THỰC TRẠNG VÀ GIẢI PHÁP NÂNG CAO AN TOÀN BẢO MẬT THÔNG TIN CÁ NHÂN TRONG DỊCH VỤ NGÂN HÀNG TRỰC TUYẾN TẠI CÁC NHTM VIỆT NAM

● **BÙI THỊ HẠNH[1]* - NGUYỄN CÔNG MINH[2] - NGUYỄN HOÀI ANH[2] - TRẦN MINH ĐỨC[2] - NGUYỄN NHẬT LỆ[2] - PHẠM THANH TÚ[2]**

[1]Khoa Tài chính, Trường Kinh tế - Đại học Công nghiệp Hà Nội

[2]Sinh viên Khoa Tài chính, Trường Kinh tế - Đại học Công nghiệp Hà Nội

*Tác giả liên hệ: buithihanh@haui.edu.vn

TÓM TẮT:

Nghiên cứu sử dụng phương pháp định tính kết hợp phân tích và tổng hợp dữ liệu thứ cấp từ Ngân hàng Nhà nước Việt Nam, Trung tâm Giám sát an toàn không gian mạng quốc gia và các nghiên cứu liên quan nhằm đánh giá thực trạng bảo mật thông tin trong dịch vụ ngân hàng trực tuyến. Kết quả cho thấy, các hình thức lừa đảo, tấn công mạng và đánh cắp dữ liệu ngày càng phức tạp, trong khi nhận thức bảo mật của một bộ phận khách hàng còn hạn chế. Mặc dù các ngân hàng đã đầu tư vào các công nghệ bảo mật hiện đại, yếu tố con người vẫn là nguyên nhân chính dẫn đến nhiều sự cố an toàn thông tin. Trên cơ sở đó, nghiên cứu đề xuất các giải pháp nhằm nâng cao an toàn bảo mật thông tin cá nhân trong ngân hàng trực tuyến.

Từ khóa: bảo mật thông tin, thông tin cá nhân, an toàn thông tin cá nhân, ngân hàng trực tuyến.

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, các ngân hàng thương mại (NHTM) Việt Nam đang đẩy mạnh phát triển dịch vụ ngân hàng trực tuyến nhằm nâng cao chất lượng phục vụ, tối ưu hóa quy trình giao dịch và đáp ứng nhu cầu ngày càng đa dạng của khách hàng. Theo Ngân hàng Nhà nước Việt Nam (NHNN), ngành Ngân hàng là một trong những lĩnh vực tiên phong trong ứng dụng công nghệ số với số lượng người dùng dịch vụ ngân hàng trực tuyến liên tục gia tăng (NHNN, 2022). Tuy nhiên, sự phát triển nhanh chóng của các nền tảng số cũng kéo theo nhiều rủi ro liên quan đến an toàn bảo mật thông tin cá nhân như lộ lọt dữ liệu, giả mạo giao dịch, tấn công mạng và đánh cắp thông tin khách hàng.

Theo Trung tâm Giám sát an toàn không gian mạng quốc gia, khoảng 80% sự cố lộ lọt thông tin cá nhân xuất phát từ yếu tố con người, trong khi khoảng 20% đến từ lỗi hệ thống (NCSC, 2023). Thực tế này cho thấy, việc nâng cao an toàn bảo mật thông tin cá nhân trong dịch vụ ngân hàng trực tuyến không chỉ phụ thuộc vào hạ tầng công nghệ mà còn cần tăng cường nhận thức, kỹ năng và trách nhiệm của cả ngân

hàng và khách hàng. Vì vậy, việc nghiên cứu thực trạng và đề xuất giải pháp nâng cao an toàn bảo mật thông tin cá nhân trong dịch vụ ngân hàng trực tuyến tại các NHTM Việt Nam có ý nghĩa quan trọng cả về lý luận và thực tiễn.

