LỚP TẬP HUẤN AN NINH MẠNG

Buổi 1 - Bảo mật tài khoản và phòng chống tấn công giả mạo

Mục tiêu của Buổi 1

- Hiểu rõ bộ ba nguyên lý an ninh mạng CIA để áp dụng vào xử lý tài liệu.
- Biết cách nhận diện các chiêu trò lừa đảo trực tuyến phổ biến.
- Nắm vững kỹ thuật tạo mật khẩu mạnh và quản lý tài khoản an toàn.
- Hoàn thành bài thực hành nhận diện email lừa đảo và quản lý mật khẩu.

Phần 1

Tổng quan về An ninh mạng

01 **Khái niệm cơ bản**

Khái niệm cơ bản về an ninh mạng trong môi trường số.

02 **Vai trò**

Vai trò của an ninh mạng đối với cơ quan quản lý nhà nước.

03 **Các nguy cơ mất an ninh mạng**

Các nguy cơ mất an ninh mạng từ thói quen người dùng cuối.

Khái niệm An ninh mạng là gì?

Là việc bảo vệ thông tin
và các hệ thống thông tin.

Tránh các hành vi truy cập, sử dụng,
tiết lộ, sửa đổi hoặc phá hoại trái phép.

Nhằm bảo đảm tính liên tục
và độ tin cậy của các dịch vụ công vụ.

Tránh các thiệt hại về tài chính
và uy tín của cơ quan, đơn vị.

Tầm quan trọng của an ninh mạng

- Bảo vệ dữ liệu cá nhân của người dân khi làm thủ tục hành chính.
- Bảo vệ bí mật nhà nước, tài liệu nội bộ của cơ quan trước kẻ xấu.
- Đảm bảo các hệ thống công dịch vụ công hoạt động ổn định và thông suốt.
- Tránh các thiệt hại về tài chính và uy tín của cơ quan, đơn vị.

Rủi ro phổ biến trong mỗi trường cơ quan

01 Lộ lọt văn bản mật do gửi qua các kênh chat chưa được kiểm duyệt.

02 Máy tính bị nhiễm virus lây lan từ thiết bị USB của đồng nghiệp.

03 Mất quyền truy cập tài khoản thư điện tử công vụ do lộ mật khẩu.

04 Bị lừa đảo chuyển tiền từ các cuộc gọi mạo danh lãnh đạo cơ quan pháp luật.

Tình hình an ninh mạng tại Việt Nam và thế giới

- **Tấn công mạng** ngày càng gia tăng về quy mô và tính chất phức tạp.
- **Tại thế giới** - Các vụ rò rỉ dữ liệu khổng lồ, tấn công ransomware tê liệt cơ sở hạ tầng trong yếu (y tế, năng lượng).
- **Tại Việt Nam** - Nhiều cơ quan nhà nước, doanh nghiệp tài chính bị tấn công ransomware mã hóa dữ liệu gây ngưng trệ dịch vụ.
- **Yếu tố con người** - Hơn 90% các sự cố mất an ninh mạng bắt nguồn từ thói quen sơ hở của người dùng cuối.

Nguy cơ tấn công mạng sử dụng trí tuệ nhân tạo (AI)

01 ● **Sự phát triển của AI**

Sự phát triển của AI cung cấp cho tin tặc những công cụ tấn công tinh vi hơn:

02 ● **AI viết email lừa đảo (Phishing)**

Viết thư lừa đảo tự động, cá nhân hóa cực kỳ trôi chảy, không sai lỗi chính tả hay ngữ pháp, rất khó nhận biết.

03 ● **AI quét lỗ hổng**

Tự động rà quét và tìm ra điểm yếu bảo mật trên máy tính, hệ thống của cơ quan trong vài giây.

04 ● **Deepfake giả mạo hình ảnh và giọng nói**

Nguy cơ lớn nhất hiện nay.

Hiểm họa từ công nghệ Deepfake sử dụng AI

01

Cách thức hoạt động

- Kẻ xấu sử dụng AI **để học hình ảnh**, giọng nói của một người (lãnh đạo, đồng nghiệp, người thân).

02

Kịch bản lừa đảo

- Thực hiện cuộc gọi video giả danh người thân gặp tai **nạn cần** tiền gấp, hoặc giả danh Lãnh đạo cơ quan **chỉ** đạo chuyển tiền hoặc gửi tài liệu gấp.

03

Đặc điểm nhận diện

- Hình ảnh chuyển động hơi giật, giọng nói hơi đơ, cuộc gọi thường rất ngắn với lý do "mạng yếu" để tránh bị phát hiện.

Cảnh giác – Xác minh – Bảo vệ

Luôn xác minh thông tin qua nhiều kênh trước khi thực hiện bất kỳ giao dịch quan trọng nào.

Bộ ba nguyên lý bảo mật CIA

Mọi giải pháp an ninh mạng đều xoay quanh việc bảo vệ **3 thuộc tính:**

C — Confidentiality (Tính Bí mật)

Đảm bảo thông tin chỉ được truy cập bởi những người được ủy quyền.

Ví dụ
Bảo vệ dữ liệu khách hàng, thông tin nội bộ, tài liệu mật.

I — Integrity (Tính Toàn vẹn)

Đảm bảo thông tin luôn chính xác, không bị thay đổi hoặc phá hoại trái phép.

Ví dụ
Chống sửa đổi dữ liệu, bảo vệ tính chính xác của giao dịch, báo cáo.

A — Availability (Tính Sẵn sàng)

Đảm bảo hệ thống và dữ liệu luôn sẵn sàng khi người dùng hợp lệ cần truy cập.

Ví dụ
Đảm bảo hệ thống hoạt động ổn định, giảm thiểu thời gian gián đoạn dịch vụ.

Tính Bí mật (Confidentiality) là gì?

Tính Bí mật (Confidentiality)
là nguyên tắc đảm bảo thông tin chỉ được truy cập bởi những người có thẩm quyền.

Đảm bảo thông tin
chỉ được tiếp cận bởi những người có thẩm quyền.

Ngăn chặn người không phận sự
đọc hoặc sao chép thông tin trái phép.

Là thuộc tính hàng đầu
trong quản lý tài liệu lưu hành nội bộ và tài liệu mật.

Nguy cơ vi phạm tính Bí mật

01 **Để lộ mật khẩu**
máy tính cho đồng nghiệp hoặc người ngoài cơ quan.

02 **Chụp ảnh tài liệu nội bộ**
đăng tải lên các hội nhóm mạng xã hội công cộng.

