TẦM QUAN TRỌNG CỦA HỆ THỐNG BẢO MẬT THÔNG TIN KHÁCH HÀNG TRONG THƯƠNG MẠI ĐIỆN TỬ

● NGUYỄN THỊ PHONG DUNG

TÓM TẮT:

Trong thời đại phát triển mạnh mẽ về các thiết bị thông minh, chuyển đổi số, hệ thống thanh toán đa dạng, các công nghệ giao hàng nhanh ra đời, hạ tầng internet wifi (4G, 5G) phủ sóng khắp mọi nơi,... là những yếu tố góp phần thúc đẩy ngành kinh doanh thương mại điện tử phát triển ồ ạt. Ngày càng có nhiều khách hàng với các độ tuổi khác nhau có niềm tin và thói quen mua hàng online trên các nền tảng thương mại điện tử. Do đó, bảo mật thông tin khách hàng trong thương mại điện tử là vấn đề luôn được các doanh nghiệp quan tâm nhiều nhất. Bài báo này đưa ra các vấn đề nhằm bảo mật thông tin trong hệ thống thương mại điện tử, liên quan đến việc bảo vệ thông tin cá nhân, tài khoản ngân hàng và giao dịch của khách hàng.

Từ khóa: hệ thống thương mại điện tử, bảo mật thông tin khách hàng.

1. Đặt vấn đề

Trong bài báo này, chúng tôi có thể cung cấp những mối đe dọa cụ thể các trang web thương mại điện tử (TMĐT) gặp phải trong thời điểm hiện nay. Điều này có thể bao gồm các cuộc tấn công mạng, lừa đảo liên quan đến thẻ tín dụng, sử dụng thông tin cá nhân không đúng cách và nhiều mối nguy hiểm khác. Nêu rõ các biện pháp bảo mật thông thường các trang web TMĐT nên áp dụng, chẳng hạn như: mã hóa dữ liệu, xác thực hai yếu tố, kiểm tra thường xuyên và giám sát hệ thống. Bài báo còn đề cập đến sự quan trọng của việc tuân thủ các quy định và tiêu chuẩn an ninh thông tin, như GDPR ở châu Âu hoặc HIPAA trong lĩnh vực chăm sóc sức khỏe. Các doanh nghiệp kinh doanh thương mại điện tử áp dụng các phương pháp và công nghệ sáng tạo để bảo vệ dữ liệu trước những hiểm họa mới. Điều này đặc biệt quan trọng đối với các trang web TMĐT hoạt động quốc tế.

2. Tổng quan tình hình bảo mật thông tin trong thương mại điện tử

Các doanh nghiệp kinh doanh TMĐT đang phải đối mặt với các mối đe dọa an ninh mạng (ANM). Các ứng dụng công nghệ trong TMĐT đang thu hút sự quan tâm của cả giới học thuật và ngành công nghiệp. Các mối lo ngại về ANM có nhiều dạng, nhưng nghiên cứu [1] tập trung vào tấn công từ chối dịch vụ, phần mềm độc hại và tấn công vào dữ liệu cá nhân. Các công ty trên toàn thế giới bỏ ra nhiều chi phí và tăng hàng năm vào việc giải quyết các vấn đề ANM. Vì vậy, các doanh nghiệp luôn phải

vượt qua thử thách phức tạp vì những kẻ tấn công liên tục tìm kiếm các lỗ hổng mới ở con người, tổ chức và công nghệ. Để giảm bớt rủi ro, các doanh nghiệp cần sử dụng các công nghệ đáng tin cậy, đào tạo nhân viên và người tiêu dùng, đồng thời Nhà nước và doanh nghiệp cũng cần có chính sách và quy định chặt chẽ.

Ngày nay, Internet đang đóng một vai trò rất quan trọng đối với con người trong nhiều lĩnh vực đời sống. Một lượng lớn giao dịch tiền tệ đang được thực hiện giao dịch bằng kỹ thuật số. Do đó, việc đảm bảo an toàn cho giao dịch trực tuyến đã trở nên bắt buộc vì số lượng tội phạm mạng cũng ngày càng gia tăng. Trong phần này, chúng tôi đã minh họa các điều kiện và giao thức nên sử dụng để bảo mật mạng trong khi giao dịch.