2. Tổng quan nghiên cứu

Các nghiên cứu trong nước thời gian qua đã đề cập tương đối đa dạng đến vấn đề an toàn bảo mật thông tin trong hoạt động ngân hàng số và dịch vụ ngân hàng trực tuyến. Nguyễn Quốc An và cộng sự (2021), Lương Văn Hải và Nguyễn Thị Hồng Lan (2022), Trịnh Hoàng Minh (2025) cho thấy hệ thống công nghệ bảo mật và chính sách an toàn thông tin tại nhiều NHTM vẫn còn tồn tại những hạn chế nhất định, chưa theo kịp tốc độ phát triển của chuyển đổi số và các hình thức tấn công mạng ngày càng phức tạp. Bên cạnh đó, Võ Thị Ngọc Hà (2023) nhấn mạnh nhận thức về rủi ro bảo mật của khách hàng còn thấp, làm gia tăng nguy cơ lộ lọt thông tin cá nhân trong quá trình sử dụng dịch vụ ngân hàng trực tuyến. Đồng thời, Trần Linh Anh và cộng sự (2024) cho thấy, kỹ năng số của nhân viên ngân hàng có ảnh hưởng trực tiếp đến hiệu quả quản lý, kiểm soát rủi ro và bảo mật thông tin khách hàng.

Các nghiên cứu của nhiều học giả nước ngoài cũng khẳng định, an toàn bảo mật thông tin trong ngân hàng trực tuyến không chỉ phụ thuộc vào nền tảng công nghệ mà còn chịu tác động bởi yếu tố con người và môi trường quản trị. Amar Johri và Shailendra Kumar (2023), Saqib Saeed và cộng sự (2023), Md. Waliullah và cộng sự (2025) cho thấy, nhận thức của người dùng, kỹ năng số của nhân viên, mức độ tin cậy của khách hàng và chính sách quản trị an toàn thông tin có ảnh hưởng đáng kể đến hiệu quả bảo vệ dữ liệu cá nhân trong ngân hàng số.

Các nghiên cứu cho thấy, các công trình chủ yếu tập trung phân tích từng khía cạnh riêng lẻ liên quan đến bảo mật thông tin trong ngân hàng trực tuyến, trong khi chưa đánh giá toàn diện thực trạng an toàn bảo mật thông tin cá nhân tại các NHTM Việt Nam cũng như chưa đề xuất đồng bộ các giải pháp từ góc độ công nghệ, quản trị và con người. Do đó, nghiên cứu thực trạng và giải pháp nâng cao an toàn bảo mật thông tin cá nhân trong dịch vụ ngân hàng trực tuyến tại các NHTM Việt Nam có ý nghĩa thực tiễn.

3. Phương pháp nghiên cứu

Để đạt được mục đích nghiên cứu, tác giả sử dụng phương pháp nghiên cứu định tính kết hợp với phương pháp thống kê, phân tích và tổng hợp dữ liệu thứ cấp nhằm đánh giá thực trạng an toàn bảo mật thông tin cá nhân trong hoạt động ngân hàng trực tuyến. Dữ liệu nghiên cứu được thu thập từ các báo cáo của NHNN, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), các NHTM, bài báo khoa học, công trình nghiên cứu trong và ngoài nước cùng các văn bản pháp lý liên quan đến an toàn thông tin và chuyển đổi số trong lĩnh vực ngân hàng.

4. Thực trạng an toàn bảo mật thông tin cá nhân trong dịch vụ ngân hàng trực tuyến tại các NHTM Việt Nam

Theo NHNN, đến cuối năm 2024, hơn 87% người trưởng thành tại Việt Nam đã sở hữu tài khoản thanh toán tại ngân hàng. Đồng thời, nhiều NHTM cho biết, trên 95% tổng số giao dịch của khách hàng hiện nay được thực hiện thông qua các kênh kỹ thuật số. Điều này cho thấy, hoạt động ngân hàng đang phụ thuộc ngày càng lớn vào môi trường số và dữ liệu điện tử. (Bảng 1)

