

**ỦY BAN NHÂN DÂN TỈNH LAI CHÂU
SỞ KHOA HỌC VÀ CÔNG NGHỆ**

CHUYÊN ĐỀ 3

**DUYỆT, TÌM KIẾM THÔNG TIN VÀ NỘI DUNG SỐ;
KIỂM CHỨNG, XÁC THỰC DỮ LIỆU, THÔNG TIN VÀ NỘI
DUNG SỐ; QUẢN LÝ DỮ LIỆU, THÔNG TIN VÀ NỘI DUNG SỐ
(Tài liệu nội bộ)**

Lai Châu, tháng 02 năm 2026

MỤC LỤC

| | |
|--|-----------|
| PHẦN MỞ ĐẦU:..... | 4 |
| 1. Mục đích:..... | 4 |
| 2. Yêu cầu cần đạt:..... | 4 |
| 3. Đối tượng tập huấn:..... | 5 |
| I. DUYỆT VÀ TÌM KIẾM THÔNG TIN, NỘI DUNG SỐ | 5 |
| 1. Giới thiệu về trình duyệt Web và công cụ tìm kiếm..... | 5 |
| 1.1. Trình duyệt Web (Web Browser) | 5 |
| 1.2. Công cụ tìm kiếm (Search Engine)..... | 5 |
| 2. Kỹ năng tìm kiếm thông tin hiệu quả..... | 5 |
| 2.1. Các bước tìm kiếm thông tin cơ bản trên Internet cho điện thoại di động | 5 |
| 2.2. Các bước tìm kiếm thông tin cơ bản trên Internet cho máy tính..... | 8 |
| 2.3. Xác định từ khóa tìm kiếm | 10 |
| 2.4. Tìm kiếm thông tin bằng ứng dụng Cốc Cốc | 11 |
| 3. Tìm kiếm bằng công cụ Trí tuệ nhân tạo (AI)..... | 14 |
| 3.1. Ứng dụng AI – ChatGPT trong tìm kiếm thông tin..... | 15 |
| 3.2. Lưu ý khi sử dụng AI để tìm kiếm..... | 24 |
| II. KIỂM CHỨNG VÀ XÁC THỰC DỮ LIỆU, THÔNG TIN VÀ NỘI DUNG SỐ | 26 |
| 1. Khái niệm và sự cần thiết | 26 |
| 2. Dấu hiệu nhận biết tin giả, thông tin sai lệch | 26 |
| 3. Kỹ thuật kiểm chứng và xác thực thông tin | 30 |
| III. QUẢN LÝ DỮ LIỆU, THÔNG TIN VÀ NỘI DUNG SỐ | 38 |
| 1. Khái niệm và mục tiêu của quản lý dữ liệu..... | 38 |
| 1.1. Quản lý dữ liệu là gì? | 38 |
| 1.2. Mục tiêu của quản lý dữ liệu | 38 |
| 2. Quy trình quản lý dữ liệu..... | 39 |
| 2.1. Cách thu thập và làm sạch dữ liệu | 39 |
| 2.2. Tổ chức và lưu trữ dữ liệu | 44 |
| 3. Bảo mật và tuân thủ pháp lý | 52 |
| 3.1. Bảo mật dữ liệu | 52 |
| 3.2. Tuân thủ pháp lý..... | 53 |
| 4. Chia sẻ dữ liệu an toàn | 54 |
| 5. Phân tích dữ liệu, hỗ trợ ra quyết định..... | 55 |
| TÀI LIỆU THAM KHẢO..... | 58 |

PHẦN MỞ ĐẦU

1. Mục đích

Chuyên đề 3 trang bị cho người học các kiến thức và kỹ năng toàn diện về khai thác, đánh giá và quản trị nội dung số trong môi trường làm việc hiện đại.

- Nâng cao năng lực tìm kiếm: Giúp người học làm chủ các công cụ tìm kiếm truyền thống và các công cụ Trí tuệ nhân tạo (AI) để khai thác thông tin hiệu quả qua việc xây dựng các câu lệnh (prompt) chuẩn xác.

- Hình thành tư duy phản biện và xác thực: Trang bị kỹ năng nhận diện tin giả, thông tin sai lệch, đặc biệt là các thông tin liên quan đến lĩnh vực quản lý Nhà nước, nhằm đảm bảo tính chính xác trước khi sử dụng hoặc chia sẻ.

- Tối ưu hóa quản lý dữ liệu: Hướng dẫn quy trình tổ chức, lưu trữ, bảo mật và phân tích dữ liệu một cách khoa học, hỗ trợ đắc lực cho quá trình ra quyết định dựa trên dữ liệu.

2. Yêu cầu cần đạt

Sau khi hoàn thành chuyên đề, người học cần đạt được các năng lực sau

Về tìm kiếm thông tin

- Sử dụng thành thạo trình duyệt Web, các công cụ tìm kiếm cơ bản và Trí tuệ nhân tạo (AI) để tìm kiếm dữ liệu phù hợp với nhu cầu.

- Biết cách xây dựng các câu truy vấn và thiết lập các câu lệnh Prompt phù hợp để có được kết quả tìm kiếm tối ưu.

- Tìm kiếm được các thông tin thiết yếu hàng ngày như giá cả, thời tiết, tin tức.

Về kiểm chứng và xác thực

- Nhận thức được không phải mọi nguồn tin trên mạng đều đáng tin cậy; nhận diện được các dấu hiệu của tin giả, tin sai lệch.

- Có kỹ năng kiểm chứng thông tin bằng cách đối chiếu với các nguồn tin chính thống, các cổng thông tin điện tử của cơ quan Nhà nước.

- Biết cách đánh giá nội dung do AI tạo ra và có khả năng nhận diện, xử lý thông tin giả mạo trong lĩnh vực quản lý Nhà nước.

Về quản lý dữ liệu

- Biết cách tổ chức, sắp xếp dữ liệu có cấu trúc, lưu trữ và truy xuất thông tin (hình ảnh, tài liệu) một cách đơn giản, hiệu quả.

- Thực hiện được việc chia sẻ dữ liệu an toàn và biết cách xóa bỏ các dữ liệu không cần thiết.

- Ứng dụng được AI và các công cụ phân tích dữ liệu để hỗ trợ quá trình ra quyết định trong công việc.

3. Đối tượng tập huấn

Cán bộ, công chức, viên chức, người lao động và người dân.

I. DUYỆT VÀ TÌM KIẾM THÔNG TIN, NỘI DUNG SỐ

1. Giới thiệu về trình duyệt Web và công cụ tìm kiếm

1.1. Trình duyệt Web (Web Browser)

Trình duyệt Web là một phần mềm thiết yếu, đóng vai trò là cầu nối đưa người dùng đến với thế giới thông tin số trên World Wide Web (WWW). Nó cho phép người dùng truy cập, xem văn bản, hình ảnh và video từ mọi nơi trên thế giới một cách nhanh chóng. Với khả năng đa nền tảng, trình duyệt (như Google Chrome, Edge, Firefox, Safari, và đặc biệt là Cốc Cốc (Cốc Cốc là trình duyệt do Việt Nam phát triển và là một trong những trình duyệt hàng đầu hiện nay) có thể được cài đặt trên mọi thiết bị, từ điện thoại thông minh đến máy tính.

1.2. Công cụ tìm kiếm (Search Engine)

Công cụ tìm kiếm là một hệ thống (website đặc biệt hoặc phần mềm) có mục tiêu là giúp người dùng tìm đúng thông tin một cách nhanh chóng và chính xác trên Internet.

