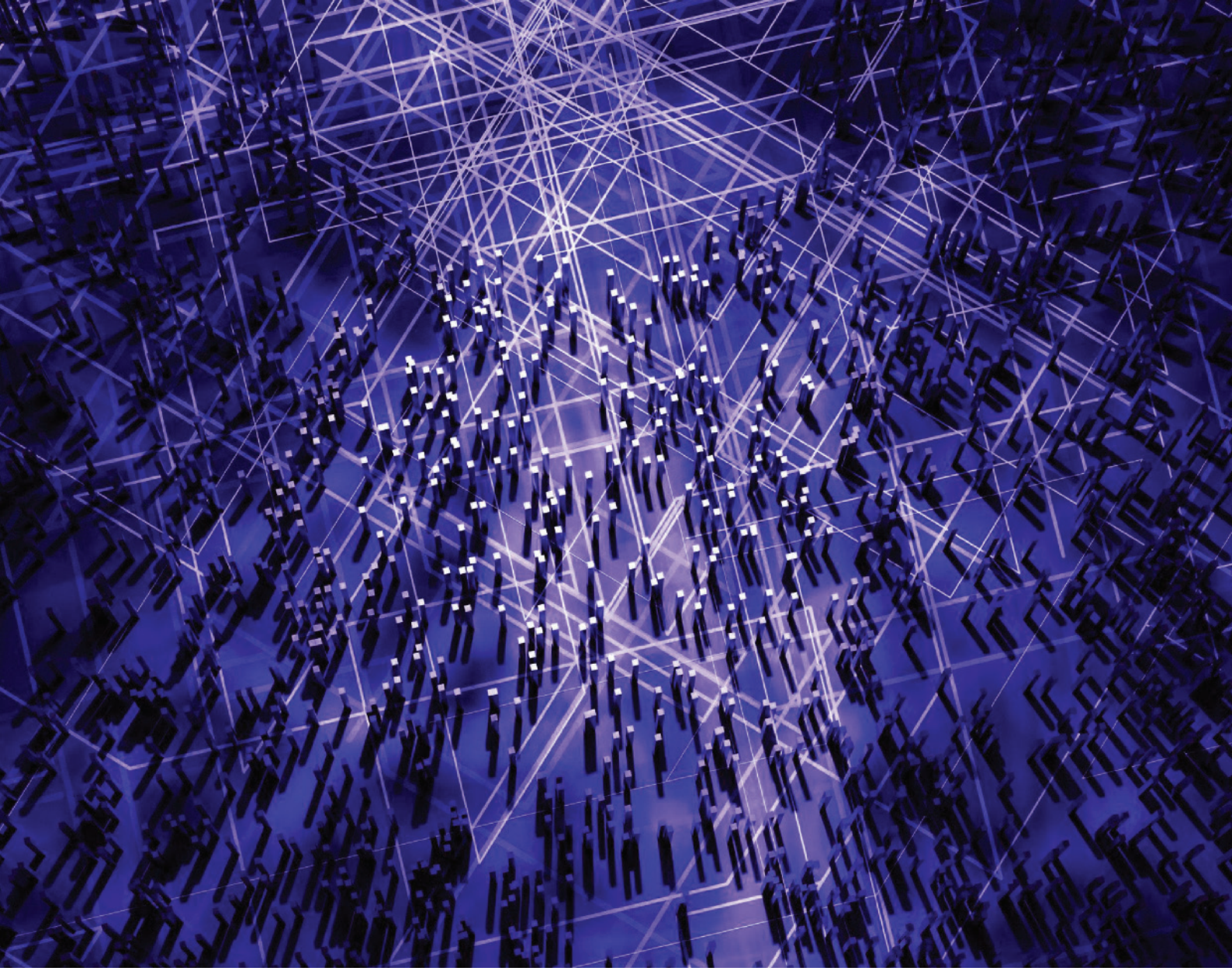


Proof of Human – Xác minh Người thật

Xây dựng mạng lưới xác thực danh tính người thật nhằm xây dựng hệ sinh thái số đáng tin cậy và tăng cường phòng chống gian lận, lừa đảo tại khu vực Châu Á - Thái Bình Dương

Tháng 12 năm 2025

Japan Trust & Safety Association
一般社団法人トラスト＆セーフティ協会

Southeast Asia
Public Policy Institute

Lời giới thiệu

Sách trắng này được nghiên cứu và phát hành bởi Viện Chính sách Công Đông Nam Á phối hợp với Hiệp hội vì Niềm tin & An toàn trên Không gian mạng Nhật Bản (JTSA) với sự hỗ trợ từ Tools for Humanity nhằm cung cấp bức tranh tổng quan về niềm tin trong môi trường số tại khu vực châu Á - Thái Bình Dương. Các thông tin và phân tích trong tài liệu được xây dựng dựa trên các cuộc phỏng vấn với các bên liên quan, nguồn thông tin công khai và phân tích của nhóm tác giả. Những đóng góp chiến lược từ JTSA, đặc biệt là các góc nhìn của Kiyotaka Tanaka liên quan đến quản trị, tính liên thông và việc triển khai sáng kiến Proof of Human (PoH) dựa trên quản trị rủi ro, đã đóng vai trò quan trọng trong quá trình phát triển sách trắng này.

Sách trắng này không đại diện cho quan điểm của Tools for Humanity. Đồng thời, tài liệu này không nhằm mục đích cung cấp một đánh giá toàn diện về chính sách, pháp luật hay quy định và do đó cần được sử dụng một cách thận trọng, đồng thời cần cân nhắc về phạm vi và các hạn chế của tài liệu.

Mục lục

Tóm tắt Tổng quan

Lừa đảo trực tuyến đã trở thành một ngành công nghiệp không biên giới. Quy mô nền kinh tế tội phạm mạng toàn cầu hiện đã vượt 10.000 tỷ USD, trong đó thiệt hại do các vụ lừa đảo mỗi năm chiếm hơn 1.000 tỷ USD. Không chỉ dừng lại ở việc gây thiệt hại tài chính, lừa đảo còn làm xói mòn sức khỏe tinh thần, suy giảm niềm tin của công chúng và làm cạn kiệt nguồn lực thực thi pháp luật. Khu vực châu Á - Thái Bình Dương vừa là mục tiêu lớn vừa là trung tâm vận hành của tội phạm mạng: Đông Nam Á là địa bàn diễn ra các hoạt động lừa đảo quy mô lớn, thường liên quan đến buôn người, trong khi các thị trường phát triển như Nhật Bản và Hàn Quốc đối mặt với làn sóng lừa đảo đầu tư và mạo danh. Vấn đề này mang tính khu vực và có tác động xuyên biên giới, đòi hỏi các biện pháp ứng phó mang tính phối hợp giữa các nền kinh tế.

Công nghệ nhân bản giọng nói bằng AI và deepfake ngày càng có khả năng thuyết phục và thao túng trên quy mô công nghiệp; công nghệ tạo tài khoản tự động cho phép mở rộng phạm vi tiếp cận; trong khi tiền mã hóa và các hình thức thanh toán tức thì thúc đẩy tốc độ thu lợi. Tuy nhiên, chính các công nghệ này cũng có thể củng cố niềm tin của người dùng thông qua việc cải thiện các cơ chế bảo đảm danh tính, chỉ báo về tính xác thực và các biện pháp bảo vệ quyền riêng tư -- khi được hỗ trợ bởi các cơ chế quản trị và minh bạch phù hợp nhằm giảm thiểu rủi ro mới phát sinh.

Các nỗ lực thực thi pháp luật và nâng cao nhận thức hiện có tuy cần thiết nhưng vẫn chưa đủ, trong bối cảnh tội phạm có thể tạo ra hàng nghìn danh tính tổng hợp hoặc tự động với chi phí thấp. Để đạt được tiến triển bền vững trong ngăn ngừa tội phạm mạng, cần xây dựng hai lớp niềm tin trong môi trường số để lấp đầy các lỗ hổng mà đối tượng lừa đảo đang khai thác:

- **Danh tính số (ID số):** Trả lời cho câu hỏi "Bạn là ai?", sử dụng thông tin định danh không ẩn danh, cho phép xác thực danh tính (KYC) cho các môi trường chịu sự quản lý (như lĩnh vực tài chính, chính phủ điện tử).

- **Xác thực con người (Proof of Human - PoH):** Trả lời cho câu hỏi "Bạn có phải là một con người có thật và duy nhất hay không?", sử dụng các chỉ báo theo hướng bảo vệ quyền riêng tư, có thể áp dụng trong các môi trường mở, đa nền tảng, nơi việc tiết lộ đầy đủ danh tính là không cần thiết hoặc không mong muốn.

PoH không phải là sự thay thế cho ID số mà là một lớp bổ sung, giúp mở rộng niềm tin trong môi trường số tới các khu vực trên internet -- nơi phát sinh phần lớn các hoạt động lừa đảo (như mạng xã hội, nền tảng nhắn tin, sàn giao dịch). Cơ chế này góp phần giảm thiểu tài khoản giả/danh tính tổng hợp và tình trạng lạm dụng do phần mềm tự động (bot) điều khiển trong khi vẫn bảo đảm quyền riêng tư của người dùng. Các diễn biến gần đây cho thấy sự cần thiết của việc triển khai PoH trong một khu-ôn khổ dựa trên nguyên tắc bảo đảm niềm tin và sự an toàn, nhằm giải quyết tình trạng lạm dụng tự động hóa trên quy mô lớn đồng thời tránh việc công nghệ này bị hiểu nhầm là sự đảm bảo về ý định hay mức độ đáng tin cậy của người dùng.

Trên toàn khu vực châu Á - Thái Bình Dương, các chính phủ đã xây dựng các nền tảng ID số vững chắc nhằm tăng cường KYC và trách nhiệm giải trình trong các lĩnh vực chịu sự quản lý. Tuy nhiên, phần lớn hoạt động lừa đảo lại xuất phát từ các không gian mở, không chịu sự quản lý trực tiếp, như mạng xã hội, nền tảng nhắn tin và sàn giao dịch trực tuyến, nơi mà ID số không được áp dụng. Trong các môi trường này, PoH mang lại giá trị riêng biệt: thông qua các cơ chế như token xác thực con người theo hướng bảo vệ quyền riêng tư và xác minh dựa trên thiết bị, PoH có thể hạn chế việc tạo hàng loạt tài khoản giả, ngăn chặn các hoạt động gian lận do bot điều khiển và củng cố mạng lưới tương tác giữa những người dùng thật trước khi nạn nhân bị nhắm tới. Để phát huy hiệu quả, các công nghệ này cần đi kèm với các biện pháp bảo vệ rõ ràng, bảo đảm quyền kiểm soát của người dùng và các cấu trúc quản trị nhằm ngăn ngừa lạm dụng, bảo vệ tính ẩn danh và duy trì niềm tin của công chúng.

Các ví dụ điển hình

- **Nhật Bản — My Number:** Tính duy nhất của danh tính được xác minh bởi cơ quan nhà nước trên quy mô lớn, nhưng niềm tin vào hệ thống này từng bị ảnh hưởng bởi các sự cố trong xử lý dữ liệu. Đây có thể là một nền tảng tiềm năng cho các mô hình lai (hybrid) kết hợp ID do Nhà nước cấp với PoH, phục vụ mục đích xác minh theo hướng bảo vệ quyền riêng tư ngoài phạm vi các dịch vụ công.

- **Hàn Quốc — Chế độ tên thật:** Khả năng tích hợp sâu trong các lĩnh vực tài chính, viễn thông và chính phủ điện tử đóng vai trò hiệu quả như một hình thức xác minh PoH. Tuy nhiên, hiệu quả đó cũng đi kèm với nhữnglo ngại về quyền riêng tư vàtự do dân sự, từ đó thúc đẩy mối quan tâm về các mô hình xác thực phi tập trung do người dùng kiểm soát.

