Rủi ro và thách thức an ninh mạng trong lĩnh vực ngân hàng tại Việt Nam

Risks and challenges for cybersecurity in the banking sector in Vietnam

Nguyễn Văn Phương[1*], Trần Văn Diễn[1]

[1]Trung tâm Đào tạo Quản lý công, Trường Đại học Quốc tế, Đại học Quốc gia Thành Phố Hồ Chí Minh, Việt Nam

[*]Tác giả liên hệ, Email: nvphuong@hcmiu.edu.vn

THÔNG TIN

DOI:10.46223/HCMCOUJS.econ.vi.16.2.612.2021

Ngày nhận: 09/08/2020

Ngày nhận lại: 28/09/2020

Duyệt đăng: 19/11/2020

Từ khóa:

an ninh mạng; rủi ro; thách thức; ngân hàng trực tuyến; Internet

TÓM TẮT

Không gian mạng cung cấp tiềm năng vô hạn về hội nhập toàn cầu và phát triển kinh tế xã hội trong thế kỷ 21. Tuy nhiên, rủi ro và thách thức về an ninh mạng đã trở thành mối quan tâm hàng đầu của người sử dụng Internet; đặc biệt trong lĩnh vực ngân hàng. Chính vì thế nghiên cứu này nhằm khám phá và làm rõ những rủi ro, thách thức về an ninh mạng trong lĩnh vực ngân hàng tại Việt Nam. Nghiên cứu này sử dụng phương pháp định tính thông qua 10 cuộc phỏng vấn chuyên sâu và ứng dụng phần mềm NVIVO để phân tích nội dung phỏng vấn. Kết quả nghiên cứu nhằm giúp cho người sử dụng dịch vụ ngân hàng online và các nhà quản lý ngân hàng thấy rõ vấn đề an ninh mạng. Đồng thời kết quả nghiên cứu này sẽ làm sáng tỏ cách thức mà các nhà hoạch định chính sách có thể phát triển khung chính sách an ninh mạng trong lĩnh vực ngân hàng, cân bằng các khía cạnh lợi ích của việc sử dụng dịch vụ ngân hàng trực tuyến.

Keywords:

Cybersecurity; risks; challenges; online banking; Internet

ABSTRACT

Cyberspace provides limitless potentialities for global integration and socio-economic development in the 21st century. However, cybersecurity risks and challenges have become the top concerns of Internet users, especially in the banking sector. Therefore, this study aims to explore and clarify the risks and challenges of cybersecurity in the banking sector. This study uses a qualitative method and utilizes NVIVO software to analyze the findings from 10 in-depth interviews. The research results aim to help online banking users and banking managers clarify the problems of cybersecurity. In addition, the findings shed new light on how policymakers can develop a cybersecurity policy framework in the banking sector and balance the beneficial aspects of using online banking services.

1. Giới thiệu

Ngày nay, thương mại kỹ thuật số, việc trao đổi thông tin và mạng lưới cơ sở hạ tầng Viễn thông chủ yếu dựa vào nền tảng mạng lưới toàn cầu, gần hơn nửa dân số Thế giới đã kết nối vào mạng lưới Internet (Nye, 2017; Weiss & Jankauskas, 2018). Khi những tiềm ẩn rủi ro của không gian mạng ngày một gia tăng trong xã hội hiện đại (Choucri, 2019), cả hai lĩnh vực công và tư đều quan tâm đến khả năng ứng phó với các vấn đề an ninh mạng (Bossong & Wagner, 2017; Weiss & Jankauskas, 2018). Thực tế, một cuộc tấn công mạng thành công có thể làm sập mạng của các đơn vị Chính phủ, làm mất kiểm soát của hoạt động kinh doanh, làm xói mòn niềm tin của công chúng về các giao dịch tài chính hay phát tán thông tin không chính xác làm thiệt hại rất lớn về kinh tế và uy tín của chính quyền hay doanh nghiệp. Ví dụ, cụ thể như trường hợp mạng của hãng hàng không Vietnam Airlines bị tấn công vào tháng 07 năm 2016. Một trường hợp gần đây thông tin cá nhân của gần 5 triệu khách hàng của công ty Thế Giới Di Động bị lộ, bị rò rỉ vào tháng 11 năm 2018. Trong lĩnh vực Ngân hàng, Ngân hàng Sacombank bị làm giả thẻ tín dụng (tháng 04 năm 2017), và ngân hàng Đông Á cũng xảy ra trường hợp tương tự vào tháng 11 năm 2018. Trong thực tế ngày càng nhiều khách hàng sử dụng điện thoại cho các giao dịch mua bán và thanh toán online. Điều đó làm cho việc đảm bảo an toàn thông tin của khách hàng trước sự tấn công của tin tặc ngày trở nên quan trọng. Đặc biệt, việc đảm bảo xác thực thông tin của người được cấp quyền truy cập dữ liệu đòi hỏi phải nhanh và tiện lợi là vô cùng quan trọng.

Các kỹ thuật nén và giải mã nội dung giao dịch online qua thiết bị điện thoại di động được thiết kế dựa trên nền tảng của giao dịch ngân hàng trực tuyến. Mà cấu trúc thiết kế hệ thống giao dịch ngân hàng trực tuyến lại có sự khác biệt tùy theo cách vận hành của từng ngân hàng và nghiệp vụ phát sinh; ví dụ như các dịch vụ bên trong ngân hàng và các dịch vụ qua bên thứ ba, đơn vị lưu trữ dịch vụ. Như vậy, việc đảm bảo an ninh dịch vụ ngân hàng trực tuyến là vấn đề nan giải thông qua mô hình yêu cầu - phản hồi mà ở đó đòi hỏi sự xác thực thông tin của khách hàng, hệ thống ngân hàng phải thông suốt thông qua hệ thống cơ sở hạ tầng gồm hệ thống mạng công nghệ thông tin, bộ định tuyến (routers), các máy chủ và bộ chuyển mạch (Aljawarneh, 2017). Như vậy, hệ thống khi một trong những mắt xích bị lỗi hoặc bị tấn công, thì hệ thống dịch vụ ngân hàng trực tuyến sẽ không còn giao dịch chính xác và tin cậy nữa. Thực thi quá trình an ninh mạng tập trung vào rủi ro phát sinh trong quá trình xử lý dữ liệu nội bộ hoặc lỗi của người vận hành hoặc từ những điều kiện tác động từ bên ngoài (Belás, Korauš, Kombo, & Korauš, 2016; Grubicka & Matuska, 2015; Peker, Tvaronavičienė, & Aktan, 2014). Bên cạnh đó, an ninh vật lý gắn kết với việc đảm bảo tiền mặt tại các chi nhánh ngân hàng hay tại các máy ATM (Automatic Teller Machines). Tóm lại hệ thống an ninh bao gồm cả quá trình giao dịch bên trong và bên ngoài của ngân hàng được ghi nhận bởi hệ thống thông tin mạng.

Trong thời đại ngày nay khi không gian mạng ngày càng rộng mở và các hình thức tấn công mạng ngày một tinh vi hơn, tần xuất ngày càng nhiều hơn làm tổn hại rất lớn đến doanh nghiệp và chủ quyền Quốc gia. Vì vậy, các Chính phủ đã có những hành động cụ thể về việc hoàn thiện hệ thống Pháp lý đảm bảo và xử lý an toàn thông tin mạng, đặc biệt trong việc bảo vệ An ninh Quốc phòng. Các Chính phủ cần quan tâm đến năng lực và kinh nghiệm vận hành của các bên thứ 3 trong việc xây dựng hệ thống Pháp lý chặt chẽ giúp quản lý tốt hơn an toàn thông tin mạng, giảm thiểu những rủi ro và các mối đe dọa từ không gian mạng. Theo xu hướng này, Quốc Hội Việt Nam đã thông qua Luật an ninh mạng vào ngày 12 tháng 06 năm 2018 và chính thức có hiệu lực từ ngày 01 tháng 01 năm 2019. Tuy nhiên, trong thực tế vận hành cho tới nay Luật này cũng cần nghiên cứu và hoàn thiện tốt hơn liên quan đến trách nhiệm và quyền lợi của các bên trên không gian mạng. Đây cũng là một trong những mục tiêu của nghiên cứu này.