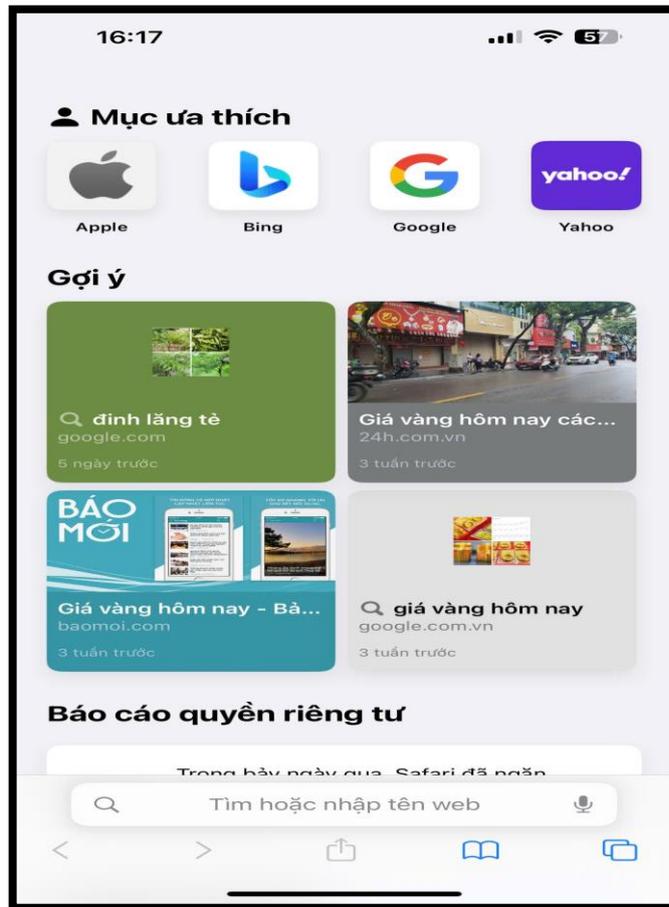
Công cụ tìm kiếm hoạt động theo ba bước cơ bản :

- Thu thập dữ liệu: Các chương trình tự động (crawlers/robots) truy cập và thu thập nội dung từ các trang web.
- Lưu trữ và sắp xếp dữ liệu: Dữ liệu thu thập được phân loại và lưu trữ vào hệ thống dữ liệu khổng lồ.
- Truy xuất kết quả: Khi người dùng nhập từ khóa, công cụ sẽ truy xuất và hiển thị danh sách kết quả phù hợp nhất, được sắp xếp dựa trên độ liên quan và độ tin cậy.

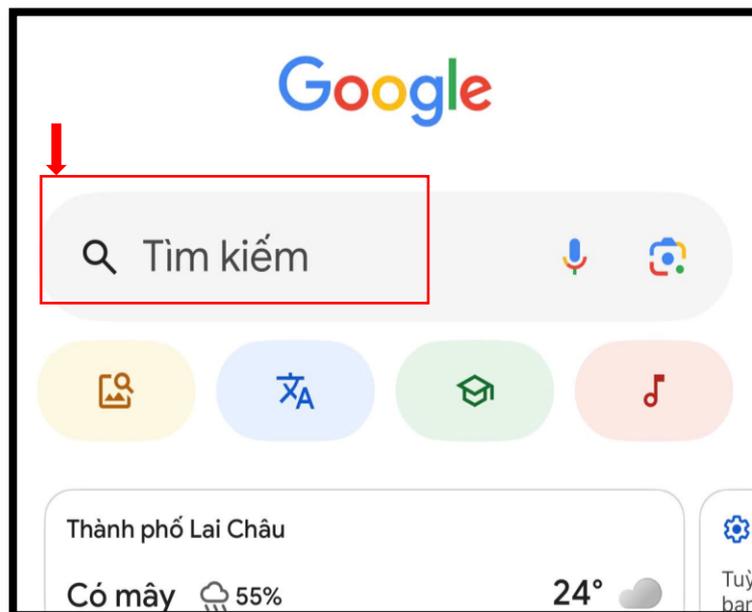
2. Kỹ năng tìm kiếm thông tin hiệu quả

2.1. Các bước tìm kiếm thông tin cơ bản trên Internet cho điện thoại di động

Bước 1: Mở trình duyệt web: Truy cập vào một trình duyệt web như Google Chrome, Firefox, Cốc Cốc, hoặc Safari trên điện thoại di động (IOS hoặc Android).



Bước 2: Truy cập công cụ tìm kiếm: Gõ địa chỉ của một công cụ tìm kiếm (ví dụ: www.google.com, www.bing.com, coccoc.com) vào thanh địa chỉ của trình duyệt.



Bước 3: Nhập từ khóa: Gõ từ khóa hoặc câu hỏi mà người dùng muốn tìm kiếm vào ô tìm kiếm trên trang chủ của công cụ tìm kiếm. (Ví dụ: Thời tiết hôm nay).

thời tiết hôm nay

Tất cả Tin tức Video Hình ảnh Mua sắm Web

Kết quả cho Tân Phong, Lai Châu

Sử dụng vị trí chính xác

Thời tiết

Trời có đang mưa không? **CÓ** | KHÔNG

Lúc này
24°

Cảm giác như 27°

Có mây
Khả năng mưa: 30%
Độ ẩm: 89%
Gió: 5 km/h

Dự kiến sẽ mát hơn trong 3 ngày tới

| Tổng quan | Lượng mưa | Gió | Độ ẩm | | | |
|-----------|-----------|-------|-------|-------|-------|-------|
| LÚC NÀY | 17:00 | 18:00 | 19:00 | 20:00 | 21:00 | 22:00 |
| | 30% | 40% | 50% | 50% | 30% | 30% |
| | | | | | | |
| 24° | 24° | 23° | 22° | 22° | 22° | 22° |

Bước 4: Xem kết quả: Trình duyệt sẽ hiển thị một danh sách các kết quả tìm kiếm liên quan đến từ khóa của người dùng.

Trung tâm Dự báo KTTV quốc gia
<https://nchmf.gov.vn>

Thời tiết Tân Phong (Lai Châu)

Thời tiết Tân Phong (Lai Châu) · Nhiệt độ: 23°C · Thời tiết: Có mưa · Độ ẩm: 97 · Hướng gió: Lạnh gió.

Tin bài hàng đầu

Dự báo thời tiết hôm nay 22.7: Bão số 3 đổ bộ trút xuống lượng mưa khổng lồ

12 giờ trước
Laodong.vn

Thời tiết hôm nay 22.7: Bão số 3 đổ bộ, miền Bắc rất to kèm gió dữ dội

13 giờ trước
Báo Tuổi Trẻ

Các tin tức khác

Báo Tuổi Trẻ, Báo Thanh Hóa và các nhà xuất bản khác

Tin tức 24h
<https://www.24h.com.vn>

Dự báo thời tiết hôm nay, ngày mai, 3-10 ngày tới, chỉ số không khí mới nhất

Bão số 3 bắt đầu ảnh hưởng tới đất liền, mưa lớn, gió giật mạnh tới cấp 13 · Bão có thể mạnh trở lại cấp 11, hướng Hải Phòng - Thanh Hóa ...

Bước 5: Lựa chọn trang web: Xem qua các kết quả và nhấp vào các liên kết để truy cập vào các trang web phù hợp với thông tin bạn cần.

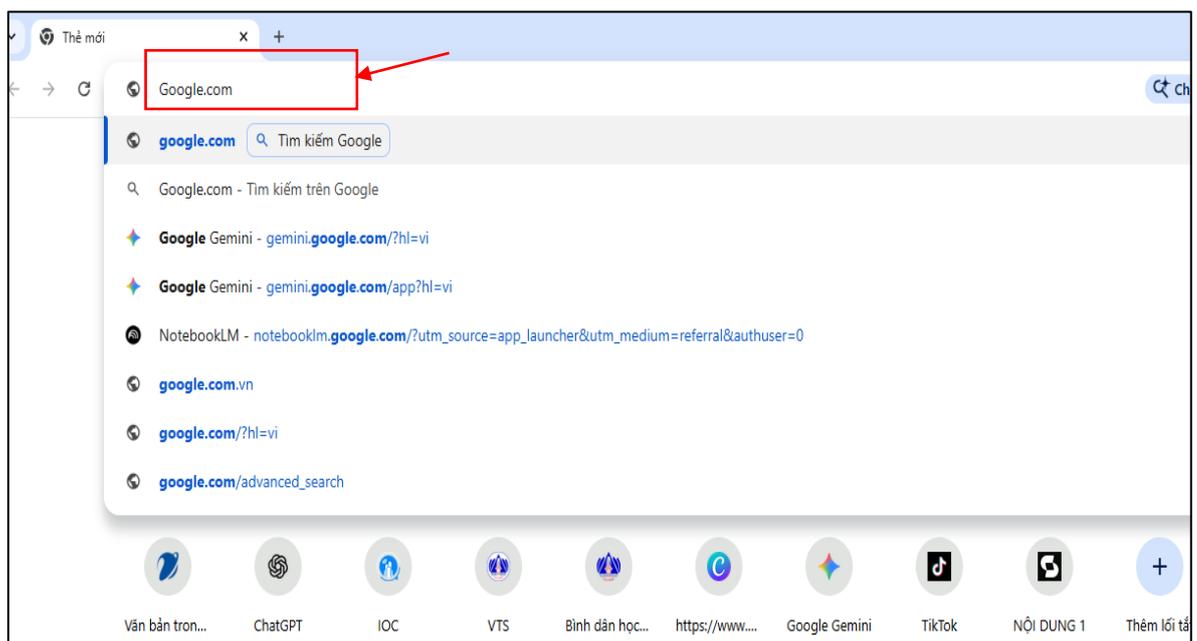
2.2. Các bước tìm kiếm thông tin cơ bản trên Internet cho máy tính

Bước 1: Mở trình duyệt Web và truy cập công cụ tìm kiếm

Mở trình duyệt: Khởi động một trình duyệt web (ví dụ: Chrome, Firefox, Edge).