- **Malaysia — MyDigital ID (mới triển khai):** Hệ thống sử dụng thông tin xác thực dựa trên sinh trắc học được liên kết với cơ sở dữ liệu quốc gia. Lộ trình triển khai cho thấy định hướng hỗ trợ quản trị ngay từ khâu thiết kế, phù hợp với nguyên tắc PoH, nhưng vẫn cần các biện pháp bảo vệ mạnh mẽ và sự tin tưởng của công chúng để có thể mở rộng quy mô.

- **Philippines — PhilSys (đang mở rộng nhanh):** Hệ thống đã đạt được mức độ tiếp nhận lớn, cho phép tải xuống ID số và xác minh điện tử. Cách vận hành của hệ thống này có những điểm tương đồng với PoH, đồng thời cho thấy sự cần thiết cần duy trì song song công tác quản trị và giáo dục người dùng.

Khả năng phòng, chống lừa đảo hiệu quả đòi hỏi một cơ chế bảo đảm nhiều lớp: các tương tác trong môi trường chịu sự quản lý cần gắn với định danh đã được xác minh, trong khi các nền tảng mở cần được củng cố bằng cơ chế xác minh người dùng thật theo hướng bảo vệ quyền riêng tư. Tính minh bạch, tính liên thông và quyền kiểm soát của người dùng là các yếu tố xuyên suốt. Các cơ chế quản trị trung lập,thông qua các tổ chức xây dựng tiêu chuẩn, đơn vị trung gian trong ngành hay khuôn khổ đa bên liên quan, sẽ đóng vai trò then chốt trong việc chuyển hóa các yêu cầu ở cấp quốc gia thành thực tiễn vận hành trên các nền tảng toàn cầu.

Khuyến nghị chính sách

• Tích hợp ID số và PoH vào các chiến lược phòng, chống lừa đảo: Lồng ghép các bước kiểm tra thông tin và xác minh tính duy nhất vào các luồng giao dịch tài chính, thương mại điện tử và truyền thông nhằm hạn chế tình trạng mạo danh, sử dụng danh tính tổng hợp và lạm dụng bot. Việc này cần được định hướng thông qua quá trình triển khai dựa trên các nguyên tắc về niềm tin và an toàn, đồng thời có các biện pháp bảo vệ để tránh tình trạng phụ thuộc quá mức vào một cơ chế xác minh duy nhất.

• Hỗ trợ các tiêu chuẩn bảo vệ quyền riêng tư và có tính liên thông: Kết hợp các biện pháp bảo đảm dựa trên sinh trắc học/thông tin xác thực với các kỹ thuật mã hóa (ví dụ: bằng phương thức xác minh tính xác thực không tiết lộ tri thức), nhằm bảo vệ tính ẩn danh trong những trường hợp phù hợp và cho phép khả năng sử dụng xuyên biên giới, đồng thời đảm bảo rằng PoH không bị sử dụng sai mục đích để theo dõi hoặc lập hồ sơ người dùng.

• Thúc đẩy đối thoại và phối hợp chính sách khu vực: Tận dụng các diễn đàn như Hội đồng Tư vấn Kinh doanh của Diễn đàn Hợp tác Kinh tế châu Á – Thái Bình Dương (APEC), Nguyên tắc chung G20 về Tài chính số Toàn diện và các sáng kiến kinh tế số của Liên Hợp Quốc để điều chỉnh mục tiêu, chia sẻ bằng chứng và triển khai các chương trình thí điểm xác minh bằng PoH trên nhiều lĩnh vực, bao gồm thử nghiệm trong môi trường có kiểm soát (sandbox) để đánh giá khả năng sử dụng, tính bao trùm và tính tương xứng.

Các vụ lừa đảo cho thấy tình trạng thiếu hụt niềm tin mang tính hệ thống và kéo dài. Một kiến trúc kết hợp giữa ID số và Proof of Human, nếu được triển khai cùng với các biện pháp bảo vệ quyền riêng tư, cơ chế quản trị phù hợp và tính liên thông mạnh mẽ, có thể làm tăng chi phí của hành vi lạm dụng trên quy mô lớn, đồng thời bảo vệ quyền của người dùng và giúp châu Á tiến nhanh hơn tới một nền kinh tế số an toàn và bao trùm hơn.

Giới thiệu: Vấn nạn lừa đảo và khoảng trống chính sách

Kể từ khi xã hội và nền kinh tế chuyển đổi sang môi trường số, tội phạm mạng đã gia tăng cả về quy mô lẫn mức độ tinh vi. Quy mô nền kinh tế tội phạm mạng toàn cầu hiện ước tính vượt 10.000 tỷ USD, tương đương với nền kinh tế lớn thứ ba thế giới nếu xét theo GDP. [1] Trong đó, lừa đảo là một trong những dạng tội phạm mạng phổ biến và đang ngày càng gia tăng, với thiệt hại đối với người tiêu dùng vượt 1.000 tỷ USD mỗi năm. [2] Tuy nhiên, tác động của lừa đảo không chỉ dừng lại ở tổn thất tài chính. Nạn nhân còn phải đối mặt với những hệ lụy lâu dài về sức khỏe tinh thần và phúc lợi tổng thể; niềm tin vào các dịch vụ số và nền kinh tế số bị xói mòn; đồng thời nguồn lực công bị phân tán sang các hoạt động thực thi pháp luật, nâng cao nhận thức và đảm bảo an ninh mạng quốc gia. [3]

Vai trò kép của châu Á

Trong bối cảnh vấn nạn lừa đảo toàn cầu này, khu vực châu Á - Thái Bình Dương nổi lên như một trong những khu vực chịu ảnh hưởng nặng nề nhất. Các hình thức lừa đảo với tên gọi 'mổ lợn' (pig-butchering), lừa đảo đầu tư hoặc tình cảm, trong đó đối tượng lừa đảo sử dụng kỹ thuật thao túng tâm lý để xây dựng mối quan hệ với nạn nhân và dụ dỗ họ chuyển tiền hoặc đầu tư, đang trở nên đặc biệt phổ biến. Các hoạt động lừa đảo dạng này thường bắt nguồn từ mạng xã hội hoặc nền tảng nhắn tin, và được vận hành bởi các tổ chức tội phạm quy mô lớn tại các trung tâm lừa đảo chuyên biệt do các mạng lưới tội phạm có tổ chức xuyên quốc gia điều hành.

Đông Nam Á đóng vai trò trung tâm trong hệ sinh thái này: vừa là nguồn phát sinh nạn nhân, vừa là địa bàn vận hành của các tổ chức lừa đảo tại những khu vực thiếu kiểm soát, đồng thời cũng là nguồn cung lao động - trong đó nhiều người bản thân họ cũng là nạn nhân của nạn buôn người. [4,5]

Trong khi đó, các thị trường phát triển tại khu vực châu Á – Thái Bình Dương như Đài Loan, Nhật Bản và Hàn Quốc có mối liên hệ chặt chẽ với xu thế này. . Với mức độ chuyển đổi số cao và niềm tin lớn vào các dịch vụ số, người tiêu dùng tại các quốc gia này thường xuyên trở thành mục tiêu của các vụ lừa đảo đầu tư và mạo danh. Đồng thời, các quốc gia này cũng đã ghi nhận nhiều trường hợp công dân bị dụ dỗ tham gia vào các hoạt động lừa đảo tại các trung tâm ở nước ngoài. Xét tổng thể, các xu thế trên cho thấy rõ ràng đây không chỉ là một vấn đề mang tính địa phương mà còn là một thách thức khu vực có tính liên kết cao và tác động qua lại giữa các quốc gia. Do đó, cần có các biện pháp ứng phó mang tính phối hợp, kết nối giữa các nền kinh tế phát triển và các quốc gia chịu ảnh hưởng bởi nạn buôn người. [7]

Công nghệ: Yếu tố thúc đẩy tội phạm và cũng là giải pháp

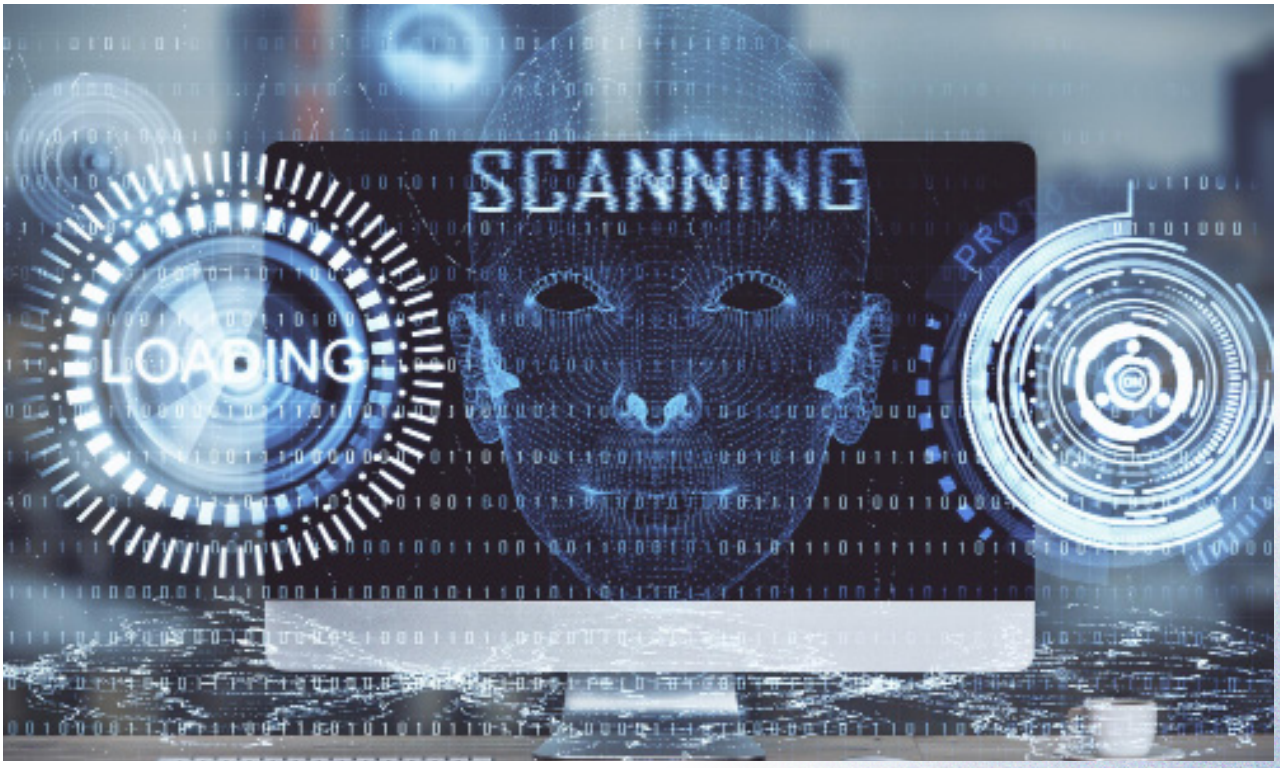
Công nghệ đã làm thay đổi căn bản "kinh tế học" của hành vi lừa đảo, đến mức ngay cả các chính phủ có nguồn lực tốt nhất cũng gặp khó khăn trong việc theo kịp tốc độ tiến hóa của các phương thức tội phạm.