Sự phát triển mạnh mẽ của ngân hàng trực tuyến đã khiến lĩnh vực tài chính - ngân hàng trở thành một trong những mục tiêu trọng điểm của tội phạm mạng. Theo Hiệp hội An toàn thông tin Việt Nam (2023), số lượng các cuộc tấn công mạng tại Việt Nam tăng hơn 30% so với năm trước, trong đó lĩnh vực tài chính - ngân hàng là nhóm chịu ảnh hưởng lớn. Các hình thức tấn công phổ biến hiện nay bao gồm phishing (giả mạo), malware (phần mềm độc hại), ransomware (mã độc tống tiền), đánh cắp mã OTP, giả mạo ứng dụng ngân hàng và chiếm quyền truy cập tài khoản khách hàng. Bên cạnh đó, theo báo cáo của Ban Công nghệ thuộc Hiệp hội An ninh mạng quốc gia công bố cuối năm 2024, trong tổng số 4.935 cơ quan và tổ chức được khảo sát tại Việt Nam, có tới 46,15% đơn vị từng bị tấn công mạng ít nhất một lần trong vòng một năm và khoảng 6,77% thường xuyên đối mặt với các cuộc tấn công mạng. (Bảng 2)

Bảng 1. Một số chỉ tiêu phản ánh sự phát triển của ngân hàng số tại Việt Nam

Chỉ tiêu	Giá trị	Nguồn
Tỷ lệ người trưởng thành sở hữu tài khoản ngân hàng năm 2024	Trên 87%	NHNN Việt Nam
Tỷ lệ giao dịch thực hiện qua kênh số tại nhiều ngân hàng	Trên 95%	NHNN Việt Nam
Tốc độ tăng trưởng thanh toán không dùng tiền mặt giai đoạn 2020-2023	Trên 50%/năm	NHNN Việt Nam (2023)
Tỷ lệ ngân hàng triển khai Internet Banking và Mobile Banking	Trên 90%	NHNN Việt Nam (2023)
Tỷ lệ người trưởng thành có tài khoản ngân hàng năm 2021	Khoảng 69%	World Bank (2022)

Nguồn: Tổng hợp từ NHNN Việt Nam (2023, 2024) và World Bank (2022)

Bảng 2. Thực trạng các nguy cơ mất an toàn thông tin tại Việt Nam

Nội dung	Kết quả	Nguồn
Tổ chức từng bị tấn công mạng ít nhất một lần	46,15%	Hiệp hội An ninh mạng quốc gia (2024)
Tổ chức thường xuyên bị tấn công mạng	6,77%	Hiệp hội An ninh mạng quốc gia (2024)
Mức tăng các cuộc tấn công mạng năm 2023	Trên 30%	Hiệp hội An toàn thông tin Việt Nam
Người dùng lo ngại nguy cơ lừa đảo trực tuyến	55,5%	Kaspersky Lab và B2B International
Người dùng chưa thực sự an tâm khi giao dịch trực tuyến	57%	Kaspersky Lab và B2B International
Người dùng sẽ sử dụng ngân hàng trực tuyến nhiều hơn nếu bảo mật tốt	68,5%	Kaspersky Lab và B2B International

Nguồn: Tổng hợp từ Hiệp hội An toàn thông tin Việt Nam (2023), Hiệp hội An ninh mạng quốc gia (2024), Kaspersky Lab và B2B International

Trong thực tế, các hình thức lừa đảo công nghệ cao liên quan đến tài khoản ngân hàng đang diễn biến ngày càng phức tạp. Nhiều đối tượng lợi dụng sự thiếu cảnh giác của khách hàng để giả mạo nhân viên ngân hàng, cơ quan chức năng hoặc gửi các tin nhắn chứa đường link giả mạo nhằm đánh cắp thông tin đăng nhập và mã OTP. Sau khi có được thông tin bảo mật, các đối tượng có thể nhanh chóng thực hiện giao dịch và chiếm đoạt tiền trong tài khoản.

Ngoài các hình thức lừa đảo trực tiếp đối với người dùng, hệ thống công nghệ thông tin của các ngân hàng cũng đối mặt với nguy cơ bị tấn công nhằm khai thác lỗ hổng bảo mật. Việc mở rộng hệ sinh thái ngân hàng số, kết nối với ví điện tử, cổng thanh toán và nền tảng tài chính số đã làm gia tăng số lượng điểm kết nối dữ liệu, từ đó làm tăng nguy cơ bị tấn công nếu công tác bảo mật không được kiểm soát chặt chẽ.