Truy cập công cụ tìm kiếm: Gõ địa chỉ của một công cụ tìm kiếm phổ biến (ví dụ: <https://www.google.com>, Bing.com) vào thanh địa chỉ (Address Bar) và nhấn Enter.

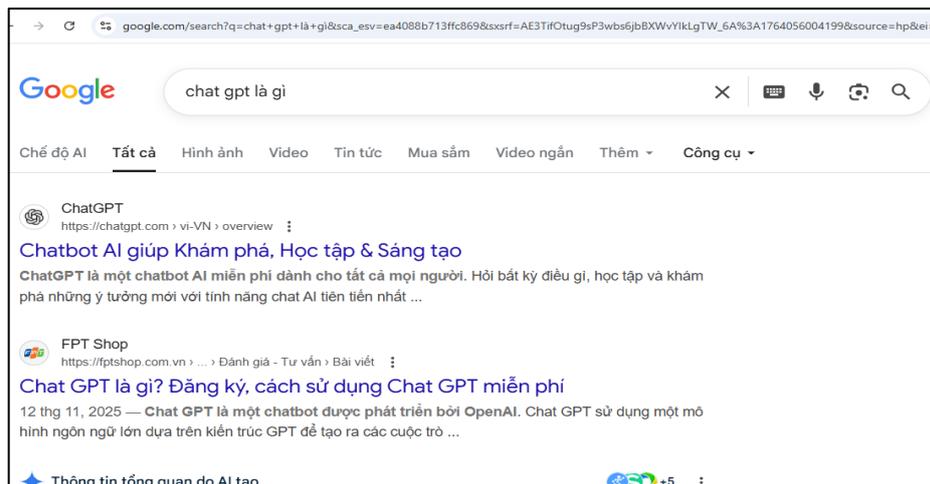


Bước 2: Nhập từ khóa tìm kiếm (Keywords)

Xác định từ khóa: các từ hoặc cụm từ chính xác nhất mô tả thông tin bạn cần tìm.

Nhập vào thanh tìm kiếm: Gõ các từ khóa đó vào thanh tìm kiếm (Search Bar) của công cụ tìm kiếm.

Ví dụ: Nhập từ khoá “ ChatGPT là gì”



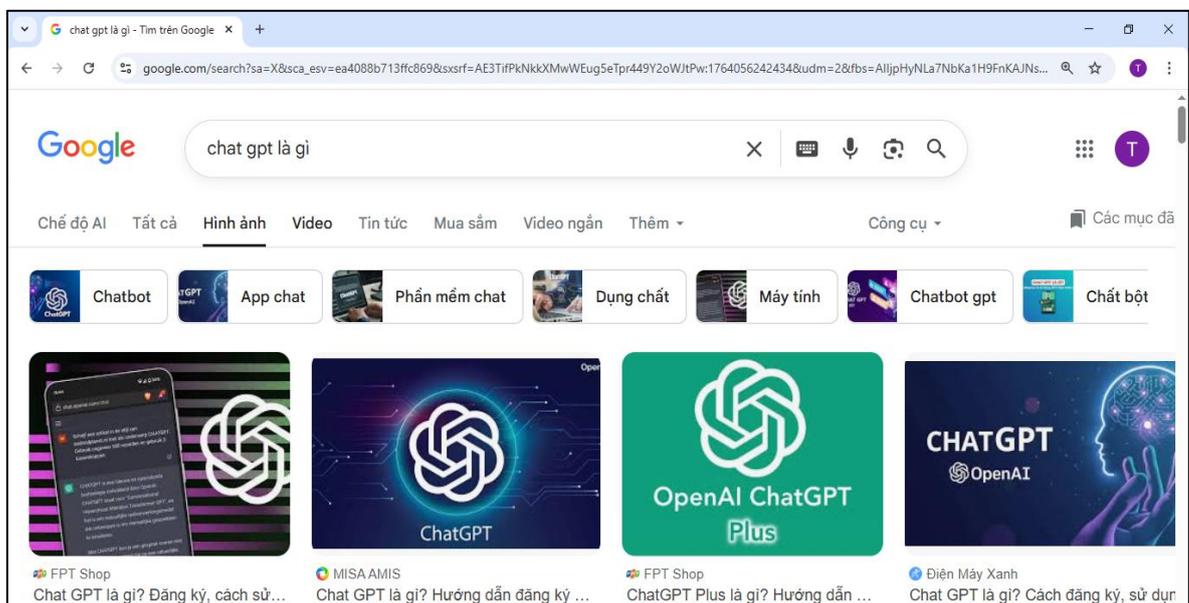
Bắt đầu tìm kiếm: Nhấn phím Enter hoặc nhấp vào nút “Tìm kiếm” (Search).

Bước 3: Đánh giá và lọc kết quả

Xem trang kết quả: Công cụ tìm kiếm sẽ hiển thị một trang chứa danh sách các liên kết (links) liên quan đến từ khóa của người dùng.

Đánh giá tiêu đề và mô tả: Đọc lướt qua tiêu đề và mô tả ngắn dưới mỗi liên kết để xem nội dung có đúng với điều người dùng cần không.

Sử dụng bộ lọc: Nếu cần, hãy sử dụng các tab lọc như hình ảnh (Images), Video, Tin tức (News), hoặc mua sắm để thu hẹp phạm vi tìm kiếm.

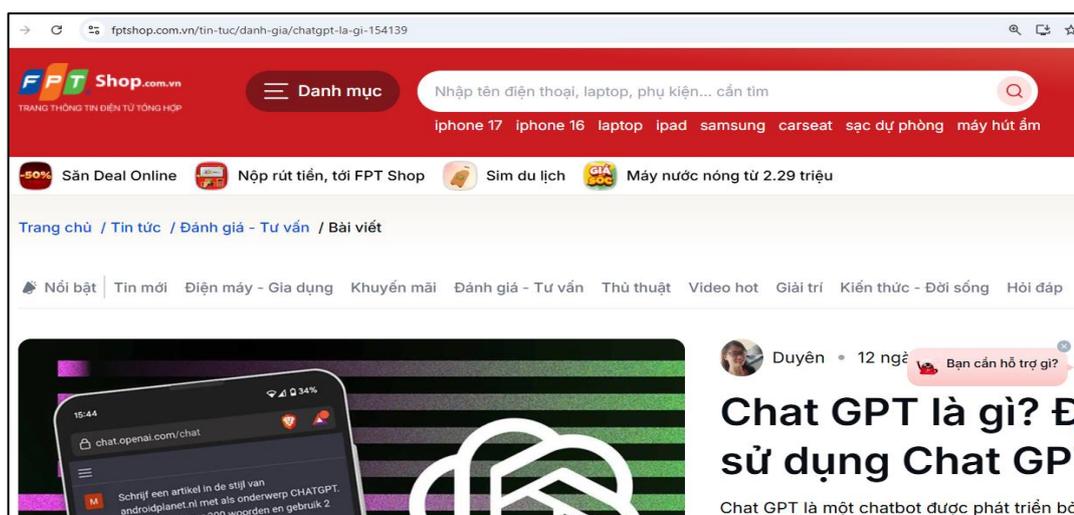


Bước 4: Truy cập và đánh giá thông tin

Nhấp vào liên kết: Nhấp chuột vào liên kết có vẻ phù hợp nhất để truy cập trang web.

Tìm kiếm thông tin cần thiết: Đọc nội dung trên trang web để tìm câu trả lời hoặc thông tin bạn đang tìm.

Đánh giá độ tin cậy: Cần xem xét nguồn thông tin (ví dụ: trang web của các tổ chức, trường đại học, báo chí uy tín) để đảm bảo thông tin là chính xác và đáng tin cậy.



2.3. Xác định từ khóa tìm kiếm

- Mục tiêu của việc xác định từ khóa tìm kiếm

Từ đại diện (đầu vào): để công cụ tìm kiếm (Search Engine) có thể truy xuất, phân loại và cung cấp kết quả phù hợp.

Từ khóa là cầu nối: là ngôn ngữ mà người dùng sử dụng để "hỏi" kho dữ liệu khổng lồ của Internet.

