MÔ HÌNH BẢO MẬT KẾT HỢP MÃ XÁC THỰC OTP VÀO ỨNG DỤNG VNEID

Trần Ngọc Quế Anh, Vũ Tú Anh, Đào Nguyễn Ý Nhi, Hồ Thị Thu Thảo, Nguyễn Trần Minh Trang.
Trường đại học Kinh tế - Tài chính TP.HCM
Giảng Viên hướng dẫn: ThS Trần Thành Công

Tóm tắt: *Các trang web thương mại điện tử (TMĐT) ngày càng phát triển, đi cùng với điều đó là tỉ lệ mua hàng trực tuyến gia tăng đáng kể. Tuy nhiên, vấn đề về bảo mật và khả năng sử dụng khiến chỉ một số người chuyển từ việc tìm kiếm trực tuyến sang việc mua hàng. Nghiên cứu này tập trung vào việc phát triển một mô hình bảo mật nhằm tối ưu hóa khả năng bảo mật trong thanh toán trực tuyến cho người tiêu dùng. Phương pháp nghiên cứu bao gồm xem xét các mô hình hiện có và tiến hành một cuộc khảo sát để thu thập dữ liệu từ các người tham gia. Từ việc khảo sát và phân tích, nhóm tác giả đã đề xuất xây dựng một mô hình bảo mật kết hợp giữa OTP (Mã một lần) và VNeID (Nhận diện Điện tử Việt Nam) nhằm đảm bảo tính an toàn và đáng tin cậy trong việc thực hiện giao dịch thương mại điện tử. Mô hình này nhằm đảm bảo rằng việc thực hiện giao dịch trực tuyến thông qua OTP và VNeID diễn ra một cách an toàn, nhằm giảm thiểu nguy cơ lừa đảo và vi phạm bảo mật thông tin cá nhân của người dùng.*

Từ khóa: *tính khả dụng, bảo mật thương mại điện tử, thanh toán trực tuyến.*

I. PHÂN TÍCH THỊ TRƯỜNG

1. Thương mại điện tử tại Việt Nam

Mua sắm trực tuyến là quá trình giao dịch thương mại giữa người bán và người mua thông qua các phương tiện điện tử, đặc biệt là qua mạng internet (Speck, 2005). Hình thức này mang lại lợi ích cho doanh nghiệp bằng cách tiết kiệm chi phí bán hàng và tiếp thị. Đồng thời, nó cũng giúp người tiêu dùng và doanh nghiệp tiết kiệm thời gian và chi phí giao dịch.

Trong những năm gần đây, thương mại điện tử (TMĐT) đã trở nên quen thuộc đối với người tiêu dùng Việt Nam và đất nước này đã trở thành một thị trường TMĐT tiềm năng trong khu vực ASEAN. Theo Hiệp hội TMĐT Việt Nam (VECOM), trong giai đoạn 2016-2019, tốc độ tăng trưởng trung bình của TMĐT là khoảng 30%, và quy mô TMĐT bán lẻ hàng hoá và dịch vụ tiêu dùng đã đạt khoảng 11,5 tỷ USD vào năm 2019. VECOM dự đoán tốc độ tăng trưởng trong năm 2020 sẽ tiếp tục trên 30%, và quy mô TMĐT Việt Nam sẽ vượt qua 15 tỷ USD. Báo cáo của Google, Temasek và Bain&Company về TMĐT Đông Nam Á năm 2019 dự đoán tốc độ tăng trưởng trung bình trong giai đoạn 2015-2025 của TMĐT Việt Nam là 29%. Dự báo này cho biết quy mô TMĐT của Việt Nam sẽ đạt 43 tỷ USD và xếp hạng thứ ba trong khu vực ASEAN.

2. Rủi ro mua sắm.

Với sự phát triển nhanh chóng của các trang thương mại điện tử, hoạt động mua sắm trực tuyến đã trở nên sôi động hơn bao giờ hết. Nhiều doanh nghiệp đã tạo website để tận dụng cơ hội kinh doanh trực tuyến và tạo thuận lợi cho việc giao dịch hàng hóa. Khách hàng có thể dễ dàng lựa chọn và thanh toán trực tiếp cho sản phẩm mà không cần đến cửa hàng. Tuy nhiên, mua sắm trực tuyến ở Việt Nam vẫn còn gặp nhiều hạn chế. Người tiêu dùng chưa có thói quen mua hàng trên mạng và nhiều khách hàng vẫn lo ngại về rủi ro giao dịch, điều này dẫn đến sự giảm thiểu ý định mua hàng. Các rủi ro như thiệt hại tài chính và lộ thông tin cá nhân khi mua sắm trực tuyến thường xảy ra, gây ảnh hưởng đến uy tín của doanh nghiệp và giảm doanh số bán hàng.

3. Tổng quan mô hình đánh giá tính khả dụng và bảo mật trong website thương mại điện tử.

Trong lĩnh vực thương mại điện tử, đảm bảo tính khả dụng và bảo mật là hai yếu tố quan trọng để đảm bảo sự tin cậy và an toàn cho người dùng. Để đạt được mục tiêu này, có nhiều mô hình đánh giá tính khả dụng và bảo mật đã được phát triển và áp dụng trong các hệ thống thương mại điện tử.