Một số điều kiện để giao dịch an toàn

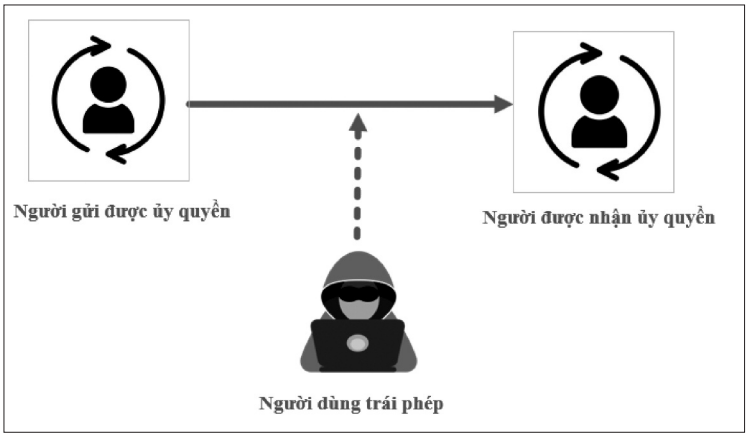
Tính bí mật: bảo vệ thông tin nhằm ngăn chặn sự truy cập trái phép như trong Hình 1. Ví dụ: thông tin xác thực ngân hàng chỉ có người dùng và ngân hàng biết, nhưng bất kỳ ai khác ngoài họ tiết lộ thông tin xác thực ngân hàng thì xảy ra lỗi bảo mật. Một khi thông tin đăng nhập ngân hàng bị tiết lộ sẽ gây ra nhiều vấn đề. Vì vậy, việc duy trì tính bảo mật là điều kiện rất quan trọng để giao dịch được an toàn. Sử dụng một số thuật toán mã hóa để duy trì tính bảo mật cho giao dịch an toàn là tiêu chuẩn mã hóa nâng cao (AES), tiêu chuẩn mã hóa dữ liệu (DES) [2].

Tính toàn vẹn: là phương pháp duy trì độ tin cậy, tính nhất quán và chính xác của dữ liệu trong suốt vòng đời của nó, dữ liệu được bảo vệ khỏi sự sửa đổi của người dùng trái phép. Điều này có thể đạt được trong mạng bằng cách sử dụng thuật toán băm như SHA (secure hashing algorithm) [3]

Tính sẵn sàng: dữ liệu, hệ thống hoặc ứng dụng phải có sẵn cho người dùng được phép truy xuất bất cứ khi nào họ muốn [4]. Hình thức tấn công từ chối dịch vụ (DoS) của hacker luôn muốn cản trở tính sẵn sàng của hệ thống.

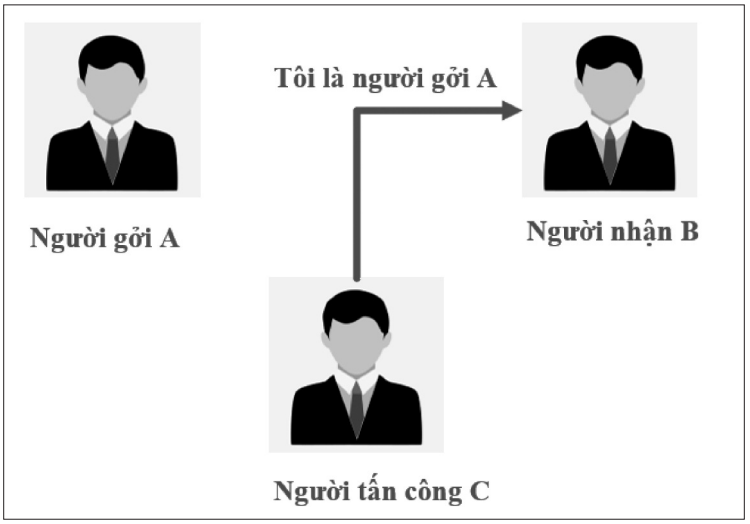
Xác thực: xác nhận một giao dịch, tin nhắn hoặc dữ liệu có nguồn gốc. Nói cách khác, xác thực có nghĩa là chứng minh danh tính của người gửi [5]. Mã xác thực thông báo (MAC: message authentication code) là một trong những loại thuật toán được sử dụng phổ biến để xác thực tin nhắn. Cuộc tấn công mạo danh là một ví dụ về tấn công xác thực, trong đó kẻ tấn công cố gắng truy cập tài nguyên mà không có thông tin xác thực và hành động chính xác. Hình 2 giải thích cuộc tấn công xác thực.