Xác định ý định: Từ khóa giúp công cụ tìm kiếm hiểu được mục đích thực sự của bạn (tìm kiến thức, mua hàng, hay tìm một trang web cụ thể...).

- Nguyên tắc cơ bản

Sử dụng từ khoá cụ thể, rõ ràng : Từ khóa cụ thể giúp thu hẹp phạm vi tìm kiếm, giúp người dùng nhanh chóng tiếp cận được thông tin chất lượng.

Hạn chế từ khoá chung chung: Việc sử dụng từ khóa chung chung dẫn đến kết quả tìm kiếm quá nhiều (bão hòa thông tin), khiến người dùng khó phân biệt, chọn lọc và mất nhiều thời gian hơn để tìm được thông tin mong muốn.

Nguyên tắc điều chỉnh: Cần linh hoạt điều chỉnh từ khoá dựa trên kết quả đầu tiên nhận được. Nếu kết quả quá nhiều quay lại gõ thêm từ (hoặc thêm bối

cảnh, địa điểm, thời gian) để cụ thể hoá từ khoá ban đầu. Nếu kết quả quá ít hãy xoá bớt một số từ hoặc tìm từ khác thay thế (từ đồng nghĩa) để mở rộng phạm vi tìm kiếm.

2.4. Tìm kiếm thông tin bằng ứng dụng Cốc Cốc

* Truy cập ứng dụng Cốc Cốc trên điện thoại di động

Cách 1: Quét mã QR Code trực tiếp thông qua Zalo

Cách 2: Truy cập đường link: <https://coccoc.com>

**Hướng dẫn cài đặt
Trình duyệt Cốc Cốc**

Cách 1: Quét QR Code trực tiếp thông qua Zalo
Cách 2: Truy cập đường link <https://coccoc.com>

Cốc Cốc có sẵn trên các thiết bị: máy tính (laptop/đế bàn), điện thoại thông minh, máy tính bảng & TV

