

QUẢN TRỊ RỦI RO TRONG PHÁT TRIỂN NGÂN HÀNG SỐ: KINH NGHIỆM QUỐC TẾ VÀ BÀI HỌC CHO VIỆT NAM

● NGUYỄN HOÀNG PHAN

Trường Đại học Văn Lang

DOI: <https://doi.org/10.62831/202504046>

TÓM TẮT:

Bài viết phản ánh những vấn đề về quản trị rủi ro trong phát triển ngân hàng số. Sau khi phân tích thực trạng những rủi ro số trong lĩnh vực ngân hàng trên thế giới và những vấn đề về rủi ro số đang diễn ra ở Việt Nam, bài viết đã đưa ra nhận định về những ảnh hưởng rủi ro khi ngân hàng số ngày càng phát triển tại Việt Nam và những kinh nghiệm mà thế giới đã áp dụng để hạn chế rủi ro. Bài viết cũng đề xuất những giải pháp phù hợp cho ngành Ngân hàng tại Việt Nam nhằm quản trị rủi ro an toàn trước xu hướng phát triển ngân hàng số.

Từ khóa: thanh toán không dùng tiền mặt, rủi ro số, ngân hàng số, quản trị rủi ro, ngân hàng.

1. Đặt vấn đề

Trong những năm gần đây, các vụ lừa đảo liên quan đến ngân hàng số ngày càng diễn ra phổ biến. Các đối tượng sử dụng không gian mạng để lừa đảo chiếm đoạt tài sản, mua bán trái phép thông tin tài khoản ngân hàng, rửa tiền có tổ chức, xuyên quốc gia. Nhận diện các hình thức lừa đảo mới, tinh vi phối hợp với công tác tăng cường an toàn thông tin và phòng chống lừa đảo kết hợp với truyền thông sẽ hạn chế rủi ro ngân hàng số. Bên cạnh đó, việc học hỏi kinh nghiệm quản trị rủi ro ngân hàng số từ các quốc gia trên thế giới để từ đó

ngành Ngân hàng Việt Nam thiết lập các giải pháp nhằm quản trị rủi ro số an toàn và hiệu quả là cần thiết.

Trước xu hướng phát triển của ngân hàng số, quản trị rủi ro số phải đối mặt với 7 rủi ro số, bao gồm: rủi ro tấn công mạng, rủi ro quản lý dữ liệu và quyền riêng tư, rủi ro tự động hóa quy trình, rủi ro số có liên quan đến con người, rủi ro liên quan đến tính bền vững của hoạt động kinh doanh, rủi ro liên quan đến điện toán đám mây, rủi ro trách nhiệm của bên thứ ba.

Tác giả sử dụng các công cụ phân tích gồm

thống kê mô tả, thống kê phân tích, so sánh, hệ thống hóa... Để phục vụ cho nội dung nghiên cứu là các lý thuyết cơ bản và những vấn đề chung về quản trị rủi ro an toàn trước xu hướng phát triển ngân hàng số, tác giả sử dụng nguồn dữ liệu lấy từ các sách, các bài báo được đăng tải trên các tạp chí trong nước và nước ngoài, thông tin lấy từ internet, từ các dữ liệu báo cáo ngành ngân hàng...

2. Thực trạng về rủi ro số trước xu hướng phát triển ngân hàng số trên thế giới và ở Việt Nam

2.1. Trên thế giới

Một số loại gian lận ngân hàng số phổ biến bao gồm thanh toán đẩy (push payments) thanh toán theo kiểu chủ động đẩy tiền đi (sử dụng trong thanh toán QR Code); lừa đảo giả mạo (Phishing scam) - hình thức tấn công mạng nhằm đánh cắp thông tin cá nhân, mật khẩu, thẻ tín dụng,... của người dùng thông qua email hoặc tin nhắn giả mạo. Đối tượng giả mạo một tổ chức uy tín, chẳng hạn như ngân hàng, công ty dịch vụ, hoặc cơ quan chính phủ, để gửi email, tin nhắn cho người dùng; đánh cắp danh tính (identity theft), chiếm đoạt tài khoản và gian lận thẻ tín dụng hoặc thẻ ghi nợ. Để đạt được điều này, những kẻ lừa đảo thường sử dụng mạng xã hội để lừa nạn nhân tin rằng họ là người hợp pháp hoặc các thực thể để yêu cầu họ ủy quyền thanh toán hoặc bàn giao tài khoản của họ chi tiết.