Trước thực trạng đó, nhiều NHTM tại Việt Nam đã tăng cường đầu tư vào hạ tầng bảo mật và ứng dụng các công nghệ hiện đại nhằm bảo vệ thông tin khách hàng. Các giải pháp phổ biến hiện nay bao gồm xác thực đa yếu tố (MFA), sinh trắc học, mã hóa dữ liệu, trí tuệ nhân tạo trong giám sát giao dịch bất thường và hệ thống cảnh báo giao dịch theo thời gian thực. (Bảng 3)

Tuy nhiên, mặc dù các ngân hàng đã chú trọng đầu tư vào công nghệ bảo mật, yếu tố con người vẫn là điểm yếu lớn trong công tác đảm bảo an toàn thông tin. Nhiều khách hàng chưa có đầy đủ kiến thức về bảo mật thông tin cá nhân, dễ dàng truy cập các đường link giả mạo hoặc cung cấp mã OTP cho đối tượng lừa đảo. Đây là nguyên nhân dẫn đến nhiều vụ việc mất tiền trong tài khoản ngân hàng thời gian gần đây.

Bảng 3. Một số giải pháp bảo mật được áp dụng tại các NHTM Việt Nam

Giải pháp bảo mật	Nội dung
Xác thực đa yếu tố (MFA)	Tăng cường xác minh khách hàng khi đăng nhập và giao dịch
Sinh trắc học	Xác thực bằng khuôn mặt hoặc vân tay
Mã hóa dữ liệu	Bảo vệ dữ liệu khách hàng khi lưu trữ và truyền tải
Trí tuệ nhân tạo (AI)	Phát hiện giao dịch bất thường và cảnh báo gian lận
Hệ thống giám sát an ninh mạng	Theo dõi và phát hiện nguy cơ tấn công 24/7
Cảnh báo biến động tài khoản	Thông báo giao dịch qua SMS hoặc ứng dụng ngân hàng

Nguồn: Tổng hợp từ báo cáo thường niên và công bố thông tin của các NHTM Việt Nam

Bên cạnh đó, sự chênh lệch về năng lực công nghệ giữa các ngân hàng cũng tạo ra sự không đồng đều trong mức độ an toàn bảo mật. Các ngân hàng lớn như Vietcombank, BIDV, VietinBank và Techcombank có điều kiện đầu tư mạnh vào hạ tầng số và hệ thống bảo mật hiện đại, trong khi nhiều ngân hàng quy mô nhỏ vẫn gặp khó khăn về nguồn lực tài chính và nhân sự công nghệ thông tin. Ngoài ra, việc thu thập, lưu trữ và xử lý dữ liệu cá nhân trong môi trường số cũng đặt ra nhiều thách thức liên quan đến quyền riêng tư và bảo vệ dữ liệu khách hàng. Trong một số trường hợp, dữ liệu cá nhân có nguy cơ bị khai thác trái phép hoặc sử dụng sai mục đích nếu không có cơ chế quản trị dữ liệu chặt chẽ.

Về mặt pháp lý, Việt Nam đã từng bước hoàn thiện hành lang pháp lý liên quan đến bảo vệ dữ liệu và an ninh mạng. Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân được xem là cơ sở pháp lý quan trọng nhằm tăng cường kiểm soát việc thu thập, xử lý và sử dụng dữ liệu cá nhân trong môi trường số. Tuy nhiên, trong bối cảnh công nghệ phát triển nhanh và các hình thức tấn công mạng ngày càng tinh vi, hệ thống pháp lý vẫn cần tiếp tục hoàn thiện để đáp ứng yêu cầu thực tiễn. (Bảng 4)

Nhìn chung, thực trạng an toàn bảo mật thông tin cá nhân trong dịch vụ ngân hàng trực tuyến tại các NHTM Việt Nam cho thấy, quá trình chuyển đổi số đã tạo ra nhiều cơ hội nâng cao hiệu quả hoạt động và

Bảng 4. Tác động của chuyển đổi số đến an toàn bảo mật thông tin trong ngân hàng trực tuyến