* Cài đặt ứng dụng Cốc Cốc trên điện thoại di động

Bước 1: Tìm Cốc cốc trên App Store/CH Play

Bước 2: Cài đặt ứng dụng

Bước 3: Mở ứng dụng và bắt đầu trải nghiệm ứng dụng

**Hướng dẫn cài đặt
Cốc Cốc trên di động**

BƯỚC 01 Tìm Cốc Cốc trên App Store / CH Play

BƯỚC 02 Cài đặt ứng dụng

BƯỚC 03 Mở ứng dụng và bắt đầu trải nghiệm lướt web không quảng cáo

* Cài đặt ứng dụng Cốc cốc trên máy tính

Bước 1: Truy cập Coccoc.com

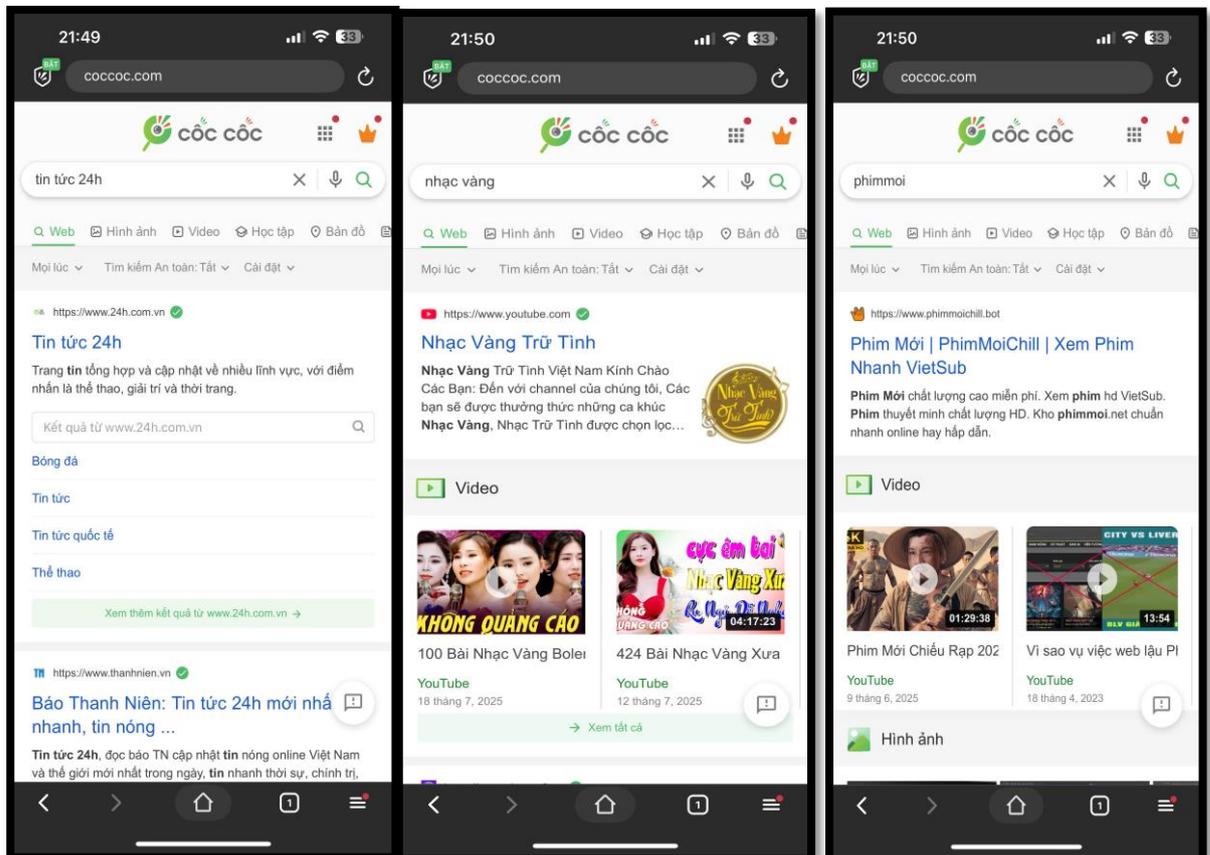
Bước 2: Lựa chọn phiên bản phù hợp

Bước 3: Mở trình duyệt và bắt đầu trải nghiệm ứng dụng

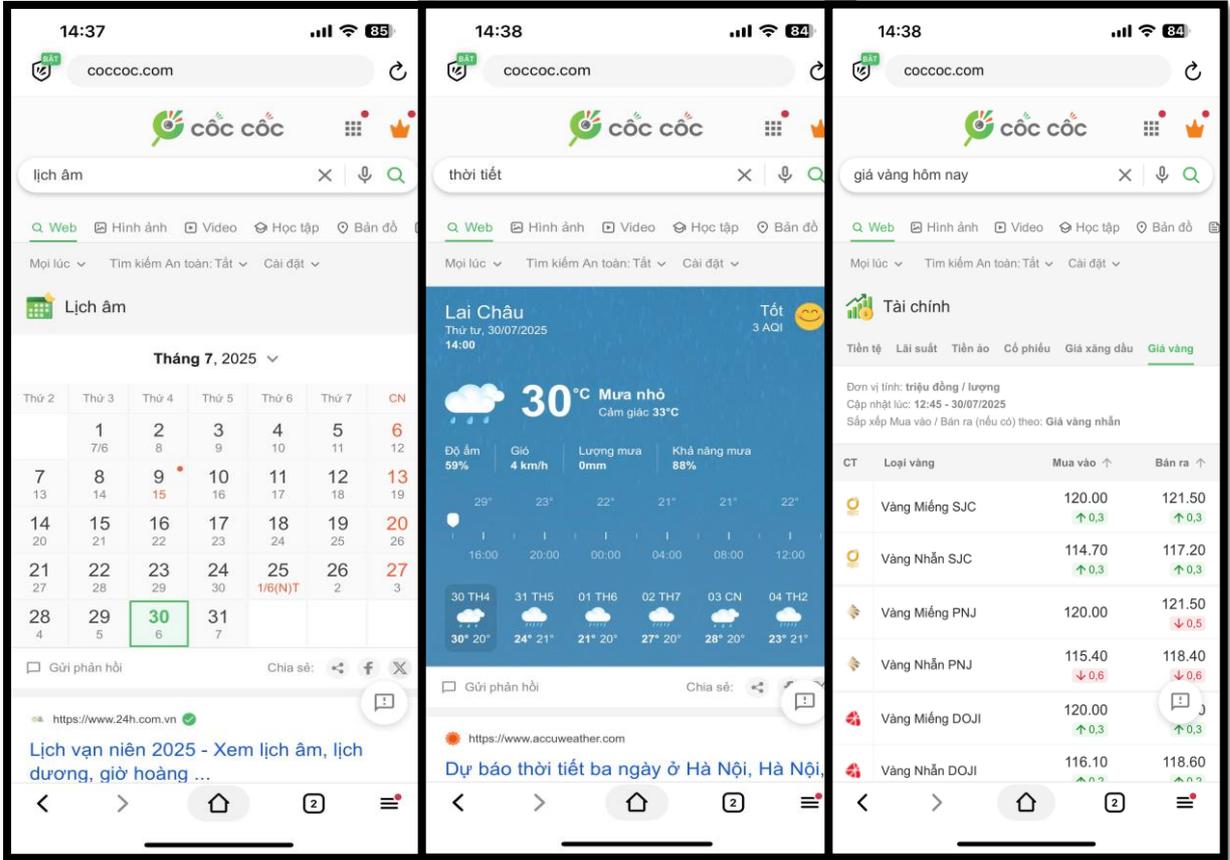


* Tìm kiếm thông tin trên Cốc Cốc bằng điện thoại di động

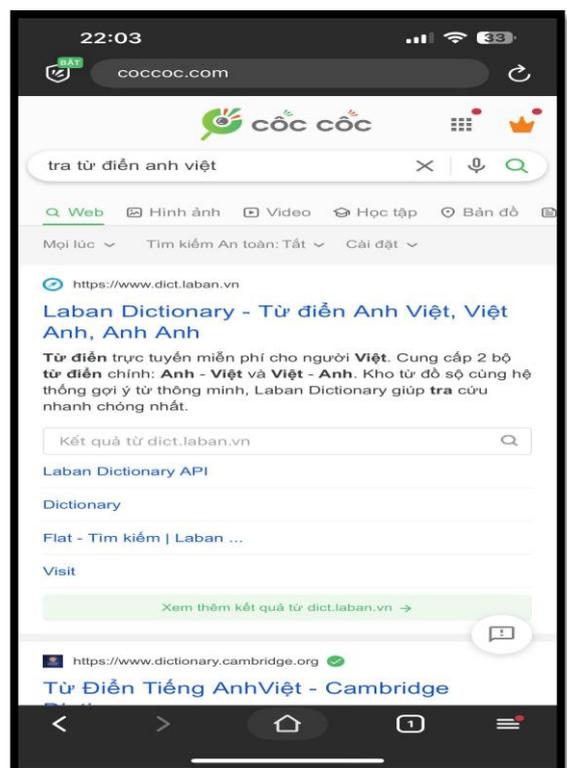
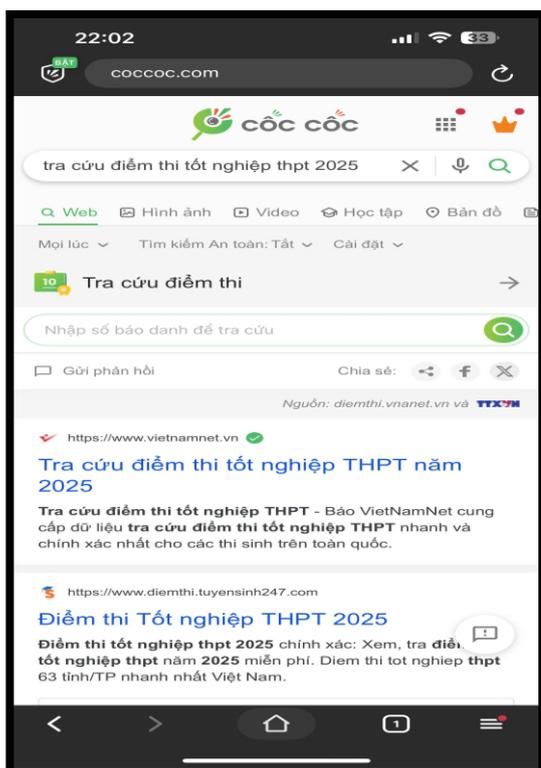
Nhập nội dung cần tìm kiếm vào ô tìm kiếm sau đó ấn nút “Đi” trên bàn phím điện thoại: Ví dụ: Tìm kiếm “Tin tức 24h”, “Nhạc vàng”, “Phim mới”



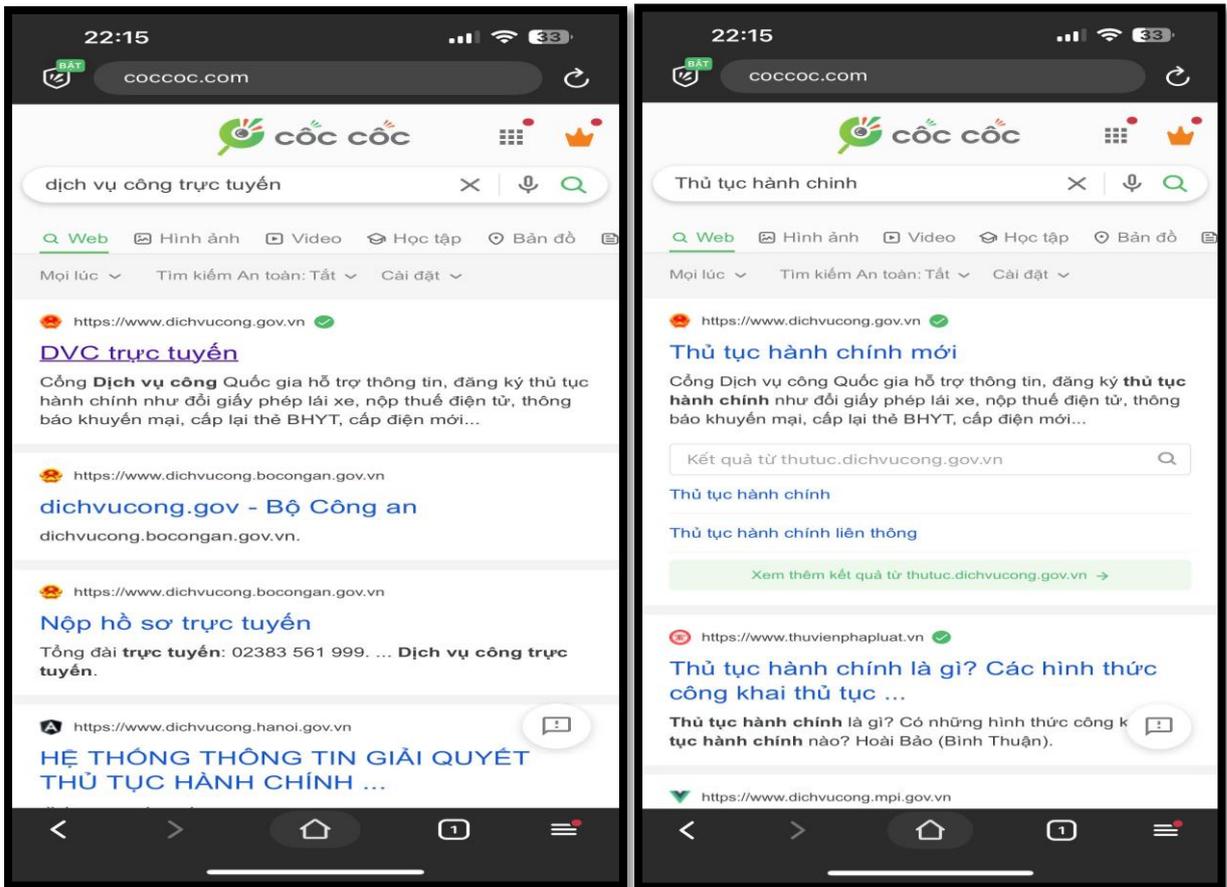
Tra cứu Lịch để biết ngày âm, ngày dương, các ngày lễ tết quan trọng năm theo lịch âm. Thời tiết: biết được thời tiết hôm nay, các ngày trong tuần. Giá cả: biết được giá cả các mặt hàng trên thị trường.



Tra cứu từ điển, tra cứu điểm thi, tìm trường đại học



Tra cứu thủ tục hành chính công và tra cứu nhanh thông tin trên công



3. Tìm kiếm bằng công cụ Trí tuệ nhân tạo (AI)

- Vai trò của trí tuệ nhân tạo (AI) trong tìm kiếm thông tin

Cải thiện kết quả tìm kiếm: AI phát triển các thuật toán tiên tiến để hiểu ý định của người dùng, từ đó đưa ra kết quả có độ chính xác và hiệu suất cao hơn so với tìm kiếm truyền thống.