Khái niệm không gian mạng được cho là mạng ảo mà trong đó hệ thống mạng thông tin liên lạc kết nối giữa máy tính và thiết bị điện tử cho phép lưu trữ, thay đổi và trao đổi dữ liệu (Lantis & Bloomberg, 2018). Các rủi ro và mối đe dọa trên mạng ban đầu được giải thích như thế nào và liệu người sử dụng dịch vụ ngân hàng trực tuyến tại Việt Nam hiện nay có hiểu biết sâu sắc về khái niệm an ninh mạng và tấn công mạng không? Các vấn đề không an toàn của người dùng Internet khi truy cập vào các hoạt động trực tuyến là gì? Làm thế nào mà chính sách luôn phù hợp với các hoạt động phát triển Quốc gia theo thời gian?

Hiện nay, có một số nghiên cứu trước đây ở nước ngoài đã cố gắng trả lời một số câu hỏi trên, xem xét trên nhiều khía cạnh lý thuyết và thực tế đã vận hành tại một số nước đã phát triển, có hệ thống pháp lý chặt chẽ và thường xuyên cập nhật theo thực tế phát sinh của xã hội đương đại. Ví dụ, các nghiên cứu tập trung khai thác vấn đề an ninh mạng tại Hoa Kỳ, Vương quốc Anh, Úc, Singapore và các Quốc gia khác thuộc liên minh Châu Âu. Chính phủ ở các nước phát triển đã tăng cường bảo mật dữ liệu tổng thể để kích thích tăng trưởng kinh tế thông qua hỗ trợ kinh doanh kỹ thuật số. Chẳng hạn, Vương quốc Anh thúc đẩy một trong những mức độ sử dụng thương mại Kỹ thuật số cao nhất, với số lượng lớn công dân chuyển từ mua sắm truyền thống sang mua sắm trực tuyến mà ở đó mọi thanh toán đều thông qua online (Chakravorti & Chaturvedi, 2017). Bên cạnh đó, vấn đề thiết kế chính sách phù hợp để đảm bảo an toàn thông tin tránh được những rủi ro và mối đe dọa về an ninh mạng cũng được các nước rất quan tâm. Tuy nhiên, có rất ít nghiên cứu liên quan đến vấn đề này tại Việt Nam, vì vậy đây cũng là lý do mà tác giả chọn chủ đề nghiên cứu này.

Nghiên cứu này thực hiện trên cơ sở nghiên cứu định tính thông qua phỏng vấn chuyên sâu bốn chuyên gia về an ninh mạng và công nghệ thông tin đang công tác tại ba trường Đại học trong nước và một trường Đại học ở Hoa Kỳ. Đồng thời, tác giả cũng triển khai sáu cuộc phỏng vấn chuyên sâu với các nhà quản lý mạng công nghệ thông tin đang công tác tại ngân hàng thương mại trong nước và nước ngoài tại Việt Nam để khám phá các vấn đề an ninh mạng và an toàn thông tin tại các ngân hàng thương mại.

Mục đích của nghiên cứu này nhằm khai thác những rủi ro tiềm ẩn và các thách thức trong quá trình thanh toán trực tuyến hiện nay. Làm rõ những vấn đề liên quan trong quá trình bảo mật thông tin của hệ thống ngân hàng thương mại và thông tin cá nhân của khách hàng trong quá trình truy cập vào mạng Internet hay sử dụng các thiết bị có khả năng truy cập Internet. Từ đó, kết quả nghiên cứu nhằm đưa ra những khuyến cáo cho mọi người sử dụng dịch vụ ngân hàng trực tuyến và các nhà quản lý đề ra những đối sách phù hợp với tình hình an ninh mạng trong giai đoạn hiện nay. Bên cạnh đó nghiên cứu hướng đến xác định những nguyên nhân ảnh hưởng đến an toàn an ninh mạng và rủi ro đối với người dùng dịch vụ ngân hàng trực tuyến, từ đó nhằm tìm ra những khiếm khuyết trong chính sách an ninh mạng, đề ra những phương pháp trong quản lý an ninh mạng tại Việt Nam thật sự được hiệu quả, thích nghi với tình hình thực tế của xã hội và toàn thế giới trong quá trình phát triển kinh tế và hội nhập.

2. Lý thuyết tổng quan

An ninh mạng đã trở thành vấn đề trọng tâm đối với tất cả các Chính phủ khắp mọi nơi trên Thế giới. Ví dụ, năm 2017 các mối đe dọa đến từ không gian mạng lại được xếp vào những mối đe dọa cao nhất đối với An ninh Quốc gia của cơ quan tình báo Hoa Kỳ theo đánh giá của tổ chức World Wide Threat Assessement (Christensen & Petersen, 2018). Khắp mọi nơi trên Thế giới, các Chính phủ đã xây dựng các chiến lược an ninh mạng Quốc gia và thành lập các đơn vị đặc biệt về an ninh mạng. Ví dụ, các nước trong Khối Bắc Đại Tây Dương (NATO-North Atlantic Treaty Organization) đã thiết kế một đơn vị đặc nhiệm phụ trách ứng phó đối với chiến tranh không gian mạng, nhằm thu thập và xử lý thông tin để ứng phó kịp thời khi có tấn công

mạng đến các nước thuộc liên minh này. Một ví dụ khác, Trung Quốc gần đây cũng thông qua luật an ninh mạng có ảnh hưởng rất nhiều đến cộng đồng kinh doanh tại Quốc gia này. Nhìn chung, quản trị rủi ro an ninh mạng là vô cùng quan trọng đối với An ninh Quốc gia.

Vấn đề làm sao hạn chế rủi ro bị đánh cấp thông tin trong hệ thống mạng máy tính kết nối Internet trở nên vô cùng cấp thiết. Ngày càng có nhiều người quan tâm đến việc xây dựng hệ thống an ninh mạng nhằm hạn chế rủi ro mất an toàn thông tin-an ninh mạng. Đây cũng là nhiệm vụ vô cùng thách thức đối với các nhà quản trị mạng thông tin của tất cả các tổ chức và doanh nghiệp. Jackson (1989) đã phát triển các khái niệm về an ninh mạng (cybersecurity), an ninh máy tính (computer security), bảo mật công nghệ thông tin (Information Technology security) là việc bảo vệ hệ thống mạng máy tính khỏi các hành vi trộm cắp danh tính, dữ liệu hoặc làm tổn hại đến phần cứng, phần mềm và các nguyên nhân dẫn đến sự gián đoạn của máy tính. An ninh mạng là thực tiễn của việc bảo vệ các hệ thống điện tử, mạng lưới, máy tính, thiết bị di động, chương trình và dữ liệu tránh khỏi những cuộc tấn công kỹ thuật số độc hại có chủ đích. Hacker (tội phạm mạng) có thể triển khai một loạt các cuộc tấn công vào mạng máy tính nhằm chống lại các nạn nhân hoặc doanh nghiệp; quyền truy cập, điều khiển làm thay đổi hoặc xóa bỏ dữ liệu; với mục đích kinh tế; tống tiền; can thiệp trực tiếp vào các quy trình kinh doanh.