Các đối tượng có xu hướng dùng AI để tạo ra các văn bản giả mạo, hoặc các đoạn hội thoại giả giọng nói để lừa đảo nạn nhân. Bằng cách sao chép giọng nói của một người, những đối tượng này đóng giả bạn bè hoặc người thân nạn nhân thuyết phục họ gửi tiền khẩn cấp bằng cách tạo ra tình trạng khẩn cấp giả. Điều đáng quan tâm là giọng nói đó có thể dùng để hack vào tài khoản ngân hàng với trường hợp nạn nhân cài đặt dùng lời nói để đăng nhập vào ứng dụng ngân hàng.

Theo một cuộc thăm dò năm 2023 với 7.000

người, 25% trong số được khảo sát cho biết họ đã trải qua một vụ lừa đảo nhân bản giọng nói AI. Nghiên cứu của McAfee - một công ty phần mềm an ninh toàn cầu của Mỹ có trụ sở tại Santa Clara, California cũng phát hiện ra rằng những kẻ lừa đảo cũng có thể dễ dàng sao chép giọng nói từ khắp nơi trên thế giới bằng công cụ nhân bản giọng nói (voice cloning Tools).

Vào tháng 1/2024, một công ty đa quốc gia ở Hồng Kông đã bị mất 25 triệu USD sau khi một nhân viên đã bị lừa đảo bằng cuộc gọi video call giữa CFO và đồng nghiệp.

Theo Digital Banking Experience Report 2023, dữ liệu khách hàng tại các ngân hàng Pháp bị hack cao nhất trong số các ngân hàng tại châu Âu. Nghiên cứu cho thấy, gần 15% khách hàng Pháp phản nản tính bảo mật của dữ liệu của họ đã bị xâm phạm, so với 10% khách hàng ở Anh, 10% khách hàng Ý và 9% của khách hàng tại ngân hàng Thụy Điển. (Erika Kessler, 2024) [5].

2.2. Ở Việt Nam

Tình trạng tội phạm tài chính, lừa đảo ngày càng gia tăng với những thủ đoạn tinh vi và liên tục biến hóa đã gây nhiều tác động tiêu cực đến khách hàng và ngân hàng. Theo ông Nguyễn Thanh Sơn - Giám đốc Trung tâm đào tạo (Hiệp hội Ngân hàng Việt Nam), Việt Nam nằm trong nhóm các quốc gia bị thiệt hại nặng nề nhất do gian lận thanh toán số. Tỷ lệ thiệt hại do gian lận số gây ra tại Việt Nam là 3,6% GDP cao hơn mức trung bình toàn cầu (1,1%) và vượt qua các nước như Brazil hay Thái Lan (cùng 3,2%).

Các hình thức gian lận trong thanh toán số tại Việt Nam gồm tấn công mạng (phần mềm độc hại, lừa đảo, tấn công trung gian), mạo danh, gian lận phi kỹ thuật, lạm dụng chính sách hoàn tiền, gian lận của bên thứ nhất... Trong báo cáo Liên minh chống lừa đảo toàn cầu (GASA) năm 2023, 70% người trả lời cho biết họ gặp phải các vụ lừa đảo ít nhất mỗi tháng 1 lần. Bên cạnh đó, theo báo

cáo của Cục An ninh mạng và phòng chống tội phạm công nghệ cao - Bộ Công An, năm 2023 thống kê có gần 16.000 phản ánh lừa đảo qua mạng với gần 10.000 tỷ đồng bị chiếm đoạt. (T.Đ, 2024) [3]