Nội dung chuyển đổi số	Tác động	Rủi ro an toàn thông tin	Yêu cầu đặt ra
Mở rộng dịch vụ ngân hàng trực tuyến	Gia tăng số lượng giao dịch trực tuyến	Tăng nguy cơ lừa đảo và tấn công mạng	Tăng cường bảo mật giao dịch
Số hóa dữ liệu khách hàng	Gia tăng lượng dữ liệu cá nhân lưu trữ	Nguy cơ rò rỉ và đánh cắp dữ liệu	Nâng cao bảo vệ dữ liệu cá nhân
Kết nối với ví điện tử và nền tảng số	Mở rộng hệ sinh thái tài chính số	Gia tăng "bề mặt tấn công"	Kiểm soát chặt chẽ kết nối hệ thống
Ứng dụng AI, Big Data và Cloud Computing	Tăng mức độ phụ thuộc vào công nghệ	Phát sinh rủi ro an ninh mạng	Đầu tư hạ tầng và công nghệ bảo mật
Gia tăng giao dịch trên thiết bị di động	Khách hàng giao dịch mọi lúc, mọi nơi	Nguy cơ giả mạo ứng dụng và đánh cắp OTP	Nâng cao nhận thức bảo mật của khách hàng

Nguồn: Tác giả tổng hợp từ NHNN Việt Nam, Hiệp hội An toàn thông tin Việt Nam và World Economic For

chất lượng dịch vụ, nhưng đồng thời cũng làm gia tăng đáng kể các nguy cơ mất an toàn thông tin. Các hình thức tấn công mạng và lừa đảo công nghệ cao đang diễn biến ngày càng phức tạp, trong khi nhận thức bảo mật của một bộ phận khách hàng còn hạn chế.

5. Giải pháp nâng cao an toàn bảo mật thông tin cá nhân trong dịch vụ ngân hàng trực tuyến tại các NHTM Việt Nam

Thứ nhất, nâng cao nhận thức của khách hàng về rủi ro bảo mật

Phần lớn các vụ lừa đảo ngân hàng trực tuyến hiện nay xuất phát từ việc khách hàng để lộ thông tin đăng nhập, mã OTP hoặc truy cập vào các đường link giả mạo. Vì vậy, các ngân hàng cần tập trung nâng cao nhận thức bảo mật cho khách hàng thông qua cảnh báo thường xuyên trên ứng dụng ngân hàng số, tin nhắn và mạng xã hội. Nội dung tuyên truyền cần tập trung vào các hình thức lừa đảo phổ biến như giả mạo nhân viên ngân hàng, website giả mạo và chiếm đoạt tài khoản. Đồng thời, ngân hàng cần xây dựng hướng dẫn sử dụng an toàn đối với nhóm khách hàng lớn tuổi hoặc ít sử dụng công nghệ nhằm giảm nguy cơ bị lừa đảo trong quá trình giao dịch trực tuyến.

Thứ hai, tăng cường đầu tư và hoàn thiện công nghệ bảo mật

Sự gia tăng các cuộc tấn công mạng vào lĩnh vực ngân hàng đòi hỏi các NHTM phải tiếp tục nâng cấp hệ thống bảo mật nhằm bảo vệ dữ liệu khách hàng và hạn chế truy cập trái phép. Các ngân hàng cần ưu tiên triển khai xác thực đa yếu tố, sinh trắc học, mã hóa dữ liệu và hệ thống phát hiện giao dịch bất thường bằng trí tuệ nhân tạo. Bên cạnh đó, cần thường xuyên kiểm tra, đánh giá an toàn hệ thống và khắc phục kịp thời các lỗ hổng bảo mật nhằm giảm nguy cơ bị tấn công mạng.

Thứ ba, đẩy mạnh chuyển đổi số theo hướng an toàn

Quá trình chuyển đổi số cần đi kèm với đầu tư bảo mật tương ứng nhằm hạn chế nguy cơ rò rỉ dữ liệu và mất an toàn thông tin. Các ngân hàng cần tích hợp yêu cầu bảo mật ngay từ quá trình thiết kế sản phẩm và dịch vụ ngân hàng số thay vì chỉ bổ sung sau khi triển khai. Đồng thời, cần tăng cường đầu tư vào hạ tầng công nghệ thông tin, hệ thống giám sát an ninh mạng và quản trị dữ liệu nhằm bảo đảm hoạt động ngân hàng số diễn ra an toàn và ổn định.