03 **Soạn thảo tài liệu mật**
trên máy tính kết nối Internet không an toàn.

04 **Gửi nhầm file nhạy cảm**
cho địa chỉ email lạ.

unknown@email.com

Hậu quả có thể xảy ra:

- Rò rỉ thông tin nội bộ, bí mật kinh doanh.
- Thiệt hại tài chính, mất uy tín.
- Vi phạm pháp luật, bị xử phạt.
- Ảnh hưởng đến khách hàng, đối tác và tổ chức.

Nguy cơ vi phạm tính Bí mật

01 **Để lộ mật khẩu**
máy tính cho đồng nghiệp hoặc người ngoài cơ quan.

02 **Chụp ảnh tài liệu nội bộ**
đăng tải lên các hội nhóm mạng xã hội công cộng.

03 **Soạn thảo tài liệu mật**
trên máy tính kết nối Internet không an toàn.

04 **Gửi nhầm file nhạy cảm**
cho địa chỉ email lạ.

unknown@email.com

Hậu quả có thể xảy ra:

- Rò rỉ thông tin nội bộ, bí mật kinh doanh.
- Thiệt hại tài chính, mất uy tín.
- Vi phạm pháp luật, bị xử phạt.
- Ảnh hưởng đến khách hàng, đối tác và tổ chức.

Tính Toàn vẹn (Integrity) là gì?

01

Đảm bảo thông tin luôn chính xác và đầy đủ.

Dữ liệu không bị sai lệch, thiếu sót khi lưu trữ, xử lý hoặc truyền đi.

02

Ngăn chặn việc sửa đổi, xóa bỏ hoặc chèn thêm thông tin trái phép.

Chỉ những người có thẩm quyền mới được phép thay đổi dữ liệu.

03

Bảo đảm dữ liệu không bị sai lệch trong quá trình truyền gửi qua mạng.

Dữ liệu được kiểm tra và xác thực để phát hiện mọi thay đổi trái phép.

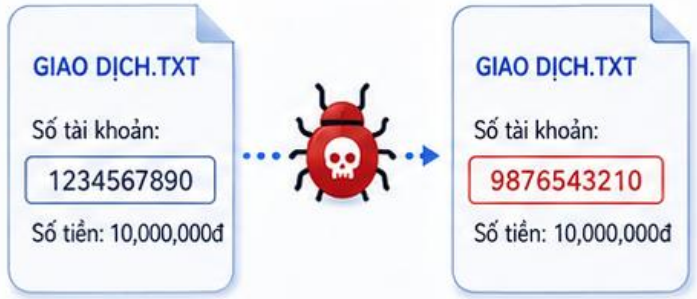
Tóm lại

Tính Toàn vẹn đảm bảo dữ liệu luôn nguyên vẹn, tin cậy và đúng như ban đầu, từ khi tạo ra cho đến khi được sử dụng.

Nguy cơ vi phạm tính Toàn vẹn

01 Mã độc tự động thay đổi thông tin số tài khoản trong tệp tin giao dịch.

Phần mềm độc hại có thể âm thầm sửa đổi số tài khoản, số tiền hoặc nội dung trong tệp giao dịch.



Dữ liệu bị thay đổi mà người dùng không hề hay biết.

02 Hacker can thiệp sửa đổi nội dung quyết định hành chính trước khi gửi đi.

Kẻ tấn công có thể thay đổi nội dung văn bản, quyết định, hợp đồng hoặc thông tin quan trọng trước khi được gửi đến người nhận.

Quyết định có thể bị sai lệch, gây thiệt hại về tài chính và uy tín.

03 Lỗi phần cứng hoặc lỗi đường truyền mạng làm mất mát một phần số liệu báo cáo.

Dữ liệu có thể bị lỗi, mất gói tin hoặc ghi không đầy đủ trong quá trình truyền hoặc lưu trữ.

Báo cáo không đầy đủ, sai lệch thông tin, ảnh hưởng đến hiệu quả công việc.

Hậu quả chung:

Dữ liệu không còn nguyên vẹn, dẫn đến quyết định sai lầm, thiệt hại tài chính, mất niềm tin và vi phạm pháp luật.

Các biện pháp bảo vệ tính Toàn vẹn

01

Sử dụng chữ ký số

để xác thực nguồn gốc và nội dung văn bản.

- Đảm bảo người gửi là thật và nội dung không bị thay đổi.

02

Áp dụng các thuật toán kiểm tra tính toàn vẹn

(như mã băm MD5, SHA-256).

- Kiểm tra và đối chiếu giá trị băm để phát hiện thay đổi dữ liệu.

03

Cấu hình phân quyền chỉ đọc (Read-only)

đối với các thư mục dữ liệu chung.

- Ngăn chặn việc sửa đổi, xóa hoặc ghi đè dữ liệu trái phép.

04

Quét virus tệp tin thường xuyên

để phát hiện mã độc chỉnh sửa file.

- Giúp đảm bảo tệp tin an toàn trước khi mở, sử dụng hoặc chia sẻ.

Lợi ích:

- Đảm bảo dữ liệu chính xác, tin cậy
- Ngăn chặn thay đổi trái phép
- Đáp ứng yêu cầu kiểm soát và tuân thủ
- Nâng cao hiệu quả và độ tin cậy hệ thống

Tính Sẵn sàng (Availability) là gì?

1. Đảm bảo dữ liệu và hệ thống luôn sẵn sàng phục vụ khi người dùng cần.

Người dùng có thể truy cập và sử dụng dữ liệu, hệ thống bất cứ lúc nào, ở bất cứ đâu.

2. Bảo đảm các hoạt động hành chính công không bị ngắt quãng.

Hệ thống hoạt động ổn định, giảm thiểu gián đoạn, duy trì hiệu suất và năng suất công việc.

3. Cung cấp dịch vụ công trực tuyến liên tục cho người dân và doanh nghiệp.

Đáp ứng nhu cầu sử dụng dịch vụ mọi lúc, mọi nơi, nâng cao sự hài lòng và tin cậy.

Tóm lại: Tính Sẵn sàng giúp hệ thống và dịch vụ luôn hoạt động liên tục, ổn định, không gián đoạn, đáp ứng kịp thời nhu cầu của người dùng.

Tính Sẵn sàng (Availability) là gì?

01

Đảm bảo dữ liệu và hệ thống luôn sẵn sàng phục vụ khi người dùng cần.

Người dùng có thể truy cập và sử dụng dữ liệu, hệ thống bất cứ lúc nào, ở bất cứ đâu.

