Tấn công Mật khẩu và Chiến lược Phòng thủ Mật khẩu Toàn diện: Phân tích chuyên sâu từ cơ chế đến ứng phó

Lời mở đầu: Mật khẩu - Vấn đề cốt lõi của An ninh mạng

Trong kỷ nguyên số, mật khẩu là tuyến phòng thủ đầu tiên và quan trọng nhất để bảo vệ thông tin và tài sản trên không gian mạng. Mật khẩu đóng vai trò như một cơ chế xác thực danh tính cơ bản, là cầu nối giữa người dùng và các dịch vụ trực tuyến. Tuy nhiên, chính sự phổ biến và sự phụ thuộc vào mật khẩu đã biến chúng thành mục tiêu hàng đầu của các cuộc tấn công mạng. Kẻ tấn công không ngừng phát triển các phương pháp tinh vi để khai thác các điểm yếu cố hữu của mật khẩu, từ việc người dùng đặt mật khẩu yếu, dễ đoán cho đến việc tái sử dụng mật khẩu trên nhiều nền tảng.

Bối cảnh tấn công hiện đại đã vượt ra khỏi việc đoán mật khẩu ngẫu nhiên đơn thuần, thay vào đó tập trung vào việc khai thác các lỗ hổng về mặt con người và quy trình. Điều này đòi hỏi một cách tiếp cận đa lớp, toàn diện hơn trong bảo mật, thay vì chỉ dựa vào sự phức tạp của mật khẩu. Báo cáo này được biên soạn nhằm cung cấp một cái nhìn tổng quan chuyên sâu và toàn diện về các phương thức tấn công mật khẩu phổ biến, từ cơ chế kỹ thuật đến hậu quả thực tế. Bên cạnh đó, báo cáo sẽ trình bày một chiến lược phòng thủ chủ động, tích hợp và đa tầng, bao gồm cả các giải pháp công nghệ hiện đại và các quy trình ứng phó sự cố hiệu quả, giúp các tổ chức và cá nhân có thể xây dựng một lá chắn bảo vệ vững chắc trong bối cảnh rủi ro ngày càng cao.

Chương 1: Phân loại Tấn công Mật khẩu và Cơ chế Vận hành

1.1. Định nghĩa và Bản chất của Tấn công Mật khẩu

Tấn công mật khẩu là một thuật ngữ chỉ một loạt các phương pháp được thiết kế để xâm nhập, đánh cắp hoặc lừa đảo nhằm lấy được thông tin xác thực, bao gồm tên người dùng và mật khẩu, của một tài khoản người dùng.[1] Bản chất của các cuộc tấn công này thường tập trung vào việc khai thác điểm yếu cốt lõi trong hệ thống xác thực: sự chủ quan của người dùng trong việc đặt mật khẩu quá đơn giản, dễ đoán hoặc thói quen sử dụng lại thông tin đăng nhập trên nhiều dịch vụ khác nhau.[1]

1.2. Các Loại Tấn công Phổ biến và Phân tích Kỹ thuật

1.2.1. Tấn công vét cạn (Brute Force Attack): Nguyên lý và các biến thể

Tấn công vét cạn, hay còn gọi là tấn công dò mật khẩu, là một trong những hình thức tấn công mạng đã có từ lâu và vẫn còn rất phổ biến.[2] Về cơ bản, đây là một phương pháp thử và sai có hệ thống, trong đó kẻ tấn công sử dụng các công cụ phần mềm tự động để đoán mật khẩu hoặc khóa mã hóa của một tài khoản cụ thể bằng cách thử tất cả các tổ hợp ký tự có thể xảy ra cho đến khi tìm được mật khẩu đúng.[1] Phương pháp này hoạt động bằng cách tạo ra các chuỗi ký tự dựa trên cơ sở toán học và thay đổi ký tự luân phiên cho đến khi trùng khớp.[2]

Mặc dù có vẻ đơn giản, tấn công vét cạn lại rất nguy hiểm vì khả năng tự động hóa cao và dễ dàng triển khai. Các biến thể chính của loại tấn công này bao gồm:

- **Tấn công vét cạn đơn giản (Simple Brute Force):** Đây là hình thức tấn công nguyên thủy nhất, trong đó kẻ tấn công sẽ thử tất cả các tổ hợp ký tự có thể xảy ra theo một trình tự logic, ví dụ như từ "0000" đến "zzzz" nếu mật khẩu có 4 ký tự.[2] Dù tốn thời gian nhưng nếu mật khẩu ngắn và không đủ phức tạp, khả năng thành công của phương pháp này là rất cao.
- **Tấn công vét cạn kết hợp (Hybrid Brute Force):** Kẻ tấn công kết hợp tấn công từ điển với việc thêm các ký tự đặc biệt, số hoặc chữ cái ngẫu nhiên vào các từ có sẵn để tạo ra các mật khẩu phức tạp hơn, chẳng hạn như NewYork1993 hoặc Spike1234.[1]
- **Tấn công vét cạn đảo ngược (Reverse Brute Force):** Ngược lại với các phương pháp trên, tấn công vét cạn đảo ngược sẽ bắt đầu với một mật khẩu phổ biến đã biết (thường

là từ các vụ rò rỉ dữ liệu) và thử mật khẩu đó với hàng triệu tên người dùng cho đến khi tìm thấy sự trùng khớp.[2]

1.2.2. Tấn công từ điển (Dictionary Attack)

Tấn công từ điển là một phiên bản tối ưu hóa của tấn công vét cạn, sử dụng một danh sách các từ và cụm từ có khả năng được dùng làm mật khẩu cao nhất.[1] Danh sách này có thể bao gồm các từ trong từ điển, tên riêng, ngày sinh, tên người thân hoặc các mật khẩu phổ biến như "

password".[1] Bằng cách sử dụng các danh sách này, kẻ tấn công có thể tiết kiệm đáng kể thời gian và tài nguyên so với việc thử ngẫu nhiên hoàn toàn.[7]

1.2.3. Tấn công nhồi thông tin xác thực (Credential Stuffing)

Tấn công nhồi thông tin xác thực là một hình thức tấn công tự động, trong đó kẻ tấn công sử dụng các cặp tên người dùng và mật khẩu hợp lệ đã bị đánh cắp từ một vụ vi phạm dữ liệu trước đó để thử đăng nhập vào hàng loạt các dịch vụ khác.[2] Phương thức này hoạt động hiệu quả vì nhiều người dùng có thói quen tái sử dụng mật khẩu trên nhiều trang web khác nhau.[11] Kẻ tấn công không cần đoán mật khẩu mà chỉ cần "nhồi" thông tin xác thực đã có, thường chỉ thử một lần duy nhất cho mỗi tài khoản để tránh bị các hệ thống phát hiện và khóa tài khoản.[11]