Thứ tư, nâng cao năng lực đội ngũ chuyên viên bảo mật

Nhiều sự cố an toàn thông tin tại ngân hàng xuất phát từ lỗi vận hành và thiếu kỹ năng xử lý của nhân viên. Vì vậy, các ngân hàng cần tăng cường đào tạo kiến thức an toàn thông tin cho đội ngũ công nghệ thông tin và nhân sự trực tiếp vận hành hệ thống ngân hàng số. Nội dung đào tạo cần cập nhật theo các hình thức tấn công mạng mới nhằm nâng cao khả năng phát hiện và xử lý sự cố. Đồng thời, các ngân hàng cần chú trọng tuyển dụng và phát triển nguồn nhân lực chuyên sâu về an ninh mạng.

Thứ năm, hoàn thiện chính sách và khung pháp lý về an toàn thông tin

Các ngân hàng cần xây dựng và cập nhật thường xuyên chính sách bảo mật thông tin theo quy định hiện hành và các tiêu chuẩn quốc tế nhằm nâng cao hiệu quả bảo vệ dữ liệu khách hàng. Nội dung chính sách cần quy định rõ trách nhiệm quản lý, lưu trữ và sử dụng dữ liệu cá nhân trong môi trường số. Bên cạnh đó, cần công khai chính sách bảo mật thông tin khách hàng một cách rõ ràng và minh bạch nhằm nâng cao niềm tin của khách hàng đối với dịch vụ ngân hàng trực tuyến ■

TÀI LIỆU THAM KHẢO:

Chính phủ Nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023). Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân.

Hiệp hội An ninh mạng Quốc gia (2023, 2024). Báo cáo tổng quan an toàn thông tin mạng Việt Nam năm 2023, 2024.

Kaspersky (2023). Báo cáo về tình hình tấn công phishing đối với lĩnh vực tài chính tại Đông Nam Á năm 2023.

Kaspersky Lab, B2B International (2016). Khảo sát mức độ quan tâm của người dùng đối với an toàn giao dịch ngân hàng trực tuyến.

Ngân hàng Nhà nước Việt Nam (2023). Báo cáo chuyển đổi số ngành ngân hàng năm 2023.

Ngân hàng Nhà nước Việt Nam (2024). Báo cáo hoạt động ngân hàng và thanh toán số năm 2024.

McKinsey & Company (2021). Digital Banking in Emerging Markets.

World Economic Forum (2022). Global Cybersecurity Outlook 2022.

Ngày nhận bài: 4/3/2026
Ngày phản biện đánh giá và sửa chữa: 27/3/2026
Ngày chấp nhận đăng bài: 6/4/2026

CURRENT SITUATION AND SOLUTIONS TO IMPROVE PERSONAL INFORMATION SECURITY IN ONLINE BANKING SERVICES AT VIETNAMESE COMMERCIAL BANKS

● **BUI THI HANH[1]***
● **NGUYEN CONG MINH[2]**
● **NGUYEN HOAI ANH[2]**
● **TRAN MINH DUC[2]**
● **NGUYEN NHAT LE[2]**
● **PHAM THANH TU[2]**

[1]Lecture, Faculty of Finance, School of Economics, Hanoi University of Industry
[2]Student, Faculty of Finance, School of Economics, Hanoi University of Industry
*E-mail: buithihanh@haui.edu.vn

ABSTRACT:

This study adopts a qualitative approach that combines the analysis and synthesis of secondary data obtained from the State Bank of Vietnam, the National Cybersecurity Monitoring Center, and relevant scholarly literature to assess the current state of information security in online banking services. The findings indicate that fraud, cyberattacks, and data theft are becoming increasingly sophisticated, while a considerable proportion of customers continue to exhibit limited awareness of cybersecurity risks. Although commercial banks have invested substantially in advanced security technologies, human error remains the leading cause of many information security incidents. Based on these findings, the study proposes a set of measures to strengthen the protection of personal information and enhance the overall security of online banking services in Vietnam.

Keywords: information security, personal information security, personal data safety, online banking.