Các mô hình này bao gồm đổi mới, sáng tạo, cung cấp thêm lợi ích, dịch vụ, bảo mật, thông tin sản phẩm, thiết kế trang web, và nhiều mô hình khác. Mỗi mô hình tập trung vào một khía cạnh cụ thể để đảm bảo tính khả dụng cao và bảo mật thông tin trong thương mại điện tử.

Bằng cách áp dụng các mô hình này, các doanh nghiệp có thể xác định, đánh giá và nâng cao tính khả dụng và bảo mật của hệ thống thương mại điện tử của mình, giúp đảm bảo sự tin tưởng và sự hài lòng của khách hàng.

Bảng 1 trình bày phân loại của một số mô hình đã được sử dụng để đo lường khả năng sử dụng và bảo mật của các website thương mại điện tử:

Models	**Khả năng sử dụng và các thuộc tính bảo mật được đo lường**
E-satisfaction Model Szymanski and Hise (2000)	Đổi mới, sáng tạo, cung cấp thêm lợi ích, dịch vụ, bảo mật, thông tin sản phẩm, thiết kế trang web.
McKnight et al., (2002)	Hành vi tin tưởng.
Devaraj et al., (2002)	Chức năng thân thiện với người dùng.
McCloskey (2003, 2004)	Dễ sử dụng, Hữu ích, An toàn.
The ‘Direct Impact’ model, Pikkarainen et al., (2004)	Nhận thức an ninh, cảm nhận dễ sử dụng. hữu ích.

Lim et al., (2005)	An toàn, thân thiện với người dùng.
Dwairi and Kamala (2009)	Quyền riêng tư, sự hài lòng, xu hướng tin tưởng, trải nghiệm trực tuyến, nhân khẩu học, bảo mật, thiết kế, nội dung, rủi ro.
Green and Pearson (2010)	Thời gian tải xuống, tính tương tác, tính thân thiện với người dùng và chức năng, độ trễ tải xuống, độ tin cậy của giao diện, nội dung, khả năng điều hướng, khả năng phản hồi, sự hài lòng, mối đe dọa, niềm tin của khách hàng, ý định mua hàng.
Chong et al., (2010)	Chất lượng thông tin, hệ thống và dịch vụ, giá trị cảm nhận, ý định sử dụng lặp lại, sự hài lòng.
Safa and Ismai (2013)	Chất lượng hệ thống và thông tin, tính hữu ích, tính dễ sử dụng.
Ali et al., (2018)	Sự hài lòng, tin tưởng, quyền riêng tư, hệ thống và chất lượng dịch vụ.

Bảng 1. Phân loại các mô hình đánh giá khả năng sử dụng.

4. So sánh các mô hình

Các mô hình được xếp thứ tự theo các thuộc tính được đo lường thành các khía cạnh về khả năng sử dụng và tính bảo mật sẽ cung cấp một cái nhìn tổng quan về ưu điểm và hạn chế của từng mô hình. Việc này giúp đánh giá xem các mô hình hiện có trong lĩnh vực thương mại điện tử có thể đáp ứng đầy đủ cả khía cạnh về khả năng sử dụng và bảo mật trong một mô hình duy nhất hay không.

Dựa vào sự xếp thứ tự này, Bảng 2 đã trình bày các đánh giá của các mô hình để xác định xem chúng có thể đáp ứng được tất cả các khía cạnh về khả năng sử dụng theo tiêu chuẩn của Nielsen và có tính đến các yếu tố bảo mật trong quá trình đánh giá hay không.

Mô hình	Các thuộc tính về khả năng sử dụng được đo lường					Yếu tố bảo mật	
	Khả năng học hỏi	Hiệu quả	Khả năng ghi nhớ	Lỗi	Sự thỏa mãn	Độ riêng tư	Sự an toàn
Szymanski & Hise	X				X	X	
McKnight et al.					X		
Devaraj et al.	X	X			X		

McCloskey	X	X			X		X
Safa & Ismail	X	X					
Lim et al	X				X		X
Al-Dwairi & Kamala	X				X	X	X
Green and Pearson	X			X	X		
Pikkarainen et al. and Dillon and Reif	X	X				X	
Chong et al.	X	X	X		X		
Ali and Raza	X	X	X				