1.2.4. Tấn công rải mật khẩu (Password Spraying)

Tấn công rải mật khẩu là một kỹ thuật tấn công "chậm và thấp" (low-and-slow) được thiết kế để né tránh các cơ chế khóa tài khoản truyền thống.[1] Thay vì thử nhiều mật khẩu cho một tài khoản, kẻ tấn công sẽ sử dụng một số ít mật khẩu rất phổ biến (ví dụ:

Password123 hoặc Winter2024!) và thử lần lượt với một danh sách lớn các tên người dùng.[1] Phương pháp này đặc biệt nguy hiểm đối với các hệ thống có nhiều tài khoản sử dụng mật khẩu yếu hoặc mật khẩu mặc định.[16]

Bảng 1: Phân loại và Đặc điểm các Loại Tấn công Mật khẩu

Tên tấn công	Mục tiêu	Cơ chế hoạt động	Đặc điểm nổi bật	Cách thức né tránh phòng thủ
Tấn công vét cạn (Brute Force)	Đoán mật khẩu của một tài khoản cụ thể	Thử mọi tổ hợp ký tự có thể xảy ra bằng phần mềm tự động.	Dựa vào sức mạnh tính toán, thường bị chặn bởi chính sách khóa tài khoản.	Sử dụng các danh sách từ điển, kết hợp ký tự để tối ưu hóa việc đoán.
Tấn công từ điển (Dictionary Attack)	Đoán mật khẩu của một tài khoản cụ thể	Sử dụng danh sách các từ phổ biến, tên riêng để thử đăng nhập.	Hiệu quả và nhanh hơn vét cạn đơn giản.	Dựa vào dữ liệu thu thập được từ các nguồn công khai hoặc vi phạm.
Tấn công nhồi thông tin xác thực (Credential Stuffing)	Chiếm quyền nhiều tài khoản trên nhiều dịch vụ khác nhau.	Sử dụng cặp tên người dùng-mật khẩu đã bị rò rỉ để thử đăng nhập tự động.	Tận dụng thói quen tái sử dụng mật khẩu của người dùng, khó bị phát hiện vì mỗi tài khoản chỉ bị thử một lần.	Sử dụng botnet và hạ tầng proxy để phân tán yêu cầu đăng nhập.
Tấn công rải mật khẩu (Password Spraying)	Tìm kiếm các tài khoản có mật khẩu yếu trên quy mô lớn.	Dùng một mật khẩu phổ biến duy nhất để thử trên nhiều tài khoản khác nhau.	"Chậm mà chắc" (low-and-slow), hiệu quả trong việc né tránh chính sách khóa tài	Phân tán các nỗ lực đăng nhập trên nhiều địa chỉ IP và trong khoảng thời gian dài.

			khoản.	

Một trong những phân tích quan trọng nhất về tấn công mật khẩu là sự chuyển dịch từ các cuộc tấn công kỹ thuật thuần túy sang việc khai thác hành vi và điểm yếu của con người. Ban đầu, tấn công vét cạn tập trung vào việc thử mọi khả năng kỹ thuật để tìm ra mật khẩu. Tuy nhiên, các phương pháp như tấn công nhồi thông tin xác thực và tấn công rải mật khẩu đã cho thấy kẻ tấn công nhận ra rằng điểm yếu lớn nhất không phải ở thuật toán băm mà ở chính thói quen của người dùng. Kẻ tấn công đã thay đổi chiến lược từ "đoán mật khẩu hệ thống" sang "đoán mật khẩu người dùng" bằng cách tận dụng việc đặt mật khẩu yếu và tái sử dụng mật khẩu. Điều này nhấn mạnh rằng các tổ chức không chỉ cần đầu tư vào công nghệ bảo mật mà còn phải tập trung vào việc giáo dục, nâng cao nhận thức cho nhân viên.

Một phân tích sâu hơn về tấn công rải mật khẩu cho thấy mối đe dọa này rất khó bị phát hiện. Các hệ thống bảo mật truyền thống như chính sách khóa tài khoản được thiết kế để chống lại các cuộc tấn công vét cạn tốc độ cao từ một IP duy nhất. Tấn công rải mật khẩu đã đảo ngược mô hình này bằng cách thử một mật khẩu trên nhiều tài khoản khác nhau trong một thời gian dài, sử dụng nhiều địa chỉ IP xoay vòng. Do đó, cuộc tấn công này có thể dễ dàng vượt qua các hệ thống giám sát đơn giản. Để chống lại loại tấn công này, các tổ chức cần có các hệ thống giám sát và phân tích hành vi nâng cao, có khả năng tổng hợp các nỗ lực đăng nhập thất bại trên quy mô lớn, liên tục trong nhiều giờ hoặc nhiều ngày, chứ không chỉ dựa vào giới hạn số lần thử trong một khoảng thời gian ngắn.

Chương 2: Công cụ và Phương pháp Đánh cắp Mật khẩu

2.1. Phân tích Công cụ Kỹ thuật

2.1.1. Công cụ tấn công offline: Bảng cầu vồng (Rainbow Table)

Bảng cầu vồng là một cơ sở dữ liệu lớn đã được tính toán trước, lưu trữ các cặp mật khẩu văn bản gốc và giá trị băm tương ứng.[18] Thay vì thử đoán và băm mật khẩu theo thời gian thực, kẻ

tấn công chỉ cần lấy giá trị băm đã bị đánh cắp từ một hệ thống bị xâm nhập và tìm kiếm trong bảng này để tra ra mật khẩu gốc.[18] Phương pháp này cực kỳ hiệu quả đối với các hàm băm cũ, không được "thêm muối" (unsalted) như MD5 hoặc SHA-1.[6]

2.1.2. Công cụ tấn công online: John the Ripper và Hydra

John the Ripper là một công cụ bẻ khóa mật khẩu phổ biến, mạnh mẽ, thường được sử dụng để thực hiện các cuộc tấn công từ điển offline trên các tệp chứa hàm băm mật khẩu.[2] Công cụ này có nhiều chế độ tấn công khác nhau, bao gồm chế độ "đơn lẻ" sử dụng thông tin cá nhân của người dùng để đoán mật khẩu.[21]

Hydra là một công cụ tấn công brute force online nổi tiếng, có khả năng tấn công nhiều giao thức và dịch vụ khác nhau như HTTP, HTTPS, FTP, SSH, và Telnet.[22] Công cụ này hoạt động bằng cách tự động thử các cặp tên người dùng và mật khẩu từ các danh sách có sẵn để tìm ra thông tin đăng nhập hợp lệ.[10]