Thứ nhất, khả năng thuyết phục và thao túng nạn nhân đã đạt đến quy mô công nghiệp. Trí tuệ nhân tạo, công nghệ nhân bản giọng nói và deepfake – tức là các công nghệ ứng dụng trí tuệ nhân tạo (AI), đặc biệt là các thuật toán học sâu (Deep Learning) để tạo ra nội dung giả mạo có độ chân thực cao, bao gồm hình ảnh, video và âm thanh – đang bị "vũ khí hóa" nhằm phục vụ hành vi gian lận. Ước tính hơn 42% các nỗ lực lừa đảo trong lĩnh vực tài chính được cho là có sự tham gia của AI. [8] Những công cụ này cho phép tạo ra kịch bản, hình ảnh và cuộc gọi có độ chân thực cao bằng nhiều ngôn ngữ, giúp triển khai các mô hình lừa đảo "đầu tư" hoặc lừa đảo tình cảm phức tạp được vận hành bởi các đối tượng không cần có trình độ kỹ năng cao thông qua các kịch bản đã được tối ưu hóa bằng thử nghiệm A/B (thử nghiệm nhằm so sánh hai phiên bản A và B của cùng một yếu tố trong điều kiện giống nhau).

Thứ hai, khả năng mở rộng quy mô đã trở nên gần như không còn giới hạn. Các công cụ tạo tài khoản tự động, "trang trại SIM" và hệ thống vận hành đa nền tảng cho phép các nhóm nhỏ tiếp cận hàng triệu người qua mạng xã hội, dịch vụ nhắn tin và điện thoại chỉ trong thời gian rất ngắn. Đồng thời, bot và các hệ thống đề xuất có thể bị lợi dụng để xác định và nhắm mục tiêu vào những nhóm người dễ bị lừa. [9]

Thứ ba, tội phạm liên tục đổi mới các phương thức thu lợi. Hạ tầng tiền mã hóa, các nền tảng công nghệ tài chính (fintech), mạng lưới chuyển tiền phi pháp và các công cụ kết hợp chuỗi chéo cho phép di chuyển và che giấu dòng tiền nhanh chóng. Trong khi đó, các phương thức thanh toán tức thì và sự phân mảnh trong các cơ chế xác thực khách hàng cá nhân và doanh nghiệp (KYC/KYB) làm rút ngắn đáng kể thời gian can thiệp của hệ thống ngân hàng truyền thống. [10]

Hệ quả là một khoảng trống niềm tin mang tính hệ thống và kéo dài trong nền kinh tế số: tội phạm đang áp dụng và thích nghi với công nghệ mới nhanh hơn so với khả năng ứng phó của các chính phủ và cơ quan quản lý.



Tuy nhiên, chính những công nghệ này, nếu được triển khai trên quy mô lớn kết hợp với các biện pháp bảo vệ phù hợp, có thể góp phần khôi phục niềm tin của người dùng.

• Tăng cường cơ chế bảo đảm danh tính và thực thể số: Bao gồm xác minh con người, thiết bị và doanh nghiệp theo hướng bảo vệ quyền riêng tư; cơ chế đánh giá uy tín SIM/số; và các mức độ xác thực nâng cao đối với các giao dịch có rủi ro cao, qua đó làm tăng chi phí của các hoạt động lừa đảo quy mô lớn.

• Cải thiện các chỉ báo về tính xác thực cho nội dung và thông tin truyền thông: Các giải pháp như gắn nguồn gốc mã hóa cho hình ảnh và video, cơ chế xác minh người gọi/người gửi cho các dịch vụ thoại và nhắn tin, cũng như tăng cường kiểm soát tính toàn vẹn của quảng cáo và tài khoản có thể giảm thiểu khả năng mạo danh thành công.

• Tăng cường chia sẻ chỉ báo theo hướng bảo vệ quyền riêng tư: Việc chia sẻ các chỉ báo rủi ro giữa các nền tảng và mạng lưới thanh toán có thể giúp phát hiện các hành vi lừa đảo có tổ chức. Đồng thời, các công cụ chấm điểm rủi ro thanh toán theo thời gian thực và các biện pháp "cool-off" (xác nhận người nhận thanh toán, kiểm tra bổ sung, trì hoãn giao dịch đáng ngờ) có thể giảm thiểu thiệt hại ngay tại thời điểm thực hiện giao dịch.

• Áp dụng mô hình lấy nạn nhân làm trung tâm: Bao gồm các cơ chế gỡ bỏ nhanh các công cụ lừa đảo, các kênh thu hồi tiền hiệu quả hơn cho nạn nhân, và xây dựng quy trình rõ ràng để nhận diện những người bị ép buộc tham gia lừa đảo như là nạn nhân thay vì là tội phạm. Các biện pháp này cần được triển khai song song với các biện pháp thực thi pháp luật nhằm phá vỡ vòng xoáy bóc lột. [11]

Do đó, công nghệ vừa là yếu tố thúc đẩy tội phạm vừa là một phần thiết yếu của giải pháp phòng, chống tội phạm mạng. Các chính phủ, nền tảng và tổ chức tài chính cần liên tục áp dụng và cập nhật các công nghệ phòng vệ với tốc độ tương đương với tốc độ tiến hóa của tội phạm, vì lừa đảo không chỉ là các vụ việc đơn lẻ mà còn phản ánh một vấn đề sâu xa hơn, đó là sự thiếu hụt niềm tin mang tính hệ thống và kéo dài trong nền kinh tế số. [12]

Nếu lừa đảo phơi bày sự mong manh của niềm tin trên môi trường trực tuyến, thì danh tính số (ID) là một trong những công cụ rõ ràng nhất để khắc phục tình trạng này. Bằng việc cung cấp sự bảo đảm có thể xác minh về chủ thể thực sự đứng sau mỗi giao dịch hay tương tác, ID số làm gia tăng chi phí của hành vi lừa đảo, đồng thời đặt nền tảng cho một môi trường kinh tế số an toàn hơn. Phần tiếp theo sẽ phân tích các vấn đề mà ID số được thiết kế ra để giải quyết, các công nghệ liên quan, cũng như các phản ứng chính sách mới trong khu vực.

Hai lớp niềm tin trong môi trường số: Danh tính số và Proof of Human

Phòng, chống lừa đảo đòi hỏi các hệ thống niềm tin đa lớp. Các biện pháp thực thi pháp luật và nâng cao nhận thức, dù quan trọng, vẫn chưa đủ để đạt được tiến triển bền vững nếu thiếu các cơ chế định danh và xác thực có khả năng khép kín những kẽ hở mà tội phạm khai thác trên quy mô lớn. Biện pháp xác thực bằng Danh tính số (ID số) và Proof of Human (PoH) đại diện cho hai lớp bổ sung - nhưng khác biệt về bản chất - của hạ tầng niềm tin này. ID số trả lời câu hỏi "Bạn là ai?" bằng cách liên kết cá nhân với các thông tin định danh thực tế đã được xác minh và công nhận bởi các tổ chức như ngân hàng hoặc cơ quan nhà nước. Trong khi đó, Proof of Human trả lời câu hỏi "Bạn có phải là con người thật và duy nhất không?" bằng cách xác nhận người thật và tính duy nhất mà không yêu cầu tiết lộ danh tính. Một lớp là cơ chế xác thực không ẩn danh và phù hợp với các môi trường chịu sự quản lý như ngân hàng và chính phủ điện tử; lớp còn lại là cơ chế xác thực theo hướng bảo vệ quyền riêng tư nhưng có thể xác minh, phù hợp với các không gian số mở nơi mà việc tiết lộ đầy đủ danh tính là không cần thiết hoặc không phù hợp. Khi kết hợp với nhau, hai lớp xác thực này tạo ra một nền tảng cân bằng hỗ trợ đảm bảo cả trách nhiệm giải trình và quyền riêng tư trong môi trường kinh tế số.

Proof of Human không phải là sự thay thế cho hệ thống ID số quốc gia mà đóng vai trò là một lớp bổ sung, bảo vệ quyền riêng tư, mở rộng niềm tin tới các khu vực của môi trường trực tuyến nơi việc xác minh đầy đủ danh tính là không khả thi hoặc không phù hợp.

Các hình thức công nghệ ID số

Các giải pháp ID số tồn tại dưới nhiều hình thức, mỗi loại nhằm giải quyết các rủi ro khác nhau:

• **Hệ thống danh tính số dựa trên thông tin xác thực** dựa vào các thông tin xác thực được cấp và có thể kiểm chứng bằng công nghệ số, thường xuất phát từ ID do chính phủ cấp hoặc từ các tổ chức đáng tin cậy như ngân hàng, nhà mạng di động hoặc cơ sở giáo dục. Các thông tin này cho phép xác thực an toàn các thuộc tính danh tính như tên, độ tuổi hoặc quốc tịch. Các thông tin này có thể được lưu trữ trong ví số và sử dụng cho mục đích xác minh trên nhiều dịch vụ, cho phép xác thực một lần nhưng dùng cho nhiều nền tảng, đồng thời bảo vệ quyền riêng tư tốt hơn nhiều so với việc chỉ dựa vào bản quét giấy tờ. [13]

• **Xác thực sinh trắc học** xác minh rằng người truy cập dịch vụ trùng khớp với cá nhân đã đăng ký trước đó thông qua các đặc điểm sinh học hoặc hành vi mang tính duy nhất, như vân tay hoặc nhận diện khuôn mặt. Biện pháp này giúp ngăn chặn truy cập trái phép, ngay cả khi các thông tin xác thực khác (như mật khẩu hoặc thiết bị) bị xâm phạm. Điều quan trọng là, sinh trắc học chỉ xác thực người dùng chứ không xác nhận danh tính. [14]

• **Mô hình định danh số hybrid** kết hợp nhiều yếu tố, như thông tin xác thực do chính phủ cấp và xác thực sinh trắc học, để tạo ra hệ thống danh tính số có mức độ bảo đảm cao. Các hệ thống này thường chỉ cần xác thực một lần để sử dụng trên nhiều nền tảng, đồng thời được thiết kế để hỗ trợ tính liên thông đa nền tảng, xác thực mạnh mẽ và kiểm soát quyền riêng tư. [15]

Tất cả các hệ thống này đều được thiết kế để hỗ trợ KYC và có tính không ẩn danh, nhằm mục đích truy vết, tuân thủ và đảm bảo trách nhiệm giải trình trong các hệ sinh thái chịu sự quản lý.

Phản ứng chính sách tại khu vực châu Á – Thái Bình Dương

Các công nghệ ID số không thể phát huy hiệu quả nếu được triển khai đơn độc; chúng cần được hỗ trợ bởi các khuôn khổ chính sách phù hợp nhằm thiết lập các tiêu chuẩn, đảm bảo quyền riêng tư và thúc đẩy việc áp dụng rộng rãi. Trên thực tế, điều này bao gồm:

- Công nhận pháp lý rõ ràng, để ID số có giá trị pháp lý trong các giao dịch tài chính, hợp đồng và dịch vụ công.
- Các biện pháp bảo vệ dữ liệu mạnh mẽ, bao gồm yêu cầu lưu trữ an toàn, có giới hạn mục đích và phạm vi sử dụng. cùng cơ chế khiếu nại trong trường hợp bị lạm dụng.
- Triển khai rộng rãi trong cả khu vực công và tư, bảo đảm rằng ID không chỉ được chấp nhận bởi cơ quan nhà nước mà còn bởi các nền tảng số, ngân hàng và các đơn vị cung cấp dịch vụ thiết yếu là những chủ thể thường xuyên nằm ở tuyến đầu trong các vụ lừa đảo.

Trên khắp Đông Nam Á, các chính phủ đang từng bước phát triển hệ thống ID số nhằm xây dựng nền tảng cho các môi trường kinh tế số đáng tin cậy hơn.