Bảng 2. Điểm mạnh và điểm yếu của mô hình khả năng sử dụng hiện có

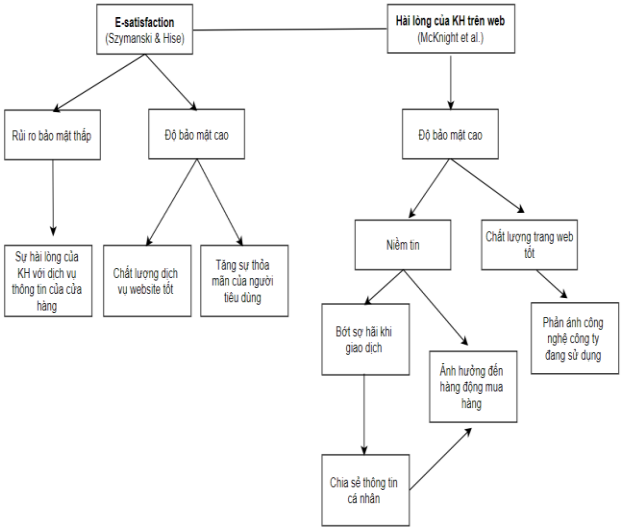
Bên cạnh việc so sánh 11 mô hình đánh giá tính khả dụng và bảo mật trong website thương mại điện tử, nhóm tác giả cũng đã đánh giá 2 mô hình nổi bật: mô hình "Hài lòng điện tử (E-satisfaction Model)" được phát triển bởi Szymanski và Hise và mô hình "Hành vi tin tưởng" được phát triển bởi Mcknight và đồng nghiệp. Nhóm tác giả đã so sánh 2 mô hình vừa được nêu tên dựa trên sự ảnh hưởng của mỗi mô hình đối với các khách hàng trong lĩnh vực thương mại điện tử.

Theo Szymanski và Hise, khi nhận thức về rủi ro bảo mật giảm, sự hài lòng với dịch vụ thông tin của cửa hàng trực tuyến dự kiến sẽ tăng. Điều này được hỗ trợ bởi nhận thức của người tiêu dùng về tiện lợi của mua sắm trực tuyến, bao gồm cung cấp sản phẩm và thông tin sản phẩm, thiết kế trang web và tính bảo mật. Các yếu tố này đóng vai trò quan trọng trong đánh giá sự hài lòng khi mua sắm trực tuyến. Một nghiên cứu đã chỉ ra mối quan hệ giữa chất lượng dịch vụ trang web và sự hài lòng của khách hàng (Szymanski, 2000).

Ngoài ra, Mcknight và đồng nghiệp cũng cho rằng quá trình mua sắm trực tuyến bao gồm việc xem thông tin sản phẩm hoặc tư vấn từ người bán trên trang web. Sau đó, người tiêu dùng chia sẻ thông tin cá nhân và cuối cùng, họ thực hiện mua hàng bằng cách cung cấp thông tin tài khoản để đặt hàng và thanh toán trên trang web. Chất lượng của trang web phản ánh công nghệ mà công ty sử dụng, và công nghệ không đáng tin cậy sẽ làm mất niềm tin của người tiêu dùng. Giao dịch trực tuyến thường có mức rủi ro cao hơn giao dịch truyền thống, và trong trường hợp này, niềm tin đóng vai trò

quan trọng trong việc giảm sự lo lắng khi thực hiện giao dịch trực tuyến (McKnight, 2002).

Sơ đồ dưới đây thể hiện quan điểm của hai mô hình nghiên cứu, bao gồm mô hình của Szymanski & Hise và Mcknight cùng cộng sự, trong việc đánh giá yếu tố ảnh hưởng đến niềm tin trong mua sắm trực tuyến.



5. Khảo sát tầm quan trọng trong bảo mật TMĐT.

Sau thời gian khảo sát và chọn lọc dữ liệu, nhóm nghiên cứu đã tổng hợp được 153 phiếu khảo sát hợp lệ. Dữ liệu lấy từ khảo sát được chúng tôi thống kê và phân loại theo bảng sau:

Câu hỏi	**Kết quả**	**Số lượng**	**Tỷ lệ phần trăm**
Độ tuổi	Từ 18 đến 25 tuổi	93	60,8%
	Từ 26 đến 35 tuổi	40	26,1
	Từ 36 đến 50 tuổi	19	12,4%
	Từ 51 tuổi trở lên	1	0,7%
Giới tính	Nam	68	44,4%
	Nữ	85	55,6%
Nghề nghiệp	Sinh viên	89	58,2%
	Đi làm	64	41,8%
Bạn có thường xuyên sử dụng hình thức thanh toán trực tuyến hay không? Và phải xác thực bằng OTP không?	Có	148	96,7%
	Không	5	3,3%
Bạn đã từng bị lộ thông tin đăng nhập hay nhận phải OTP	Có, đã xảy ra một lần	37	24,2%
	Có, đã xảy ra nhiều lần	20	13,1%

giả/ link giả dẫn đến mất tiền ở các dịch vụ thanh toán trực tuyến chưa?	Không, chưa từng bị nhưng đã từng thấy người thân, bạn bè gặp phải	96	62,7%
Theo bạn, vấn đề bị lộ mã OTP là do nguyên nhân gì?	Tin nhắn SMS bị hack, không an toàn	113	73,9%
	Mã độc hoặc phần mềm độc hại trong máy dẫn đến bị lộ thông tin	106	69,3%
	Lỗ hổng bảo mật trong hệ thống	104	68%
	Tin nhắn hoặc email được gửi đến địa chỉ sai hoặc bị đọc	90	58,8%
	Câu trả lời khác (Bị lộ thông tin về yếu tố con người, hành vi lừa đảo tinh vi, quản lý bảo mật kém, người dùng chủ quan,..)	9	5,9%
Bạn nghĩ bảo mật trong thanh toán điện tử có quan trọng hay không?	Rất không quan trọng	9	5,9%
	Không quan trọng	2	1,31%
	Bình thường	5	3,26%