2.2. Các Phương thức Phi kỹ thuật và Mã độc

2.2.1. Lừa đảo qua mạng (Phishing) và kỹ thuật xã hội

Lừa đảo qua mạng (Phishing) là một hình thức tấn công phi kỹ thuật, trong đó kẻ tấn công giả mạo các tổ chức hoặc người quen để lừa người dùng tiết lộ thông tin nhạy cảm như mật khẩu và thông tin thẻ tín dụng.[6] Phương thức này thường được thực hiện qua email lừa đảo, tin nhắn giả mạo hoặc trang web giả mạo, dụ dỗ người dùng nhập mật khẩu vào một trang không an toàn.[4]

2.2.2. Keylogger và các phần mềm độc hại

Keylogger là một loại phần mềm hoặc phần cứng độc hại được thiết kế để ghi lại mọi phím được gõ trên bàn phím của người dùng một cách bí mật.[1] Sau khi được cài đặt (thường qua

các file đính kèm email độc hại), keylogger sẽ theo dõi và thu thập tên người dùng, mật khẩu cùng các thông tin bí mật khác, sau đó gửi về cho kẻ tấn công.[6]

2.2.3. Các kỹ thuật tiên tiến

Một trong những kỹ thuật tiên tiến đáng chú ý là tấn công WindTalker, cho phép kẻ tấn công đọc được chuyển động ngón tay của người dùng trên màn hình điện thoại thông minh bằng cách phân tích sự giao thoa của tín hiệu sóng Wi-Fi, từ đó đoán được mật khẩu và mã PIN.[29] Kỹ thuật này chỉ cần các thiết bị phần cứng đơn giản và có thể đạt độ chính xác cao.

Các phương thức tấn công không tồn tại độc lập mà thường được xâu chuỗi trong một chiến dịch tấn công. Ví dụ, một cuộc tấn công lừa đảo qua mạng có thể là bước đầu tiên để cài đặt keylogger lên máy tính của nạn nhân. Tương tự, dữ liệu bị rò rỉ từ một vụ vi phạm bảo mật có thể được dùng làm nguồn dữ liệu cho tấn công nhồi thông tin xác thực hoặc tấn công vét cạn đảo ngược. Do đó, việc phòng thủ cần phải là một chiến lược tích hợp, đa tầng.

Mặc dù các cuộc tấn công online như tấn công nhồi thông tin xác thực đang gia tăng, các phương thức tấn công offline như bảng cầu vồng vẫn là một mối đe dọa nghiêm trọng. Khi một hệ thống bị vi phạm, tất cả các hàm băm mật khẩu có thể bị đánh cắp cùng lúc. Các cuộc tấn công offline không bị giới hạn bởi tốc độ nhập liệu của máy chủ, cho phép kẻ tấn công sử dụng sức mạnh tính toán khổng lồ để bẻ khóa hàng loạt mật khẩu mà không bị phát hiện. Điều này nhấn mạnh tầm quan trọng của việc sử dụng các thuật toán băm mật khẩu hiện đại, chậm và được thêm "muối" (salt) độc nhất cho mỗi người dùng, ngay cả khi các biện pháp bảo mật bên ngoài đã rất tốt.

Chương 3: Tác động và Hậu quả của Tấn công Mật khẩu

3.1. Hậu quả đối với Cá nhân và Người dùng cuối

Đối với cá nhân, hậu quả của việc bị tấn công mật khẩu có thể rất nghiêm trọng. Các thông tin, hình ảnh nhạy cảm có thể bị rò rỉ.[2] Kẻ tấn công có thể chiếm đoạt danh tính, truy cập các

tài khoản ngân hàng, email hoặc mạng xã hội, dẫn đến các hình thức lừa đảo và gian lận khác.[18] Ngoài ra, kẻ tấn công có thể chèn các mã độc vào tài khoản để thực hiện các hành vi xấu, gây hậu quả không lường trước.[2]

3.2. Thiệt hại Toàn diện đối với Doanh nghiệp và Tổ chức

3.2.1. Thiệt hại tài chính và gián đoạn kinh doanh

Tấn công mật khẩu là một trong những nguyên nhân hàng đầu dẫn đến các vụ vi phạm dữ liệu, gây ra những tổn thất tài chính khổng lồ cho doanh nghiệp. Các chi phí trực tiếp bao gồm tiền chuộc ransomware, phí luật sư, phí bảo hiểm cao hơn và chi phí khôi phục hệ thống.[25] Các cuộc tấn công này có thể gây gián đoạn hoạt động kinh doanh, dẫn đến thất thoát đáng kể về doanh thu.[2] Các ước tính cho thấy chi phí tội phạm mạng toàn cầu sẽ đạt 10.5 nghìn tỷ USD mỗi năm vào năm 2025.[30] Riêng các cuộc tấn công nhồi thông tin xác thực đã gây thiệt hại hàng tỷ USD mỗi năm cho người tiêu dùng và doanh nghiệp.[11]

3.2.2. Mất mát tài sản trí tuệ và tổn thất danh tiếng

Một khi kẻ tấn công có được quyền truy cập vào hệ thống, họ có thể đánh cắp các tài liệu mật, tài sản trí tuệ, gây ảnh hưởng lớn đến lợi thế cạnh tranh của doanh nghiệp.[2] Hậu quả lớn nhất là tổn thất uy tín và lòng tin của khách hàng sau các vụ vi phạm dữ liệu.[19] Các doanh nghiệp cũng có thể phải đối mặt với các khoản phạt theo quy định pháp lý về bảo vệ dữ liệu.[25]

Một phân tích sâu hơn cho thấy chi phí của một cuộc tấn công vượt xa thiệt hại trực tiếp. Các thiệt hại tài chính chỉ là phần nổi của tảng băng chìm. Phần lớn chi phí đến từ các yếu tố "ẩn" và dài hạn như phí bảo hiểm cao hơn, chi phí pháp lý và đặc biệt là tổn thất về danh tiếng, lòng tin của khách hàng. Khi một cuộc tấn công vào doanh nghiệp xảy ra, dữ liệu của khách hàng bị rò rỉ, dẫn đến các cuộc tấn công lừa đảo khác nhằm vào chính khách hàng đó. Điều này biến việc phòng chống tấn công mật khẩu không chỉ là một khoản chi phí mà là một khoản đầu tư chiến lược để bảo vệ uy tín và giá trị cốt lõi của doanh nghiệp.

Tấn công mật khẩu hiếm khi là mục tiêu cuối cùng của kẻ xấu. Một số nguồn tin cho thấy sau khi có được quyền truy cập, kẻ tấn công thường tiếp tục bằng cách cài đặt malware hoặc

ransomware vào hệ thống.[4] Điều này biến một cuộc tấn công mật khẩu ban đầu trở thành một mối đe dọa đa diện hơn nhiều. Do đó, việc bảo vệ mật khẩu mạnh mẽ không chỉ ngăn chặn việc chiếm đoạt tài khoản mà còn có tác dụng như một lớp phòng thủ quan trọng chống lại các loại tấn công mạng nguy hiểm khác.