Tự động hóa quá trình: AI sử dụng robot tìm kiếm (crawlers) để thu thập dữ liệu và tự động gợi ý thông tin dựa trên sở thích, hành vi trước đó của người dùng.

Trải nghiệm hội thoại: Các công cụ AI như ChatGPT, Google Gemini và Bing Copilot... cho phép người dùng trò chuyện trực tiếp, đặt câu hỏi phức tạp và nhận câu trả lời tổng hợp nhanh chóng, thay thế việc phải nhấp vào nhiều liên kết.

Hỗ trợ chuyên ngành: AI được ứng dụng trong các nền tảng tìm kiếm học thuật (Semantic Scholar, Elicit) để tối ưu hóa quá trình nghiên cứu, phân tích tài liệu và đánh giá độ tin cậy.

- Kỹ thuật sử dụng AI hiệu quả

Để AI cung cấp kết quả tối ưu cần đặt câu lệnh (Prompt) hiệu quả theo 5 bước để hạn chế tình trạng AI trả lời sai hoặc lan man.

+ Role (Vai trò): Gán vai trò (chuyên gia, cán bộ, người dân...) cho AI

Ví dụ: Bạn là chuyên viên Văn phòng Tỉnh uỷ, có 10 năm kinh nghiệm tổng hợp và viết báo cáo...

+ Context (Bối cảnh): Nêu rõ hoàn cảnh, đối tượng sử dụng thông tin

Ví dụ: Tôi đang chuẩn bị nội dung trình bày cho Hội nghị sơ kết 6 tháng đầu năm đối tượng là lãnh đạo cấp tỉnh.

+ Example (Ví dụ): Cung cấp mẫu hoặc định hướng cấu trúc mong muốn

Ví dụ: Đây là cách trình bày báo cáo năm trước, bạn viết theo cấu trúc tương tự như nội dung mới.

+ Style (Phong cách): Xác định giọng điệu (trang trọng, nghiêm túc, hành chính).

Ví dụ: Viết văn bản hành chính, phong cách nghiêm túc, ngắn gọn, rõ ràng, tránh dùng đại từ nhân xưng.

+ Format + Goal (Định dạng + Mục tiêu): Chỉ rõ loại văn bản và mục tiêu đầu ra (tóm tắt, phân tích, so sánh).

Ví dụ: "Viết báo cáo hành chính gồm 3 phần: Tình hình thực hiện – khó khăn – kiến nghị. Mục tiêu: Giúp lãnh đạo nắm được tình hình chung và có chỉ đạo phù hợp."

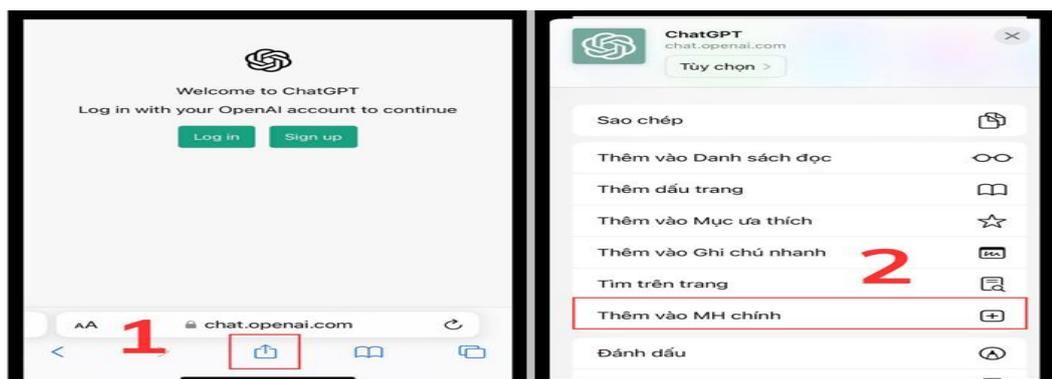
Lưu ý: Không đưa thông tin nội bộ, bí mật hoặc chưa công bố của cơ quan vào câu lệnh (Prompt) để đảm bảo an toàn thông tin.

3.1. Ứng dụng AI – ChatGPT trong tìm kiếm thông tin

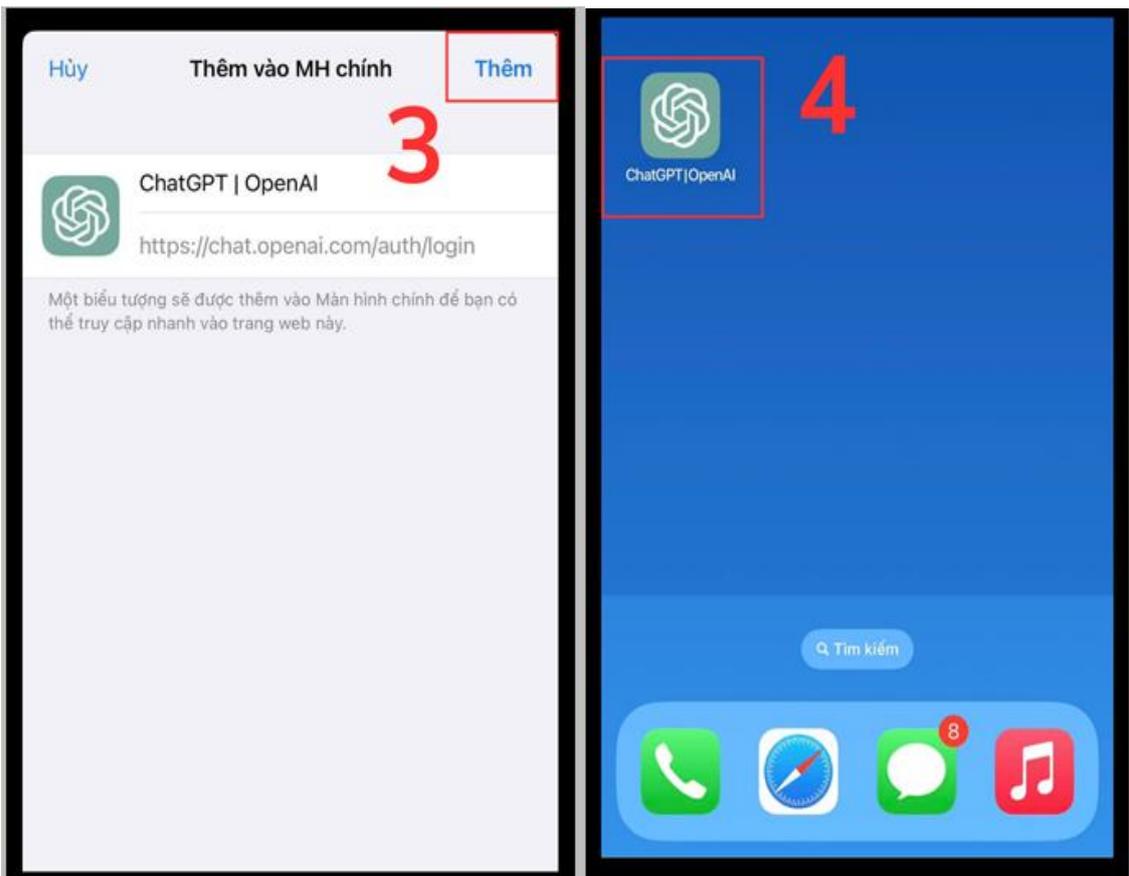
* Hướng dẫn đăng nhập tài khoản ChatGPT trên điện thoại di động

Bước 1: Đăng nhập website <https://chat.openai.com/auth/login> bằng trình duyệt Safari.