	Bình thường	47	30,71 %
	Rất quan trọng	90	58,82 %
Theo bạn, việc nâng cấp độ bảo mật có quan trọng hay không?	Rất không quan trọng	6	3,9%
	Không quan trọng	3	1,45%
	Bình thường	3	1,45%
	Bình thường	46	30,1%
	Rất quan trọng	95	62,1%
Bạn có còn an tâm khi tiếp tục sử dụng những phương pháp xác thực hiện tại khi thực hiện thanh toán trực tuyến không?	Rất không tin tưởng	1	9,8%
	Không tin tưởng	18	11,8%
	Bình thường	51	33,3%
	Tin tưởng	59	38,6%
	Rất tin tưởng	10	6,5%
Nếu tích hợp xác thực mã OTP vào một ứng dụng bảo mật và an toàn hơn, bạn sẽ sử dụng chứ?	Có	149	97,4%
	Không	4	2,6%

Bảng 3 : Dữ liệu được thu thập và phân tích sơ bộ

Như đã thấy trong bảng , người được khảo sát thuộc nhiều độ tuổi khác nhau, từ 18 đến ngoài 50 tuổi.

- Có 68 người được khảo sát là nam, 85 người là nữ giới, họ đều đã đi học hoặc là đi làm.
- Trong đó có đến 148 người (chiếm 96,7%), là những người thường xuyên sử dụng hình thức thanh toán trực tuyến và phải xác thực bằng OTP.
- Họ đã từng thấy người thân, bạn bè gặp phải (96 người chiếm 62,7%) hoặc có ít nhất một lần gặp phải trường hợp bị lộ thông tin đăng nhập hay nhận phải OTP giả/ link giả dẫn đến mất tiền ở các dịch vụ thanh toán trực tuyến.
- Nguyên nhân dẫn đến vấn đề bị lộ mã OTP được

73,9% số người làm khảo sát cho rằng là do tin nhắn SMS bị hack, không an toàn.

- Việc bảo mật trong thanh toán điện tử được cho là rất quan trọng (58,82%) và việc nâng cấp độ bảo mật cũng như vậy (62,1%).
- Qua form khảo sát còn cho thấy, người được khảo sát không hoàn toàn an tâm khi tiếp tục sử dụng những phương pháp xác thực hiện tại khi thực hiện thanh toán trực tuyến, chỉ ở mức tin tưởng (38,6%) và rất là mong chờ sử dụng nếu tích hợp xác thực mã OTP vào một ứng dụng bảo mật và an toàn hơn (97,4%).

Ngoài ra, khi được đặt câu hỏi "Bạn có giải pháp nào cho vấn đề bảo mật xác thực này không?", chỉ có một bộ phận nhỏ có câu trả lời nhưng đều khá chung chung hoặc không có sự mới mẻ.

6. Tầm quan trọng của bảo mật thương mại điện tử.

Bảo mật trong thương mại điện tử là một yếu tố vô cùng quan trọng để đảm bảo sự tin tưởng và an toàn cho các hoạt động mua bán trực tuyến. Với sự phát triển của công nghệ và internet, thương mại điện tử đã trở thành một phần không thể thiếu trong cuộc sống hiện đại, và bảo mật là một yếu tố không thể bỏ qua. Bảo mật trong thương mại điện tử là một yếu tố vô cùng quan trọng để đảm bảo sự tin tưởng và an toàn cho các hoạt động mua bán trực tuyến. Với sự phát triển của công nghệ và internet, thương mại điện tử đã trở thành một phần không thể thiếu trong cuộc sống hiện đại, và bảo mật là một yếu tố không thể bỏ qua.

7. Giới thiệu ứng dụng VneID

VNeID là một ứng dụng di động được phát triển bởi Trung tâm dữ liệu quốc gia về dân cư, thuộc Bộ Công An Việt Nam. Ứng dụng này đã được tạo ra với mục tiêu thay thế giấy tờ truyền thống trong quá trình xác thực và cung cấp các tiện ích liên quan đến công dân số, chính phủ số và xã hội số.

VNeID được xây dựng trên một nền tảng cơ sở dữ liệu về định danh, dân cư và xác thực điện tử. Nó cung cấp cho người dùng các tiện ích và dịch vụ trong lĩnh vực công dân số, bao gồm quản lý thông tin cá nhân, xác thực điện tử, chứng thực dịch vụ trực tuyến và truy cập vào các dịch vụ công và dân sự trên một giao diện tiện ích và bảo mật.

Với VNeID, người dùng có thể trải nghiệm một loạt các tiện ích và dịch vụ công nghệ thông tin tiên tiến, như xác thực điện tử, giao dịch trực tuyến, xem và quản lý thông tin cá nhân, tương tác với cơ quan chính phủ và thực hiện các thủ tục hành chính một cách thuận tiện và an toàn hơn.