Chương 4: Chiến lược Phòng tránh và Bảo vệ Toàn diện

4.1. Nền tảng: Chính sách Mật khẩu Mạnh và Quản lý Tích cực

4.1.1. Hướng dẫn tạo mật khẩu mạnh và duy nhất

Một mật khẩu mạnh là tuyến phòng thủ đầu tiên và quan trọng nhất.[25] Các mật khẩu này phải có ít nhất 12-14 ký tự và là sự kết hợp của chữ hoa, chữ thường, số và ký hiệu đặc biệt.[13] Cần tránh sử dụng thông tin cá nhân dễ đoán như tên, ngày sinh, số điện thoại.[2] Một trong những nguyên tắc vàng là sử dụng mật khẩu duy nhất cho mỗi tài khoản để phòng chống tấn công nhồi thông tin xác thực.[13] Việc thay đổi mật khẩu định kỳ cũng giúp giảm thiểu rủi ro.[1]

4.1.2. Vai trò thiết yếu của các trình quản lý mật khẩu chuyên nghiệp

Để giải quyết bài toán khó nhớ các mật khẩu phức tạp, các trình quản lý mật khẩu là một giải pháp tối ưu.[9] Các công cụ này giúp người dùng tạo và lưu trữ an toàn tất cả các mật khẩu độc nhất trong một kho dữ liệu được mã hóa.[13] Một số trình quản lý mật khẩu còn cung cấp tính năng kiểm tra xem mật khẩu của bạn có bị rò rỉ trong các vụ vi phạm dữ liệu hay không, và hỗ trợ xác thực đa yếu tố để truy cập vào chính kho mật khẩu đó.[13]

Bảng 2: Hướng dẫn Tạo Mật khẩu Mạnh và An toàn

Tiêu chí	Tại sao quan trọng	Ví dụ tốt	Ví dụ xấu
Độ dài tối thiểu 12-14 ký tự	Càng dài càng khó bị bẻ khóa bằng các cuộc tấn công vét cạn và từ điển.	Th!sIsA5trongP@ssw0rd	password
Kết hợp chữ hoa, chữ thường, số, và ký hiệu đặc biệt	Làm tăng đáng kể số lượng tổ hợp ký tự có thể xảy ra, kéo dài thời gian bẻ khóa.	VeQuwamyfaPore97!	nguyenlananh123
Tính duy nhất cho mỗi tài khoản	Ngăn chặn tấn công nhồi thông tin xác thực. Nếu một tài khoản bị lộ, các tài khoản khác vẫn an toàn.	Fb_pa$$w0rd_2024 (Facebook) và Gmai1@_P@ssw0rd (Gmail)	LanAnh123 (cho cả Facebook và Gmail)
Không chứa thông tin cá nhân dễ đoán	Các cuộc tấn công từ điển và kỹ thuật xã hội thường sử dụng thông tin công khai để đoán mật khẩu.	*BraVe_He@rT_1888*	nguyenlananh1990
Thay đổi định kỳ	Giảm thiểu rủi ro từ các vụ rò rỉ dữ liệu trước đó.	Thay đổi mật khẩu mỗi 3-6 tháng.[1]	Giữ một mật khẩu trong nhiều năm.

4.2. Lớp bảo vệ tiếp theo: Các Công nghệ Xác thực Hiện đại

4.2.1. Phân tích chuyên sâu về Xác thực Đa yếu tố (MFA)

Xác thực Đa yếu tố (MFA) là một cơ chế bảo mật bổ sung thêm một tầng bảo vệ vào quy trình đăng nhập.[39] Nó yêu cầu người dùng cung cấp hai hoặc nhiều yếu tố xác minh danh tính khác nhau để truy cập tài khoản.[39] Các yếu tố này thường được phân loại là: thứ gì đó bạn biết (mật khẩu), thứ gì đó bạn có (điện thoại, khóa bảo mật) và thứ gì đó thuộc về bạn (sinh trắc học như vân tay, khuôn mặt).[40]

Lợi ích của MFA là rất lớn. Ngay cả khi mật khẩu bị lộ qua các cuộc tấn công như phishing hoặc keylogger, kẻ tấn công vẫn không thể truy cập tài khoản vì không có yếu tố xác thực thứ hai.[13] MFA giúp tăng cường bảo mật cho các tài khoản có rủi ro cao và bảo vệ tài nguyên khỏi truy cập trái phép.[40]

Bảng 3: So sánh Bảo mật Mật khẩu và Xác thực Đa yếu tố (MFA)

Tiêu chí	Mật khẩu truyền thống	Xác thực Đa yếu tố (MFA)
Lợi ích chính	Lớp bảo vệ đầu tiên, dễ sử dụng.	Tăng cường bảo mật, bảo vệ danh tính, giảm rủi ro lừa đảo qua mạng.
Chống lại Brute Force và Dictionary	Có thể bị bẻ khóa nếu mật khẩu yếu hoặc đơn giản.	Ngăn chặn hiệu quả vì kẻ tấn công không thể có được yếu tố thứ hai.
Chống lại Phishing	Rất dễ bị lừa lấy mật khẩu trên các trang web giả mạo.	Mã xác thực thứ hai không thể bị kẻ lừa đảo thu thập được.
Chống lại Keylogger	Hoàn toàn vô hiệu hóa nếu mật khẩu bị ghi lại.	Kẻ tấn công có thể lấy mật khẩu nhưng không thể lấy được mã xác thực thứ hai (ví dụ: mã OTP).
Chống lại Credential	Kẻ tấn công có thể chiếm quyền nếu mật khẩu được	Kẻ tấn công không thể chiếm quyền vì không có

Stuffing	tái sử dụng.	mã xác thực thứ hai.