- Nền tảng Danh tính số Quốc gia (NDID) của Thái Lan kết nối các ngân hàng, nhà mạng viễn thông và cơ quan nhà nước trong một khuôn khổ liên thông tập trung. [16]

- Indonesia và Philippines đang triển khai các chương trình danh tính điện tử (e-ID) quốc gia có liên kết với dịch vụ tài chính toàn diện và dịch vụ xã hội.

- Việt Nam đã bắt đầu tích hợp xác minh sinh trắc học vào các cổng thông tin chính phủ điện tử.

Mặc dù mức độ phát triển chính sách chưa đồng đều, xu hướng chung trong khu vực đang chuyển dịch từ xây dựng các hệ thống quốc gia sang thúc đẩy tính liên thông giữa các hệ thống. Các nhà hoạch định chính sách ngày càng nhận ra rằng các dòng dịch chuyển, di cư và thương mại đòi hỏi các hệ thống định danh có thể được công nhận xuyên biên giới, thay vì chỉ giới hạn trong phạm vi quốc gia.

Tại những nền kinh tế phát triển hơn trong khu vực, các khuôn khổ ID quốc gia toàn diện đã được đưa vào sử dụng và đang tiếp tục được tích hợp sâu hơn.

- SingPass của Singapore trở thành “chìa khóa số” để truy cập dịch vụ ngân hàng, y tế và thương mại điện tử. [17]

- Hàn Quốc đang mở rộng hệ thống đăng ký cư trú quốc gia thành một nền tảng danh tính số hoàn chỉnh tích hợp cho dịch vụ chính phủ điện tử, giao dịch tài chính và xác thực di động.

- Hệ thống “My Number” của Nhật Bản cung cấp cho mỗi cư dân một mã định danh duy nhất gồm 12 chữ số, ngày càng được liên kết nhiều hơn với dịch vụ y tế, thuế và hành chính. [18] Các nỗ lực cũng đang được triển khai để mở rộng tiện ích của hệ thống này sang dịch vụ tài chính và cho phép công nhận xuyên biên giới.

Các lộ trình này khác nhau về phạm vi và tốc độ, nhưng cùng cho thấy cách các hệ thống cấp thông tin xác thực ở quy mô quốc gia có thể phát triển vượt ra khỏi mục tiêu đăng nhập an toàn để trở thành trụ cột thể chế của nền kinh tế số, đồng thời cung cấp các điểm tham chiếu cho các chính phủ ASEAN khi cân nhắc triển khai trong nước hoặc thúc đẩy tính liên thông trong khu vực.

Đồng thời, những kinh nghiệm này cho thấy chỉ hành động của chính phủ thôi là chưa đủ. Điều quan trọng là, hiệu quả của ID số phụ thuộc vào việc tích hợp trên toàn hệ sinh thái số rộng khắp thông qua hợp tác giữa chính phủ, tổ chức tài chính và nền tảng công nghệ.

Vai trò của danh tính số trong phòng, chống lừa đảo

Các công nghệ ID số là một trong những công cụ mang tính hệ thống có nhiều tiềm năng trong hoạt động phòng, chống lừa đảo và gian lận. Bằng cách xác thực con người, thiết bị và tổ chức theo phương thức có thể kiểm chứng và không ẩn danh, các hệ thống ID số giảm thiểu tình trạng mạo danh, hạn chế ẩn danh và làm gia tăng chi phí đối với hành vi lừa đảo. Mặc dù không phải là một giải pháp toàn diện, các hệ thống này là yếu tố 'xương sống' đối với niềm tin trong môi trường số với khả năng định danh khách hàng, đảm bảo rằng các giao dịch và dịch vụ chịu sự quản lý luôn gắn với các cá nhân hoặc thực thể thực tế mang trách nhiệm giải trình.

Khắc phục các lỗ hổng bị lợi dụng bởi tội phạm lừa đảo

Lừa đảo phát triển mạnh nhờ các lỗ hổng trong hoạt động xác minh. Kẻ gian sử dụng bot và tài khoản giả để lan truyền thông tin với chi phí thấp, khai thác deepfake và công nghệ nhân bản giọng nói để mạo danh những chủ thể đáng tin cậy, đồng thời chiếm đoạt các tài khoản hợp pháp để lừa đảo chiếm đoạt tiền, tài sản của nạn nhân. Sự thiếu nhất quán hoặc yếu kém trong các cơ chế xác thực giữa các nền tảng làm gia tăng đáng kể tỷ lệ thành công của các cuộc tấn công này.

ID số khắc phục những lỗ hổng này trong các môi trường có sự quản lý: bằng cách liên kết các tương tác số với danh tính đã được xác minh, tội phạm gặp khó khăn hơn trong việc hoạt động ẩn danh, đồng thời giúp người dùng, doanh nghiệp, cũng như cơ quan quản lý nâng cao mức độ tin cậy trong các giao dịch trực tuyến. Tuy nhiên, phần lớn các vụ lừa đảo bắt nguồn từ các không gian không chịu sự quản lý, như mạng xã hội, ứng dụng nhắn tin và các sàn giao dịch phi chính thức, nơi mà các cơ chế KYC không được áp dụng. Việc xử lý rủi rotrong các môi trường này đòi hỏi một cách tiếp cận bổ sung theo hướng bảo vệ quyền riêng tư, như hệ thống Proof of Human.

Tuy nhiên, ngay cả hệ thống ID số mạnh nhất cũng không thể giải quyết toàn bộ các hành vi lạm dụng liên quan đến tài khoản giả và tự động hóa. Lỗ hổng này đã thúc đẩy mối quan tâm ngày càng gia tăng về các khái niệm mới như Proof of Human – giải pháp khám phá những phương thức xác minh người dùng là người thật theo hướng bảo vệ quyền riêng tư mà không yêu cầu tiết lộ thông tin định danh cá nhân.

Proof of Human: Khái niệm và ý nghĩa đối với chính sách

Định nghĩa về ‘proof of human’

Proof of Human (PoH) là một phương pháp tiếp cận mới, mang tính sáng tạo và đang phát triển trong việc tăng cường niềm tin trong môi trường số. PoH thường được định nghĩa là một hệ thống được thiết kế để ngăn chặn việc sử dụng nhiều danh tính giả, đồng thời cung cấp bằng chứng có thể xác minh rằng một người dùng trực tuyến là con người thật chứ không phải bot tự động hay danh tính giả mạo.[19] Không giống như các cơ chế đăng ký tài khoản đơn giản hoặc các bài kiểm traCAPTCHA, PoH hướng tới việc cung cấp một chỉ báo về người thật chỉ cần xác thực một lần nhưng có thể sử dụng lại, có thể được công nhận trên nhiều nền tảng và dịch vụ khác nhau, đồng thời không tiết lộ dữ liệu cá nhân vượt quá mức cần thiết. Cách tiếp cận này góp phần đặt nền móng cho các mạng lưới người dùng đáng tin cậy trong toàn bộ hệ sinh thái số.

Điều quan trọng là PoH không thay thế hay cạnh tranh với các hệ thống ID số quốc gia. Thay vào đó, PoH đóng vai trò bổ trợ, giải quyết một lớp khác của bài toán niềm tin: xác minh người dùng là con người thật thay vì xác định danh tính cụ thể của họ.

Về mặt khái niệm, PoH khác với các lớp bảo đảm số khác. Các khuôn khổ ID số truyền thống trả lời cho câu hỏi “bạn là ai?” bằng cách liên kết các cá nhân với các thuộc tính đã xác minh như tên hoặc số định danh. Các cơ chế xác thực như mật khẩu hoặc xác thực đa yếu tố (MFA) giúp bảo vệ tài khoản sau khi đã được tạo, nhưng không ngăn chặn việc tạo ra các hồ sơ giả hoặc danh tính tổng hợp ngay từ đầu. Trong gần hai thập kỷ qua, CAPTCHA đã cố gắng lấp đầy khoảng trống này bằng cách kiểm tra khả năng giải các bài toán nhận thức như một tín hiệu để nhận biết người dùng là con người thật. Tuy nhiên, hiệu quả của CAPTCHA đang suy giảm khi bot và các công cụ AI ngày càng có khả năng vượt qua các bài kiểm tra này, đồng thời chính công cụ này cũng gây ra sự phiền toái cho người dùng hợp pháp. Trong khi đó, PoH trực tiếp giải quyết câu hỏi cốt lõi “bạn có phải là con người không?”, cung cấp một dạng bảo đảm phù hợp với các nỗ lực bao quát hơn trong việc triển khai thông tin xác thực đã được xác minh, giảm thiểu bot và các cơ chế chống tấn công sybil (là hình thức tấn công mạo nhận nhằm chiếm quyền kiểm soát hoặc làm suy giảm tính toàn vẹn của hệ thống), đặc biệt trong các mạng blockchain. Ở góc độ này, PoH có thể được xem là một phần của làn sóng đổi mới rộng hơn, hướng tới việc cân bằng giữa tính xác thực, quyền riêng tư và khả năng mở rộng trong các hệ sinh thái số.

Các hình thức xác minh PoH

Hệ thống Proof of Human có thể được triển khai theo nhiều cách khác nhau, mỗi phương thức cung cấp mức độ bảo đảm và bảo vệ quyền riêng tư khác nhau. Bảng dưới đây trình bày các hình thức xác minh PoH chính và cơ chế hoạt động trong thực tiễn.

Loại hình xác minh PoH	Cơ chế hoạt động	Trải nghiệm của người dùng	Ví dụ về các tình huống sử dụng
Dựa trên sinh trắc học (bảo vệ quyền riêng tư)	Kiểm tra bằng công nghệ xác minh thực thể sống (liveness check) một lần (ví dụ: chớp mắt/quay đầu). Hệ thống phát hành "token con người" dưới dạng mã hóa mà không lưu trữ hay chia sẻ dữ liệu sinh trắc học.	Xác minh một lần, trong thời gian ngắn, tương tự như mở khóa thiết bị; không tiết lộ thông tin danh tính.	Ngăn chặn tạo tài khoản giả hàng loạt; phù hợp với các nền tảng xử lý giao dịch tài chính hoặc có rủi ro cao.
Dựa trên thiết bị/phần cứng	Sử dụng cơ chế xác thực thiết bị để xác nhận thiết bị là thật, không bị giả lập; có thể thiết lập ánh xạ "một người = một thiết bị" mà không cần định danh cá nhân.	Kiểm tra thông tin cơ bản tích hợp trong quy trình đăng ký, không yêu cầu sinh trắc học.	Hạn chế trang trại bot; giảm tạo tài khoản tự động trong ứng dụng nhắn tin, trên mạng xã hội hoặc nền tảng trò chơi.
Dựa trên tương tác/thử thách	Người dùng thực hiện các tác vụ dạng tín hiệu hành vi hoặc nhiệm vụ thử thách–phản hồi mã hóa mà bot khó tái tạo một cách đáng tin cậy. Không sử dụng dữ liệu sinh trắc học.	Các tác vụ đơn giản, yêu cầu tương tác của con người (ví dụ: chuyển động có kiểm soát, chỉ dẫn hoặc tín hiệu nhằm hỗ trợ người dùng đưa ra câu trả lời đúng sau một khoảng thời gian nhất định (timed prompts)), ít gây phiền hơn nhiều so với các CAPTCHA truyền thống.	Phù hợp với các nền tảng xã hội và cộng đồng trực tuyến để ngăn chặn hồ sơ tổng hợp mà không cần yêu cầu ID hoặc sinh trắc học.
Xác thực xã hội / xác thực bằng mạng uy tín (web-of-trust)	Người dùng được xác minh bởi các thành viên cộng đồng đã được tin cậy hoặc mạng lưới uy tín; nền tảng chuyển đổi điều này thành chỉ báo PoH.	Một xác nhận hoặc xác thực đơn giản và nhanh chóng từ người dùng/ cộng đồng đã được xác minh.	Sàn giao dịch P2P, nền tảng lao động tự do (nền tảng gig), hoặc môi trường xác minh dựa vào cộng đồng.