02

Bảo đảm các hoạt động hành chính công không bị ngắt quãng.

Hệ thống hoạt động ổn định, giảm thiểu gián đoạn, duy trì hiệu suất và năng suất công việc.

03

Cung cấp dịch vụ công trực tuyến liên tục cho người dân và doanh nghiệp.

Đáp ứng nhu cầu sử dụng dịch vụ mọi lúc, mọi nơi, nâng cao sự hài lòng và tin cậy.

Tóm lại: Tính Sẵn sàng giúp hệ thống và dịch vụ luôn hoạt động liên tục, ổn định, không gián đoạn, đáp ứng kịp thời nhu cầu của người dùng.

Nguy cơ vi phạm tính Sẵn sàng

01

Máy chủ dữ liệu bị ngưng hoạt động do sự cố mất điện hoặc lỗi phần cứng.

Sự cố về điện hoặc hỏng hóc phần cứng có thể khiến hệ thống và dữ liệu không thể truy cập.

02

Mã độc tống tiền Ransomware khóa toàn bộ dữ liệu máy tính của cán bộ.

Ransomware mã hóa dữ liệu, yêu cầu tiền chuộc để khôi phục, gây gián đoạn nghiêm trọng hoạt động.

03

Kẻ xấu thực hiện tấn công từ chối dịch vụ làm treo cổng dịch vụ công của tỉnh.

Tấn công DDoS làm quá tải hệ thống, khiến dịch vụ không thể truy cập bởi người dân và doanh nghiệp.

Hậu quả:

Gián đoạn dịch vụ, ảnh hưởng đến công việc và hoạt động của người dùng, gây thiệt hại về thời gian, uy tín và chi phí khắc phục.

Các biện pháp bảo vệ tính Sẵn sàng

01

Xây dựng hệ thống nguồn điện dự phòng UPS và máy phát điện cho phòng máy chủ.

Đảm bảo hệ thống luôn có nguồn điện ổn định, liên tục ngay cả khi mất điện lưới, giảm thiểu gián đoạn dịch vụ.

02

Thực hiện sao lưu dữ liệu thường xuyên để sẵn sàng khôi phục khi gặp sự cố.

Sao lưu theo nhiều phiên bản và lưu trữ ở vị trí an toàn, kiểm tra khả năng khôi phục định kỳ.

03

Cài đặt phần mềm diệt virus bản quyền để ngăn ngừa ransomware phá hoại.

Cập nhật thường xuyên, bật tính năng bảo vệ thời gian thực, quét định kỳ để phát hiện và xử lý sớm mối đe dọa.

04

Thiết lập hệ thống tường lửa để ngăn chặn các cuộc tấn công mạng gây nghẽn băng thông.

Cấu hình tường lửa, IDS/IPS và giới hạn lưu lượng hợp lý để phát hiện, chặn đứng các cuộc tấn công DDoS và truy cập trái phép.

Lợi ích:

- Hệ thống hoạt động liên tục, ổn định
- Giảm thiểu gián đoạn, tăng hiệu suất
- Bảo vệ dữ liệu và uy tín tổ chức
- Tiết kiệm chi phí khắc phục và thời gian downtime

Phần 2 - Tấn công tâm lý và giả mạo (Social Engineering & Phishing)

01 Khái niệm về các kỹ thuật thao túng tâm lý con người.

- Tấn công tâm lý (Social Engineering) là việc khai thác tâm lý, hành vi để lừa người dùng tiết lộ thông tin hoặc thực hiện hành động có lợi cho kẻ tấn công.
- Kẻ tấn công không khai thác lỗ hổng kỹ thuật mà khai thác yếu tố con người.
- Mục tiêu: chiếm được niềm tin, sự tò mò, lòng sợ hãi, sự cả tin, lòng tham,...

02 Cách thức kẻ xấu triển khai các đợt tấn công giả mạo.

- Giả mạo email, tin nhắn, cuộc gọi, website, hoặc người quen, cơ quan, tổ chức uy tín.
- Dẫn dụ người dùng nhấp vào liên kết độc hại, tải tệp, cung cấp thông tin đăng nhập, mã OTP, thông tin cá nhân, tài chính.
- Kịch bản thường tạo cảm giác khẩn cấp, hấp dẫn hoặc đáng tin cậy để gây mất cảnh giác.

03 Các dấu hiệu nhận diện hành vi lừa đảo trực tuyến.

- Email/tin nhắn có lỗi chính tả, ngữ pháp; địa chỉ gửi lạ hoặc đáng ngờ.
- Yêu cầu cung cấp thông tin nhạy cảm, mật khẩu, mã OTP.
- Liên kết không rõ nguồn gốc, khác tên miền chính thức.
- Tạo áp lực thời gian, đe dọa khóa tài khoản hoặc hứa hẹn phần thưởng quá hấp dẫn.
- Nội dung không nhất quán, thiếu thông tin liên hệ chính thống.

Lưu ý: Luôn kiểm tra kỹ trước khi nhấp vào liên kết, tải tệp hoặc cung cấp thông tin.

✓ Xác minh nguồn gốc | ✓ Không chia sẻ thông tin nhạy cảm | ✓ Báo cáo khi nghi ngờ lừa đảo | ✓ Cập nhật kiến thức an toàn thông tin

Tấn công tâm lý là gì?

Tấn công tâm lý (Social Engineering) là phương pháp khai thác yếu tố con người để đánh lừa, lợi dụng và chiếm đoạt thông tin hoặc gây thiệt hại.

01

Là phương pháp lừa đảo dựa trên việc thao túng hành vi của con người.

Kẻ tấn công sử dụng tâm lý, cảm xúc, sự tin tưởng hoặc mối quan hệ để thuyết phục nạn nhân làm theo yêu cầu, vô tình tiết lộ thông tin hoặc thực hiện hành động có hại.

02

Không tập trung vào lỗi kỹ thuật của máy tính mà khai thác điểm yếu con người.

Thay vì tấn công hệ thống bằng công cụ kỹ thuật, kẻ tấn công nhắm vào sự thiếu cảnh giác, thiếu hiểu biết hoặc tâm lý tin tưởng của người dùng để đạt mục đích.

03

Kẻ xấu tìm cách chiếm lòng tin hoặc tạo ra sự sợ hãi để lấy thông tin.

Các chiêu trò thường lợi dụng sự tò mò, lòng tham, sự sợ hãi, áp lực thời gian, sự cả tin hoặc mong muốn được giúp đỡ để khiến nạn nhân chủ động cung cấp thông tin hoặc thực hiện yêu cầu.