4.2.2. Tương lai không mật khẩu: Công nghệ FIDO2 và Passkeys

Công nghệ xác thực không mật khẩu (passwordless) là một bước tiến mới, loại bỏ hoàn toàn mật khẩu truyền thống và thay thế bằng các phương thức an toàn và thuận tiện hơn như khóa bảo mật, sinh trắc học hoặc mã PIN trên thiết bị đáng tin cậy.[4]

FIDO2 là một tiêu chuẩn mở do Liên minh FIDO phát triển, nhằm cung cấp một phương pháp xác thực an toàn và chống lừa đảo. **Passkeys** là một cách triển khai của FIDO2, sử dụng mật mã bất đối xứng (cặp khóa công khai/riêng tư) để xác thực. Khóa riêng tư (private key) được lưu trữ an toàn trên thiết bị của người dùng, được bảo vệ bằng sinh trắc học hoặc mã PIN, và không bao giờ rời khỏi thiết bị. Khóa công khai (public key) được lưu trên máy chủ của dịch vụ.[45]

Ưu điểm nổi bật của công nghệ này là khả năng kháng lừa đảo qua mạng (phishing-resistant) vì khóa riêng tư chỉ hoạt động trên tên miền đã đăng ký chính xác, do đó ngay cả khi người dùng truy cập vào một trang web giả mạo, khóa sẽ không được gửi đi.[42] Thêm vào đó, vì không có mật khẩu để lưu trữ, các vụ vi phạm dữ liệu không thể làm rò rỉ mật khẩu và không thể bị tấn công bằng các phương pháp bẻ khóa offline.[44]

4.3. Bảo vệ Hạ tầng: Biện pháp từ phía Hệ thống

4.3.1. Thiết lập chính sách khóa tài khoản và sử dụng Captcha

Để chống lại các cuộc tấn công vét cạn, các hệ thống cần thiết lập chính sách khóa tài khoản sau một số lần đăng nhập sai nhất định trong một khoảng thời gian nhất định.[1] Ngoài ra, việc sử dụng các công cụ như Captcha giúp phân biệt người dùng thật với các bot tấn công tự động.[47]

4.3.2. Vai trò của Tường lửa ứng dụng web (WAF) và Hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS)

Tường lửa ứng dụng web (WAF) và Hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS) là các công cụ bảo mật chủ động, có khả năng giám sát và phân tích lưu lượng truy cập mạng để phát hiện các truy vấn bất thường hoặc các dấu hiệu tấn công vét cạn. Các công cụ này có thể tự động chặn các địa chỉ IP độc hại, giảm thiểu rủi ro tấn công vào hạ tầng mạng.[5]

Sự ra đời của các công nghệ xác thực mới như MFA và passwordless là một hệ quả trực tiếp của sự thất bại của mật khẩu truyền thống. Các mật khẩu, dù mạnh đến đâu, vẫn có thể bị đánh bại bởi các cuộc tấn công phức tạp như phishing hoặc bị rò rỉ trong các vi phạm dữ liệu. MFA ra đời để bù đắp điểm yếu này, sau đó passwordless xuất hiện để loại bỏ hoàn toàn mật khẩu. Đây là một lộ trình phát triển rõ ràng của ngành bảo mật, từ "củng cố mật khẩu" đến "thay thế mật khẩu". Do đó, các tổ chức nên bắt đầu áp dụng MFA ngay lập tức và từng bước lên kế hoạch triển khai các giải pháp passwordless cho tương lai.

Một chiến lược phòng thủ hiệu quả đòi hỏi sự kết hợp của nhiều lớp bảo vệ. Một mật khẩu mạnh có thể chống lại tấn công vét cạn nhưng không chống được phishing. MFA chống được phishing nhưng không thể ngăn chặn keylogger nếu mã OTP bị đánh cắp. WAF có thể chặn các cuộc tấn công tự động, nhưng không thể bảo vệ người dùng khỏi việc nhập mật khẩu vào một trang web giả mạo. Vì vậy, một chiến lược phòng thủ toàn diện phải là sự kết hợp chặt chẽ giữa: (1) Chính sách mật khẩu mạnh và công cụ quản lý mật khẩu; (2) Lớp xác thực bổ sung như MFA hoặc passwordless; và (3) Các biện pháp bảo vệ cấp hạ tầng như WAF/IDS/IPS.

Chương 5: Nhận biết, Ứng phó và Khắc phục sự cố

5.1. Dấu hiệu Nhận biết Tài khoản bị Tấn công

Việc nhận biết sớm một cuộc tấn công mật khẩu là rất quan trọng để giảm thiểu thiệt hại. Các dấu hiệu phổ biến bao gồm:

- Nhận được cảnh báo về hoạt động đăng nhập bất thường từ một thiết bị hoặc vị trí địa lý lạ.[48]
- Không thể đăng nhập vào tài khoản của mình mặc dù đã nhập đúng mật khẩu.[48]
- Nội dung hoặc cài đặt trong tài khoản bị thay đổi mà không phải do bạn thực hiện, ví dụ

như các tin nhắn đã gửi nhưng bạn không hề biết.[48]
- Bạn nhận được tin nhắn hoặc mã xác thực một lần (OTP) mà không hề yêu cầu.[49]

5.2. Kế hoạch Ứng phó Sự cố (Incident Response Plan)

5.2.1. Các bước ứng phó khẩn cấp: Ngăn chặn và cô lập

Khi phát hiện tài khoản bị tấn công, hành động nhanh chóng là yếu tố then chốt.

1. **Ngăn chặn thiệt hại:** Đăng xuất tài khoản ra khỏi tất cả các thiết bị ngay lập tức và liên hệ với nhà cung cấp dịch vụ để báo cáo sự cố.[4]
2. **Thay đổi mật khẩu:** Thay đổi mật khẩu của tài khoản bị hack ngay lập tức. Nếu mật khẩu này được sử dụng cho các tài khoản khác, cần thay đổi tất cả các mật khẩu đó.[4]
3. **Tăng cường bảo mật:** Kích hoạt tính năng xác thực đa yếu tố (MFA) cho tất cả các tài khoản quan trọng để thêm một lớp bảo vệ.[50] Cần kiểm tra bộ lọc email và các quy tắc chuyển tiếp email lạ và xóa chúng đi.[52]

5.2.2. Quy trình phục hồi: Khôi phục tài khoản và hệ thống

Đối với các tổ chức, việc ứng phó sự cố cần tuân theo một kế hoạch có cấu trúc, được gọi là Kế hoạch Ứng phó Sự cố (Incident Response Plan).[53] Kế hoạch này bao gồm bốn giai đoạn chính:

1. **Giai đoạn Chuẩn bị:** Xây dựng kế hoạch trước khi sự cố xảy ra. Kế hoạch phải được tài liệu hóa chi tiết, xác định rõ vai trò và trách nhiệm của từng thành viên trong đội ứng phó, và được diễn tập định kỳ.[53]
2. **Giai đoạn Nhận diện:** Phát hiện sự cố, xác định thời điểm, phạm vi và nguồn gốc của cuộc tấn công.[53]
3. **Giai đoạn Ngăn chặn, Loại bỏ và Phục hồi:** Cô lập hệ thống bị xâm nhập để ngăn chặn thiệt hại lan rộng, loại bỏ hoàn toàn các dấu vết của kẻ tấn công và mã độc, sau đó khôi phục dữ liệu từ các bản sao lưu sạch.[4]
4. **Giai đoạn Đánh giá sau sự cố:** Tổ chức cuộc họp để phân tích sự cố, tìm ra nguyên nhân gốc rễ và những lỗ hổng đã bị khai thác. Dựa trên những bài học kinh nghiệm này,

cần cập nhật và cải thiện các chính sách bảo mật và kế hoạch ứng phó.[53]