Tại Hội thảo “Giải pháp bảo vệ khách hàng sử dụng dịch vụ ngân hàng” do Ngân hàng Nhà nước Việt Nam (NHNN) tổ chức cho biết có hơn 87% người trưởng thành có tài khoản thanh toán tại ngân hàng và nhiều ngân hàng đã có trên 95% số lượng giao dịch được xử lý trên kênh số. Bên cạnh đó, thanh toán không dùng tiền mặt cũng gia tăng mạnh mẽ, đặc biệt số lượng giao dịch thanh toán qua di động (Mobile) và QR code bình quân qua các năm từ 2017-2023 đạt trên 100%/năm. Tuy nhiên, bên cạnh những tiện ích và tiện lợi của các sản phẩm, dịch vụ ngân hàng trên không gian mạng đem lại, ngành Ngân hàng cũng đang phải đối mặt với nhiều rủi ro và thách thức liên quan đến an ninh, an toàn và bảo mật. Các thủ đoạn tấn công mạng, sử dụng công nghệ cao để lừa đảo, chiếm đoạt tiền và tài khoản ngân hàng của người dân ngày càng tinh vi và phức tạp, có xu hướng ngày càng gia tăng. Hai hình thức phổ biến nhất là lừa đảo chiếm đoạt trực tiếp tiền của khách hàng, lừa đảo thông qua chiếm đoạt thông tin đăng nhập và xác thực. (Thành Đức, 2024) [4]

Thời gian gần đây cũng xuất hiện nhiều thủ đoạn lừa đảo phức tạp trên không gian mạng điển hình là hình thức lừa đảo qua thuê, mua tài khoản ngân hàng với thủ đoạn tinh vi. Các đối tượng thường đăng bài thông tin trên các diễn đàn, hội nhóm mạng xã hội về việc thuê, mua tài khoản ngân hàng hoặc tiếp cận với những người lao động có thu nhập thấp, người thiếu hiểu biết về pháp luật hoặc sinh viên để nhờ thuê mở tài khoản ngân hàng và nhận tiền công từ 500.000 đồng đến 1.000.000 đồng. Sau khi mở tài khoản, chủ tài khoản bàn giao thông tin đăng nhập Internet Banking, sim điện thoại đăng ký tài khoản, thẻ ngân hàng... cho các đối tượng lừa đảo và các đối

tượng này sẽ sử dụng các tài khoản ngân hàng để lừa đảo chiếm đoạt tài sản. (HM, 2024) [1]

Theo các chuyên gia công nghệ, những vụ lừa đảo mất tiền trong tài khoản ngân hàng đang diễn ra hàng ngày, số tiền bị chiếm đoạt càng lớn từ hàng trăm triệu đến hàng chục tỷ đồng. Bên cạnh những thủ đoạn lừa đảo như cuộc gọi video deepfake, giả công an, viện kiểm soát hay cơ quan thuế,... thì đối tượng lừa đảo còn áp dụng hình thức chiếm quyền trợ năng (Accessibility) trên điện thoại sử dụng hệ điều hành Android bằng mã độc Android Banking Trojan và dùng tính năng Accessibility Service trên nền tảng Android để nắm quyền kiểm soát điện thoại, từ đó dễ dàng thực hiện giao dịch rút tiền trong tài khoản ngân hàng hay tài khoản chứng khoán. Gần đây, kẻ giả mạo mạo danh công an để yêu cầu xác thực định danh thông tin cá nhân, từ đó người dùng nghe theo và cài link độc do kẻ giả mạo công an hướng dẫn từ đó chiếm quyền điện thoại và các tài khoản ngân hàng. (Minh Thành, 2024) [2]

3. Kinh nghiệm quản trị rủi ro số an toàn trên thế giới và ứng dụng cho Việt Nam

3.1. Kinh nghiệm từ thế giới

Các ngân hàng và tổ chức tài chính trên thế giới thường sử dụng các giải pháp giám sát gian lận với các công cụ dựa trên quy tắc để xác định các giao dịch gian lận. Tuy nhiên, phương pháp này có những hạn chế - đặc biệt là trong trường hợp thanh toán ngay lập tức - vì chúng bị điều khiển bởi các quy tắc được mã hóa cứng không thể thích ứng với các mối đe dọa ngày càng gia tăng, cũng như các quy tắc nhị phân không thể xử lý các biến đầu vào phức tạp và không thể phát hiện gian lận trong thời gian thực.