Bảng 3.1: Các hình thức xác minh Proof of Human (PoH)

Cơ chế hỗ trợ phòng, chống lừa đảo của công nghệ ‘proof of human’

Mặc dù vẫn còn là một khái niệm mới, PoH có tiềm năng đóng vai trò đáng kể trong cuộc chiến chống lừa đảo và gian lận. Gian lận trực tuyến hiện nay tận dụng lợi thế quy mô: các tổ chức buôn người và nhóm tội phạm có thể tạo ra hàng nghìn tài khoản giả để dụ dỗ nạn nhân, tự động hóa các mô hình lừa đảo “mổ lợn”, hoặc vận hành các mạng lưới tài khoản trung gian để chuyển dòng tiền bất hợp pháp. Khả năng tạo ra danh tính số với chi phí thấp và số lượng lớn làm giảm chi phí thực hiện gian lận, đồng thời khiến năng lực phát hiện hoạt động độc hại của các nền tảng và cơ quan quản lý bị quá tải. Ngược lại, PoH có thể giúp tái cân bằng cục diện bằng cách củng cố các mạng lưới người dùng đã được xác minh là con người, đồng thời hạn chế tình trạng lan rộng danh tính tổng hợp hoặc tự động ở quy mô lớn.

Về nguyên tắc, PoH có thể tạo ra rào cản ngay tại thời điểm tạo tài khoản hoặc thực hiện giao dịch, qua đó hạn chế tốc độ và quy mô lan rộng của các tài khoản giả.

Tính xác thực thực thể người có thể kiểm chứng phục vụ một số chức năng như sau:

1. Ngăn chặn hồ sơ cá nhân giả được sử dụng làm mồi nhử trong các hình thức lừa đảo tình cảm, việc làm hoặc đầu tư. Thay vì phụ thuộc vào các biện pháp xử lý hậu kiểm sau khi nạn nhân đã bị lôi kéo, PoH có thể giúp giảm nguồn cung tài khoản gian lận ngay từ đầu.

2. Bảo vệ hệ thống tài chính thông qua việc giảm luồng giao dịch đi qua các tài khoản trung gian phục vụ chuyển tiền bất hợp pháp. Ngân hàng và mạng lưới thanh toán thường gặp khó khăn trong việc phân biệt người dùng hợp pháp và tài khoản gian lận; một chỉ báo người thật chỉ cần xác thực một lần nhưng có thể sử dụng trên nhiều nền tảng có thể củng cố các cơ chế xác thực khách hàng và phòng chống rửa tiền hiện có mà không yêu cầulặp lại việc tiết lộ dữ liệu cá nhân.

3. Củng cố niềm tin vào thương mại số và cộng đồng trực tuyến. Tại các thị trường nơi mà lừa đảo và mạo danh đã làm xói mòn niềm tin, khả năng xác minh người mua, người bán hoặc thành viên cộng đồng là con người thực, về lâu dài, có thể giúp khôi phục niềm tin vào giao dịch ngang hàng (P2P), nền tảng gig và không gian xã hội số.

Các biện pháp bảo vệ và quản trị

Các biện pháp bảo vệ đóng vai trò thiết yếu để đảm bảo bản thân PoH không trở thành công cụ giám sát. Các mô hình mới nổi nhấn mạnh thiết kế bảo vệ quyền riêng tư. Các bằng chứng mật mã và phương thức không tiết lộ tri thức cho phép người dùng chứng minh mình là người thật mà không cần tiết lộ dữ liệu danh tính cơ bản. Sự phân biệt giữa xác minh danh tính (người dùng có phải là con người không?) và tiết lộ danh tính (người dùng là ai?) có ý nghĩa then chốt trong việc duy trì quyền và niềm tin giữa các hệ thống, quốc gia khác nhau. Các biện pháp bảo vệ cũng đòi hỏi cơ chế quản trị mạnh mẽ: giám sát bởi cơ quan quản lý, tổ chức tiêu chuẩn hoặc các cơ chế kiểm tra, đánh giá độc lập phục vụ xác minh, có thể giúp ngăn chặn việc chỉ báo PoH bị bị lạm dụng cho mục đích theo dõi hoặc xây dựnghồ sơ người dùng mang tính xâm phạm.

Quyền của người dùng và tính bao trùm là các yếu tố không kém phầnquan trọng. Việc xác minh người dùng nên được thực hiện theo nguyên tắc tự nguyện, minh bạch và có thể thu hồi, và đồng thời người dùng cần có khả năng hiểu và kiểm soát cách thức chỉ báo PoH của họ được sử dụng. Các công cụ bổ trợ như cơ chế bảo đảm độ tuổi có thể giúp bảo vệ trẻ vị thành niên mà không yêu cầu tiết lộ thông tin nhạy cảm. Đồng thời việc cung cấp nhiều phương thức xác minh khác nhau giúp tránh loại trừ những nhóm người không có điện thoại thông minh, không sử dụng sinh trắc học hoặc không có kết nối ổn định. Độ tin cậy của PoH phụ thuộc vào khả năng tăng cường an toàn, bảo mật đồng thời vẫn tôn trọng quyền riêng tư, bảo đảm khả năng tiếp cận, và phù hợp với các cam kết ở cấp khu vực về niềm tin trong môi trường số.

Tuy nhiên, các biện pháp bảo vệ kỹ thuật đơn thuần là chưa đủ. Việc triển khai PoH hiệu quả đòi hỏi các cấu trúc quản trị phản ánh thực tiễn của các hệ sinh thái số tại khu vực châu Á – Thái Bình Dương. Trong khi cáchệ thống ID số quốc gia hoạt động theo khuôn khổ pháp lý trong nước, phần lớn tương tác thực tế của người dùng cũng như các rủi ro liên quan đến quyền riêng tư lại diễn ra trên các nền tảng toàn cầu. Khoảng cách về mặt cấu trúc này khiến việc tích hợp trực tiếp giữa chính phủ và nền tảng hiếm khi khả thi. Do vậy, cần có một lớp trung gian liên thông mang tính trung lập bao gồm các tổ chức trung gian độc lập có khả năng chuyển hóa các yêu cầu chính sách, tập hợp các bên liên quan và hỗ trợ thử nghiệm an toàn trước khi mở rộng quy mô.

Các bên trung gian này có thể giúp đảm bảo PoH được triển khai theo cách khả thi về mặt kỹ thuật, tôn trọng quyền riêng tư và phù hợp với cả các khuôn khổ pháp lý quốc gia lẫn môi trường đa nền tảng. Các tổ chức trung gian có thể chuyển hóa tiêu chuẩn trong nước thành hướng dẫn triển khai, tổ chức thảo luận đa bên về quyền riêng tư và khả năng kiểm tra, đánh giá phục vụ xác minh, đồng thời tạo điều kiện cho môi trường thử nghiệm có kiểm soát (sandbox) cho phép thử nghiệm PoH an toàn mà không gây rủi ro ngoài ý muốn cho người dùng hoặc nền tảng.

Một yếu tố bảo vệ quan trọng khác là niềm tin của công chúng. PoH là một khái niệm mới—khác biệt với danh tính số, xác thực hoặc xác thực khách hàng bằng phương thức điện tử (eKYC)—và dễ bị hiểu lầm là công cụ giám sát hoặc thu thập dữ liệu người dùng. Do đó, việc xây dựng năng lực có tầm quan trọng không kém với bản thân hiệu quả của công nghệ. Các bên trung gian trung lập, hiệp hội ngành và tổ chức xã hội dân sự có thể giúp giải thích cách thức hoạt động của các cơ chế bảo vệ quyền riêng tư, nhấn mạnh rằng PoH trả lời câu hỏi "Bạn có phải là con người không?" mà không tiết lộ "Bạn là ai?", và cung cấp hướng dẫn thực tiễn cho việc triển khai có trách nhiệm. Chính truyền thông hiệu quả và giáo dục người dùng mới là yếu tố quyết định để chuyển một hệ thống PoH được thiết kế tốt thành một hệ thống được chấp nhận và tin cậy.

Cuối cùng, PoH cần được tích hợp trong một khuôn khổ bảo đảm niềm tin và an toàn tổng thể. Việc xác minh người dùng là con người không đồng nghĩa với việc đảm bảo hành vi của họ là an toàn. Trong số các vụ lừa đảo gây thiệt hại lớn nhất tại khu vực châu Á – Thái Bình Dương như lừa đảo đầu tư, mạo danh và các chiêu trò lừa đảo bằng kỹ nghệ xã hội phức tạp, có nhiều vụ được thực hiện bởi chính con người thật. Vì vậy, PoH chỉ nên được xem là lớp bổ sung, không thay thế các cơ chế kiểm soát an toàn khác. Việc áp dụng các khuôn khổ như ISO/IEC 25389 (Khuôn khổ an toàn) có thể giúp đảm bảo PoH được sử dụng một cách phù hợp:

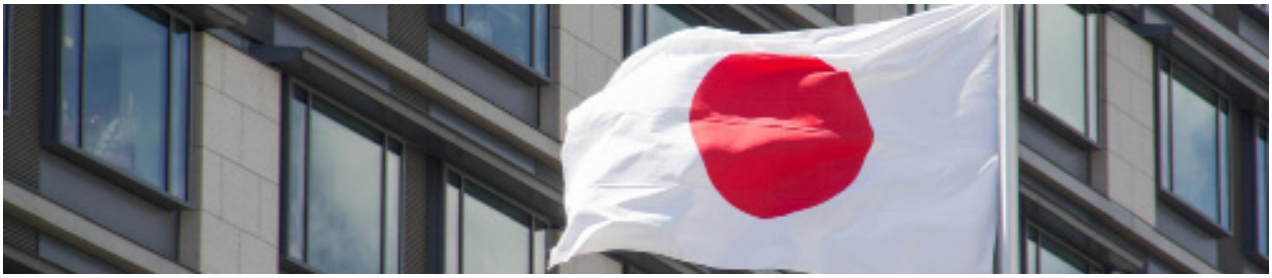
- như một lớp phòng vệ chống lại tấn công tự động và quy mô lớn;
- kết hợp với các chỉ báo hành vi và uy tín để phát hiện các mối đe dọa do con người gây ra;
- đi kèm với hướng dẫn triển khai rõ ràng nhằm tránh tình trạng phụ thuộc quá mức.

Do đó, PoH nên được áp dụng thí điểm như một công cụ đổi mới mang tính bổ trợ, không phải là biện pháp thay thế, nhằm củng cố các khuôn khổ định danh hiện có. Nếu được thiết kế và quản trị một cách cẩn trọng, PoH có thể giúp thử nghiệm các phương thức mới để xác minh người dùng thực trong các môi trường số có rủi ro cao, qua đó tạo cơ sở bằng chứng cho những cách tiếp cận có thể mở rộng ở quy mô lớn hơn. Ở phạm vi rộng hơn, các khuôn khổ PoH có tính liên thông và tôn trọng quyền riêng tư có thể bổ trợ cho sáng kiến ID số quốc gia, hỗ trợ công nhận xuyên biên giới và cung cấp một nền tảng niềm tin mới cho hợp tác khu vực về phòng, chống lừa đảo và gian lận trên toàn khu vực châu Á – Thái Bình Dương. Qua đó các quốc gia có thể xây dựng mạng lưới người dùng bền vững, có thể xác minh, có khả năng chống chịu trước quy mô và tốc độ của tội phạm mạng hiện đại.

Phần tiếp theo sẽ xem xét các kinh nghiệm ở cấp quốc gia tại khu vực châu Á – Thái Bình Dương, nhằm đánh giá cách PoH có thể được triển khai trong thực tiễn.