Một điểm phân tích quan trọng là khắc phục sự cố cần là một quy trình có cấu trúc, không phải phản ứng ngẫu hứng. Các cá nhân chỉ cần làm theo các bước khẩn cấp để khôi phục tài khoản. Ngược lại, một tổ chức cần một kế hoạch ứng phó chi tiết, được chuẩn bị từ trước với đầy đủ vai trò, trách nhiệm và quy trình rõ ràng. Việc không có kế hoạch này sẽ dẫn đến các sai lầm tốn kém và tăng thiệt hại. Vì vậy, các doanh nghiệp cần đầu tư vào việc xây dựng một Kế hoạch Ứng phó Sự cố toàn diện, coi đó là một phần không thể thiếu của chiến lược an ninh mạng. Hơn nữa, việc sao lưu và khôi phục dữ liệu định kỳ là lớp phòng thủ cuối cùng để giảm thiểu thiệt hại khi các lớp bảo mật khác đã thất bại.

Chương 6: Tương lai của Tấn công và Phòng thủ: Vai trò của Trí tuệ Nhân tạo (AI)

Cuộc chiến mật khẩu đang bước vào một kỷ nguyên mới với sự tham gia của trí tuệ nhân tạo (AI). AI không chỉ là một công cụ mà là một nhân tố thay đổi cuộc chơi trong cuộc chiến này.

6.1. AI trong Tấn công: Khả năng bẻ khóa mật khẩu của AI

Kẻ tấn công đang sử dụng AI để tạo ra các cuộc tấn công mật khẩu hiệu quả hơn. Các công cụ bẻ khóa mật khẩu ứng dụng AI như PassGAN có thể bẻ khóa các mật khẩu ngắn (dưới 8 ký tự) trong vài phút, ngay cả khi chúng chứa ký tự đặc biệt.[55] AI có thể được sử dụng để tạo ra các danh sách mật khẩu có tính logic và khả năng thành công cao hơn nhiều so với các phương pháp vét cạn truyền thống.[56]

6.2. AI trong Phòng thủ: Sử dụng AI để phát hiện bất thường và tăng cường bảo mật

Ở chiều ngược lại, các chuyên gia bảo mật cũng đang sử dụng AI để xây dựng các hệ thống phòng thủ tinh vi hơn. Các giải pháp bảo mật dựa trên AI có thể phân tích hành vi đăng nhập của người dùng và nhanh chóng phát hiện các nỗ lực bất thường, từ đó tự động chặn đăng

nhập hoặc yêu cầu xác thực hai yếu tố.[57]

AI đặc biệt hữu ích trong việc xử lý và phân tích lượng lớn dữ liệu log từ nhiều nguồn để phát hiện các mối đe dọa tinh vi mà con người khó có thể nhận ra, bao gồm cả các cuộc tấn công "chậm và thấp" như tấn công rải mật khẩu.[57] Điều này giúp các tổ chức có cách tiếp cận chủ động hơn đối với rủi ro.

AI đang tạo ra một "cuộc chạy đua vũ trang" mới trong an ninh mạng. Một mặt, kẻ tấn công sử dụng AI để tạo ra các cuộc tấn công hiệu quả hơn. Mặt khác, các chuyên gia bảo mật sử dụng AI để phát hiện các cuộc tấn công đó. Trong tương lai, các cuộc tấn công sẽ ngày càng tinh vi và tự động hóa. Do đó, các biện pháp phòng thủ cũng cần phải được tự động hóa và có khả năng học hỏi để thích ứng. Các tổ chức cần đầu tư vào các giải pháp bảo mật dựa trên AI để không bị tụt lại phía sau.

Kết luận và Khuyến nghị

Phân tích chuyên sâu về tấn công mật khẩu cho thấy đây là một mối đe dọa đa diện và không ngừng tiến hóa. Không có một giải pháp đơn lẻ nào có thể bảo vệ hoàn toàn. Việc chỉ dựa vào mật khẩu mạnh, dù quan trọng, cũng không còn đủ để đối phó với các cuộc tấn công tinh vi như lừa đảo qua mạng hay nhồi thông tin xác thực.

Từ những phân tích trên, các khuyến nghị toàn diện được đưa ra bao gồm:

- **Đối với cá nhân:**
  - **Áp dụng mật khẩu mạnh và duy nhất:** Luôn sử dụng mật khẩu dài, phức tạp và không tái sử dụng trên các tài khoản khác nhau.
  - **Sử dụng trình quản lý mật khẩu:** Đây là công cụ thiết yếu để tạo và lưu trữ mật khẩu an toàn mà không cần phải ghi nhớ.
  - **Bật Xác thực Đa yếu tố (MFA):** Luôn bật MFA cho tất cả các tài khoản quan trọng như email, ngân hàng và mạng xã hội. Đây là lớp bảo vệ hiệu quả nhất chống lại các cuộc tấn công lừa đảo và đánh cắp mật khẩu.
- **Đối với tổ chức:**
  - **Xây dựng chính sách mật khẩu chặt chẽ:** Áp dụng các chính sách mật khẩu mạnh và có thời hạn, đồng thời triển khai MFA bắt buộc cho toàn bộ nhân viên.
  - **Triển khai các công nghệ phòng thủ đa lớp:** Sử dụng các công cụ bảo vệ hạ tầng như tường lửa ứng dụng web (WAF) và hệ thống phát hiện/ngăn chặn xâm nhập (IDS/IPS) để giám sát và chặn các cuộc tấn công tự động.
  - **Đầu tư vào các giải pháp tiên tiến:** Từng bước nghiên cứu và triển khai các công nghệ xác thực không mật khẩu (passwordless) như FIDO2 và Passkeys để loại bỏ hoàn toàn rủi ro từ mật khẩu truyền thống.

- **Phát triển Kế hoạch Ứng phó Sự cố (Incident Response Plan):** Xây dựng một kế hoạch chi tiết, có cấu trúc để ứng phó khi sự cố xảy ra, đồng thời tổ chức đào tạo và diễn tập định kỳ cho đội ngũ nhân viên.
- **Nâng cao nhận thức:** Thường xuyên giáo dục và đào tạo nhân viên về các mối đe dọa từ tấn công mật khẩu và các kỹ thuật xã hội.