Lưu ý: Hiểu đúng về tấn công tâm lý giúp chúng ta nâng cao cảnh giác, bảo vệ thông tin cá nhân và hệ thống.

Cơ chế lợi dụng tâm lý của kẻ xấu

Kẻ xấu thường đánh vào các trạng thái tâm lý sau để người dùng mất cảnh giác:

Sự sợ hãi - Đe dọa khóa tài khoản hoặc báo cáo kỷ luật nếu không làm theo.

→ Ví dụ: "Tài khoản của bạn sẽ bị khóa trong 24 giờ nếu không xác minh ngay."

Lòng tham - Hứa hẹn trao quà tặng, giải thưởng hoặc cơ hội thăng tiến.

→ Ví dụ: "Bạn may mắn nhận được iPhone miễn phí, nhấp vào để nhận ngay!"

Sự tò mò - Gửi liên kết giật gân, tệp tin chứa thông tin nhạy cảm hư cấu.

→ Ví dụ: "Xem ngay ảnh bạn bè trong video này!" hoặc "Tệp tài liệu nội bộ quan trọng."

Lòng tốt - Giả danh đồng nghiệp đang gặp nạn cần mượn tiền gấp.

→ Ví dụ: "Mình đang gấp, tài khoản bị lỗi, bạn chuyển giúp mình 2 triệu nhé."

Ghi nhớ: Nhận diện cảm xúc đang bị tác động là bước đầu tiên để không trở thành nạn nhân của tấn công tâm lý.

Nhận thức về Tấn công giả mạo (Phishing)

01

Là hình thức tấn công tâm lý phổ biến nhất hiện nay trên môi trường số.

Kẻ tấn công giả mạo các tổ chức hoặc cá nhân đáng tin cậy để tạo niềm tin, sau đó lừa người dùng thực hiện hành động có lợi cho chúng.

02

Kẻ tấn công giả mạo làm các tổ chức uy tín (cơ quan nhà nước, ngân hàng).

Chúng tạo email, tin nhắn, website giả mạo giống thật đến mức khó phân biệt, khiến người dùng dễ dàng tin tưởng và làm theo yêu cầu.

03

Mục tiêu là dụ dỗ người dùng cung cấp mật khẩu, mã OTP hoặc mã PIN.

Những thông tin này giúp kẻ tấn công chiếm quyền truy cập tài khoản, đánh cắp dữ liệu, chiếm đoạt tài sản hoặc phát tán mã độc.

Hãy luôn cảnh giác!

Kiểm tra kỹ địa chỉ email, đường link.

Không cung cấp mật khẩu, OTP, PIN cho bất kỳ ai.

Khi nghi ngờ, hãy liên hệ trực tiếp với tổ chức qua kênh chính thức.

Các kênh tấn công giả mạo phổ biến

01

Hòm thư điện tử (Email Phishing)

Gửi thư điện tử chứa liên kết độc hại hoặc tệp đính kèm.

- Mạo danh tổ chức, đối tác hoặc người quen để lừa bạn nhấp vào link hoặc mở file chứa mã độc.

02

Tin nhắn di động (SMS Phishing)

Gửi tin nhắn SMS giả mạo thương hiệu ngân hàng, dịch vụ, cơ quan.

- Lừa bạn truy cập vào đường link giả mạo để đánh cắp thông tin đăng nhập, mã OTP hoặc thông tin cá nhân.

03

Tin nhắn Zalo/Facebook

Sử dụng tài khoản mạng xã hội bị chiếm đoạt để liên hệ và gửi link lừa đảo.

- Mạo danh bạn bè, người thân hoặc đồng nghiệp để tạo lòng tin, rồi dẫn dụ bạn truy cập link độc hại hoặc cung cấp thông tin.

04

Cuộc gọi thoại (Vishing)

Cuộc gọi tự động hoặc do kẻ xấu giả danh công an, tòa án, ngân hàng...

- Dọa nạt, yêu cầu xác minh thông tin, chuyển tiền hoặc cung cấp mã OTP để chiếm đoạt tài sản.

Lưu ý: Luôn cảnh giác với các yêu cầu cung cấp thông tin, mã OTP, mật khẩu. Không nhấp vào link lạ, không mở tệp đính kèm từ nguồn không rõ ràng.

Dấu hiệu nhận biết email giả mạo

1. Địa chỉ email người gửi có tên miền lạ, không khớp với tên hiển thị chính thống.

Ví dụ: hiển thị "Ngân hàng ABC" nhưng email gửi từ `abc-bank.support@gmail.com` hoặc tên miền không liên quan.

2. Lời chào chung chung không ghi rõ họ tên đầy đủ của người dùng.

Ví dụ: "Kính gửi Quý khách hàng", "Xin chào bạn", "Dear Customer"...

3. Nội dung thư chứa nhiều lỗi chính tả hoặc tử ngữ không tự nhiên.

Câu văn lủng củng, sai ngữ pháp, dùng từ bất thường hoặc dịch máy.

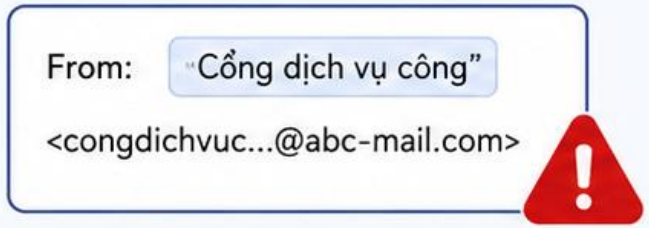
4. Yêu cầu người dùng bấm vào liên kết để xác minh tài khoản khẩn cấp.

Các liên kết thường dẫn đến trang web giả mạo nhằm đánh cắp thông tin đăng nhập, mật khẩu, OTP hoặc dữ liệu cá nhân.

Lưu ý:

- Không bấm vào liên kết hoặc tải file đính kèm từ email đáng ngờ.
- Không cung cấp thông tin đăng nhập, OTP, mã PIN cho bất kỳ ai qua email.
- Khi nghi ngờ, hãy liên hệ trực tiếp với tổ chức qua kênh chính thức.

Cách kiểm tra địa chỉ email người gửi



01 Không chỉ nhìn vào tên hiển thị bên ngoài

Tên hiển thị có thể bị giả mạo.