VNeID là một bước tiến quan trọng trong việc xây dựng hệ thống công nghệ thông tin

trong lĩnh vực dân cư và định danh tại Việt Nam, giúp nâng cao hiệu quả và tiện ích của quá trình quản lý thông tin cá nhân và dịch vụ công trực tuyến.

Để hiểu rõ hơn về VNeID, hãy khám phá các tính năng nổi bật đã được tích hợp trong ứng dụng này:

(1) Tích hợp giấy tờ cá nhân điện tử: VNeID cho phép tích hợp giấy tờ cá nhân của người dùng trên nền tảng kỹ thuật số. Điều này giúp giảm bớt việc mang theo các tài liệu giấy khi thực hiện các giao dịch hành chính và tạo sự tiện lợi cho người dùng.

(2) Khai báo y tế toàn dân: Với VNeID, người dân có thể dễ dàng khai báo thông tin y tế từ bất kỳ đâu, miễn là có kết nối internet. Điều này giúp dễ dàng truy vết các trường hợp nhiễm Covid-19 và hạn chế sự lan rộng của đại dịch.

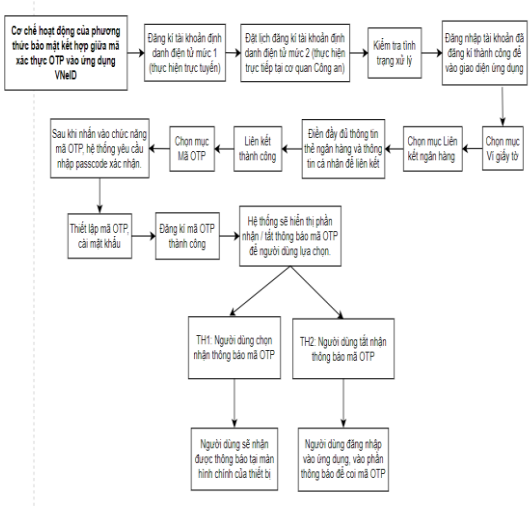
(3) Thông báo lưu trú: Qua VNeID, người dùng có thể thực hiện thông báo lưu trú một cách dễ dàng ngay trên điện thoại di động, giúp tiết kiệm thời gian và giấy tờ liên quan đến quá trình lưu trú.

(4) Kiến nghị, phản ánh về an ninh trật tự: Người dùng có thể gửi kiến nghị, phản ánh về các hành vi vi phạm an ninh trật tự một cách nhanh chóng và tiện lợi thông qua VNeID, trực tiếp đến cơ quan Công an. Điều này thúc đẩy sự tham gia cộng đồng và đảm bảo an ninh xã hội.

Ngoài ra, VNeID cũng đang định hướng tích hợp thêm các ứng dụng cốt lõi khác như ví điện tử, thanh toán không dùng tiền mặt, chứng khoán, điện, nước... Điều này tạo ra một hệ sinh thái đa dịch vụ trong ứng dụng, mang đến sự tiện ích và tối ưu cho người dùng trong các giao dịch hàng ngày.

II. HOẠT ĐỘNG ĐẾN KẾT QUẢ

1. Mô hình cơ chế hoạt động của dự án



Mô hình: Cơ chế hoạt động dự án

Bước 1: Để đăng ký tài khoản định danh điện tử mức 1 (thực hiện trực tuyến), bạn có thể làm theo các bước sau:

Truy cập trang web hoặc ứng dụng của dịch vụ định danh điện tử mà bạn muốn đăng ký. Thường thì trang web của dịch vụ này sẽ có thông tin chi tiết về quy trình đăng ký và các yêu cầu cần thiết.

Xác định loại thông tin cần đăng ký: Đối với tài khoản định danh điện tử mức 1, thông tin cá nhân cơ bản như tên, ngày sinh, địa chỉ, số điện thoại và địa chỉ email có thể được yêu cầu. Đảm bảo rằng bạn đã chuẩn bị thông tin này trước khi bắt đầu quy trình đăng ký.

Điền thông tin cá nhân: Theo hướng dẫn trên trang web hoặc ứng dụng, bạn sẽ được yêu cầu điền thông tin cá nhân vào biểu mẫu đăng

ký. Hãy đảm bảo bạn cung cấp thông tin chính xác và chính xác như được yêu cầu.

Xác minh danh tính: Sau khi bạn đã điền thông tin cá nhân, quá trình xác minh danh tính sẽ diễn ra. Điều này có thể được thực hiện thông qua một số phương thức như xác minh qua email, số điện thoại, hoặc cung cấp một số tài liệu như giấy tờ tùy thân.

Hoàn thành quá trình đăng ký: Sau khi thông tin và danh tính của bạn đã được xác minh, bạn sẽ hoàn thành quá trình đăng ký tài khoản định danh điện tử mức 1. Bạn có thể nhận được một thông báo xác nhận hoặc tài khoản của bạn đã sẵn sàng để sử dụng.