Bằng cách kết hợp các biện pháp phòng thủ này, các tổ chức và cá nhân có thể xây dựng một lá chắn bảo vệ kiên cố và chủ động, giảm thiểu rủi ro và thiệt hại trong một thế giới số đầy rẫy mối đe dọa.

Nguồn trích dẫn

1. KỸ THUẬT PASSWORD ATTACK – SAIGONLAB, truy cập vào tháng 9 10, 2025, https://www.saigonlab.edu.vn/ki-thuat-password-attack.html
2. Tấn công brute-force là gì? Cách phòng chống tấn công vét cạn - LPTech, truy cập vào tháng 9 10, 2025, https://lptech.asia/kien-thuc/tan-cong-brute-force-la-gi
3. Tấn công brute-force là gì? - Viblo.asia, truy cập vào tháng 9 10, 2025, https://viblo.asia/p/tan-cong-brute-force-la-gi-oOVlYbz458W
4. Tấn công qua mạng là gì? | Microsoft Security, truy cập vào tháng 9 10, 2025, https://www.microsoft.com/vi-vn/security/business/security-101/what-is-a-cyberattack
5. Brute Force Attack là gì? Cách hoạt động, mối đe dọa và giải pháp ..., truy cập vào tháng 9 10, 2025, https://viettelidc.com.vn/tin-tuc/brute-force-attack-la-gi-va-lam-the-nao-de-chong-cho-wordpress
6. 6 cách để hacker có thể phá mật khẩu - Aptech Việt Nam, truy cập vào tháng 9 10, 2025, https://aptechvietnam.com.vn/6-cach-de-hacker-co-the-pha-mat-khau/
7. Tấn công Brute Force: Bảo vệ mật khẩu - Kaspersky, truy cập vào tháng 9 10, 2025, https://www.kaspersky.com.vn/resource-center/definitions/brute-force-attack
8. en.wikipedia.org, truy cập vào tháng 9 10, 2025, https://en.wikipedia.org/wiki/Dictionary_attack
9. Cách Hacker Đánh Cắp Mật Khẩu Của Bạn - Locker Password Manager, truy cập vào tháng 9 10, 2025, https://locker.io/vi/blog/hacker-danh-cap-mat-khau
10. Tấn công Password Spraying Attack - Cookie Arena - Penetration ..., truy cập vào tháng 9 10, 2025, https://cookiearena.org/hoc-pentester/tan-cong-password-spraying-attack/
11. What Is Credential Stuffing? How to Detect and Prevent - Fortinet, truy cập vào tháng 9 10, 2025, https://www.fortinet.com/resources/cyberglossary/credential-stuffing
12. What Is Credential Stuffing? - Palo Alto Networks, truy cập vào tháng 9 10, 2025, https://www.paloaltonetworks.com/cyberpedia/credential-stuffing
13. Tạo và sử dụng mật khẩu mạnh - Hỗ trợ của Microsoft, truy cập vào tháng 9 10,

2025, https://support.microsoft.com/vi-vn/windows/t%E1%BA%A1o-v%C3%A0-s%E1%BB%AD-d%E1%BB%A5ng-m%E1%BA%ADt-kh%E1%BA%A9u-m%E1%BA%A1nh-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb
14. Làm thế nào để chống lại các cuộc tấn công credential stuffing, truy cập vào tháng 9 10, 2025, https://ictvietnam.vn/lam-the-nao-de-chong-lai-cac-cuoc-tan-cong-credential-stuffing-39858.html
15. www.kaspersky.com, truy cập vào tháng 9 10, 2025, https://www.kaspersky.com/resource-center/definitions/what-is-password-spraying#:~:text=What%20is%20a%20password%20spraying,on%20to%20try%20another%20one.
16. What Is Password Spraying? - Palo Alto Networks, truy cập vào tháng 9 10, 2025, https://www.paloaltonetworks.com/cyberpedia/password-spraying
17. Tấn công Password Spraying là gì? Dấu hiệu, Hậu quả & Cách phòng - InterData, truy cập vào tháng 9 10, 2025, https://interdata.vn/blog/tan-cong-password-spraying-la-gi/
18. What's a Rainbow Table Attack—and How Can You Stop It? - Huntress, truy cập vào tháng 9 10, 2025, https://www.huntress.com/cybersecurity-101/topic/rainbow-table-defined
19. Rainbow Table Attack Explained - StrongDM, truy cập vào tháng 9 10, 2025, https://www.strongdm.com/what-is/rainbow-table-attack
20. Top 10 công cụ hack tốt nhất cho các nhà nghiên cứu an ninh-Phiên bản 2017 - Aptech, truy cập vào tháng 9 10, 2025, https://aptechvietnam.com.vn/top-10-cong-cu-hack-tot-nhat/
21. John the Ripper - Wikipedia, truy cập vào tháng 9 10, 2025, https://en.wikipedia.org/wiki/John_the_Ripper
22. HYDRA Brute Force - NetWitness Community, truy cập vào tháng 9 10, 2025, https://community.netwitness.com/s/article/HYDRABruteForce?
23. Hydra or the Password Auditor: the best tool for brute-force attacks - Pentest-Tools.com, truy cập vào tháng 9 10, 2025, https://pentest-tools.com/vs/hydra
24. en.wikipedia.org, truy cập vào tháng 9 10, 2025, https://en.wikipedia.org/wiki/Phishing
25. Tính năng bảo vệ bằng mật khẩu là gì? | Microsoft Security, truy cập vào tháng 9 10, 2025, https://www.microsoft.com/vi-vn/security/business/security-101/what-is-password-protection
26. Các hình thức tấn công mạng phổ biến hiện nay - VNTT, truy cập vào tháng 9 10, 2025, https://vntt.com.vn/cac-hinh-thuc-tan-cong-mang/
27. Keystroke logging, truy cập vào tháng 9 10, 2025, https://en.wikipedia.org/wiki/Keystroke_logging
28. What Is A Keylogger? Definition And Types - Fortinet, truy cập vào tháng 9 10, 2025, https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers
29. Hacker đánh cắp mật khẩu bằng phương pháp phân tích chuyển động ngón tay,