Ví dụ: tên hiển thị là "Cổng dịch vụ công"
nhưng địa chỉ email thật là congdichvucccong@abc-mail.com

02 Bấm vào chi tiết thông tin người gửi

Trong hầu hết các dịch vụ email (Gmail, Outlook…),
hãy bấm vào tên người gửi hoặc biểu tượng mũi tên/ba chấm
để xem "Show original", "View original" hoặc "Chi tiết thư".
Kiểm tra kỹ địa chỉ email trong phần "From", "Return-Path".

03 Nếu địa chỉ có đuôi tên miền miễn phí hoặc tên miền lạ, đó là giả mạo

Các tổ chức, cơ quan uy tín thường dùng email tên miền riêng
(ví dụ: @cong.gov.vn, @bank.com.vn…), không dùng @gmail.com,
@yahoo.com, @outlook.com hoặc các tên miền lạ.

Ghi nhớ:

- Khi nghi ngờ, không trả lời email, không nhấp vào link, không tải file đính kèm.
- Liên hệ trực tiếp với tổ chức qua kênh chính thức để xác minh.

Phân tích liên kết đáng ngờ

01 **Rà chuột qua liên kết (không click) để xem đường dẫn thực tế hiển thị ở thanh trạng thái.**

Trên máy tính: di chuyển chuột vào liên kết.

Trên điện thoại: nhấn giữ vào liên kết (nếu có tùy chọn xem trước).

02 **Tên miền giả mạo thường có tính viết gần giống tên miền thật** (ví dụ `dichvucong-tinh.xyz`).

Hãy kiểm tra kỹ chính tả, dấu gạch, ký tự đặc biệt, hoặc phần mở rộng tên miền (.xyz, .top, .info…).

03 **Các cổng thông tin chính thức của cơ quan nhà nước Việt Nam luôn dùng đuôi `.gov.vn`.**

Ví dụ: dichvucong.gov.vn, thuế.gov.vn, baohiemxahoi.gov.vn...

Lưu ý:

- Không nhập thông tin cá nhân, tài khoản, mật khẩu vào các trang web không rõ nguồn gốc.
- Khi nghi ngờ, hãy truy cập trực tiếp trang web chính thức bằng cách gõ tên miền vào trình duyệt.
- Liên hệ với cơ quan, tổ chức qua kênh chính thức để xác minh thông tin.

Cách nhận diện tin nhắn SMS giả mạo

01

Kẻ xấu dùng trạm phát sóng di động giả mạo để chèn tin nhắn vào luồng SMS thật.

Tin nhắn có thể hiển thị tên người gửi quen thuộc như ngân hàng, công ty, cơ quan...
nhưng thực chất không phải do họ gửi.

02

Tin nhắn có nội dung thông báo tài khoản bị khóa hoặc phát sinh giao dịch lạ.

Nội dung thường tạo cảm giác khẩn cấp, đe dọa,
gây hoang mang để bạn mất bình tĩnh và làm theo hướng dẫn.

Ví dụ nội dung thường gặp:

- Tài khoản của bạn bị khóa.
- Giao dịch bất thường 10,000,000đ.
- Nhấn vào link để xác thực ngay.
- Nếu không sẽ bị khóa tài khoản.

03

Yêu cầu đăng nhập vào đường link lạ có giao diện giống trang chủ ngân hàng để hủy dịch vụ hoặc xác thực thông tin.

Đây là trang web giả mạo nhằm đánh cắp
tài khoản, mật khẩu, mã OTP của bạn.

Dấu hiệu đường link giả mạo:

- Không dùng tên miền chính thức (.com.vn, .gov.vn).
- Có thêm ký tự lạ, gạch ngang, số...
- Dùng giao thức không an toàn (http://).

Lưu ý quan trọng

- Không bấm vào link lạ, không tải app từ SMS.
- Liên hệ trực tiếp ngân hàng qua số hotline chính thức.
- Kiểm tra kỹ tên miền, nội dung và nguồn gửi trước khi thực hiện.

Cuộc gọi giả danh cơ quan chức năng

- **Đối tượng tự xưng là cán bộ công an, viện kiểm sát hoặc tòa án đang thụ lý vụ án.**

  Họ thường sử dụng lời lẽ nghiêm trọng, đe dọa để tạo áp lực và khiến bạn hoảng sợ.

- **Yêu cầu người dùng chuyển tiền vào "tài khoản tạm giữ" để xác minh nguồn tiền sạch.**

  Họ viện lý do bạn liên quan đến vụ án, rửa tiền, trốn thuế… rồi yêu cầu chuyển tiền ngay để chứng minh vô tội hoặc phục vụ điều tra.

- **Đe dọa sẽ khởi tố, bắt tạm giam nếu người dùng tiết lộ thông tin cuộc gọi cho người khác.**

  Chúng yêu cầu giữ bí mật tuyệt đối, không thông báo cho gia đình hoặc cơ quan khác để dễ dàng thao túng và chiếm đoạt tài sản.

- ***Lưu ý - Cơ quan nhà nước không bao giờ làm việc với công dân qua điện thoại.***

  Mọi yêu cầu cung cấp thông tin cá nhân, tài khoản, mật khẩu, mã OTP hoặc chuyển tiền qua điện thoại đều là giả mạo.

KHUYẾN CÁO

- Không cung cấp thông tin cá nhân qua điện thoại.
- Không cung cấp mật khẩu, mã OTP cho bất kỳ ai.
- Không chuyển tiền vào bất kỳ tài khoản nào theo yêu cầu qua điện thoại.
- Nghi ngờ, hãy liên hệ cơ quan chính thức qua số hotline hoặc đến trực tiếp để xác minh.

Quy tắc ứng xử khi gặp thông tin giả mạo

01 **Giữ bình tĩnh, không thực hiện theo các yêu cầu khẩn cấp của đối tượng.**

Hãy dừng lại, kiểm tra kỹ thông tin trước khi hành động.

02 **Tuyệt đối không bấm vào liên kết lạ hoặc mở các tệp tin đính kèm không rõ nguồn gốc.**

Các liên kết, tệp tin có thể chứa mã độc, đánh cắp thông tin hoặc chiếm quyền thiết bị.

03 **Gọi điện xác minh chéo qua số điện thoại đường dây nóng chính thức của đơn vị liên quan.**

Kiểm tra thông tin qua kênh chính thức để đảm bảo tính chính xác, tránh bị lợi dung.

04 **Chụp ảnh màn hình làm bằng chứng và báo cáo cho bộ phận kỹ thuật công nghệ thông tin.**

Cung cấp đầy đủ thông tin, bằng chứng để hỗ trợ điều tra và ngăn chặn kịp thời.

GHI NHỚ!

Cảnh giác hôm nay – An toàn ngày mai!