Nghiên cứu tình huống: Công nghệ tiên tiến trong thực tiễn

Trên khắp châu Á, các chính phủ đã xây dựng các nền tảng danh tính số vững mạnh phục vụ việc xác minh công dân trong các dịch vụ công và tài chính. Tuy nhiên, phần lớn các vụ lừa đảo xảy ra bên ngoài các hệ thống chịu sự quản lý, cụ thể là trên các nền tảng xã hội, nhắn tin và chia sẻ nội dung, nơi mà tính ẩn danh chiếm ưu thế. Các công nghệ Proof of Human (PoH) mới nổi mang lại một cách tiếp cận nhằm mở rộng độ tin cậy của định danh số sang các môi trường mở này, thông qua việc xác nhận người dùng là con người thật và có tính duy nhất, mà không cần tiết lộ dữ liệu cá nhân. Các nghiên cứu tình huống dưới đây phân tích cách bốn nền kinh tế – Nhật Bản, Hàn Quốc, Malaysia và Philippines – đang xây dựng các thành tố xác minh tương tự PoH thông qua các hệ thống quốc gia của mình, đồng thời rút ra những bài học kinh nghiệm cho việc hoạch định các chiến lược tăng cường khả năng phòng, chống lừa đảo trong tương lai.



Nhật Bản: Hệ thống My Number và thách thức về niềm tin

Hệ thống My Number của Nhật Bản, ra mắt năm 2016, cấp một mã định danh duy nhất gồm 12 chữ số cho mỗi cư dân để phục vụ các nghĩa vụ thuế, an sinh xã hội và ứng phó thảm họa. [20] Với mục tiêu thống nhất dữ liệu hành chính và nâng cao hiệu quả, hệ thống này đã mở rộng sang lĩnh vực số nói chung thông qua hình thức Thẻ My Number, là một thẻ ID thông minh cho phép xác thực trực tuyến an toàn cho các dịch vụ chính phủ điện tử, y tế và giao dịch tài chính. [21] Đến năm 2025, hơn 90 triệu thẻ, tương đương trên 70% dân số, đã được cấp, tuy nhiên mức độ sử dụng trên môi trường số vẫn còn hạn chế do việc tích hợp dịch vụ chưa được triển khai đồng bộ và những lo ngại kéo dài liên quan đến niềm tin. [22]

Mặc dù My Number bảo đảm tính duy nhất được xác minh ở quy mô quốc gia, hệ thống này vẫn mang bản chất của một mô hình danh tính truyền thống, chứ chưa phải là một khuôn khổ Proof of Human (PoH). Việc xác minh được thực hiện dựa trên dữ liệu đăng ký với cơ quan nhà nước và cơ chế xác minh giấy tờ, nhưng chưa tích hợp các cơ chế bảo vệ quyền riêng tư hay các bảo đảm bằng mã hóa – những đặc trưng của các công nghệ PoH. Tuy nhiên, kinh nghiệm của Nhật Bản cho thấy việc xác minh tính duy nhất do nhà nước bảo đảm có thể đóng vai trò nền tảng cho việc mở rộng niềm tin trong môi trường số và tăng cường phòng, chống gian lận, với điều kiện được kết hợp cùng các cơ chế hiện đại nhằm tăng cường bảo vệ quyền riêng tư.

Đồng thời, từ kinh nghiệm của Nhật Bản cũng cho thấy rõ những giới hạn của các hệ thống danh tính tập trung trong việc phòng, chống lừa đảo. Phần lớn các hành vi gian lận và mạo danh trực tuyến diễn ra trong các môi trường thiếu sự quản lý, cụ thể là mạng xã hội, nền tảng nhắn tin và thương mại điện tử. Các nền tảng này hoạt động trong khuôn khổ các quy định chung về bảo vệ người tiêu dùng và quản lý nội dung, nhưng nằm ngoài các cơ chế bảo đảm gắn với danh tính tại Nhật Bản. Trong khi đó, các sự cố liên quan đến xử lý dữ liệu, chẳng hạn như vụ liên kết nhầm hồ sơ bảo hiểm y tế năm 2023, đã làm xói mòn niềm tin của công chúng và khơi lại các tranh luận xoay quanh quyền riêng tư, cơ chế giám sát và trách nhiệm giải trình. [23] Những sự kiện này cho thấy niềm tin, chứ không chỉ công nghệ, vẫn là rào cản then chốt trong việc mở rộng sử dụng danh tính đã được xác minh. Tại Nhật Bản, văn hóa coi trọng quyền riêng tư được định hình bởi các chuẩn mực cao về tính ẩn danh và thái độ thận trọng đối với hoạt động xử lý dữ liệu của cơ quan nhà nước, khiến sự chấp nhận của xã hội trở thành yếu tố then chốt trong triển khai bất kỳ cơ chế xác minh mới nào, bao gồm cả PoH.

Trong bối cảnh đó, chính phủ đã triển khai các biện pháp quản trị và tăng cường tính liên thông, nhằm mở rộng việc xác thực dựa trên Thẻ My Number (JPKI) sang khu vực tư nhân như ngân hàng, đăng ký SIM và thương mại điện tử. [24] Qua quá trình triển khai minh bạch, Nhật Bản có thể từng bước phát triển hệ thống của mình thành một mô hình niềm tin số hybrid, dựa trên nền tảng danh tính có giá trị pháp lý được xác thực bởi cơ quan nhà nước, đồng thời cho phép xác minh tính duy nhất theo hình thức PoH thông qua các phương pháp mã hóa bảo vệ quyền riêng tư. Sự phát triển này sẽ cho phép Nhật Bản kết nối danh tính đáng tin cậy với các cơ chế xác minh có khả năng mở rộng quy mô và tôn trọng quyền riêng tư, qua đó tăng cường khả năng phòng, chống lừa đảo và củng cố niềm tin của công chúng đối với môi trường kinh tế số. [25]

Hàn Quốc: Tích hợp ID số và xác minh tên thật

Hàn Quốc vận hành một trong những hệ sinh thái danh tính số tiên tiến và tích hợp nhất thế giới, được xây dựng trên hạ tầng e-ID quốc gia kết nối với các dịch vụ trong lĩnh vực ngân hàng, viễn thông và chính phủ điện tử. [26] Dựa trên hệ thống Số đăng ký cư trú (RRN) được triển khai từ năm 1968, khuôn khổ hệ thống danh tính của Hàn Quốc đã phát triển theo nhiều lớp, bao gồm xác minh tên thật, xác thực sinh trắc học và hạ tầng khóa công khai (PKI), nhằm hỗ trợ cho nền kinh tế trực tuyến tăng trưởng nhanh. [27] Thẻ ID số (2020) và Giấy phép lái xe di động (2022) đánh dấu các cột mốc trong quá trình chuyển đổi từ giấy tờ vật lý sang thông tin xác thực hoàn toàn số hóa. [28] Đến năm 2025, hơn 50 triệu người Hàn Quốc sử dụng xác thực số hằng ngày thông qua các hệ thống như PASS, Kakao, Naver hoặc Samsung Pass để truy cập các dịch vụ trong lĩnh vực tài chính, chính phủ và khu vực tư nhân. [29]

Sự tích hợp sâu của danh tính trên các nền tảng đã trở thành trụ cột trong cơ chế xác thực tên thật và an ninh mạng của Hàn Quốc, theo đó cá nhân phải xác minh danh tính pháp lý trước khi thực hiện hầu hết các giao dịch trực tuyến. Các cơ chế này trên thực tế vận hành tương tự một lớp Proof of Human (PoH), bảo đảm rằng các chủ thể trong môi trường số tương ứng với những cá nhân có thật và duy nhất, đồng thời giảm đáng kể các hành vi gian lận, danh tính tổng hợp và lạm dụng công cụ tự động. Tính liên thông giữa các hệ thống trong khu vực công và tư đã tạo ra mức độ tin tưởng cao, đồng thời giúp Hàn Quốc trở thành một trong những quốc gia có tỷ lệ gian lận danh tính tài chính thấp nhất trên toàn cầu. [30]

Tuy nhiên, mô hình này của Hàn Quốc cũng bộc lộ những đánh đổi đi kèm với mức độ tập trung hóa cao. Các quy định bắt buộc về xác thực tên thật, cùng với việc chia sẻ dữ liệu giữa các chủ thể trong lĩnh vực viễn thông, tài chính và khu vực công, đã làm dấy lên những lo ngại liên quan đến quyền riêng tư và các quyền tự do dân sự. Các vụ rò rỉ dữ liệu quy mô lớn, bao gồm các sự cố từ các tổ chức báo cáo tín dụng và các nền tảng thương mại điện tử, đã làm gia tăng sự hoài nghi của công chúng đối với nguyên tắc đồng thuận và tối thiểu hóa dữ liệu. Trong bối cảnh đó, các nhà hoạch định chính sách đã tăng cường các biện pháp bảo vệ theo Đạo luật Bảo vệ Thông tin Cá nhân (PIPA) và triển khai chương trình Thí điểm Danh tính số (2023) nhằm nghiên cứu các mô hình xác thực phi tập trung do người dùng kiểm soát. Đây được coi như một bước tiến quan trọng hướng tới các khuôn khổ bảo vệ quyền riêng tư mạnh mẽ hơn. [32]

Kinh nghiệm của Hàn Quốc cho thấy đồng thời cả những thế mạnh và hạn chế của các hệ thống PoH gắn với vai trò của nhà nước. Sự kết hợp giữa danh tính pháp lý đã được xác minh, các cơ chế xác thực sinh trắc học và các khuôn khổ liên thông tạo ra một nền tảng mạnh mẽ cho việc phòng, chống lừa đảo và xây dựng niềm tin trong môi trường số. Tuy nhiên, các tranh luận chính sách tại Hàn Quốc cũng cho thấy xu hướng chuyển dịch sang các mô hình bảo vệ quyền riêng tư và quyền kiểm soát của người dùng cao hơn. Đây là những nguyên tắc phù hợp với định hướng phát triển của các công nghệ Proof of Human (PoH) đang nổi lên. Trong bối cảnh Hàn Quốc tiếp tục hoàn thiện kiến trúc bảo đảm niềm tin trong môi trường số, các bước phát triển trong tương lai có thể sẽ giảm bớt trọng tâm vào việc thực thi nghiêm ngặt xác minh tên thật, và dần chuyển sang các mô hình cân bằng hơn, tức là những mô hình vừa xác minh người dùng là cá nhân có thật, vừa bảo đảm các quyền cá nhân và duy trì niềm tin đối với môi trường kinh tế số.