Chính vì tính phức tạp, bản chất năng động và phân tán của hệ thống Công nghệ Thông tin (CNTT), nên các rủi ro an ninh mạng là không dễ dàng quản lý. Chính vì vậy các nhà quản lý doanh nghiệp và ngân hàng đang phải đương đầu với nhiều thách thức về đảm bảo an toàn thông tin cho khách hàng. CNTT phổ biến khắp mọi nơi và là nền tảng cơ sở hạ tầng quan trọng cho việc kết nối mạng lưới Internet toàn cầu, giúp cho việc truy cập Internet và sử dụng mạng lưới xã hội đang trở thành nhu cầu tất yếu và phổ biến của xã hội hiện tại. Chính sự phát triển và mở rộng không ngừng của Internet vạn vật làm gia tăng những rủi ro và thách thức đối với việc truy cập Internet từ góc độ quản lý Nhà nước, Doanh nghiệp và Người dân. Hơn nữa, bản chất của CNTT và mạng Internet, các rủi ro về an ninh mạng không giới hạn trong phạm vi địa lý cụ thể nào cả, các cuộc tấn công mạng có thể xuất phát từ mọi nơi. Nói tóm lại, an ninh mạng có đặc trưng riêng bởi những nền tảng không an toàn của không gian mạng (Christensen & Petersen, 2018).

Hiện nay các phần mềm ứng dụng mới cho điện thoại di động ngày càng phổ biến và tiện lợi giúp cho việc mua bán và thanh toán qua hệ thống trực tuyến trở nên phổ biến. Thông tin của khách hàng trong quá trình thanh toán qua hệ thống ngân hàng trực tuyến cần phải được bảo vệ an toàn. Tuy nhiên, thực tế tin tặc tìm mọi cách để tấn công vào những lỗ hổng trong toàn bộ hệ thống và chỉ cần một cuộc tấn công nhỏ có thể làm toàn hệ thống giao dịch ngân hàng bị sập và chịu những tổn thất rất lớn. Các ngân hàng thương mại thường phải đầu tư nhiều chi phí cho việc bảo vệ máy chủ ở mức độ an toàn cao nhất (Peotta, Holtz, David, Deus, & Timoteo de Sousa, 2011). Chính vì vậy việc tấn công vào máy chủ của các ngân hàng thương mại thường không thành công nên tin tặc thường tập chung tấn công vào hệ thống từ chối dịch vụ (Denial of Service Attack). Đây là loại hình tấn công khai thác tình huống khi mà tất cả nguồn không sẵn sàng đối với ý định của người sử dụng dịch vụ. Việc tấn công gây sập mạng bằng cách tạo ra các yêu cầu quá nhiều bất thường vượt quá khả năng đáp ứng của hệ thống. Bên cạnh đó, việc tấn công có thể triển khai một cách đơn giản thông qua khai thác một lỗ hổng như: qua email, phần mềm độc hại hoặc trang webs không có hệ thống phòng vệ tốt (Kaur, 2015).

Người dùng có thông tin xác thực tài khoản của mình là mục tiêu chính của tin tặc bằng cách đánh cắp thông tin xác thực, kỹ thuật mạng xã hội, lừa đảo. Trong hành vi trộm cắp thông tin cá nhân của người sử dụng cho mục đích xác thực của tài khoản bị đánh cắp. Sự thành công

của cuộc tấn công phụ thuộc vào việc sử dụng tài khoản xác thực bị đánh cắp. Hành vi trộm cắp thông tin xác thực bằng cách sử dụng phần mềm độc hại để ăn cắp thông tin từ người dùng. Phần mềm độc hại được sử dụng để làm gián đoạn các hoạt đồng bình thường máy tính của khách hàng và thu thập thông tin nhạy cảm. Phần mềm độc hại có thể ở dạng mã hóa, tập lệnh hoặc phần mềm (Kaur, 2015).

Để gia tăng sự cảnh giác về mối đe dọa tấn công mạng đối với khách hàng khi sử dụng dịch vụ ngân hàng trực tuyến, điều quan trọng là người sử dụng cần hiểu về những loại hình tội phạm phổ biến như trình bày trong Bảng 1.

Bảng 1

Các loại hình tấn mạng phổ biến

STT	Loại hình	Nguồn
1	Đánh cắp danh tính (Identity Theft): Sử dụng danh tính người khác như tên, ngày sinh và địa chỉ để lừa đảo là một hoạt động phổ biến được bọn tội phạm mạng sử dụng, là một trong những chiến thuật được chúng áp dụng khi thực hiện giao dịch với các doanh nghiệp kinh doanh trực tuyến, đặc biệt là dịch vụ ngân hàng trực tuyến. Thông tin thu được thông qua hành vi trộm cắp danh tính của tội phạm mạng có thể sau này được chúng sử dụng cho nhiều mục đích khác nhau như: mở tài khoản ngân hàng mới; chiếm đoạt thẻ tín dụng hoặc tài khoản ngân hàng hay làm giả thủ tục giấy tờ để thế chấp vay ngân hàng trong nước. Trộm cắp danh tính là một trong những tội phạm phát triển nhanh nhất trên thế giới và Vương quốc Bahrain là một trong những nạn nhân của tội phạm trộm cắp danh tính.	(Ali, Ali, Surendran, & Thomas, 2017)
2	Lừa đảo (Phishing): Lừa đảo là các thủ thuật được kẻ tội phạm mạng và kẻ lừa đảo áp dụng để khiến nạn nhân tiết lộ thông tin tài chính cá nhân và bí mật khác. Đối với lừa đảo, có nhiều thủ thuật được sử dụng bởi những kẻ lừa đảo qua mạng nhưng chiến thuật quan trọng nhất là gửi email lừa đảo đến khách hàng ngân hàng trực tuyến bằng cách giả vờ rằng một công ty/tổ chức hợp pháp đang cung cấp các dịch vụ điện tử. Một trang web giả mạo, đã được những kẻ lừa đảo máy tính đã thiết kế trang web tương tự như trang web hợp pháp của các tổ chức tài chính, cũng có thể được sử dụng cho các hoạt động lừa đảo và lấy cắp thông tin tài chính của khách hàng khi giao dịch ngân hàng trực tuyến. Việc bảo vệ dữ liệu ngân hàng trực tuyến đang trở nên khó khăn trong thời đại ứng dụng di động ngày nay vì phát hiện ra rằng các nhà nghiên cứu tại Phòng thí nghiệm Bảo mật Websense đã tình cờ phát hiện ra một Trojan ăn cắp mật khẩu sử dụng các kỹ thuật chuyển hướng DNS (Domain Name System) phức tạp để tránh việc máy chủ ngừng hoạt động và chiếm quyền điều hành dữ liệu ngân hàng trực tuyến. Lừa đảo qua điện thoại di động, ứng dụng máy tính và các trang web mạng xã hội là những nền tảng phổ biến thường được sử dụng bởi những tin tặc máy tính. Nó được báo cáo bởi AFCC (Anti-Fraud Command Center), Trung tâm	(Ali et al., 2017; CRIC, 2005; RSA, 2016)