Các ngân hàng đang ngày càng chuyển sang các giải pháp công nghệ tiên tiến như thuật toán AI để xác định các điểm bất thường và mô hình bất thường trong dữ liệu giao dịch, cho phép các tổ chức tài chính phát hiện các hành vi lừa đảo một

cách hiệu quả (theo Báo cáo của Sopra Steria's Digital Banking Experience Report 2023). Các công cụ AI có khả năng xác định và vô hiệu hóa các mối đe dọa mạng bắt nguồn từ phần mềm độc hại như Trojan, vi rút và rootkit. Bằng cách đó, họ có thể bảo vệ dữ liệu nhạy cảm khỏi bị vi phạm, đảm bảo an ninh cho ngân hàng và khách hàng của họ. Những công cụ này rất cần thiết để phát hiện và ứng phó với mối đe dọa vì chúng có thể xử lý lượng lớn dữ liệu lịch sử và tài chính cũng như học hỏi từ mỗi cuộc tấn công. Họ có thể phát hiện lưu lượng truy cập mạng bất thường, quyền truy cập hệ thống và hoạt động của người dùng, đồng thời liên tục nâng cao cơ chế bảo vệ của họ. Do đó, chúng cho phép các tổ chức chủ động chuẩn bị và bảo vệ hệ thống của mình trước các mối đe dọa trên mạng.

Các công cụ phân tích hành vi sinh trắc học và máy học được hỗ trợ bởi AI cũng có thể phát hiện các cuộc tấn công gian lận và lừa đảo bằng cách phân tích các chỉ số quan trọng để ngăn chặn việc chiếm đoạt tài khoản và đánh cắp danh tính. Ví dụ: Sopra Steria, công ty tư vấn, dịch vụ kỹ thuật số và phát triển phần mềm có trụ sở tại châu Âu với 50.000 chuyên gia tư vấn đã phát triển một giải pháp mới được hỗ trợ bởi AI cho Iberpay, một công ty thanh toán liên ngân hàng của Tây Ban Nha, nhằm phát hiện và phân loại rủi ro gian lận để thanh toán ngay lập tức. Giải pháp của họ liên tục cải tiến bằng cách thêm thông tin mới về các nỗ lực gian lận được phát hiện vào cơ sở dữ liệu, giúp thuật toán ngày càng hiệu quả hơn theo thời gian.

Các công nghệ mới nổi có tiềm năng cách mạng hóa việc ngăn chặn gian lận trong lĩnh vực ngân hàng. Các công nghệ chuỗi khối và phi tập trung đang được khám phá để tăng cường bảo mật vì chúng mang lại tính minh bạch cao hơn. Đồng thời, sinh trắc học, phân tích hành vi và các phương pháp tiếp cận đổi mới khác cũng đang được xem xét cho các chiến lược phòng chống

gian lận trong tương lai. Những công nghệ này có thể giúp cung cấp quy trình xác thực an toàn và liền mạch hơn, gây khó khăn cho tội phạm mạng trong việc phạm tội tài chính. Bằng cách khám phá những công nghệ này, các tổ chức tài chính có thể phát triển các chiến lược ngăn chặn gian lận mạnh mẽ hơn và cung cấp cho khách hàng của họ trải nghiệm ngân hàng an toàn và bảo mật hơn.

Theo Báo cáo trải nghiệm ngân hàng số năm 2023 của Sopra Steria, mặc dù AI có thể cải thiện an ninh mạng và quản lý rủi ro trong ngân hàng nhưng vẫn phải giải quyết một số thách thức, chẳng hạn như đảm bảo quyền riêng tư và bảo mật dữ liệu, duy trì chất lượng dữ liệu và chiếm được lòng tin của khách hàng. Để vượt qua những trở ngại này, các ngân hàng phải giao tiếp hiệu quả với khách hàng bằng cách chứng minh cách AI có thể nâng cao dịch vụ khách hàng, cung cấp lời khuyên tài chính được cá nhân hóa và cải thiện bảo mật.