Hình 1: Bảo mật



Nguồn: Tác giả tự thiết kế

Hình 2: Tấn công xác thực

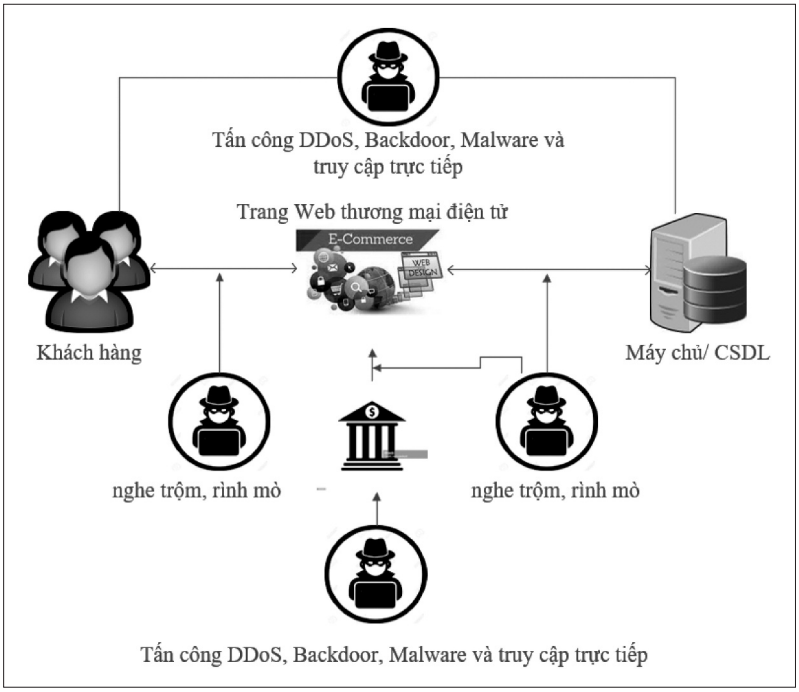


Nguồn: Tác giả tự thiết kế

3. Các loại tấn công khác nhau và các mối đe dọa trong hệ thống thương mại điện tử

Mặc dù hoạt động kinh doanh TMĐT đang rất phát triển với tốc độ theo cấp số nhân và không ngừng bùng nổ. Như đã đề cập trước đó, nó cũng đang gặp phải một số vấn đề về bảo mật. Với sự gia tăng doanh số bán hàng của doanh nghiệp TMĐT lên tới 5,5 nghìn tỷ USD vào năm 2022, bên cạnh đó cũng xuất hiện những điều không mong muốn là các mối đe dọa và tấn công. Trong phần này chúng tôi đang minh họa các loại tấn công và mối đe dọa khác nhau có thể xảy ra trong hệ thống TMĐT. Trong Hình 3, minh họa các cuộc tấn công vào hệ thống TMĐT.

Hình 3: Các cuộc tấn công vào hệ thống TMĐT



Nguồn: Tác giả tự thiết kế

3.1. Các cuộc tấn công

Một là, cuộc tấn công từ chối dịch vụ phân tán DDoS:

Đây là một cuộc tấn công với lưu lượng lớn truy cập về phía máy chủ. Các lượng yêu cầu có nguồn gốc từ hàng nghìn địa chỉ IP không thể theo dõi được [6]. Với tiến bộ của IoT, có thể có nhiều kiểu tấn công khác nhau hơn có nguồn gốc và do đó làm cho máy chủ hoàn toàn ngoại tuyến. Vấn đề này là nguyên nhân mở ra các cuộc tấn công nguy hiểm khác nhau. Các cuộc tấn công DDoS hầu hết xảy ra ở thời kỳ cao điểm bán hàng so với các thời gian khác trong năm. Thông thường trong các tháng lễ hội như giáng sinh, năm mới, tết,... mục tiêu chính của hacker tấn công DDoS để ngăn chặn các dịch vụ được cung cấp bởi máy chủ trong khoảng thời gian này nhằm làm mất doanh thu của các doanh nghiệp. Các cuộc tấn công DDoS có thể phân thành các loại:

Thứ nhất, tấn công DDoS sử dụng lưu lượng truy cập cao nhằm làm ngập băng thông: Đây là hình thức tấn công DDoS với số lượng lớn các yêu cầu trên máy chủ. Số lượng lớn yêu cầu có thể được chia thành 2 loại: yêu cầu hợp lệ và không hợp lệ. Các yêu cầu hợp lệ bao gồm gói dữ liệu giả mạo, trong khi các yêu cầu không hợp lệ được được coi là các gói dữ liệu không đúng định dạng. Mục đích chính của cuộc tấn công này nhằm làm băng thông hệ thống TMĐT luôn ở mức tối đa.