STT	Loại hình	Nguồn
	Chỉ huy Chống gian lận và tổng số vụ tấn công lừa đảo gây thiệt hại 4.5 tỷ đô la trong năm 2014.	
3	Truy cập (Vishing): Đánh lừa hoặc lừa đảo bằng giọng nói là một phương pháp sử dụng trung tâm cuộc gọi giả mạo bằng dịch vụ VOIP (điện thoại qua IP), kỹ thuật của những kẻ gian lận máy tính để có được thông tin chi tiết của khách hàng sử dụng dịch vụ ngân hàng trực tuyến và dữ liệu tài chính của họ. Để đạt được mục đích một hệ thống email được sử dụng bởi những kẻ lừa đảo yêu cầu khách hàng xác nhận chi tiết thông tin tài khoản ngân hàng và các thông tin khác như quy trình kiểm tra bảo mật định kỳ theo số điện thoại được cung cấp trong email lừa đảo.	(Web, 2013)
4	Phần mềm độc hại: Phần mềm độc hại (Virus, Worms, Trojan và các mối đe dọa khác) là mối đe dọa đáng kể nhất hiện nay khi những kẻ tội phạm mạng xâm nhập để có được quyền truy cập trái phép vào tài khoản của người dùng để lấy cắp dữ liệu tài chính của người dùng Internet và các thông tin nhạy cảm. Sự phát triển nhanh chóng trong các thiết bị di động như điện thoại thông minh và máy tính bảng dẫn đến nhiều phát triển phần mềm độc hại. Các ứng dụng phần mềm độc hại được sử dụng trong những năm qua bởi những kẻ tội phạm mạng đã thực hiện thành công hàng trăm nghìn vụ gian lận trực tuyến trong kinh doanh, đặc biệt là trong lĩnh vực ngân hàng trực tuyến để rút ra một lượng lớn tiền. Phần mềm độc hại trên điện thoại di động là điều quan trọng cần được xem xét ở đây vì một số nền tảng di động đang phát triển như Android được những tội phạm mạng khai thác cấy phần mềm độc hại. Vì vậy, thách thức lớn nhất là làm sao phát triển hệ thống phòng thủ mạnh mẽ để đủ năng lực chống lại những ứng dụng phần mềm độc hại, tinh vi nhắm vào các dịch vụ ngân hàng trực tuyến và các tổ chức tài chính khác.	(Pandalabs, 2012)
5	Lấy cắp dữ liệu và bẻ khóa máy tính (Hacking and Cracking): Thông qua việc lấy cắp dữ liệu và bẻ khóa máy tính, những tội phạm mạng có thể đột nhập vào máy tính và mạng máy tính để lấy cắp thông tin tài chính mà sau này có thể được sử dụng cho các mục đích trái phép khác. Ngày càng có nhiều phần mềm độc hại ẩn danh khác nhau có thể được sử dụng cho mục đích tấn công mạng máy tính bởi những kẻ tội phạm mạng.	(Ali et al., 2017)
6	Tự động hóa gian lận ngân hàng trực tuyến (Automating Online Banking Fraud): Tội phạm mạng và những kẻ gian lận máy tính hiện đã thực hiện những bước tiến xa hơn với sự trợ giúp của Hệ thống chuyển giao tự động (Transfer Systems). Một hệ thống mới đã được bắt đầu cho tự động hóa hệ thống gian lận ngân hàng trực tuyến bằng cách kết nối với các biến thể phần mềm độc hại SpyEye và ZeuS như một phần của tệp WebInject, là tệp văn bản có nhiều mã JavaScript và HTML.	(Ali et al., 2017; Kharouni, 2012)

STT	Loại hình	Nguồn
7	Kỹ thuật xã hội (Social Engineering): Kỹ thuật xã hội là nghệ thuật lôi kéo mọi người thực hiện các hành động hoặc tiết lộ thông tin bí mật. Ngành khoa học xã hội của kỹ thuật xã hội thường được sử dụng bởi kẻ gian lận máy tính và tội phạm mạng để lấy dữ liệu tài chính nhằm truy cập trái phép vào thông tin.	(Ali et al., 2017)
8	Mạng xã hội (Social Networks): Mạng xã hội là nền tảng phổ biến có sẵn cho những kẻ lừa đảo trên mạng truy cập thông tin do chủ tài khoản chia sẻ. Thông tin được truy cập bởi những kẻ gian lận mạng sau này có thể được sử dụng cho các mục đích trái phép. Các nền tảng mạng xã hội này như Facebook và Twitters cho phép người dùng gửi một tin nhắn tức thì và trong quá trình này, người dùng có thể bị chuyển hướng gửi tin nhắn đến một số trang web khác, bằng cách cung cấp một đường dẫn khác của những kẻ lừa đảo.	(Ali et al., 2017)
9	Tấn công từ chối dịch vụ (DoS): Tội phạm mạng nỗ lực tấn công làm cho tài nguyên mạng không khả dụng cho người dùng. Bản chất của các cuộc tấn công này nghiêm trọng đến mức cá nhân các cuộc tấn công từ chối dịch vụ phân tán có thể sớm hạ gục không chỉ một trang web mà còn bất kỳ sự can thiệp nào từ các nhà cung cấp dịch vụ. Thiệt hại về vật chất của các cuộc tấn công DoS đối với các tổ chức cơ sở hạ tầng quan trọng có thể rất đáng kể. Ví dụ, một người trả lời cuộc Điều tra Tội phạm Máy tính và An ninh của Úc năm 2005 đã báo cáo khoản lỗ một sự cố là 08 triệu phát sinh từ một cuộc tấn công DoS. Các dịch vụ ngân hàng trực tuyến phải xem xét mức độ nghiêm trọng của các cuộc tấn công qua DoS và các mối đe dọa không gian mạng đối với sự tăng trưởng kinh doanh và do đó các biện pháp nghiêm túc cần được thực hiện để cải thiện mức độ bảo mật và để duy trì tăng trưởng kinh doanh bền vững. Cần liên tục cải thiện các lớp bảo mật cho các ứng dụng của dịch vụ ngân hàng trực tuyến và để giảm thiểu các mối đe dọa hiện có đến từ không gian mạng.	(Ali et al., 2017; DOPUK, 2013)
10	Thiết bị điện tử và điện thoại Di động: Việc sử dụng điện thoại thông minh và các thiết bị điện tử khác như máy tính bảng trở thành phổ biến trong thời đại ngày nay. Các chuyên gia bảo mật dự đoán nghiêm trọng các mối đe dọa từ tội phạm mạng và kẻ gian lận máy tính trên các nền tảng có sẵn của điện thoại thông minh và máy tính bảng. Sự gia tăng khách hàng truy cập các dịch vụ ngân hàng trực tuyến và ứng dụng thông qua các thiết bị di động và các mối đe dọa sẵn có hiện nay phải được các tổ chức tài chính và các dịch vụ ngân hàng trực tuyến quan tâm để đảm bảo rằng họ có những kỹ năng vận hành các dịch vụ của mình trên nhiều nền tảng khoa học công nghệ và nhất là cách phòng vệ tội phạm mạng càng tốt (việc giáo dục tuyên truyền cách phòng vệ tội phạm mạng).	(Ali et al., 2017)

STT	Loại hình	Nguồn
11	Nền tảng đa phương tiện kỹ thuật số (Electronic Media Platforms): Mọi người đang sử dụng các nền tảng công nghệ hỗ trợ trình duyệt ngày càng phức tạp hơn. Chúng bao gồm các thiết bị phát trực tuyến phương tiện và truyền hình thông minh hoặc dựa trên Internet được cung cấp bởi nhiều nhà sản xuất. Ví dụ về Google TV, Skype, Youtube, TikTok, Facetime, Viber, Zoom, Microsoft Teams, etc. Truy cập Internet qua các nền tảng này cũng tạo ra mối quan tâm về an ninh mạng cho người tiêu dùng. Các nền tảng có thể dễ dàng cho phép tội phạm mạng và kẻ lừa đảo thao tác đa dạng các thiết bị vật lý thông qua các ứng dụng được kiểm soát. Giáo dục và nâng cao nhận thức của người tiêu dùng đang trở nên quan trọng hơn về cách sử dụng và truy cập tốt nhất các nền tảng phương tiện điện tử này.	(Ali et al., 2017)

Nguồn: Tác giả tổng hợp từ các nghiên cứu trước

Trên cơ sở các nghiên cứu trước cho thấy có rất nhiều rủi ro và thách thức trong quá trình thanh toán trực tuyến, khi tội phạm mạng càng ngày càng phát triển về quy mô và những phương thức tấn công thông qua việc khai thác những lỗ hổng về mạng, hệ điều hành và phần mềm ứng dụng ngày một tinh vi hơn.