Mỗi người đều là lá chắn bảo vệ thông tin cá nhân và an toàn cho cộng đồng.

Phần 3 - Bảo mật mật khẩu và tài khoản

Tầm quan trọng của việc bảo vệ tài khoản cá nhân và công vụ.

- Bảo vệ thông tin cá nhân, dữ liệu và tài sản số.
- Ngăn chặn truy cập trái phép, tránh mất mát và rủi ro pháp lý.
- Đảm bảo hoạt động công việc liên tục và an toàn.

Các kỹ thuật dò quét bẻ khóa mật khẩu của hacker.

- Dò mật khẩu bằng thử sai (brute force).
- Dùng từ điển mật khẩu, khai thác thông tin rò rỉ trên mạng.
- Phishing để đánh cắp mật khẩu và mã xác thực.

Phương pháp xây dựng và quản lý mật khẩu mạnh.

- Sử dụng mật khẩu dài (tối thiểu 12 ký tự), kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- Không dùng thông tin dễ đoán: ngày sinh, số điện thoại, tên,...
- Mỗi tài khoản dùng một mật khẩu khác nhau.
- Bật xác thực 2 lớp (2FA) và thay đổi mật khẩu định kỳ.

GHI NHỚ!

Bảo mật mật khẩu tốt hôm nay – Bảo vệ dữ liệu và công việc của bạn ngày mai.

Khái niệm về mật khẩu mạnh

- **Là mật khẩu có độ dài tốt và độ phức tạp cao** để ngăn chặn việc dò quét tự động.

Ví dụ mật khẩu mạnh:

`T9!kPz#7mQ$2v` | `SongHoa@2024!` | `8vF!rG2#Lp9x`

- ✓ Dài: tối thiểu 12 ký tự
- ✓ Kết hợp: chữ hoa, chữ thường, số và ký tự đặc biệt
- ✓ Không chứa thông tin dễ đoán

- **Khó đoán đối với cả người quen và hệ thống máy tính của hacker.**
  - ✓ Không dùng thông tin cá nhân: tên, ngày sinh, số điện thoại,…
  - ✓ Không dùng mặt khẩu quá đơn giản: 123456, password, qwerty,…
  - ✓ Không dùng mật khẩu đã bị lộ hoặc trùng lặp trên nhiều tài khoản.

Ví dụ mật khẩu yếu:

- ✗ 12345678
- ✗ ngaysinh1990
- ✗ password123
- ✗ tenban@2024

- **Phải dễ nhớ đối với bản thân người dùng** để tránh việc phải ghi chép ra giấy.
  - ✓ Sử dụng cụm từ dễ nhớ với bạn và biến tấu thêm ký tự.
  - ✓ Có thể dùng phương pháp viết tắt có quy tắc riêng.
  - ✓ Không ghi mật khẩu ra giấy, không lưu ở nơi dễ nhìn thấy.

Mẹo ghi nhớ:

Dùng câu hoặc cụm từ dễ nhớ và thay thế ký tự

VD: Tôi yêu bóng đá! → ToiYeuBongDa!
→ T0iYeuBongD@!

GHI NHỚ

Mật khẩu mạnh là lớp bảo vệ đầu tiên giúp giữ an toàn cho tài khoản và thông tin của bạn.
Hãy tạo thói quen sử dụng mật khẩu mạnh cho mọi tài khoản quan trọng!

Hacker bẻ khóa mật khẩu như thế nào?

01 **Hacker không đoán mò bằng tay mà sử dụng các công cụ phần mềm chuyên dụng.**

- Dùng các chương trình chuyên biệt để tự động thử nhiều mật khẩu.
- Công cụ có thể thử hàng triệu đến hàng tỷ tổ hợp mỗi giây.

02 **Có khả năng chạy hàng tỷ phép thử mật khẩu trong một giây.**

- Tận dụng sức mạnh của máy tính hiệu năng cao và buồng máy chủ chuyên dụng.
- Thử rất nhanh tất cả các kết hợp có thể của ký tự.

03 **Khai thác dữ liệu các vụ lộ lọt mật khẩu lớn trên thế giới để làm cơ sở dữ liệu dò quét.**

- Sử dụng các danh sách tài khoản – mật khẩu bị lộ từ nhiều nguồn khác nhau.
- Tự động thử các mật khẩu đã lộ này trên nhiều hệ thống để tìm tài khoản trùng khớp.

Mật khẩu càng đơn giản hoặc trùng với dữ liệu đã bị lộ, nguy cơ bị bẻ khóa càng cao!
Hãy tạo mật khẩu mạnh và thay đổi định kỳ để bảo vệ tài khoản của bạn.

Phương pháp Brute Force tự động

01

Là phương thức tấn công thử sai tất cả các tổ hợp ký tự có thể xảy ra.

- Hệ thống tự động tạo ra và thử lần lượt các mật khẩu.
- Nếu đúng, hacker sẽ truy cập được vào tài khoản.

02

Nếu mật khẩu ngắn (ví dụ chỉ có 6 ký tự số), phần mềm sẽ bẻ khóa chỉ trong vài giây.

- Số lượng tổ hợp ít → thời gian thử nhanh.
- Ví dụ 6 ký tự số: chỉ 1.000.000 (10^6) khả năng.

03

Mật khẩu càng dài, số lượng tổ hợp càng lớn, thời gian bẻ khóa tăng theo cấp số nhân.

- Ví dụ mật khẩu gồm chữ hoa, chữ thường, số và ký tự đặc biệt.
- Mỗi ký tự thêm vào làm tăng nhiều lần số tổ hợp và thời gian bẻ khóa.

Quy trình hoạt động

Phần mềm tự động tạo mật khẩu →

Thử đăng nhập vào hệ thống →

Sai mật khẩu → thử tiếp →

Đúng mật khẩu → truy cập thành công

Lưu ý: Brute Force là phương pháp tấn công bất hợp pháp. Chỉ sử dụng kiến thức này để bảo vệ hệ thống và nâng cao mật khẩu của bạn.

Phương pháp tấn công từ điển

- Phần mềm của hacker sẽ thử **các từ thông dụng** trong từ điển và **danh sách mật khẩu phổ biến.**

- Các mật khẩu như `123456', `password', `admin' hay `iloveyou' sẽ bị bẻ khóa ngay lập tức.