Thứ hai, dựa trên các giao thức được xác định trước: Các kiểu tấn công được thực hiện trên bộ cân bằng tải hoặc máy chủ. Những cuộc tấn công này khai thác liên kết giữa các hệ thống. Các gói dữ liệu được cấu hình khiến máy chủ phải chờ trong thời gian vô hạn trong giao thức bắt tay 3 chiều (TCP-SYN).

Thứ ba, phần mềm độc hại: là những phần mềm thiết kế dùng để gây hại cho hệ thống mạng, máy tính và các thiết bị khác. Nó được cài đặt bởi những kẻ xâm nhập bất hợp pháp trên hệ thống của người dùng. Những kẻ xâm nhập sử dụng nhiều kỹ thuật như SQL Injection, chèn phần mềm độc hại vào các tập tin trong website hoặc bất kỳ ứng dụng dựa trên nền tảng website.

Thứ tư, tấn công truy cập trực tiếp: tấn công truy cập trực tiếp hay tấn công vật lý là trong đó

kẻ tấn công hoặc kẻ xâm nhập có được quyền truy cập vật lý vào máy chủ hoặc máy tính. Khi kẻ xâm nhập có quyền truy cập trái phép vào máy tính có thể làm tổn hại đến tính bảo mật hoặc tính toàn vẹn bằng cách cài đặt phần mềm độc hại đa dạng như sâu, vi rút, Trojan,... Kẻ tấn công cũng có thể lấy tất cả dữ liệu có sẵn trong cơ sở dữ liệu của công ty (tên người dùng, mật khẩu, số thẻ tín dụng), cài đặt key logger (phần mềm chụp và ghi lại các phím được gõ). Tấn công truy cập trực tiếp có thể được thực hiện bằng nhiều cách khác nhau.

Hai là, rình mò (Snooping):

Kẻ xâm nhập hoặc kẻ tấn công trái phép có quyền truy cập vào dữ liệu của công ty hoặc người dùng. Rình mò giống như nghe lén nhưng không tập trung về việc truy cập dữ liệu trong quá trình truyền dữ liệu. Rà soát từ xa bao gồm cài đặt key logger để thu thập dữ liệu như mật khẩu, tên người dùng, địa chỉ... của nạn nhân. Nó cũng bao gồm việc chặn dữ liệu truyền tải và liên lạc. Kẻ tấn công có thể rình mò một cá nhân hoặc máy chủ của trang TMĐT để thu thập thông tin qua lưu lượng mạng để phân tích.

3.2. Các mối đe dọa

Một là, lừa đảo: là lừa dối nhằm mục đích lợi ích tài chính hoặc cá nhân. Trong lĩnh vực TMĐT, chúng tôi thấy có nhiều loại lừa đảo khác nhau được tổ chức thành dạng sau:

Xung đột thanh toán: Nhiều nhà bán lẻ trực tuyến cung cấp hàng hóa với giá cạnh tranh. Điều này khiến cho mọi người muốn mua hàng trên Internet bằng thẻ tín dụng. Tuy nhiên, giao dịch thanh toán có thể bị từ chối trên Internet vì các lý do như sau: thiếu tiền trong tài khoản (lý do phổ biến); Nhập sai số thẻ tín dụng khi thanh toán trực tuyến; Thẻ tín dụng hết hạn; Ngân hàng của bạn đã chặn thẻ thanh toán; Bảo trì trang website; Bạn đã vượt quá hạn mức thanh toán thẻ tín dụng.

Hai là, các mối đe dọa mã độc: mục tiêu chính là xâm phạm tính sẵn có, tính toàn vẹn hoặc tính bảo mật của thông tin trên web TMĐT nhằm làm mất tiền hoặc kiếm tiền. Chúng tôi có thể liệt kê các mối đe dọa sau đây:

- Tấn công vào các hệ thống và ứng dụng tiêu chuẩn như Cơ sở dữ liệu, SMTP, HTTP để thu thập thông tin.