Rủi ro mất an toàn thông tin - an ninh mạng hiện nay trong lĩnh vực ngân hàng tại Việt Nam là rất cao. Xuất phát từ nhiều nguyên nhân khách quan khác nhau như: cơ sở hạ tầng công nghệ thông tin còn yếu kém, chính sách xã hội của Chính phủ thiếu tính năng động, vấn đề tài chính cho đầu tư Công nghệ thông tin, vấn đề giáo dục hay ý thức, nhận thức của mọi người dân, và nhiều nguyên nhân khác trong việc bảo đảm an toàn thông tin cá nhân khi tham gia trực tuyến trên Internet (ANM) chưa được các bên quan tâm đúng mức. Chính vì vậy, việc mất an toàn thông tin – an ninh mạng sẽ gây hậu quả không lường về an ninh quốc gia, kinh tế, và chính trị xã hội. Việc một số khách hàng bị mất thông tin cá nhân hay bị thiệt hại về kinh tế như: mất tiền tại một số hệ thống ngân hàng trong nước trong thời gian qua do bọn tội phạm công nghệ cao (hacker) thực hiện cũng là một hồi chuông cảnh báo, một sự việc cần được nghiên cứu, làm rõ, tìm hiểu và đáng báo động để khách hàng cũng như các ngân hàng có những chủ trương, đối sách phù hợp trong việc bảo đảm an ninh mạng trong tương lai.

Nghiên cứu an toàn an ninh mạng sẽ giúp truyền tải và phổ biến các kiến thức quan trọng giúp cho người dùng Internet và giao dịch thanh toán trực tuyến có thể tự bảo vệ mình và giúp cho các nhà quản trị ngân hàng thương mại có thể hạn chế những rủi ro trong kinh doanh dựa vào khả năng tự phòng vệ của mình. Bên cạnh đó, việc nghiên cứu bảo vệ an toàn thông tin còn giúp cho người dùng ý thức được những rủi ro có thể xảy ra khi sao chép, chia sẻ data hay cài đặt các phần mềm không có bản quyền. Ở góc độ quản lý Nhà nước, nghiên cứu này cũng giúp cho các sở ban ngành có liên quan cần thực hiện việc đánh giá lại các điều Luật hiện hành và hoàn thiện cơ sở pháp lý. Từ đó, có những thay đổi về Chính sách thích hợp thúc đẩy phát triển Công nghệ Thông tin, trí tuệ nhân tạo nhưng vẫn đảm bảo an toàn thông tin an ninh mạng.

3. Phương pháp

3.1. Thiết kế nghiên cứu

Nghiên cứu này dựa trên phương pháp định tính thông qua phỏng vấn chuyên sâu. Cách tiếp cận này cho phép chúng tôi hiểu sâu hơn về một nghiên cứu trường hợp về tổ chức quản lý an ninh mạng tại các ngân hàng thương mại trong nước và nước ngoài tại Việt Nam trước những thách thức và yếu tố rủi ro. Eisenhardt (1989) đề xuất rằng nghiên cứu trường hợp là kỹ thuật

phù hợp nhất để thực hiện, khi một hiện tượng mới nổi và phức tạp chưa được kiểm tra và hiểu hoàn toàn. Nó cũng tạo không gian cho những hiểu biết mà nhà nghiên cứu không dễ đoán ra (Bell & Willmott, 2016). Phát hiện của quá trình này là để xác định các yếu tố rủi ro và thách thức của an ninh mạng tại các ngân hàng thương mại và người sử dụng dịch vụ thanh toán ngân hàng trực tuyến để đề ra các giải pháp hạn chế rủi ro, vượt qua những thách thức đảm bảo an toàn trong không gian mạng và tạo sự đổi mới đột phá.

3.2. Phương pháp thu thập dữ liệu

Phương pháp thu thập số liệu chủ yếu dựa vào kết quả phỏng vấn thông qua triển khai 10 cuộc phỏng vấn bao gồm bốn chuyên gia trong lĩnh vực an ninh mạng đang công tác ba trường Đại học ở Việt Nam và một trường Đại học tại Hoa kỳ và sáu nhà quản lý CNTT trong các ngân hàng hàng thương mại trong nước và nước ngoài tại Việt Nam. Bảng 1 trình bày thông tin của người trả lời phỏng vấn được mã hóa danh tính. Mỗi cuộc phỏng vấn kéo dài trung bình 90 phút. Đặc biệt có một cuộc phỏng vấn với chuyên gia về an ninh mạng kéo dài hơn ba giờ. Kết quả phỏng vấn giúp xác định những rủi ro và thách thức đối với an toàn thông tin trong quá trình truy cập Internet tại Việt Nam hiện nay. Đồng thời, với những chia sẻ kiến thức của chuyên gia và các nhà quản lý mạng CNTT đã làm rõ những vấn đề trong mục tiêu của nghiên cứu.

Sau khi tiến hành 10 cuộc phỏng vấn chuyên sâu với các chuyên gia am hiểm về ANM như trong Bảng 1, chúng tôi tiến hành tổng hợp, phân tích và phân nhóm nội hàm kết quả phỏng vấn thông qua phần mềm NVIVO cho thấy các nội dung trả lời đã bắt đầu bão hòa. Hay nói cách khác, các ý kiến của chuyên gia có sự trùng lắp và không có phát sinh nội dung mới. Vì vậy, chúng tôi đã quyết định ngừng triển khai phỏng vấn mới và tiến hành phân tích kết quả nghiên cứu.

Bảng 2

Mô tả thông tin người tham gia

Mã số	Chức danh	Đơn vị công tác, địa điểm
Đối tượng 1	Tiến sĩ - Giảng Viên - Trưởng phòng CNTT.	Đại học 1, Thành phố Hồ Chí Minh, Việt Nam.
Đối tượng 2	Tiến sĩ - Giảng Viên - Trưởng khoa CNTT.	Đại học 2, tỉnh Đắk Lắk.
Đối tượng 3	Tiến sĩ - Giảng Viên - Trưởng Trung tâm an ninh.	Đại học 3, Thành phố Hồ Chí Minh, Việt Nam.
Đối tượng 4	Tiến sĩ - Giảng Viên – Giám đốc và tư vấn.	Đại học 4, Hoa Kỳ.
Đối tượng 5	Trưởng Phòng CNTT.	Ngân hàng thương mại cổ phần 1, Thành phố Hồ Chí Minh.
Đối tượng 6	Trưởng Phòng CNTT	Ngân hàng thương mại cổ phần 2, Thành phố Hồ Chí Minh.
Đối tượng 7	Phụ trách quản lý Phòng CNTT	Ngân hàng thương mại cổ phần 3, Thành phố Hồ Chí Minh.
Đối tượng 8	Phụ trách quản lý Phòng CNTT	Ngân hàng thương mại cổ phần 4, Thành phố Hồ Chí Minh.
Đối tượng 9	Phụ trách quản lý Phòng CNTT	Ngân hàng thương mại cổ phần 5, Thành phố Hồ Chí Minh.
Đối tượng 10	Trưởng Phòng CNTT	Ngân hàng thương mại nước ngoài, Thành phố Hồ Chí Minh.

Nguồn: Kết quả phân tích dữ liệu của nhóm nghiên cứu

3.3. Phương pháp xử lý kết quả phỏng vấn

Tác giả sử dụng phần mềm NVIVO để phân tích kết quả phỏng vấn chuyên sâu của các chuyên gia và các nhà quản lý trực tiếp về Công nghệ thông tin và an toàn thông tin của doanh nghiệp. Phần mềm giúp nhóm các chủ đề chính liên quan đến an ninh mạng mà các chuyên gia trả lời phỏng vấn quan tâm nhất. Từ đó đưa ra kết quả khung khái niệm có liên quan mật thiết với nhau giúp khám phá mới kết quả nghiên cứu. Kết quả khung lý thuyết khám phá mới này giúp làm nền tảng cho các nghiên cứu định lượng trong tương lai. Đồng thời kết quả cũng giúp hình thành các nhóm nhân tố quan trọng liên quan đến an ninh mạng và cũng là cơ sở phát triển hình thành các tiêu chí để đánh giá về an ninh mạng cho các nghiên cứu định lượng trong thời gian tới.