truy cập vào tháng 9 10, 2025, https://nhandan.vn/hacker-danh-cap-mat-khau-bang-phuong-phap-phan-tich-chuyen-dong-ngon-tay-post278270.html
30. - An toàn, an ninh thông tin - Tấn công mạng gia tăng ảnh hưởng đến hành vi tiêu dùng như thế nào? - tỉnh Lâm Đồng, truy cập vào tháng 9 10, 2025, https://lamdong.gov.vn/sites/stttt/cntt/an-ninh-thong-tin/SitePages/Tan-cong-mang-gia-tang-anh-huong-den-hanh-vi-tieu-dung-nhu-the-nao.aspx
31. Credential stuffing - Wikipedia, truy cập vào tháng 9 10, 2025, https://en.wikipedia.org/wiki/Credential_stuffing
32. Công cụ tạo mật khẩu mạnh ngẫu nhiên - Locker Password Manager, truy cập vào tháng 9 10, 2025, https://locker.io/vi/password-generator
33. 10 Cách Bảo Mật Thông Tin Cá Nhân Hiệu Quả Trên Môi Trường Mạng, truy cập vào tháng 9 10, 2025, https://locker.io/vi/blog/cach-bao-mat-thong-tin-ca-nhan
34. Brute Force Attack là gì? 5 cách phòng chống Brute Force Attack mà người dùng nên biết, truy cập vào tháng 9 10, 2025, https://viettelidc.com.vn/tin-tuc/brute-force-attack-la-gi-5-cach-phong-chong-brute-force-attack-ma-nguoi-dung-nen-biet-3017
35. Quản lý mật khẩu trong Chrome - Android - Google Chrome Trợ giúp, truy cập vào tháng 9 10, 2025, https://support.google.com/chrome/answer/95606?hl=vi&co=GENIE.Platform%3DAndroid
36. Quản lý mật khẩu trong Chrome - Máy tính - Google Chrome Trợ giúp, truy cập vào tháng 9 10, 2025, https://support.google.com/chrome/answer/95606?hl=vi&co=GENIE.Platform%3DDesktop
37. Thay đổi mật khẩu không an toàn trong Tài khoản Google của bạn, truy cập vào tháng 9 10, 2025, https://support.google.com/accounts/answer/9457609?hl=vi
38. Cách Chrome bảo vệ mật khẩu của bạn - Google Chrome Trợ giúp, truy cập vào tháng 9 10, 2025, https://support.google.com/chrome/answer/10311524?hl=vi
39. Làm cách nào để bật tính năng xác thực hai yếu tố hoặc xác thực đa yếu tố cho tài khoản của tôi? | Thư viện kiến thức KnowBe4, truy cập vào tháng 9 10, 2025, https://support.knowbe4.com/hc/vi/articles/225681448-L%C3%A0m-c%C3%A1ch-n%C3%A0o-%C4%91%E1%BB%83-b%E1%BA%ADt-t%C3%ADnh-n%C4%83ng-x%C3%A1c-th%E1%BB%B1c-hai-y%E1%BA%BFu-t%E1%BB%91-ho%E1%BA%B7c-x%C3%A1c-th%E1%BB%B1c-%C4%91a-y%E1%BA%BFu-t%E1%BB%91-cho-t%C3%A0i-kho%E1%BA%A3n-c%E1%BB%A7a-t%C3%B4i
40. Xác thực đa yếu tố (MFA) | Microsoft Security, truy cập vào tháng 9 10, 2025, https://www.microsoft.com/vi-vn/security/business/identity-access/microsoft-entra-mfa-multi-factor-authentication
41. Hướng dẫn 5 cách khắc phục nguy cơ bị tấn công mạng - Song Hùng, truy cập vào tháng 9 10, 2025, https://songhung.vn/khac-phuc-nguy-co-bi-tan-cong-mang
42. What is Passwordless Authentication? - CyberArk, truy cập vào tháng 9 10, 2025, https://www.cyberark.com/what-is/passwordless-authentication/
43. Microsoft Entra passwordless sign-in - Microsoft Entra ID | Microsoft ..., truy cập

vào tháng 9 10, 2025, https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless
44. FIDO 2 là gì? Phương thức xác thực chuẩn FIDO có an toàn không? - HPT Tech Store, truy cập vào tháng 9 10, 2025, https://hpttechstore.com/blogs/news/fido-2-la-gi-phuong-thuc-xac-thuc-chuan-fido-co-an-toan-khong
45. Passkey là gì và các câu hỏi thường gặp với passkey - Gu Công Nghệ, truy cập vào tháng 9 10, 2025, https://gucongnghe.com/passkey-la-gi/
46. What Are Passkeys? What Is a Passkey? Passkey Authentication Explained, truy cập vào tháng 9 10, 2025, https://www.passkeys.com/what-are-passkeys
47. Các hình thức tấn công Brute Force và cách phòng chống, truy cập vào tháng 9 10, 2025, https://comlink.vn/tan-cong-brute-force/
48. Khôi phục tài khoản có thể bị tấn công - Security in a Box, truy cập vào tháng 9 10, 2025, https://securityinabox.org/vi/communication/account-compromise/
49. Các dấu hiệu nhận biết thiết bị của bạn đang bị hacker xâm nhập - DigiBit, truy cập vào tháng 9 10, 2025, https://digibit.vn/dau-hieu-hacker-xam-nhap/
50. Cách xử lý khi các tài khoản mạng bị tấn công, truy cập vào tháng 9 10, 2025, https://mst.gov.vn/cach-xu-ly-khi-cac-tai-khoan-mang-bi-tan-cong-197143529.htm
51. Tài khoản bị đánh cắp (hack) - Hỗ trợ Garena, truy cập vào tháng 9 10, 2025, https://hotro.garena.vn/faq/tai-khoan-bi-danh-cap-hack_287/
52. Phải làm gì khi tài khoản bị hack? - WhiteHat.vn, truy cập vào tháng 9 10, 2025, https://whitehat.vn/threads/phai-lam-gi-khi-tai-khoan-bi-hack.17400/
53. 6 Phases in the Incident Response Plan - Security Metrics, truy cập vào tháng 9 10, 2025, https://www.securitymetrics.com/blog/6-phases-incident-response-plan
54. How to Create a Cybersecurity Incident Response Plan - Hyperproof, truy cập vào tháng 9 10, 2025, https://hyperproof.io/resource/cybersecurity-incident-response-plan/
55. Công cụ AI bẻ khóa 51% mật khẩu thông thường trong 1 phút | Truyền hình Quốc hội Việt Nam - YouTube, truy cập vào tháng 9 10, 2025, https://www.youtube.com/watch?v=vbQY43O__U4
56. Tin tặc dùng AI để dò mật khẩu người dùng | Báo Dân trí, truy cập vào tháng 9 10, 2025, https://dantri.com.vn/cong-nghe/tin-tac-dung-ai-de-do-mat-khau-nguoi-dung-20250516155036316.htm
57. AI cho An ninh mạng là gì? | Microsoft Security, truy cập vào tháng 9 10, 2025, https://www.microsoft.com/vi-vn/security/business/security-101/what-is-ai-for-cybersecurity
58. Bảo mật AI là gì? Bảo vệ hệ thống AI | Microsoft Security, truy cập vào tháng 9 10, 2025, https://www.microsoft.com/vi-vn/security/business/security-101/what-is-ai-security