Nghiên cứu cho thấy, các ngân hàng truyền thống cũng cần truyền đạt tốt hơn các biện pháp bảo mật của họ tới khách hàng, vì 35% tin rằng các ngân hàng kỹ thuật số an toàn hơn các ngân hàng thông thường. Tuy nhiên, chính sách chủ quyền kỹ thuật số của EU dự kiến sẽ giúp giải quyết những thách thức đạo đức trong việc triển khai AI để chống tội phạm mạng, vì chính sách này nhằm mục đích cung cấp khuôn khổ pháp lý về cách thức truyền dữ liệu giữa các quốc gia thành viên. Phần mềm này được thiết kế để đảm bảo không có lỗ hổng bảo mật và sẽ bảo vệ quyền riêng tư của người tiêu dùng bằng cách cung cấp cho họ quyền kiểm soát tốt hơn đối với dữ liệu của họ và nơi dữ liệu được lưu trữ.

Điều đó cũng có nghĩa các ngân hàng và tổ chức tài chính hoạt động trong EU sẽ phải tuân theo các quy định chặt chẽ hơn khiến họ phải chịu trách nhiệm về các vi phạm dữ liệu hoặc tấn công mạng. (Erika Kessler, 2024) [5]

3.2. Ứng dụng cho Việt Nam

Hoàn thiện hệ thống pháp lý ngành ngân hàng liên quan đến an ninh, an toàn hoạt động thanh toán điện tử, bảo vệ khách hàng khỏi các mối đe dọa lừa đảo, đảm bảo tính toàn vẹn của các dịch vụ ngân hàng số.

Thời gian qua, Ngân hàng Nhà nước đã ban hành 03 Thông tư về dịch vụ ngân hàng trên Internet, an toàn hệ thống thông tin và thiết bị phục vụ thanh toán thẻ ngân hàng; 03 Chỉ thị về chuyển đổi số và bảo đảm an ninh, an toàn thông tin; 03 quyết định về phương án, giải pháp an toàn thông tin và chiến lược phát triển công nghệ thông tin; 14 văn bản chỉ đạo tập trung vào phòng chống lừa đảo, gian lận trong lĩnh vực thanh toán và phòng, chống giả mạo tên miền, ứng dụng mobile, tin nhắn của các tổ chức tín dụng; 03 Quyết định triển khai Đề án 06 của Thủ tướng Chính phủ; Quyết định số 2345, có hiệu lực từ ngày 01/7/2024, đã nhấn mạnh sự cần thiết của các biện pháp bảo mật mạnh mẽ trong hoạt động ngân hàng.

Để góp phần bảo vệ khách hàng sử dụng dịch vụ ngân hàng, theo Quyết định số 2345/QĐ-NHNN của Thống đốc NHNN, từ ngày 01/7/2024, các giao dịch điện tử của cá nhân có giá trị trên 10 triệu đồng hoặc tổng giá trị thanh toán trong ngày vượt 20 triệu đồng phải áp dụng một trong các biện pháp xác thực sinh trắc học. Việc triển khai Quyết định này góp phần bảo đảm các giao dịch thanh toán trực tuyến chỉ được thực hiện bởi chính chủ tài khoản, qua đó sẽ nâng cao an ninh, an toàn, bảo mật cho các giao dịch thanh toán trực tuyến, giảm thiểu rủi ro gian lận, lừa đảo trong giao dịch thanh toán trực tuyến, cũng như phòng ngừa những vụ việc cho thuê, mượn, mua bán tài khoản thanh toán, ví điện tử sử dụng cho mục đích bất hợp pháp.