4. Kết quả

4.1. Kết quả nghiên cứu

Tất cả các chuyên gia làm việc trong Ngân hàng thương mại (người trả lời số 05 - 10) đã đề cập rằng tình hình mối đe dọa An ninh Kỹ thuật số tiếp tục lan rộng vì lợi nhuận. Ví dụ: ransomware là một loại phần mềm độc hại, mã hóa tập tin ngày càng được các Tội phạm mạng triển khai để mã hóa các tập tin máy tính của một tổ chức hoặc cá nhân, sau đó thực hiện thanh toán (ví dụ: ransomedom) để đổi lấy việc giải mã các tập tin của họ. Do đó, hầu hết các Ngân hàng thương mại phải tạo ra một quy trình nghiêm ngặt để ngăn chặn các cuộc tấn công mạng, tất cả các nhân viên phải tuân theo quy trình bắt buộc khi tham gia truy cập Internet, gửi và nhận email, sử dụng trình điều khiển bên ngoài hay truy nhập thông tin khách hàng, theo dõi, kiểm soát việc thanh toán trực tuyến của khách hàng, etc.

Thật vậy, những phát hiện từ nghiên cứu định tính cung cấp thêm bằng chứng rằng trong lĩnh vực Ngân hàng, các Ngân hàng thương mại và Ngân hàng Trung ương đã chủ động đầu tư vào mạng lưới bảo mật của họ và xem xét quản lý rủi ro để ngăn chặn tin tặc trực tuyến và Tội phạm Công nghệ cao. Ngân hàng Trung Ương yêu cầu các Ngân hàng thương mại liên tục cập nhật các thủ tục, quy trình mới để tuân thủ quy trình an toàn và bảo mật thông tin. Hiện tại, hầu hết các Ngân hàng thương mại đã đầu tư một tường lửa đáng tin cậy với những tiến bộ Công nghệ và mua một phần mềm chống virus để ngăn chặn tấn công mạng và giảm thiểu tác động của rủi ro.

Kết quả nghiên cứu cũng cho thấy tất cả các chuyên gia đều có ý kiến tương tự rằng các ngân hàng thương mại phải tự xoay xở trong việc bảo vệ an toàn an ninh mạng và thông tin của khách hàng. Các ngân hàng thương mại đã có nhiều nỗ lực đầu tư và triển khai quy trình đảm bảo an toàn thông tin theo chuẩn mực quốc tế chung. Tuy nhiên, qua ghi nhận từ kết quả phỏng vấn chúng tôi nhận thấy có sự khác biệt đáng kể giữa ngân hàng thương mại trong nước và ngân hàng thương mại nước ngoài trong việc triển khai quy trình đảm bảo an toàn thông tin mạng. Cụ thể, quy trình của ngân hàng thương mại nước ngoài thực hiện nghiêm ngặt hơn. Bên cạnh đó, cũng có sự khác biệt giữa các ngân hàng thương mại trong nước và nước ngoài là do khác nhau về nguồn lực tài chính và nguồn vốn con người.

Những phát hiện từ các cuộc phỏng vấn chuyên sâu từ 10 chuyên gia về Công nghệ thông tin và an ninh mạng cho thấy người dùng Internet ở Việt Nam hiện nay có rất ít kiến thức về an ninh mạng. Do đó, họ đã bỏ qua các bước bảo mật trực tuyến khi truy cập Internet. Họ sẵn sàng cung cấp thông tin cá nhân cho các nhà cung cấp dịch vụ hoặc người bán sản phẩm khi mua sắm trực truyến. Trong khi đó, các nhà cung cấp này không có đầu tư đầy đủ về an ninh mạng để bảo vệ thông tin khách hàng.

Kết quả từ các cuộc phỏng vấn chuyên sâu cũng cho thấy có rất nhiều quảng cáo về sản phẩm công nghệ, nên việc lựa chọn sản phẩm đã phải đối mặt với những rào cản và thách thức.

Như vậy, việc lựa chọn sản phẩm công nghệ an toàn là rất khó và mức độ lựa chọn sản phẩm Công nghệ của các Ngân hàng thương mại hiện nay đều không giống nhau, để đảm bảo thực hiện thật tốt quy trình của hệ thống bảo mật hoàn hảo. Việc lựa chọn Công nghệ và mức độ đầu tư bảo mật dựa trên các điều kiện kinh doanh và các nguồn lực sẵn có của từng ngân hàng. Kết quả cung cấp bằng chứng cho thấy các Ngân hàng thương mại nước ngoài có hiệu suất tốt hơn về thủ tục bảo mật so với các Ngân hàng thương mại trong nước. Nói chung, vì tài chính, giá cả và kinh nghiệm trên toàn thế giới, các Ngân hàng thương mại nước ngoài đã đầu tư tốt hơn vào hệ thống nhân lực và an ninh mạng. An ninh mạng được giám sát tốt và đồng bộ hóa cao vì vậy mà các khách hàng là công ty lớn và các cá nhân giàu có thường có xu hướng mở tài khoản ngân hàng của họ ở các Ngân hàng nước ngoài hơn là các Ngân hàng trong nước (điều này cũng cho thấy vấn đề đảm bảo an ninh mạng gây ảnh hưởng trực tiếp trong lĩnh vực kinh doanh, năng lực cạnh tranh tài chính giữa Ngân hàng trong nước và ngoài nước).

Ở góc độ khách hàng, cá nhân, thì kết quả nghiên cứu cũng cho thấy người dùng Internet tại Việt Nam hiện nay vẫn vô tư sử dụng phần mềm lậu để tiết kiệm tiền của. Họ đã không nhận thức được những rủi ro tiềm ẩn khi sử dụng phần mềm bị bẻ khóa. Tin tặc có thể đột nhập vào máy tính của họ và chiếm quyền kiểm soát máy tính hay đánh cắp thông tin cá nhân, dữ liệu của máy tính hoặc thông qua máy tính của họ để xâm nhập vào hệ thống máy tính của một đơn vị, cơ quan, doanh nghiệp nào đấy mà máy tính cá nhân của họ được kết nối với hệ thống máy tính khác, điều này sẽ gây mất an toàn thông tin, an ninh mạng và tổn thất nghiêm trọng về kinh tế. Ngoài ra, các chương trình đào tạo về an ninh mạng và quản lý rủi ro cho người dùng trực tuyến chưa được triển khai rộng rãi. Bên cạnh đó các trường học cũng chưa cung cấp cho sinh viên, học viên của mình đủ kiến thức về an toàn thông tin và bảo đảm an ninh mạng để họ tự ngăn chặn các hành vi trộm cắp danh tính từ các hoạt động trực tuyến (như được đề cập bởi người trả lời số 1, 2 và 3).

Điều đáng chú ý là kết quả từ các cuộc thảo luận nhóm cũng cung cấp bằng chứng là việc thiếu kiến thức về an ninh mạng. Nhìn chung, hầu hết các chuyên gia khuyên cáo rằng Chính phủ nên yêu cầu các trường Trung học Cơ sở và Trung học cung cấp một chương trình đào tạo để giáo dục các mối quan tâm về quyền riêng tư và bảo mật trực tuyến cho những người trẻ tuổi để họ nên biết cách tự bảo vệ bản thân và cộng đồng xã hội trong kỷ nguyên số.