Lưu ý rằng quy trình đăng ký và yêu cầu cụ thể có thể khác nhau tùy thuộc vào dịch vụ định danh điện tử mà bạn chọn. Vì vậy, hãy đảm bảo đọc kỹ hướng dẫn cung cấp trên trang web hoặc ứng dụng của dịch vụ để biết thông tin chi tiết và tuân thủ quy trình đúng cách.

Bước 2: Để đặt lịch đăng ký tài khoản định danh điện tử mức 2 và thực hiện trực tiếp tại cơ quan Công an, bạn có thể làm theo các bước sau:

Tìm hiểu về quy trình đăng ký: Truy cập trang web hoặc cơ quan Công an có thẩm quyền để tìm hiểu về quy trình và yêu cầu đăng ký tài khoản định danh điện tử mức 2. Thông tin này thường được cung cấp trên trang web hoặc có thể yêu cầu liên hệ trực tiếp với cơ quan Công an để biết thêm chi tiết.

Chuẩn bị tài liệu cần thiết: Thông thường, bạn sẽ cần chuẩn bị các tài liệu như hộ chiếu hoặc chứng minh nhân dân, đơn đăng ký, và một số giấy tờ khác như sổ hộ khẩu hoặc giấy tờ chứng minh địa chỉ. Đảm bảo rằng bạn đã có tất cả các tài liệu cần thiết trước khi đặt lịch.

Liên hệ với cơ quan Công an: Để đặt lịch đăng ký tài khoản định danh điện tử mức 2, liên hệ với cơ quan Công an có thẩm quyền thông qua điện thoại hoặc email. Yêu cầu đặt lịch và cung cấp thông tin về mục đích đăng ký tài khoản và thông tin cá nhân của bạn.

Đặt lịch hẹn: Theo hướng dẫn từ cơ quan Công an, bạn sẽ được yêu cầu đặt lịch hẹn để thực hiện quy trình đăng ký. Chọn ngày và giờ phù hợp và xác nhận lịch hẹn với cơ quan Công an.

Thực hiện đăng ký tại cơ quan Công an: Đến đúng ngày và giờ hẹn, đến cơ quan Công an đã được chỉ định. Mang theo tất cả các tài liệu cần thiết và tuân thủ hướng dẫn của cơ quan để hoàn thành quy trình đăng ký tài khoản định danh điện tử mức 2.

Lưu ý rằng quy trình và yêu cầu đăng ký có thể khác nhau tùy thuộc vào quy định của từng cơ quan Công an và địa phương. Vì vậy, hãy đảm bảo tìm hiểu kỹ và tuân thủ quy trình và yêu cầu cụ thể của cơ quan Công

Bước 3: Kiểm tra tình trạng xử lý

Bước 4: Đăng nhập tài khoản đã đăng ký thành công để vào giao diện ứng dụng

Bước 5: Chọn mục Ví giấy tờ

Bước 6: Chọn mục Liên kết ngân hàng

Bước 7: Trong phần liên kết tài khoản ngân hàng, bạn sẽ được yêu cầu chọn ngân hàng hoặc phương thức thanh toán mà bạn muốn liên kết. Tùy thuộc vào dịch vụ hoặc ứng dụng,

có thể có một danh sách các ngân hàng hoặc phương thức thanh toán được hỗ trợ.

1. Cung cấp thông tin tài khoản: Sau khi chọn ngân hàng hoặc phương thức thanh toán, bạn sẽ được yêu cầu cung cấp thông tin tài khoản của mình. Thông tin này có thể bao gồm số tài khoản ngân hàng, mã số SWIFT/IBAN (đối với chuyển tiền quốc tế), tên chủ tài khoản và thông tin khác cần thiết.
2. Xác minh và kết nối tài khoản: Sau khi cung cấp thông tin tài khoản, bạn có thể được yêu cầu xác minh thông tin và kết nối tài khoản ngân hàng. Quá trình này có thể bao gồm việc xác minh thông qua một khoản tiền nhỏ được chuyển vào tài khoản của bạn hoặc nhập mã xác minh được gửi đến điện thoại hoặc email của bạn.

Bước 8: Hoàn tất quá trình liên kết: Sau khi xác minh và kết nối tài khoản ngân hàng, bạn sẽ hoàn tất

Bước 9: Chọn mục mã OTP.

Bước 10: Sau khi nhấn vào chức năng mã OTP, hệ thống yêu cầu nhập passcode xác nhận.

Bước 11: Thiết lập mã OTP, cài mật khẩu. Đảm bảo chọn một mật khẩu mạnh, gồm cả chữ hoa, chữ thường, chữ số và ký tự đặc biệt để tăng cường độ bảo mật.

Bước 12: Đăng ký mã OTP thành công. Sau khi bạn đã thiết lập mã OTP và cài đặt mật khẩu, đảm bảo lưu thông tin này một cách an toàn. Nên lưu trữ mã OTP trong một ứng dụng di động hoặc nơi an toàn khác và không chia sẻ nó với bất kỳ ai. Bảo vệ mật khẩu của bạn và tránh sử dụng mật khẩu dễ đoán hoặc giống nhau trên nhiều tài khoản.