Malaysia: MyDigital ID và lộ trình hướng tới niềm tin vào sinh trắc học

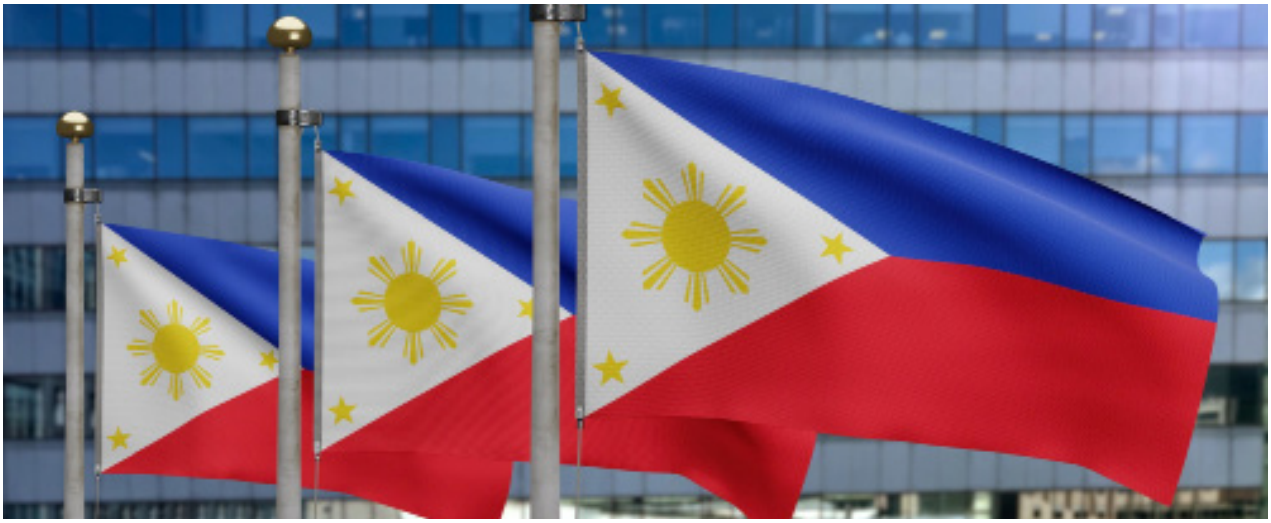
Sáng kiến MyDigital ID của Malaysia đánh dấu một bước tiến quan trọng hướng tới việc xây dựng một khuôn khổ danh tính số thống nhất do nhà nước bảo trợ, với mục tiêu đơn giản hóa khả năng tiếp cận các dịch vụ trong cả khu vực công và tư nhân. Được triển khai vào năm 2024 theo Đề cương Danh tính số, hệ thống này cấp cho mỗi cư dân một thông tin xác thực số gắn với sinh trắc học, được liên kết trực tiếp với cơ sở dữ liệu của Cục Đăng ký Quốc gia (NRD). [33] Thông qua việc sử dụng công nghệ nhận diện khuôn mặt và các cơ chế xác thực an toàn, hệ thống cho phép cá nhân xác minh danh tính trên các cổng dịch vụ chính phủ điện tử, ngân hàng, nhà mạng viễn thông và nhiều dịch vụ trực tuyến khác. Các chương trình thí điểm ban đầu với Cục Thuế Nội địa (LHDN) và một số tổ chức tài chính được lựa chọn đã đặt nền móng cho việc triển khai trên phạm vi toàn quốc, dự kiến diễn ra vào năm 2025. [34]

Không giống với các hệ thống ID trước đây, MyDigital ID được thiết kế vừa là thông tin xác thực vừa là lớp xác minh, cho phép thực hiện xác thực mà không cần lặp lại việc tiết lộ các thông tin cá nhân. Bằng cách gắn danh tính với các hồ sơ sinh trắc học đã được xác minh, hệ thống này tạo ra nền tảng cho cơ chế xác minh theo hình thức Proof of Human (PoH), qua đó bảo đảm rằng mỗi tài khoản số tương ứng với một cá nhân có thật và duy nhất. Khi Malaysia mở rộng việc xác minh số trên nhiều lĩnh vực, quốc gia này cũng đối mặt với thách thức tương tự như các nền kinh tế khác: làm thế nào để mở rộng niềm tin sang các môi trường mở, lấy người dùng làm trung tâm, nơi việc tiết lộ đầy đủ danh tính không được coi là phương án khả thi và lý tưởng. Trong trường hợp này, MyDigital ID có thể đóng vai trò là xương sống cho các cơ chế PoH trong tương lai, cho phép xác minh con người thật và tính duy nhất theo cách vừa bảo vệ quyền riêng tư vừa bảo đảm tính liên thông.

Sáng kiến này cũng phản ứng trực tiếp với tình trạng lừa đảo và gian lận số gia tăng tại Malaysia, song hành với sự phát triển của ngân hàng di động và thương mại điện tử. Một lớp xác thực danh tính đáng tin cậy có thể giúp giảm thiểu tình trạng giả mạo và tài khoản giả trong các hệ sinh thái chịu sự quản lý, trong khi các cơ chế xác minh theo hình thức PoH về lâu dài có thể mở rộng các biện pháp bảo vệ này sang những không gian không chịu sự quản lý, chẳng hạn như các sàn giao dịch trực tuyến, mạng xã hội và hệ thống thanh toán số, nơi các hành vi lừa đảo thường phát sinh.

Tuy nhiên, quá trình triển khai cũng làm dấy lên những tranh luận công khai xoay quanh quyền riêng tư, bảo vệ dữ liệu và quản trị. Các tổ chức xã hội dân sự đã bày tỏ những lo ngại liên quan đến vấn đề lưu trữ dữ liệu sinh trắc học tập trung, cũng như nguy cơ lạm dụng nếu quyền truy cập dữ liệu vượt ra ngoài mục đích ban đầu. [35] Trước bối cảnh này, chính phủ đã thành lập Ban Chỉ đạo hệ thống Danh tính số, tái khẳng định việc tuân thủ Đạo luật Bảo vệ Dữ liệu Cá nhân (PDPA), đồng thời nhấn mạnh tính liên thông với các hệ thống MySejahtera và eKYC dưới sự giám sát của Ngân hàng Trung ương Malaysia. [36] Các biện pháp này nhằm đảm bảo quá trình triển khai được tiến hành một cách minh bạch, trách nhiệm và củng cố sự tín nhiệm từ công chúng.

Nếu được triển khai với các cơ chế bảo vệ rõ ràng và bảo đảm quyền kiểm soát của người dùng, MyDigital ID có thể phát triển thành một nền tảng danh tính đáng tin cậy cho những sáng kiến đổi mới sáng tạo từ công nghệ PoH. Kiến trúc của hệ thống công nghệ này, với sự kết hợp giữa dữ liệu sinh trắc học đã được xác minh, sự đồng ý của người dùng và khả năng liên thông an toàn, là minh họa về cách các nền kinh tế mới nổi có thể tích hợp tính duy nhất đã được xác minh và tính bao trùm vào các khuôn khổ bảo đảm niềm tin trong môi trường số. Đối với Đông Nam Á, kinh nghiệm của Malaysia cho thấy cách tiếp cận phát triển nền tảng danh tính được dẫn dắt bởi cơ chế quản trị có thể thu hẹp khoảng cách giữa các hệ thống ID số truyền thống và các mô hình PoH trong tương lai, qua đó tăng cường phòng, chống lừa đảo đồng thời duy trì quyền riêng tư và niềm tin của công chúng.



Philippines: Triển khai khẩn trương hệ thống PhilSys

Hệ thống Định danh Philippines (PhilSys) đã trở thành một trong những sáng kiến danh tính số phát triển nhanh nhất tại Đông Nam Á. Được thiết lập theo Đạo luật Cộng hòa số 11055 vào năm 2018, PhilSys cấp cho mỗi công dân và cư dân một Mã số PhilSys (PSN) duy nhất gồm 12 chữ số, được hỗ trợ bởi dữ liệu sinh trắc học, bao gồm nhận diện khuôn mặt, vân tay và quét mống mắt. [37] Chương trình do Cơ quan Thống kê Philippines (PSA) quản lý, với mục tiêu cải thiện khả năng tiếp cận các dịch vụ công, thúc đẩy tài chính toàn diện và tăng cường bảo mật giao dịch số. Đến cuối năm 2025, hơn 80 triệu người dân Philippines đã đăng ký, và phiên bản số của thẻ ID được cung cấp thông qua ứng dụng eGovPH và cổng national-id.gov.ph đã được chấp nhận rộng rãi bởi các cơ quan nhà nước, ngân hàng và các nền tảng trong khu vực tư nhân. [38]

Quá trình triển khai nhanh chóng này đánh dấu một cột mốc quan trọng trong nỗ lực của khu vực nhằm xây dựng các hệ thống danh tính đáng tin cậy. Bằng cách liên kết dữ liệu sinh trắc học đã xác minh với một mã định danh duy nhất trọn đời, PhilSys tạo ra một lớp xác minh tính duy nhất gắn với vai trò của nhà nước, ngăn chặn việc đăng ký trùng lặp và các hình thức định danh tổng hợp. Việc tích hợp với các tổ chức tài chính, các nhà mạng viễn thông và các hệ thống của chính phủ đã vận hành như một dạng tương tự ở giai đoạn sớm, trên quy mô lớn, của Proof of Human (PoH), qua đó xác nhận rằng mỗi người dùng được xác minh đều tương ứng với một cá nhân có thật và duy nhất. Cổng eVerify, một website cho phép xác minh thông tin xác thực dựa trên mã QR theo thời gian thực, giúp mở rộng sự bảo đảm này sang các lĩnh vực như thanh toán số, các chương trình bảo trợ xã hội và đăng ký SIM. [39]

Tuy nhiên, tốc độ triển khai nhanh cũng kéo theo những thách thức mới liên quan đến quản trị và bảo vệ quyền riêng tư. Các lỗi kỹ thuật, tình trạng chậm trễ trong phát hành thẻ và những vấn đề liên quan đến xử lý dữ liệu đã thu hút sự giám sát của công chúng. Đồng thời, các lo ngại về vấn đề lưu trữ dữ liệu sinh trắc học tập trung và chia sẻ dữ liệu thiếu minh bạch đã dẫn đến các yêu cầu về tăng cường biện pháp bảo vệ. [40] Cơ quan Thống kê Philippines (PSA) và Ủy ban Quyền riêng tư Quốc gia (NPC) đã phản hồi bằng cách tăng cường giám sát, áp dụng các tiêu chuẩn mã hóa nghiêm ngặt hơn và tích hợp các cơ chế kiểm soát truy cập dựa trên sự đồng ý của người dùng trong hệ sinh thái chính phủ điện tử của Philippines eGovPH. [41]

Kinh nghiệm của Philippines cho thấy cả tiềm năng và rủi ro của việc mở rộng nhanh các khuôn khổ bảo đảm niềm tin trong môi trường số. Quy mô và tính liên thông của hệ thống của Philippines cho thấy một nền kinh tế mới nổi có thể "nhảy vọt" trong việc xây dựng hạ tầng danh tính đã được xác minh, qua đó hỗ trợ tài chính toàn diện và giảm gian lận. Tuy nhiên, quá trình triển khai cũng cho thấy niềm tin cần phải phát triển song hành với công nghệ: niềm tin của công chúng phụ thuộc vào trách nhiệm giải trình rõ ràng, cơ chế quản trị dữ liệu minh bạch và việc bảo đảm quyền kiểm soát của người dùng. Trong bối cảnh PhilSys tiếp tục được hoàn thiện, hệ thống này mang lại một môi trường thử nghiệm có giá trị cho các đổi mới theo hướng PoH, cho thấy việc xác minh tính duy nhất, nếu được kết hợp với các biện pháp bảo vệ mạnh mẽ về quyền riêng tư và tính bao trùm, có thể củng cố khả năng phòng, chống lừa đảo và xây dựng niềm tin lấy con người làm trung tâm trong nền kinh tế số của Đông Nam Á.