Các ngân hàng cũng tăng cường các biện pháp bảo vệ, đồng thời triển khai hệ thống thông tin hỗ trợ quản lý, giám sát và phòng ngừa rủi ro gian lận

trong hoạt động ngân hàng số.

Ngân hàng chủ động triển khai các giải pháp, quy trình, công nghệ để làm sạch dữ liệu khách hàng, tài khoản không chính chủ thông qua Cơ sở dữ liệu Quốc gia về dân cư. Triển khai các giải pháp xác thực mạnh như xác thực sinh trắc, xác thực đa thành tố trong giao dịch trực tuyến như OTP, FIDO, chữ ký số. (T.Đ, 2024) [3]

Nâng cấp hạ tầng công nghệ thường xuyên đảm bảo hoạt động liên tục, thông suốt, an toàn; hệ thống thanh toán điện tử liên ngân hàng xử lý bình quân 830 nghìn tỷ VNĐ/ngày (tương đương 40 tỷ USD), hệ thống chuyển mạch tài chính và bù trừ điện tử xử lý bình quân 20-25 triệu giao dịch/ngày.

Triển khai nhiệm vụ tại Đề án số 06/QĐ-TTg, ngành Ngân hàng phối hợp với Bộ Công An về phòng chống tội phạm và ứng dụng dữ liệu dân cư để phục vụ việc làm sạch dữ liệu, định danh và xác thực chính xác thông tin khách hàng, hỗ trợ hoạt động cho vay tiêu dùng trên kênh điện tử, bảo lãnh điện tử góp phần đảm bảo an toàn hoạt động ngân hàng.

Để thực hiện tốt Quyết định số 2345/QĐ-NHNN, nhằm hạn chế, giảm thiểu các rủi ro liên quan đến vấn đề an ninh, an toàn thông tin trong hoạt động ngân hàng trên không gian mạng, ngành Ngân hàng chủ động triển khai các nhóm giải pháp chính gồm: hoàn thiện cơ chế, chính sách và chỉ đạo thực hiện; triển khai các giải pháp công nghệ và cơ chế phối hợp; tuyên truyền, cảnh báo phòng, chống tội phạm lừa đảo; phối hợp với các cơ quan chức năng trong phòng, chống lừa đảo qua mạng.

Công tác truyền thông của ngành Ngân hàng phải đổi mới, sáng tạo với nhiều nội dung phong phú, hình thức thể hiện đa dạng, ứng dụng công nghệ hiện đại tăng tính lan tỏa, nhằm giúp khách hàng dễ hiểu, dễ nhớ, dễ thực hiện. (Thành Đức, 2024) [4]

Đối với khách hàng, người sử dụng dịch vụ ngân hàng số cần lưu ý và cẩn trọng trong việc quản lý thông tin cá nhân, tài khoản ngân hàng và thường xuyên theo dõi truyền thông về các hình thức lừa đảo.

Cục An toàn thông tin (trước đây thuộc Bộ Thông tin và Truyền thông) khuyến cáo người dân không chia sẻ thông tin cá nhân hoặc thông tin tài khoản ngân hàng với người lạ trên không gian mạng, đồng thời nói không với mọi lời đề nghị “cho thuê” hoặc “bán” tài khoản ngân hàng để hưởng lợi ích tài chính. Theo Điều 291 Bộ Luật Hình Sự năm 2015 (sửa đổi bổ sung năm 2017), chủ tài khoản có thể bị coi là đồng phạm với đối tượng hoặc sẽ bị xử lý về “Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng”. (HM, 2024) [1]

Khách hàng nên cảnh giác và kiểm chứng thông tin của các đối tượng chủ động liên lạc và tự xưng là công an, cán bộ hành chính, cán bộ hỗ trợ dịch vụ công, nhân viên ngân hàng, bằng cách gọi tới tổng đài hỗ trợ được công bố chính thức của các cơ quan, đơn vị.

Khách hàng nên cài đặt phần mềm được tìm thấy trực tiếp trên App Store (với thiết bị hệ điều

hành iOS)/CH Play (với thiết bị hệ điều hành Android);

Khách hàng nên chia sẻ thông tin cảnh giác đến bạn bè, người thân là người cao tuổi hoặc người ít am hiểu về công nghệ.