Bước 13: Hệ thống sẽ hiển thị phần nhận / tắt thông báo mã OTP để người dùng lựa chọn.

Trường hợp 1: Người dùng chọn nhận thông báo mã OTP.

→ Người dùng sẽ nhận được thông báo tại màn hình chính của thiết bị.

Trường hợp 2: Người dùng tắt nhận thông báo mã OTP.

→ Người dùng đăng nhập vào ứng dụng, vào phần thông báo để coi mã OTP.

2. Mô hình SWOT

Điểm mạnh:

- Là sự kết hợp hoàn toàn mới, chưa có tổ chức hay cá nhân nào từng thực hiện.
- Tích hợp các chức năng vào cùng một ứng dụng vô cùng tiện lợi.
- Ứng dụng do Nhà nước quản lý nên mang tính bảo mật cao, an toàn.
- Tối ưu khả năng bảo mật với cơ chế chỉ đăng nhập trên 1 thiết bị.
- Được chính phủ hỗ trợ & bảo hộ (ứng dụng VNeID).
- Số lượng người dùng lớn.
- Sản phẩm mang tính khả dụng cao.

Điểm yếu:

- Thủ tục định danh mất nhiều thời gian (người dùng cần đến trụ sở công an địa phương để cán bộ xác thực).
- Giao diện ứng dụng VNeID chưa thật sự thân thiện với người dùng.
- Yếu tố bảo mật có thể chưa hoàn thiện dẫn đến sự xuất hiện của các lỗ hổng trong bảo mật.

Cơ hội:

- Nhu cầu bảo mật thông tin trong khâu thanh toán của người dùng hiện nay là vô cùng cao & rất được quan tâm.
- Sở hữu lượng khách hàng tiềm năng khi cam kết đáp ứng được khía cạnh bảo mật và đồng bộ thông tin người dùng.
- Thao tác truyền thông dễ dàng và hiệu quả khi sản phẩm là 1 tính năng tích hợp trong ứng dụng thuộc Nhà nước (VNeID).

Thách thức:

- Thời gian tiến hành và hoàn thiện dự án khá lâu vì đây là một dự án mới hoàn toàn.
- Các phương pháp bảo mật cũ được người dùng ưa chuộng hơn bởi tính tiện dụng và quen thuộc.
- Gặp phải các lỗi xâm nhập tiên tiến, thời gian xử lý lỗi lâu và khó khăn

3. Phân tích kết quả hoạt động

Để phân tích và đánh giá Mô hình bảo mật liên kết OTP & VNeID, ta có thể xem xét các điểm phù hợp, giải quyết vấn đề, tính tối ưu và khả thi so với mô hình cũ. Dưới đây là một số phân tích và đánh giá liên quan:

- Đáp ứng vấn đề bảo mật: Mô hình bảo mật liên kết OTP & VNeID đưa ra được một giải pháp bảo mật trong thương mại điện tử bằng cách sử dụng mã OTP và VNeID. Việc kết hợp hai yếu tố này giúp tăng cường bảo mật cho việc xác thực người dùng và giao dịch trực tuyến.
- Giải quyết vấn đề lừa đảo: Mô hình này có tiềm năng giúp giảm thiểu nguy cơ lừa đảo trong thương mại điện tử. Sử dụng mã OTP (mã một lần) cùng với VNeID (nhận diện điện tử Việt Nam) tạo ra một quy trình xác thực kép, từ đó làm khó khăn cho các hoạt động gian lận và vi phạm bảo mật.
- Tối ưu vấn đề bảo mật: Kết hợp OTP và VNeID trong mô hình bảo mật mang lại một lợi thế tối ưu hóa về mặt bảo mật. OTP cung cấp mã đơn lẻ

chỉ có hiệu lực trong một khoảng thời gian ngắn, giúp hạn chế việc sử dụng lại mã và giảm nguy cơ bị tấn công từ các kỹ thuật tấn công dựa trên mã độc. VNeID đảm bảo tính duy nhất và nhận diện chính xác người dùng thông qua các phương thức nhận diện điện tử hiện đại.

- Khả thi hơn mô hình cũ: Mô hình bảo mật liên kết OTP & VNeID có khả năng khả thi và áp dụng rộng rãi hơn so với mô hình cũ. OTP là yếu tố bảo mật phổ biến, VNeID là trang thông tin định danh được quản lý bởi Bộ Công an nên tính bảo mật sẽ được tăng cao.. Sự kết hợp giữa hai yếu tố này không yêu cầu thay đổi quá nhiều trong cơ sở hạ tầng hiện có, từ đó giúp giảm chi phí triển khai và tăng tính khả thi của mô hình.

- Tăng cường tính an toàn: Mô hình này cung cấp một cơ chế bảo mật mạnh mẽ hơn cho các giao dịch trong thương mại điện tử. Sự kết hợp giữa OTP và VNeID tạo ra một lớp bảo vệ đa chiều, đồng thời sử dụng mã một lần và nhận diện điện tử, giúp đảm bảo tính an toàn và không thể đoán trước được.