- Virus: Máy chủ bị nhiễm virus có thể không hoạt động được và virus có thể lây lan tới những người dùng khác.

- Trojan: Cho phép kẻ tấn công truy cập và sửa đổi thông tin trong máy chủ như giá cả hoặc dịch vụ. Các kẻ tấn công cũng có thể sử dụng nạn nhân làm bot để thực hiện tấn công DDoS.

4. Thống kê an ninh trong thương mại

Hầu hết chúng ta đều có thiết bị cầm tay linh hoạt để truy cập Internet mọi lúc, mọi nơi thông qua hạ tầng 3G/4G/5G được phủ rộng khắp. Song do các mối đe dọa cấp độ sâu đang tác động xấu đến hoạt động kinh doanh TMĐT.

4.1. Ngành bị tấn công nhiều nhất

Theo Statista (2023), doanh số bán lẻ TMĐT toàn cầu từ năm 2014 đến 2026 [7] đang phát triển đi lên. Theo báo cáo, năm 2018-2019, ngành dễ bị tổn thương nhất từ các mối đe dọa và tấn công bảo mật chính là TMĐT. Các trang website TMĐT, ứng dụng chứa dữ liệu quan trọng và thông tin nhạy cảm, vì vậy nó thu hút các hacker thực hiện các gian lận.

4.2. Chi phí bảo mật trên thương mại điện tử

Mặc dù lĩnh vực này đang phát triển, nhưng vấn đề an ninh của các cửa hàng trực tuyến vẫn cần phải được cải thiện. Khi Internet và TMĐT phát triển, bảo mật và an toàn trang web đã trở thành một vấn đề quan trọng. Một mặt, tội phạm mạng phát triển nhiều và đe dọa đến niềm tin của TMĐT. Mặt khác, các vi phạm bảo mật trên các trang TMĐT đã thực sự gây ra thiệt hại về tài chính. Bảo mật trang web TMĐT là một khía cạnh thiết yếu. Bảo mật cần được xem xét khi tạo một trang web.

4.3. Hệ thống quản lý nội dung được nhắm mục tiêu nhiều nhất (CMS)

CMS là phần mềm được coi là hữu ích để tạo, quản lý và thay đổi nội dung có sẵn trên trang website. Với sự trợ giúp của CMS, người ta không cần phải viết bất kỳ mã phụ trợ để tạo trang

website. Hầu hết các trang TMĐT của các công ty đang sử dụng CMS. Vì vậy, điều rất quan trọng là phải biết các lỗ hổng của các CMS có sẵn khác nhau. Phần còn lại của CMS có ít lỗ hổng hơn như magneto (4,6%), Joomla (4,3%), Drupal (3,7%) và các loại khác là ít hơn 1%. Lý do đằng sau của lỗ hổng bảo mật là việc sử dụng các phiên bản lỗi thời [8]

5. Phương pháp để an toàn thương mại điện tử

Có một số phương pháp để ngăn chặn tấn công website TMĐT:

5.1. Sử dụng HTTPS thay vì HTTP và bảo mật trang web bằng chứng chỉ SSL

HTTPS an toàn là phiên bản bảo mật của HTTP. Việc sử dụng HTTP khiến trang website của bất kỳ ai cũng dễ bị tấn công. HTTPS giao thức bảo vệ thông tin được gửi. SSL hoặc bảo mật lớp socket là giao thức bảo mật phổ biến nhất. Có thể nhận ra chúng bằng biểu tượng ổ khóa trên thanh địa chỉ của trình duyệt. Các trang website TMĐT cần phải triển khai SSL để bảo mật hơn.

5.2. Bảo mật máy chủ

Để bảo vệ dữ liệu, bắt buộc phải chọn và sử dụng mật khẩu phù hợp để gây khó khăn trong việc tìm thấy bởi công cụ tự động hoặc bởi con người. Dưới đây là một số khuyến nghị:

(i) Sử dụng mật khẩu duy nhất cho mỗi dịch vụ, ứng dụng... Đặc biệt, cấm việc sử dụng mật khẩu tương tự giữa các công cụ chuyên nghiệp và cá nhân, trang web...

(ii) Không bao giờ yêu cầu bên thứ ba tạo mật khẩu cho bạn và không bao giờ để mật khẩu mặc định, ví dụ như admin.