Khách hàng tuyệt đối không cài đặt/tải trực tiếp bất kỳ ứng dụng nào từ đường link do bất kỳ ai gửi trên tin nhắn SMS, nội dung chat trên các nền tảng xã hội, ứng dụng nhắn tin; hoặc từ các trang web do các đối tượng cung cấp đường link.

Khách hàng tuyệt đối không tin và thực hiện theo hoặc liên hệ với các đối tượng quảng cáo trên mạng xã hội (Facebook, Zalo, Viber, Telegram,...) về các giải pháp "nhanh" cho bất kỳ dịch vụ công nào.

Nhằm bảo vệ khách hàng trên nền tảng giao dịch số, theo quy định của Ngân hàng Nhà nước từ ngày 01/7/2024 chuyển tiền trên 10 triệu phải xác thực sinh trắc học. Khi chuyển tiền qua tài khoản trực tuyến hoặc nạp tiền vào ví điện tử trên 10 triệu đồng phải được xác thực sinh trắc học qua khuôn mặt hoặc vân tay. Nếu chuyển tiền dưới 10 triệu đồng và tổng số tiền chuyển trong ngày không quá 20 triệu đồng thì xác thực bằng mã OTP, không cần xác thực bằng khuôn mặt, vân tay. (Minh Thành, 2024) [2] ■

TÀI LIỆU THAM KHẢO:

1. HM (2024). Cảnh báo lừa đảo qua thuê, mua tài khoản ngân hàng với thủ đoạn tinh vi. Truy cập tại <https://baochinhphu.vn/canh-bao-lua-dao-qua-thuc-mua-tai-khoan-ngan-hang-voi-thu-doan-tinh-vi-102240423080809266.htm>.
2. Minh Thành (2024). Nhận diện bẫy lừa đảo trực tuyến lấy tiền từ tài khoản ngân hàng, chứng khoán. Truy cập tại <https://tuoitre.vn/nhan-dien-bay-lua-dao-truc-tuyen-lay-tien-ti-trong-tai-khoan-ngan-hang-chung-khoan-20240409165844108.htm>.
3. T.Đ (2024). Tăng cường phòng, chống gian lận, lừa đảo trong hoạt động ngân hàng. Truy cập tại <https://vnba.org.vn/vi/tang-cuong-phong--chong-gian-lan--lua-dao-trong-hoat-dong-ngan-hang-14785.htm>.
4. Thành Đức (2024). Bảo vệ khách hàng trước nguy cơ bị lừa đảo, chiếm đoạt tiền và tài khoản. Truy cập tại <https://baokiemtoan.vn/bao-ve-khach-hang-truoc-nguy-co-bi-lua-dao-chiem-doat-tien-va-tai-khoan-32859.html>.

5. Erika Kessler (2024). Digital banking fraud: Latest challenges faced by banks. Available at: <https://www.soprabanking.com/insights/digital-banking-fraud-challenges-banks/>.

Ngày nhận bài: 3/12/2024

Ngày phản biện đánh giá và sửa chữa: 17/12/2024

Ngày chấp nhận đăng bài: 5/1/2025

RISK MANAGEMENT IN DIGITAL BANKING DEVELOPMENT: INTERNATIONAL LESSONS AND RECOMMENDATIONS FOR VIETNAM

● **NGUYEN HOANG PHAN**

Van Lang University

ABSTRACT:

This study examines risk management challenges in the development of digital banking. By analyzing the current landscape of digital risks in the global banking sector and identifying specific risks emerging in Vietnam, the study highlights key vulnerabilities associated with the rapid expansion of digital banking. Drawing from international best practices, the article provides insights into effective risk mitigation strategies. Additionally, it proposes tailored solutions for Vietnam's banking industry to enhance risk management and ensure the secure and sustainable growth of digital banking.

Keywords: cashless payment, digital risk, digital banking, risk management, banking