- Dễ sử dụng và tiện lợi: Mô hình bảo mật liên kết OTP & VNeID đòi hỏi người dùng chỉ cần sử dụng mã OTP và thông tin nhận diện VNeID của mình để thực hiện các giao dịch trực tuyến. Quá trình này đơn giản và thuận tiện, không yêu cầu các công đoạn phức tạp hoặc thiết bị phụ trợ đáng kể.

- Định vị nguồn gốc: Với sự kết hợp của VNeID, mô hình này có khả năng xác thực nguồn gốc của người dùng và tăng cường tính minh bạch trong thương mại điện tử. Người dùng có thể được xác định một cách rõ ràng thông qua VNeID, từ đó giảm thiểu nguy cơ lừa đảo và đảm bảo tính chính xác và tin cậy trong các giao dịch trực tuyến.

- Mở rộng tích hợp: Mô hình bảo mật liên kết OTP & VNeID có khả năng tích hợp với các hệ thống và dịch vụ thương mại điện tử hiện có. Điều này tạo điều kiện thuận lợi cho việc triển khai và mở rộng mô hình, từ đó thúc đẩy sự phát triển của thương mại điện tử với một cơ sở bảo mật mạnh mẽ.

Tuy nhiên, việc áp dụng mô hình bảo mật liên kết OTP & VNeID cần được

đánh giá kỹ lưỡng và thử nghiệm trong các tình huống thực tế để xác định hiệu quả và khả năng ứng dụng tốt nhất.

4. Tổng kết

Bài nghiên cứu tập trung vào vấn đề bảo mật trong thương mại điện tử và đề xuất mô hình bảo mật liên kết OTP & VNeID nhằm giải quyết vấn đề này. Mô hình này kết hợp mã OTP và VNeID nhằm tăng cường tính bảo mật trong việc xác thực người dùng và đảm bảo an toàn cho giao dịch trực tuyến.

Từ kết quả của bài nghiên cứu, chúng ta có thể đưa ra một số khuyến nghị và đề xuất nhằm phát triển lĩnh vực thương mại điện tử nói chung và bảo mật nói riêng. Cần tiếp tục nghiên cứu và phát triển các giải pháp bảo mật tiên tiến để đối phó với các mối đe dọa mới và tiềm ẩn trong thương mại điện tử. Đồng thời, việc nâng cao ý thức về bảo mật trong cộng đồng thương mại điện tử và cung cấp đào tạo chuyên sâu về bảo mật thông tin cho người dùng và doanh nghiệp cũng là điều cần thiết. Hơn nữa, cần hợp tác với các tổ chức quản lý và các nhà cung cấp dịch vụ để xây dựng chuẩn mực bảo mật và tạo ra một môi trường an toàn và đáng tin cậy cho thương mại điện tử. Cuối cùng, việc đẩy mạnh nghiên cứu và phát triển các công nghệ mới như trí tuệ nhân tạo, blockchain và các biện pháp bảo mật tiên tiến khác cũng sẽ góp phần nâng cao tính an toàn và tin cậy trong thương mại điện tử.

III. KẾT LUẬN

Từ kết quả của bài nghiên cứu, nhóm tác giả xin đưa ra một số đóng góp:

Tiếp tục nghiên cứu & phát triển các giải pháp bảo mật tiên tiến để đối phó với các mối đe dọa mới & tiềm ẩn trong TMĐT.

Nâng cao ý thức về bảo mật trong cộng đồng TMĐT & cung cấp đào tạo chuyên sâu về bảo mật thông tin cho người dùng & doanh nghiệp.

Hợp tác với các tổ chức quản lý & các nhà cung cấp dịch vụ để xây dựng chuẩn mực bảo mật & tạo ra 1 môi trường an toàn & đáng tin cậy cho TMĐT.

Đẩy mạnh nghiên cứu & phát triển các công nghệ mới như trí tuệ nhân tạo, blockchain & các biện pháp bảo mật tiên tiến khác nhằm nâng cao tính an toàn & tin cậy trong TMĐT.

Tài liệu tham khảo

1. Hải, L. T. (2022, 4 30). tapchitaichinh. Được truy lục từ Đề xuất mô hình đánh giá sự hài lòng của khách hàng đối với chất lượng dịch vụ ngân hàng điện tử: https://tapchitaichinh.vn/dexuat-mo-hinh-danh-gia-su-hai-long-cua-khach-

hang-doi-voi-chat-luong-dich-vu-ngan-hang-dien-tu.html

2. McKnight, D. C. (2002). Developing and validating trust measures for e-commerce: An integrative typology.

3. Speck, M. T. (2005). Factors that Affect Attitude Toward a Retail Web Site.

4. Szymanski, D. &. (2000). E-satisfaction: an initial examination.

5. Vecom. (2020, 06 25). Được truy lục từ Thông cáo báo chí Diễn đàn Toàn cảnh Thương mại điện tử Việt Nam – VOBF 2020: https://vecom.vn/thong-cao-bao-chi-dien-dan-toan-canh-thuong-mai-dien-tu-viet-nam-vobf-2020