4.2. Khám phá mới

Hình 1. Phân tích kết quả phỏng vấn trên phần mền NVIVO

Kết quả từ phần mềm NVIVO trình bày như trong Hình 1 cho thấy có sự quan hệ nhân quả trong an ninh mạng. Một vài nét chính của kết quả tổng hợp cho thấy: thứ nhất, ở góc độ chuyên môn, các nhà quản trị mạng cho rằng có rất nhiều lỗ hổng trong quản trị mạng tại Việt Nam hiện nay nên dễ dàng bị tin tặc xâm nhập. Nhiều nhà quản lý chưa hiểu rõ bản chất khái niệm thế nào là an ninh mạng và những tổn thất, thiệt hại do mất an ninh mạng gây ra. Vì vậy, họ chưa có đầu tư tương xứng để đảm bảo an toàn thông tin.

Thứ hai, do bản chất mạng không an toàn nên tin tặc có thể xâm nhập bất cứ lúc nào khi họ muốn. Các phần mềm gián điệp luôn tồn tại trong rất nhiều hệ thống máy tính của doanh nghiệp cho phép thanh toán trực tuyến và của người dùng hiện nay là lỗ hổng lớn bên trong máy tính để tin tặc dễ tấn công. Bên cạnh đó người dùng tại Việt Nam hiện nay chưa có thói quen đặt mật khẩu an toàn khi sử dụng thông tin cá nhân khi trao đổi qua mạng và hệ thống máy vi tính cá nhân.

Thứ ba, về quản lý nhà nước chưa có những điều luật hay chế tài cụ thể giúp hạn chế tấn công mạng và đảm bảo an toàn thông tin. Sự bùng nổ công nghệ thông tin và mạng free-wifi, mạng 4G, nên người dùng rất thuận tiện truy cập thông tin qua Internet nhưng không có đảm bảo an toàn thông tin. Đây cũng là cửa ngõ mở cho tin tặc xâm nhập vào thiết bị cá nhân để lấy cắp thông tin.

Thứ tư, các doanh nghiệp triển khai kinh doanh trực tuyến và cho phép thanh toán trực tuyến thì chưa có đầu tư bài bản về thiết kế mạng an toàn và khách hàng thì cũng không quan tâm đến việc thông tin cá nhân bị mất cắp, tiết lộ. Trong khi đó do biện pháp chế tài của nhà nước chưa có nên các nhà cung cấp dịch vụ thiếu đầu tư công nghệ để bảo vệ thông tin của khách hàng.

Thứ năm, khi có sự cố tấn công mạng xảy ra thì thiếu sự hợp tác giữa các đơn vị với đội ngũ chuyên trách trong việc khoanh vùng để hạn chế thiệt hại. Mặt khác các doanh nghiệp thường giấu thông tin bị tin tặc tấn công vì muốn giữ uy tín của doanh nghiệp.

Thứ sáu, hiện nay các doanh nghiệp đầu tư nâng cấp thiết bị công nghệ thông tin không đồng bộ nên rất khó đảm bảo an toàn thông tin. Bên cạnh đó, nhà nước chưa có chính sách quy định chuẩn hóa thiết bị công nghệ thông tin để đảm bảo an toàn cho người dùng. Bên cạnh đó, ý thức người dùng còn kém. Các chương trình đào tạo ở các cấp chưa quan tâm đến vấn đề giáo dục về an ninh mạng cho giới trẻ.

Cuối cùng, nhiều doanh nghiệp nói chung và ngân hàng thương mại nói riêng vẫn chưa đủ năng lực và nguồn lực để đưa ra một quy trình nghiêm ngặt để bảo vệ thông tin kinh doanh và thông tin khách hàng của mình. Do nguồn tài chính bị hạn chế, nhiều ngân hàng thương mại vẫn còn khó khăn trong việc triển khai các tài liệu kinh doanh được mã hóa trước khi lưu trữ trong không gian mạng.

4.3. Thảo luận kết quả

Tất cả các chuyên gia đều đồng ý rằng làm thế nào để bảo vệ an ninh mạng trong nền kinh tế Kỹ thuật số là một vấn đề đáng lo ngại và rất nan giải. Việc triển khai hệ thống giám sát, cơ sở hạ tầng Công nghệ thông tin và truyền thông, người dùng Internet có hành vi đã tạo ra nhiều rủi ro và thách thức an ninh mạng trong kinh doanh trực tuyến và thanh toán giao dịch trực tuyến.

Dựa trên các kết quả định tính, các báo cáo về vi phạm An ninh dữ liệu đã không bắt buộc các cá nhân, doanh nghiệp, ngân hàng thương mại bị sự cố phải báo cáo hay khai báo cho cơ quan, ban ngành chức năng. Ngoài ra, cộng đồng doanh nghiệp và cá nhân không được công

bố nơi họ phải báo cáo các sự cố của các cuộc tấn công mạng. Cho đến nay, Chính phủ đã thành lập Trung tâm ứng phó khẩn cấp máy tính Việt Nam (VNCERT) từ năm 2017. Tuy nhiên, hầu hết người dùng Internet bình thường không nhận ra Trung tâm này ngoại trừ các chuyên gia trong lĩnh vực bảo mật mạng hoặc khoa học máy tính. Do đó, các nhà hoạch định Chính sách nên cập nhật Luật mới trong các nghĩa vụ báo cáo, vi phạm bắt buộc và nơi công dân nên báo cáo. Kết quả này cho thấy có sự khác biệt với các nghiên cứu trước tại các Quốc gia phát triển, khi có sự cố về an ninh mạng thì họ có những quy trình nghiêm ngặt báo cáo sự cố và lực lượng phản ứng nhanh (Weiss & Jankauskas, 2018).

Kết quả nghiên cứu cho thấy rủi do trong vấn đề an ninh mạng tại các ngân hàng thương mại tại Việt Nam về cơ bản giống như cách thức mà các tin tặc thường xuyên sử dụng khi tấn công mạng (Ali et al., 2017; CRIC, 2005; DOPUK, 2013; Kaur, 2015; Pandalabs, 2012; RSA, 2016; Web, 2013). Việc các ngân hàng thương mại đã tập trung đầu tư nhất để đảm bảo đạt được đến mức độ an minh mạng trong hoạt động giao dịch ngân hàng thương mại. Kết quả này cũng giống như các nghiên cứu trước đây của (Peotta et al., 2011). Kết quả nghiên cứu cho thấy việc tấn công mạng là không có phân biệt ranh giới, địa lý trên không gian mạng. Kết quả này cũng tương đồng với nghiên cứu (Christensen & Petersen, 2018). Vấn đề khác biệt trong nghiên cứu này đã làm rõ những thách thức cụ thể mà các ngân hàng thương mại phải vượt qua để đảm bảo việc thanh toán trực tuyến được thông suốt và bảo mật được thông tin cá nhân của khách hàng.

Nghiên cứu cũng có những đóng góp nhất định trong khung lý thuyết xác định được các vấn đề rủi ro và thách thức có quan hệ nhân quả đối với việc đảm bảo an toàn thông tin mạng. Các cơ quan được giao quyền quản lý, kiểm soát về an toàn thông tin và an ninh mạng trong khi thực hiện nhiệm vụ chuyên trách của mình cũng như các hoạt động phòng, chống tấn công mạng; sau khi kiểm tra phát hiện các lỗ hổng của mạng máy tính tiềm ẩn những nguy cơ cao về mất an toàn an ninh mạng cũng như những lỗi của hệ thống về Công nghệ thông tin của các cơ quan, tổ chức không đảm bảo về an ninh mạng hay đã xử lý, ứng cứu một số tình huống nguy hiểm về an ninh mạng lại bị yêu cầu giữ bí mật về các vấn đề này là chưa phù hợp.