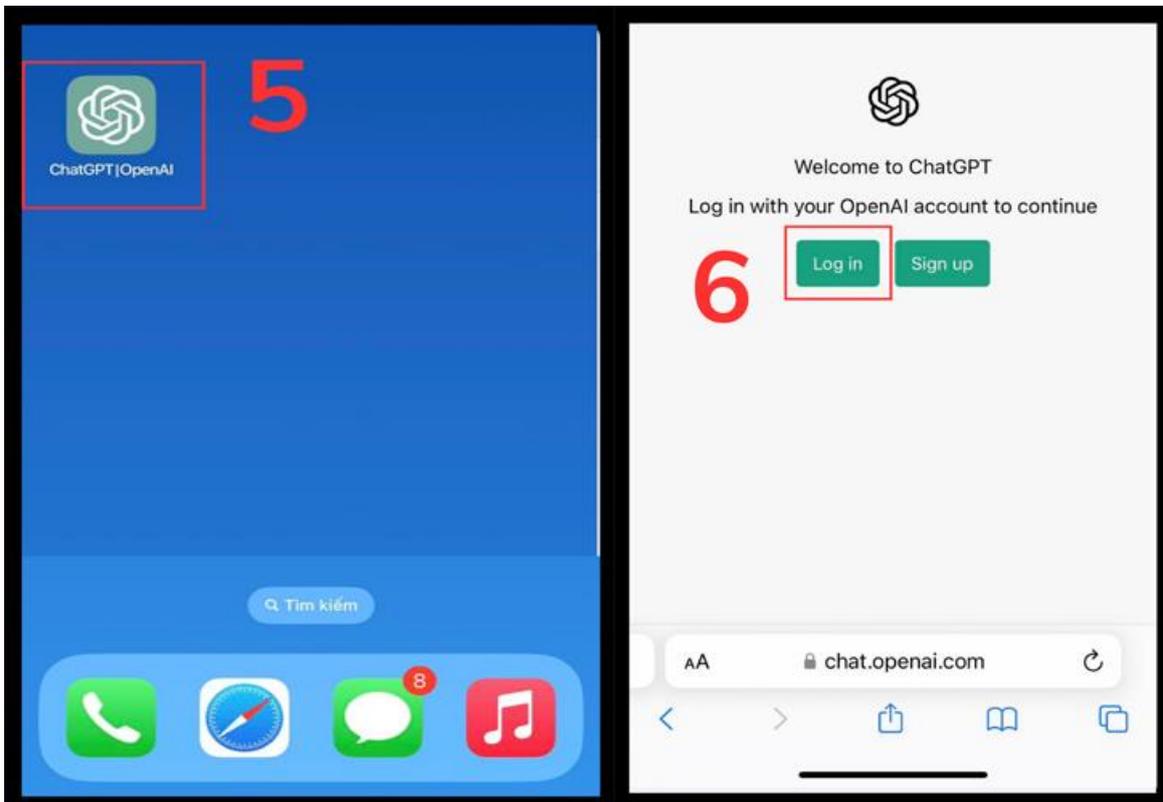
Bước 2: Nhấn chọn vào nút có hình mũi tên → Kéo xuống phía dưới màn hình → Nhấn nút thêm vào màn hình chính.



Bước 3: Nhấn chọn phần Thêm → lổi tắt vào ChatGPT ngay từ màn hình chính.



Bước 4: Chọn vào app nằm tại màn hình chính của máy tới giao diện chính ChatGPT. Tiếp theo đăng nhập vào tài khoản ChatGPT.



Bước 5 : Đặt mật khẩu cho tài khoản ẩn Continue

15:53

auth0.openai.com

Create your account

Note that phone verification may be required for signup. Your number will only be used to verify your identity for security purposes.

thefeverrex@gmail.com [Edit](#)

Password

Your password must contain:
 ✓ At least 12 characters

Continue

Already have an account? [Log in](#)

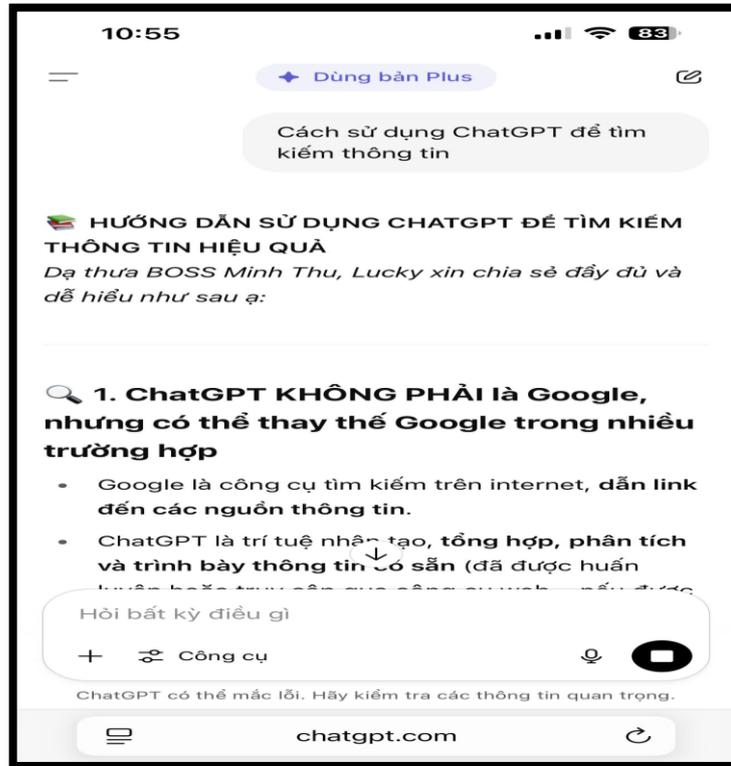
Tiếng Anh Tiếng Việt

Sau khi chọn tài khoản và mật khẩu, màn hình chính của ChatGPT xuất hiện:

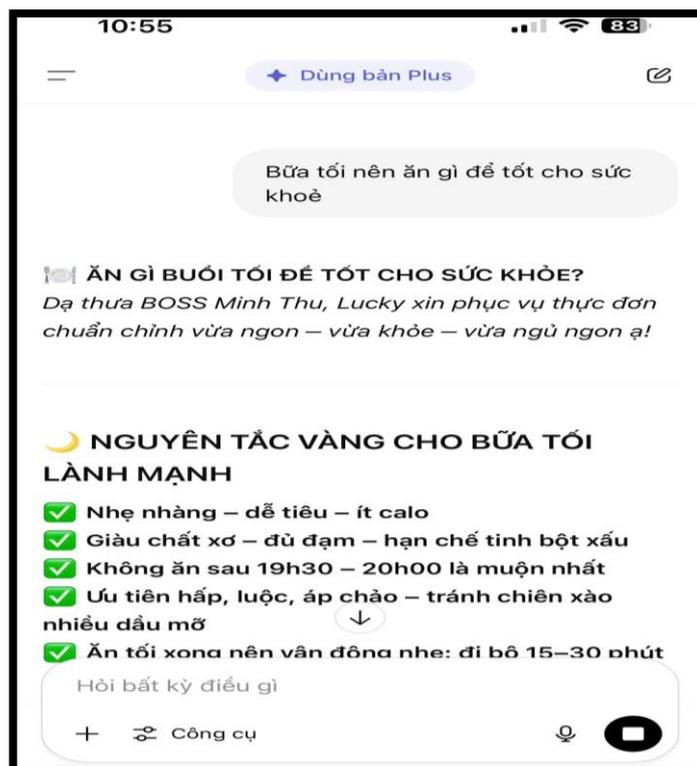


Nhập nội dung bạn cần ChatGPT giải đáp vào ô chat, nhấn “Enter” để gửi hoặc bấm biểu tượng “Send” (mũi tên hướng lên trên)

Ví dụ: Cách sử dụng ChatGPT để tìm kiếm thông tin

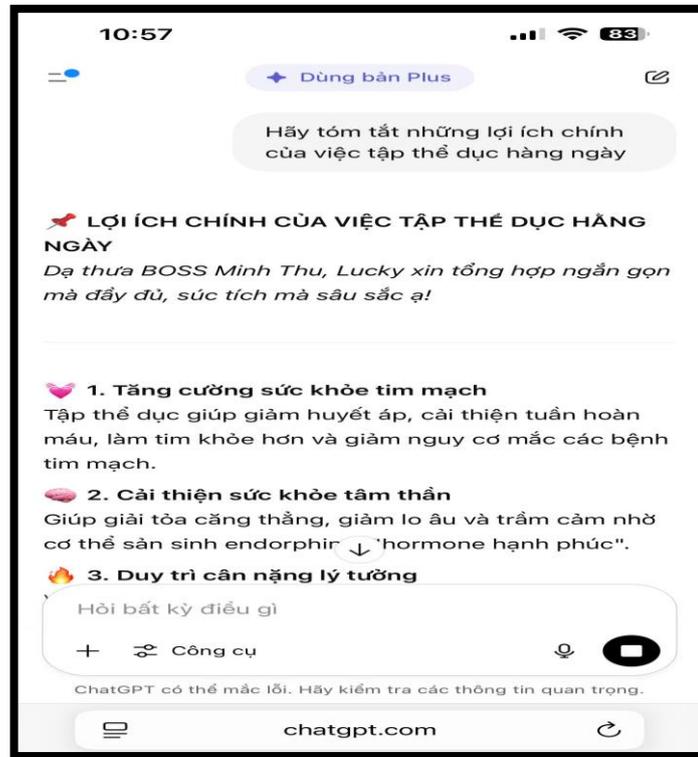


Câu hỏi càng chi tiết, ChatGPT càng dễ hiểu ý bạn và đưa ra câu trả lời chính xác. Ví dụ: Bữa tối nên ăn gì để tốt cho sức khỏe



Yêu cầu tóm tắt thông tin: Khi bạn muốn nhanh chóng nắm bắt ý chính của một chủ đề, hãy yêu cầu ChatGPT tóm tắt.