- Kết hợp thêm các thông tin cá nhân thu thập được như **ngày sinh, số điện thoại, tên con cái.**

Quy trình tấn công từ điển

1. Sử dụng từ điển và danh sách mật khẩu phổ biến

2. Thử đăng nhập vào hệ thống bằng mỗi mật khẩu

3. Sai mật khẩu → thử mật khẩu tiếp theo

4. Đúng mật khẩu → truy cập thành công

Lưu ý: Phương pháp tấn công từ điển hiệu quả với mật khẩu yếu hoặc thông tin cá nhân dễ đoán.
Hãy sử dụng mật khẩu mạnh và không sử dụng lại mật khẩu ở nhiều nơi.

Lỗi đặt mật khẩu phổ biến của cán bộ công sở

- **Sử dụng ngày tháng năm sinh hoặc số điện thoại cá nhân làm mật khẩu.**

✓ Ví dụ dễ bị đoán: 19900101, 0909123456, 12121990

✗ Hãy tránh dùng thông tin cá nhân dễ đoán.

- **Dùng chung một mật khẩu duy nhất cho cả email công vụ, zalo và facebook cá nhân.**

✓ Nếu một tài khoản bị lộ, hacker có thể truy cập tất cả các tài khoản còn lại của bạn.

✗ Hãy sử dụng mật khẩu khác nhau cho từng tài khoản.

- **Đặt mật khẩu quá ngắn hoặc dễ đoán gắn liền với tên của cơ quan, đơn vị làm việc.**

✓ Ví dụ dễ đoán: coquan123, phongnhansu, quanly2024

✗ Hãy đặt mật khẩu dài và không liên quan đến thông tin cơ quan, đơn vị.

- **Lưu mật khẩu dưới dạng file Word không đặt mã bảo vệ hoặc viết ra giấy dán ở bàn làm việc.**

✓ File Word dễ bị mở và lộ khi máy nhiễm mã độc hoặc bị người khác truy cập.

✗ Hãy dùng trình quản lý mật khẩu hoặc ghi nhớ an toàn, không lưu trữ công khai.

Lưu ý chung: Mật khẩu mạnh nên dài ít nhất 12 ký tự, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt. Thường xuyên thay đổi mật khẩu và không chia sẻ cho người khác.

Quy tắc đặt mật khẩu dài tối thiểu 12 ký tự

01 Đây là tiêu chuẩn bảo mật bắt buộc của hầu hết các hệ thống thông tin hiện đại.

- Giúp tăng độ an toàn cho tài khoản và dữ liệu của bạn.
- Phù hợp với các quy định và yêu cầu bảo mật hiện hành.

02 Mật khẩu có độ dài 12 ký tự trở lên sẽ làm nản lòng các công cụ Brute Force của hacker.

- Số ký tự càng nhiều, số tổ hợp càng lớn.
- Hacker sẽ mất rất nhiều thời gian và tài nguyên để thử đoán.

Ví dụ: 12 ký tự = $62^{\wedge 12} \approx 3.2 \times 10^{21}$ tổ hợp (một con số cực kỳ lớn)

03 Tăng thời gian bẻ khóa từ vài phút lên hàng nghìn năm.

- Mật khẩu 8 ký tự có thể bị bẻ khóa chỉ trong vài phút.
- Mật khẩu 12+ ký tự có thể khiến hacker mất hàng nghìn năm để bẻ khóa.

Độ dài ký tự tăng 1 chữ số, thời gian bẻ khóa tăng theo cấp số nhân!

Gợi ý mật khẩu mạnh (tối thiểu 12 ký tự)

- ✓ Kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- ✓ Không chứa thông tin cá nhân dễ đoán.
- ✓ Sử dụng cụm từ hoặc câu dễ nhớ để tạo mật khẩu dài.
- ✓ Thay đổi mật khẩu định kỳ.

Mạnh

Ví dụ: Y!euCongNghe@2024_VietNam#AnToan (28 ký tự)

Ví dụ mật khẩu yếu (không nên dùng)

- ✗ 1234567890 → quá đơn giản, chỉ là dãy số
- ✗ password123 → quá phổ biến, dễ đoán
- ✗ ngaysinh2001 → chứa thông tin cá nhân
- ✗ iloveyou123! → dễ đoán và quá phổ biến
- ✗ Admin@2024 → quá ngắn và dễ đoán

Yếu

Ghi nhớ: Mật khẩu dài tối thiểu 12 ký tự là lá chắn vững chắc bảo vệ tài khoản và thông tin của bạn! Hãy tạo thói quen đặt mật khẩu mạnh và không chia sẻ với bất kỳ ai.

Quy tắc kết hợp đa dạng loại ký tự

Đảm bảo mật khẩu của người dùng chứa đủ 4 nhóm ký tự sau:

1 Chữ cái viết hoa (A - Z).

Ít nhất 1 ký tự viết hoa.

Ví dụ: A, B, C, ..., Z

2 Chữ cái viết thường (a - z).

Ít nhất 1 ký tự viết thường.

Ví dụ: a, b, c, ..., z

3 Chữ số từ (0 - 9).

Ít nhất 1 ký tự số.

Ví dụ: 0, 1, 2, ..., 9

4 Ký tự đặc biệt (ví dụ '!', '@', '#', '$', '%', '*').

Ít nhất 1 ký tự đặc biệt.

Ví dụ: !, @, #, $, %, *

Mật khẩu mạnh = kết hợp từ tất cả 4 nhóm ký tự, độ dài tối thiểu 12 ký tự (khuyến nghị 12–16 ký tự).

Ví dụ mật khẩu mạnh

✓	Abc@1234xyz!	A	a	0-9	!@#
✓	KhoaIT_2024#Secure	A	a	0-9	!@#
✓	Ph0ng!AnNinh$2024	A	a	0-9	!@#

Ví dụ mật khẩu yếu (không nên dùng)

✗	password123	→ thiếu chữ hoa, ký tự đặc biệt
✗	1234567890	→ chỉ có chữ số
✗	abcdefg	→ chỉ có chữ thường
✗	ADMIN	→ chỉ có chữ hoa
✗	Qwerty!@#	→ thiếu chữ số

Sử dụng Cụm từ mật mã (Passphrase) để nhớ

Khái niệm

Passphrase là một chuỗi từ dễ nhớ với bạn nhưng khó đoán với người khác.
Dài hơn, có khoảng trắng hoặc ký tự đặc biệt → tăng độ mạnh và bảo mật.