(iii) Đừng lưu mật khẩu của trang web trong trình duyệt. Cách tốt nhất đặt mật khẩu tốt: tối thiểu 12 các ký tự có chữ hoa, chữ thường, chữ số và không phải alpha các ký tự số.

5.3. Bảo mật cổng thanh toán và giám sát hoạt động độc hại

Hầu như tất cả việc thanh toán trực tuyến được thực hiện bởi cổng thanh toán do ngân hàng quản lý. Họ sử dụng giao thức bảo mật 3-D (3 lớp) để kiểm tra xem thẻ được sử dụng là của người dùng không? Họ kiểm tra bằng cách gửi mã hoặc thư. Nếu bạn sử dụng cổng thanh toán không an toàn, kẻ tấn công có thể truy cập vào tất cả dữ liệu thẻ tín dụng. Bạn có thể sử dụng phần mềm giám sát để phân tích, thời gian dữ liệu đi vào trang website TMĐT của bạn (để ngăn chặn cuộc tấn công DDoS). Hoạt động giám sát cũng có thể giúp bạn phát hiện giao dịch gian lận.

5.4. Sử dụng phần mềm chống vi-rút, chống phần mềm độc hại và tường lửa

Phần mềm chống virus và phần mềm độc hại là để xác định, vô hiệu hóa và loại bỏ virus và phần mềm độc hại (ví dụ như: phần mềm gián điệp, phần mềm quảng cáo, Worm, Trojan và phần mềm tống tiền).

5. Kết luận

Bài báo giúp tăng cường nhận thức về vấn đề an ninh thông tin trong lĩnh vực TMĐT và cung cấp thông tin hữu ích cho các nhà nghiên cứu và doanh nghiệp hoạt động trong lĩnh vực này. Bảo mật thông tin là một phần quan trọng không thể thiếu đối với sự phát triển và thành công của mô hình kinh doanh TMĐT, bảo vệ dữ liệu cá nhân, xây dựng niềm tin, đảm bảo tuân thủ pháp luật và duy trì sự liên tục hoạt động kinh doanh. Điều này có vai trò quan trọng trong việc thúc đẩy sự phát triển và thành công của ngành TMĐT ■

TÀI LIỆU THAM KHẢO:

1. Liu, X., et al., (2022). Cyber security threats: A never-ending challenge for e-commerce. Frontiers in psychology, 13, 927398.

2. Abdullah, A.M., (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security, 16(1), 11.

3. Sumagita, M., et al., (2018). Analysis of secure hash algorithm (SHA) 512 for encryption process on web based application. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 7(4),373-381.

4. Sumra, I.A., et al., (2018). Security issues and challenges in MANET-VANET-FANET: A survey. EAI Endorsed Transactions on Energy Web, 5(17), e16-e16.

5. Kim, J.-B., (2021). A Study on the Utilization of MobileElectronic Notice Service using Korean Digital Identity Guidelines. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(5), 257-263.

6. Samanta, B., (2020). Epidemic modelling for the spread of bots through DDoS attack in E-commerce network. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, 445-459.

7. Statista (2023). Retail e-commerce sales worldwide from 2014 to 2026. Available at https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/.

8. ZDNET. WordPress accounted for 90 percent of all hacked CMS sites in 2018. Available at https://www.zdnet.com/article/wordpress-accounted-for-90-percent-of-all-hacked-cms-sites-in-2018/.

Ngày nhận bài: 1/9/2023
Ngày phản biện đánh giá và sửa chữa: 14/9/2023
Ngày chấp nhận đăng bài: 11/10/2023

Thông tin tác giả:
ThS. NGUYỄN THỊ PHONG DUNG
Trường Đại học Nguyễn Tất Thành

THE IMPORTANCE OF A GOOD CUSTOMER INFORMATION SECURITY SYSTEM IN E-COMMERCE

● Master. **NGUYEN THI PHONG DUNG**
Nguyen Tat Thanh University

ABSTRACT:

The rapid growth of e-commerce has been fueled by the increasing popularity of smart devices, digital transformation, diverse payment systems, and improvements in the Internet infrastructure (4G and 5G). E-commerce platforms have attracted more and more customers of different ages. Therefore, customer information security is one of the most concerning issues for e-commerce businesses. This paper pointed out e-commerce's information security issues about the protection of customers' personal information, bank accounts, and transactions.

Keywords: e-commerce systems, customer information security.