin thanh toán khi được truyền qua internet.

**Đào tạo nhân viên:** Doanh nghiệp nào cũng nên đào tạo nhân viên về các biện pháp và dấu hiệu của gian lận thanh toán trong tài chính.

1. **Những thách thức và xu hướng tương lai của bảo mật thanh toán di động**



**Thách thức:**

**Phần mềm độc hại và tấn công mạng:** Các thiết bị di động thường bị tấn công bởi phần mềm độc hại, phần mềm gián điệp, và các cuộc tấn công mạng như tấn công Man-in-the-Middle (MitM). Những mối đe dọa này có thể dẫn đến việc mất cắp thông tin cá nhân và tài chính.

**Sự thiếu nhận thức về bảo mật:** Nhiều người dùng vẫn chưa có đủ nhận thức về tầm quan trọng của bảo mật khi thực hiện giao dịch trên thiết bị di động. Việc sử dụng mật khẩu yếu, không cài đặt phần mềm bảo mật, và truy cập các mạng công cộng không an toàn là những ví dụ điển hình.

**Phát triển công nghệ quá nhanh:** Với sự phát triển nhanh chóng của công nghệ, các phương thức tấn công mới cũng xuất hiện liên tục. Điều này đặt ra thách thức lớn cho các nhà cung cấp dịch vụ trong việc duy trì và cập nhật các biện pháp bảo mật hiệu quả.

**Tính tương thích và tiêu chuẩn hóa:** Các thiết bị di động đến từ nhiều nhà sản xuất khác nhau với các hệ điều hành và nền tảng bảo mật khác nhau, khiến việc tiêu chuẩn hóa các biện pháp bảo mật trở nên khó khăn.

**Xu Hướng Và Công Nghệ Bảo Mật Tương Lai**



**Trí tuệ nhân tạo (AI) và học máy (Machine Learning):** AI và học máy sẽ ngày càng được sử dụng để phát hiện và ngăn chặn các hoạt động gian lận và tấn công mạng một cách nhanh chóng và hiệu quả hơn. Chúng có thể phân tích hành vi người dùng và phát hiện các dấu hiệu bất thường.

**Blockchain và thanh toán phi tập trung:** Công nghệ blockchain mang lại sự minh bạch và bảo mật cao cho các giao dịch tài chính. Việc áp dụng blockchain trong thanh toán di động có thể giúp giảm thiểu rủi ro gian lận và tăng cường bảo mật.

**Bảo mật dựa trên đám mây:** Các giải pháp bảo mật dựa trên đám mây sẽ trở nên phổ biến hơn, cung cấp các biện pháp bảo mật mạnh mẽ mà không cần dựa vào phần cứng của thiết bị.

**Xác thực đa yếu tố (MFA):** Sự kết hợp của nhiều yếu tố xác thực như mật khẩu, sinh trắc học, và mã OTP sẽ trở thành tiêu chuẩn để đảm bảo an toàn cho các giao dịch di động.

**Bảo mật sinh trắc học tiên tiến:** Công nghệ sinh trắc học như nhận diện khuôn mặt, vân tay, và giọng nói sẽ được phát triển và áp dụng rộng rãi hơn, cung cấp các phương thức xác thực an toàn và tiện lợi.

**Tăng cường hợp tác quốc tế:** Các quốc gia và tổ chức quốc tế sẽ hợp tác chặt chẽ hơn trong việc chia sẻ thông tin và phát triển các tiêu chuẩn bảo mật, nhằm đối phó với các mối đe dọa bảo mật xuyên biên giới.

Thông qua việc hiểu và áp dụng các xu hướng và công nghệ bảo mật tương lai, người dùng và các nhà cung cấp dịch vụ có thể đối phó hiệu quả với các thách thức hiện tại và nâng cao mức độ an toàn cho các giao dịch di động.

1. **Kết luận**

Bảo mật thanh toán là một vấn đề quan trọng đối với tất cả các doanh nghiệp chấp nhận thanh toán trực tuyến ngày nay. Bằng cách thực hiện các biện pháp bảo mật phù hợp, các doanh nghiệp có thể bảo vệ thông tin tài chính của khách hàng và tránh các rủi ro pháp lý.



Tóm lại, để bảo vệ tài khoản ngân hàng của bạn khi giao dịch trên thiết bị di động, luôn giữ thiết bị sạch, sử dụng mạng an toàn, cập nhật ứng dụng, tránh trang web lạ và khóa chức năng giao dịch khi không sử dụng.

1. **Tài liệu tham khảo**

<https://9pay.vn/blog/ejG-bao-mat-thanh-toan-huong-dan-chi-tiet-danh-cho-doanh-nghiep>

<https://tapchinganhang.gov.vn/5-nguyen-tac-bao-mat-khi-thanh-toan-tren-thiet-bi-di-dong.htm>

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiHlaDa342HAxXglFYBHZ5kB40QFnoECAkQAQ&url=https%3A%2F%2Fopenai.com%2F&usg=AOvVaw0428uXC88P9g34t6DemBOv&opi=89978449>

**Thực hiện: Nguyễn Minh Tâm/2274802010783**