Cách tạo Passphrase mạnh

1. **Chọn câu nói quen thuộc** — Ví dụ: **"Tôi yêu quê hương Bắc Ninh!"**
2. **Viết lại không dấu, viết hoa chữ cái đầu và thêm ký tự đặc biệt** — Ví dụ: `` `ToiYeuQueHuongBacNinh@2026!` ``
   (Bỏ dấu, viết hoa chữ cái đầu mỗi từ, thêm ký tự đặc biệt và số)
3. **Độ dài lý tưởng** — Độ dài lên tới **27 ký tự**, cực kỳ an toàn nhưng lại rất dễ nhớ đối với người dùng.

So sánh độ mạnh mật khẩu

Loại mật khẩu	Ví dụ	Độ dài	Độ mạnh	Thời gian bẻ khóa (ước tính)
Yếu (dễ đoán)	123456789	9 ký tự	★☆☆☆☆ (Rất yếu)	Vài giây
Trung bình	BacNinh2026	11 ký tự	★★★☆☆ (Trung bình)	Vài phút đến vài giờ
Mạnh (Passphrase)	ToiYeuQueHuongBacNinh@2026!	27 ký tự	★★★★★ (Rất mạnh)	Hàng chục nghìn năm

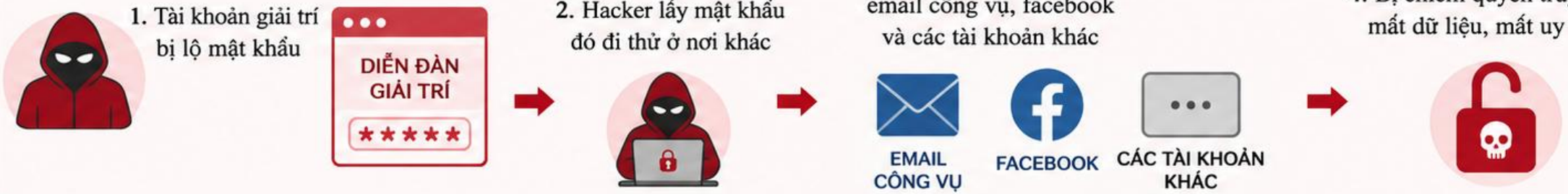
Ghi nhớ: Passphrase càng dài và đa dạng (chữ hoa, chữ thường, số, ký tự đặc biệt) → **càng an toàn và khó bị bẻ khóa.**

Không dùng chung một mật khẩu cho nhiều tài khoản

- Nếu dùng chung mật khẩu, khi một tài khoản (ví dụ diễn đàn giải trí) bị lộ, **hacker sẽ dùng mật khẩu đó** để thử đăng nhập vào email công vụ và facebook của người dùng.

- Hãy **tách biệt mật khẩu** tài khoản phục vụ công việc và tài khoản phục vụ mục đích cá nhân.

Nguy cơ khi dùng chung mật khẩu



Thực hành tốt

Tài khoản công việc
Dùng mật khẩu riêng, mạnh và bảo mật cao.

Tài khoản cá nhân
Dùng mật khẩu riêng khác với công việc.

Mật khẩu mạnh
Dài ít nhất 12 ký tự, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.

Thay đổi định kỳ
Thay đổi mật khẩu thường xuyên và khi có dấu hiệu bất thường.

Ghi nhớ: Mỗi tài khoản – một mật khẩu riêng. Bảo vệ mật khẩu là bảo vệ chính bạn!

Thay đổi mật khẩu định kỳ đúng quy định

- Nên thay đổi mật khẩu đăng nhập máy tính và tài khoản công vụ **tối thiểu 6 tháng** một lần.

- Khi thay đổi, **không được lặp lại mật khẩu cũ** hoặc chỉ thay đổi số thứ tự ở cuối (ví dụ đổi từ `Matkhau1` sang `Matkhau2`).

- **Thu hồi quyền đăng nhập** trên các thiết bị cũ sau khi thực hiện đổi mật khẩu mới.

THU HỒI QUYỀN ĐĂNG NHẬP TRÊN CÁC THIẾT BỊ CŨ SAU KHI ĐỔI MẬT KHẨU

Máy tính cá nhân
đã đăng nhập trước đó

Điện thoại, máy tính bảng
đã đăng nhập trước đó

Trình duyệt web
đã lưu phiên đăng nhập

Ứng dụng email
trên thiết bị cũ

Dịch vụ, ứng dụng khác
đã kết nối trước đó

Lưu ý quan trọng

- ✓ Sử dụng mật khẩu mạnh, duy nhất cho mỗi tài khoản.
- ✓ Không chia sẻ mật khẩu cho bất kỳ ai.
- ✓ Ghi nhớ mật khẩu mới ở nơi an toàn.

Ví dụ thay đổi đúng:
Từ: Matkhau1!@
Đổi thành: Qwe2024#Xy7 ✓

Ví dụ thay đổi sai:
Từ: Matkhau1
Đổi thành: Matkhau2 ✗

Sử dụng trình quản lý mật khẩu của trình duyệt Chrome

Trình duyệt Google Chrome có sẵn tính năng **lưu trữ mật khẩu đã được mã hóa an toàn.**

Giúp người dùng **tự động điền mật khẩu khi đăng nhập**, không sợ quên các mật khẩu phức tạp.

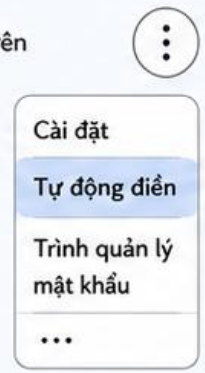
Cảnh báo người dùng nếu **mật khẩu đã lưu bị rò rỉ** trong các vụ hack trên thế giới.

CÁCH SỬ DỤNG

1 Mở Chrome và đăng nhập vào tài khoản Google.

Đăng nhập

2 Vào Cài đặt (ba chấm ở góc trên bên phải) → **Tự động điền** → **Trình quản lý mật khẩu.**



3 Bật "Đề xuất lưu mật khẩu" và "Tự động đăng nhập".

4 Khi đăng nhập vào trang web, Chrome sẽ hỏi lưu mật khẩu.

5 Lần sau, Chrome sẽ tự động điền mật khẩu cho bạn.

MẸO BẢO MẬT

- Sử dụng mật khẩu mạnh, duy nhất cho mỗi tài khoản.
- Bật xác minh 2 bước (2FA) cho tài khoản Google của bạn.
- Thường xuyên kiểm tra "Kiểm tra mật khẩu" trong Trình quản lý mật khẩu.

LƯU Ý: Luôn đăng xuất khỏi tài khoản trên máy tính dùng chung và khóa màn hình khi không sử dụng.

CẢM ƠN VÀ THẢO LUẬN BUỔI 1