Luật an ninh mạng còn đưa ra những yêu cầu bắt buộc các cá nhân, doanh nghiệp tự bảo vệ an toàn thông tin và an ninh mạng của mình và những bắt buộc về mặt Công nghệ để bảo đảm an ninh mạng nhưng chưa thật sự phù hợp với tình hình thực tế chung về mặt tài chính của toàn xã hội hiện nay như: khả năng tài chính của cá nhân, doanh nghiệp; thương mại Công nghệ hiện được bán tràn lan trên thị trường nhưng độ an toàn về chất lượng của Công nghệ chưa cao mà không có những quy định bắt buộc hay sự quản lý của Nhà nước về mặt Công nghệ nên những điều Luật này khó có thể thực thi và đi vào thực hiện.

Từ kết quả của nghiên cứu đã chỉ ra những thách thức, rủi ro về an ninh mạng cho người dùng Internet trong các giao dịch thương mại trực tuyến và thanh toán trực tuyến tại Việt Nam hiện nay, đồng thời cũng chỉ ra những khiếm khuyết về kiến thức an ninh mạng của người dùng Internet; một tỷ lệ không nhỏ, chiếm số đông trong xã hội cộng đồng người dân Việt Nam, họ thường xuyên tham gia vào các hoạt động trên không gian mạng nhưng họ hoàn toàn thiếu kiến thức về an ninh mạng, số người có kiến thức về an ninh mạng còn rất thấp và chưa thật sự đồng đều, thậm chí còn hiểu sai về an ninh mạng.

Trước thực trạng trên, để đáp ứng được yêu cầu về phát triển Công nghệ thông tin, phát triển đất nước theo kịp nền kinh tế Kỹ thuật số của thế giới mà Chính Phủ đã đề ra. Chính Phủ cần có những giải pháp cấp bách trong giáo dục như: cần cải cách nền giáo dục hiện tại để xây dựng một chương trình giáo dục phổ cập kiến thức về An toàn thông tin và an ninh mạng cho mọi người dân trên toàn xã hội. Nhằm hạn chế tối đa việc mất an toàn thông

tin, bảo đảm an ninh mạng của Quốc gia ngày càng được củng cố và bảo đảm an toàn an ninh Quốc gia trong kỷ nguyên số mới hiện nay.

5. Kết luận

Nghiên cứu này nhằm mục đích khám phá những rủi ro và thách thức tiềm năng trong việc bảo vệ thông tin khách hàng giao dịch trực tuyến và thanh toán qua ngân hàng trực tuyến tại các ngân hàng thương mại trong nước và nước ngoài tại Việt Nam. Các phát hiện giúp người dùng cá nhân quan tâm nhiều vấn đề riêng tư hơn và bảo vệ bản thân khỏi hành vi trộm cắp danh tính. Bên cạnh đó, kết quả cũng giúp các nhà quản lý tại các ngân hàng thương mại xây dựng chiến lược quản lý an ninh mạng để bảo vệ thông tin kinh doanh và ngăn chặn các cuộc tấn công mạng. Cuối cùng, nghiên cứu này cung cấp bằng chứng cho thấy các nhà hoạch định chính sách có thể sử dụng để thay đổi hệ thống pháp luật và cải thiện luật hiện hành về an ninh mạng. Hơn nữa, Chính phủ nên xem xét các khía cạnh trách nhiệm của mình trong việc cung cấp an ninh mạng như một hàng hóa và dịch vụ công. Nhìn chung, các phát hiện nêu bật một số rủi ro và thách thức thiết yếu để cải thiện an ninh mạng Quốc gia và Quốc tế trong thời gian tới khi Chính phủ muốn theo đuổi nền kinh tế kỹ thuật số.

LỜI CẢM ƠN

Nghiên cứu này được Trường Đại học Quốc tế, ĐHQG-HCM tài trợ trong đề tài có mã số SV2019-CPA-01.

Tài liệu tham khảo

Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behaviour in e-banking services. *International Journal of E-Education, e-Business, e-Management and e-Learning, 7*(1), 70-78. doi:10.17706/ijeeee.2017.7.1.70-78

Aljawarneh, S. A. (2017). Emerging challenges, security issues, and technologies in online banking systems. In *Online banking security measures and data protection* (pp. 90-112). doi:10.4018/978-1-5225-0864-9.ch006

Belás, J., Korauš, M., Kombo, F., & Korauš, A. (2016). Electronic banking security and customer satisfaction in commercial banks. *Journal of Security and Sustainability Issues, 5*(3), 411-422. doi:10.9770/jssi.2016.5.3(9)

Bell, E., & Willmott, H. (2016). *Qualitative research in business and management* (2nd ed.). London, UK: Sage Publications.

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change, 67*(3), 265-288. doi:10.1007/978-3-319-63010-6

Chakravorti, B., & Chaturvedi, R. S. (2017). *Digital planet 2017: How competitiveness and trust in digital economies vary across the world*. Medford, MA: The Fletcher School, Tufts University.

Choucri, N. (2019). *Cyberpolitics in international relations*. Cambridge, MA: MIT Press.

Christensen, K. K., & Petersen, K. L. (2018). Public-private partnerships on cyber security: A practice of loyalt. *International Affairs, 93*(6), 1435-1452. doi:10.1093/ia/iix189

CRIC. (2005). *Trojan redirector ups the ante in online banking attacks, cyber criminal investigation cell.* Paper presented at the Crime Branch Criminal Investigation Department Mumbai India.

DOPUK. (2013). *Bank Distributed Denial of Service (DDoS) attacks strikes could presage Armageddon.* Retrieved October 10, 2020, from DoS Protection UK website: http://www.dos-protection.co.uk/?p=152

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review*, *14*(4), 532-550. doi:10.2307/258557

Grubicka, J., & Matuska, E. (2015). Sustainable entrepreneurship in conditions of UN (Safety) and technological convergence. *Entrepreneurship and Sustainability Issues, 2*(4), 188-197. doi:10.9770/jesi.2015.2.4(2)

Jackson, K. (1989). Building a secure computer system. *Computer Fraud & Security Bulletin*, *11*(8), 18-19. doi:10.1016/0142-0496(86)90071-8

Kaur, N. (2015). A survey on online banking system attacks and its countermeasures. *International Journal of Computer Science and Network Security (IJCSNS), 15*(3), 57-61.

Kharouni, L. (2012). *Automating online banking fraud*. Retrieved October 12, 2020, from https://studylib.net/doc/18336044/automating-online-banking-fraud

Lantis, J. S., & Bloomberg, D. J. (2018). Changing the code ? Norm contestation and US antipreneurism in cyberspace. *International Relations*, *32*(2), 149-172. doi:10.1177/0047117818763006

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44-71. doi:10.1162/ISEC_a_00266

Pandalabs. (2012). *PandaLabs quarterly report*. Retrieved October 15, 2020, from https://www.pandasecurity.com/en/mediacenter/src/uploads/2012/08/Quarterly-Report-PandaLabs-April-June-2012.pdf

Peker, S., Tvaronavičienė, M., & Aktan, B. (2014). Sustainable risk management: Fuzzy approach to volatility and application on FTSE 100 index. *Entrepreneurship and Sustainability Issues, 2*(1), 30-36. doi:10.9770/jesi.2014.2.1(4)

Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., & Timoteo de Sousa, R. (2011). A formal classification of internet banking attacks and vulnerabilities. *International Journal of Computer Science and Information Technology*, *3*(1), 186-197. doi:10.5121/ijcsit.2011.3113

RSA. (2016). *Online fraud resource centre, inside the world of fraud and cybercrime*. Retrieved October 19, 2020, from http://www.emc.com/emc-plus/rsa-thought-leadership/online-fraud/index.htm

Onlineguards. (2013). *Online banking fraud, online guards fighting cybercrime, online banking fraud, process and safety tips.* Retrieved October 25, 2020, from http://www.onlineguards.com/topics_onlinebankingfraud.html

Weiss, M., & Jankauskas, V. (2018). Securing cyberspace: How states design governance arrangements. *Governance, 32*(4), 1-17. doi:10.1111/gove.12368