Những điểm rút ra từ nghiên cứu tình huống

Chung quy lại, bốn trường hợp này minh họa những lộ trình khác nhau mà các nền kinh tế châu Á đang theo đuổi để xây dựng hạ tầng xác minh tính duy nhất. Nhật Bản và Hàn Quốc cho thấy cách các môi trường pháp lý tiên tiến có thể thể chế hóa danh tính đã được xác minh ở quy mô lớn, dù dẫn tới những kết quả khác nhau: Hệ thống My Number của Nhật Bản cho thấy sự mong manh của niềm tin công chúng khi cơ chế quản trị dữ liệu chưa đầy đủ, trong khi chế độ xác minh tên thật của Hàn Quốc làm nổi bật cả hiệu quả lẫn những rủi ro của việc tích hợp sâu giữa danh tính, tài chính và công nghệ. Tại Đông Nam Á, MyDigital ID của Malaysia và PhilSys của Philippines cho thấy hai mô hình mới nổi: một mô hình nhấn mạnh quản trị cẩn trọng ngay từ thiết kế, trong khi mô hình còn lại ưu tiên tốc độ triển khai và khả năng tiếp cận. Xuyên suốt cả bốn trường hợp, một khuôn mẫu chung nổi lên, cụ thể là, các cơ chế xác minh theo hình thức PoH phát huy hiệu quả cao nhất khi được kết hợp với cơ chế đảm bảo tính minh bạch, tính liên thông và quyền kiểm soát của người dùng, qua đó bảo đảm rằng các hệ thống danh tính số củng cố, thay vì làm xói mòn niềm tin của công chúng đối với an toàn trực tuyến.

Kết luận và Khuyến nghị

Lừa đảo và gian lận trực tuyến đã trở thành mối đe dọa nổi bật đối với niềm tin trong môi trường số trên toàn khu vực châu Á – Thái Bình Dương. Mặc dù các hệ thống ID số quốc gia, từ My Number của Nhật Bản đến PhilSys của Philippines, đã thúc đẩy mục tiêu xây dựng nền tảng danh tính được xác minh và mang tính bao trùm, nhưng về bản chất, chúng vẫn chủ yếu là các công cụ hành chính, chưa phải là những công cụ phòng, chống gian lận theo thời gian thực. Các công nghệ Proof of Human (PoH) mới nổi cung cấp một lớp bổ sung quan trọng cho các hệ thống này: cho phép cá nhân chứng minh mình là người dùng thật duy nhất mà không cần tiết lộ thông tin định danh cá nhân trên các nền tảng số, dịch vụ tài chính và mạng lưới truyền thông. Bằng cách bổ sung một chỉ báo xác minh con người thật được thiết kế theo hướng bảo vệ quyền riêng tư, PoH có thể giải quyết các hình thức lạm dụng tự động trên quy mô lớn mà các hệ thống ID số truyền thống không được thiết kế để phát hiện. Do đó, việc tích hợp PoH vào các hệ sinh thái danh tính số có thể đồng thời nâng cao khả năng phòng, chống lừa đảo và củng cố niềm tin của công chúng đối với các giao dịch số, trong khi vẫn duy trì các cơ chế bảo vệ quyền riêng tư ở mức cao.

Như đã nêu trong phần Các biện pháp bảo vệ và Quản trị, việc triển khai PoH một cách có trách nhiệm đòi hỏi thiết kế dựa trên rủi ro, các cơ chế bảo vệ người dùng rõ ràng, và sự điều chỉnh cẩn trọng để phù hợp với các hệ sinh thái danh tính hiện có. Dựa trên các nguyên tắc này, các chính phủ trong khu vực có thể:

• Tích hợp công nghệ ID số và PoH vào các chiến lược phòng, chống lừa đảo: Tích hợp xác minh tính duy nhất vào các nền tảng tài chính, thương mại điện tử và truyền thông để giảm thiểu rủi ro mạo danh, gian lận do bot và danh tính tổng hợp, đồng thời đảm bảo triển khai một cách tương xứng, ít gây cản trở và tuân thủ các khuôn khổ an toàn như ISO/IEC 25389.

• Hỗ trợ các tiêu chuẩn bảo vệ quyền riêng tư và có tính liên thông: Khuyến khích phát triển các khuôn khổ cấp khu vực kết hợp kết hợp xác minh sinh trắc học với các cơ chế bảo vệ quyền riêng tư bằng mã hóa, nhằm bảo đảm rằng việc xác minh tính duy nhất không làm suy giảm tính ẩn danh của người dùng hay khả năng sử dụng xuyên biên giới, **đồng thời ngăn chặn việc lạm dụng các chỉ báo PoH cho mục đích theo dõi hoặc tạo hồ sơ người dụng.**

• Thúc đẩy đối thoại và phối hợp chính sách khu vực: Tận dụng các cơ chế hiện có như Hội đồng Tư vấn Kinh doanh của Diễn đàn Hợp tác Kinh tế châu Á – Thái Bình Dương, Nguyên tắc chung G20 về Tài chính số Toàn diện và các sáng kiến kinh tế số do Liên Hợp Quốc dẫn dắt để điều chỉnh các mục tiêu chính sách, chia sẻ thực tiễn tốt nhất và thử nghiệmcác khuôn khổ PoH liên ngành; bao gồm cả các môi trường thử nghiệm có kiểm soát, cho phép chính phủ và các nền tảng thử nghiệm PoH trong những môi trường rủi ro cao trước khi triển khai rộng rãi.

Những phương thức kể trên, khi được triển khai đồng bộ, sẽ góp phần xây dựng một hệ sinh thái số đáng tin cậy và lấy con người làm trung tâm hơn tại châu Á, nơi việc xác minh giúp tăng cường an toàn bảo mật mà không làm xói mòn quyền riêng tư; nơi các biện pháp bảo vệ và khuôn khổ quản trị đảm bảo việc sử dụng có trách nhiệm; và nơi hợp tác khu vực chuyển hóa các hệ thống danh tính từ những dữ liệu đăng ký mang tính hành chính thành các công cụ chủ động trong phòng, chống lừa đảo và thúc đẩy tính bao trùm trong không gian số.

Tài liệu tham khảo

[1] Cybersecurity Ventures. n.d. “The World’s Third Largest Economy Has Bad Intentions—And It’s Only Getting Bigger.” Accessed August 2025. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/.
[2] Feedzai. 2024. “GASA Global State of Scams Report: $1T Lost to Scams.” Accessed August 2025. https://www.feedzai.com/blog/gasa-global-state-of-scams-report-1t-lost-to-scams/.
[3] GSMA. 2025. Fraud and Scams Safety Report. London: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf.
[4] UNODC, Inflection Point: Global Implications of Scam Centres (2025), p. xx, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
[5] Global Initiative, CRIME CYBER SCAM OPERATIONS IN SOUTHEAST ASIA (May 2025), https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf
[6] “A New Human Trafficking Trend Emerges from Myanmar,” The Japan Times, April 2, 2025, https://www.japantimes.co.jp/news/2025/04/02/japan/crime-legal/myanmar-scam-human-trafficking/
[7] “They were forced to scam others worldwide. Now thousands are detained on the Myanmar border,” AP News, March 9, 2025, https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2
[8] Signicat. 2024. “Fraud Attempts with Deepfakes Have Increased by 2137% over the Last Three Years.” Accessed August 2025. https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year.
[9] CSIS, Cyber Scamming Goes Global: Unveiling Southeast Asia’s High-Tech Fraud Factories, December 12, 2024, https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories
[10] TRM Labs, The Illicit Crypto Ecosystem Report (2022), https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022.
[11] Meta, “Cracking Down on Organized Crime Behind Scam Centers,” November 21, 2024, https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
[12] TRM Labs, 2025 Crypto Crime Report, https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report
[13] World Bank, Digital Identity Toolkit (World Bank), section on credential and smart card based eIDs. https://documents1.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf
[14] Financial Action Task Force (FATF), Guidance on Digital Identity (Paris: FATF/OECD, March 2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf (discussion of biometric authentication as part of digital ID assurance).
[15] SITA and PRISM, Biometric Digital Identity: The Next Step in Seamless Travel and Government Services (2023), https://www.sita.aero/globalassets/docs/other/biometric-digital-identity-govt-services-prism-report.pdf
[16] OECD, National Digital Identity (NDID) Platform (Thailand), https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/thailand-national-digital-identity-platform.pdf
[17] “Digital Identity Spotlight: Singapore,” 1Kosmos, https://www.1kosmos.com/identity-management/digital-identity-spotlight-singapore/
[18] “Digital identity systems around Asia compared as Taiwan seeks path forward,” BiometricUpdate, https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-taiwan-seeks-path-forward
[19] Kleros, Proof of Humanity (PoH) Documentation, “Proof of Humanity (PoH) is a sybil-resistant registry of humans, combining social verification with video submission to create a trusted list of real humans,” https://docs.kleros.io/products/proof-of-humanity
[20] Government of Japan, Cabinet Office, “Outline of the Social Security and Tax Number System (My Number System),” 2016, https://www.cao.go.jp/bangouseido/english/.
[21] Ministry of Internal Affairs and Communications (MIC), “Overview of the Social Security and Tax Number System,” updated 2024.

[22] Digital Agency of Japan, My Number Card Statistics Portal, “Number of My Number Cards Issued,” updated October 2025; “Japan’s My Number cards hit 90m issuance but trust issues persist,” Nikkei Asia, 12 July 2025.
[23] “Japan suspends some My Number links after health-insurance data mix-up,” Reuters, 28 May 2023
[24] “Japan aims to link My Number to banking and SIM registration,” Japan Times, 9 March 2024.
[25] “Fix the flaws in the My Number system,” Japan Times (editorial), 2 June 2023; Digital Agency, “Efforts to Enhance Trust in the My Number System,” 2024.
[26] Ministry of the Interior and Safety (MOIS), “Overview of the Resident Registration System,” Government of the Republic of Korea, 2023.
[27] Korea Communications Commission (KCC), Real-Name Verification Policy in the Digital Environment, 2022.
[28] Ministry of Land, Infrastructure and Transport (MOLIT), “Launch of the Mobile Driver’s License Service,” press release, January 2022.
[29] Korea Internet & Security Agency (KISA), “Status of Digital Authentication Use in Korea,” 2024; Yonhap News, “PASS App Surpasses 50 Million Users in Korea,” 9 May 2025.
[30] OECD, Digital Government in Korea: Enabling a Smart and Inclusive Society, 2023, p. 45.
[31] Korea JoongAng Daily, “Massive Data Leaks Raise Questions About Security Practices,” 4 February 2023; Korea Times, “Credit Bureau Fined over Data Breach Affecting Millions,” 15 April 2023.
[32] MOIS, “Digital Identity Pilot Project for Secure Authentication,” 2023; Personal Information Protection Commission (PIPC), “Amendments to the Personal Information Protection Act,” December 2023.
[33] Malaysia Digital Economy Blueprint (MyDIGITAL), Digital Government Division, Ministry of Communications and Digital, “Digital Identity Blueprint,” Government of Malaysia, 2024.
[34] Department of National Registration (Jabatan Pendaftaran Negara, JPN), “Implementation of MyDigital ID Pilot with LHDN and Financial Institutions,” press release, June 2024.
[35] Malay Mail, “Privacy Advocates Raise Concerns over Centralised Biometric Database,” 5 April 2024.
[36] Ministry of Communications and Digital (KKD), “Formation of Digital ID Steering Committee,” 15 February 2024; Bank Negara Malaysia, e-KYC Implementation Guidelines, revised 2023.
[37] Republic Act No. 11055, “An Act Establishing the Philippine Identification System (PhilSys Act),” Official Gazette of the Republic of the Philippines, August 2018.
[38] Philippine Statistics Authority (PSA), PhilSys Dashboard: Registration and Issuance Data, updated October 2025; Inquirer.net, “Over 80 Million Filipinos Registered for National ID—PSA,” 14 September 2025.
[39] PSA, “PhilSys eVerify Portal Launch and QR Verification Capabilities,” 2024.
[40] Rappler, “Privacy Concerns Mount over National ID Data Sharing,” 22 June 2024; Philippine Star, “National ID Delays, Data Glitches Spur Criticism,” 10 May 2024.
[41] National Privacy Commission (NPC), “NPC Advisory on Data Protection Standards for the National ID System,” 2024; PSA, “Enhanced Security Measures for ePhilID Rollout,” 2024.