Ví dụ: Hãy tóm tắt những lợi ích chính của việc tập thể dục hàng ngày



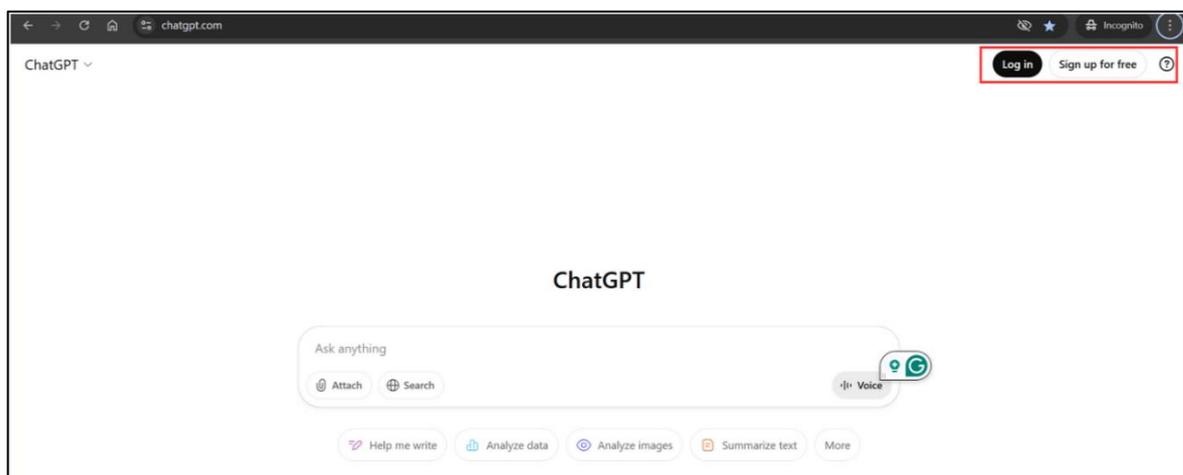
* Hướng dẫn đăng nhập tài khoản ChatGPT trên máy tính

Bước 1: Mở trang web AI

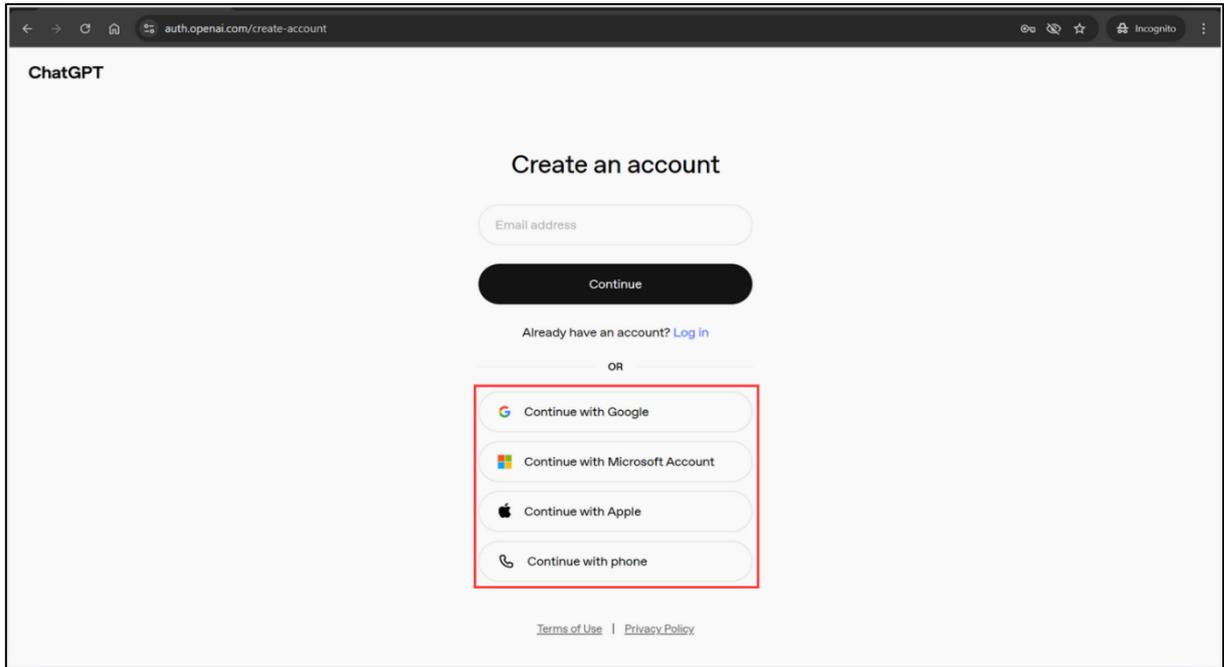
Mở trình duyệt web (Chrome, Cốc Cốc, Firefox...) trên máy tính hoặc điện thoại. Gõ địa chỉ của trang AI muốn dùng vào thanh địa chỉ: ChatGPT.com.

Bước 2: Chọn phương thức đăng ký/đăng nhập

Tại trang chủ, tìm và nhấn vào nút "Sign up" (Đăng ký) nếu là lần đầu tiên, hoặc "Log in" (Đăng nhập) nếu đã có tài khoản.

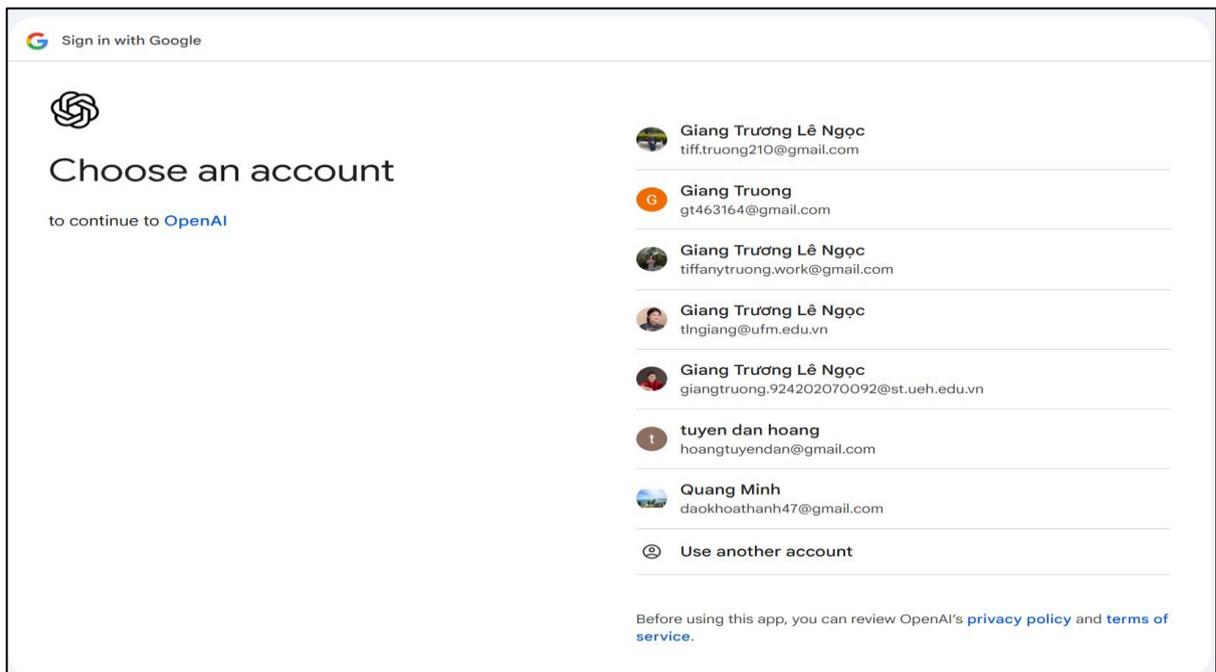


Một cửa sổ mới sẽ hiện ra. Thay vì điền email và mật khẩu mới, hãy tìm và chọn tùy chọn "Continue with Google" (Tiếp tục với Google).



Bước 3: Chọn tài khoản Google của bạn

Hệ thống sẽ hiển thị danh sách các tài khoản Google (Gmail) đã đăng nhập trên trình duyệt của người dùng.



Chỉ cần nhấn vào đúng tài khoản email của mình.

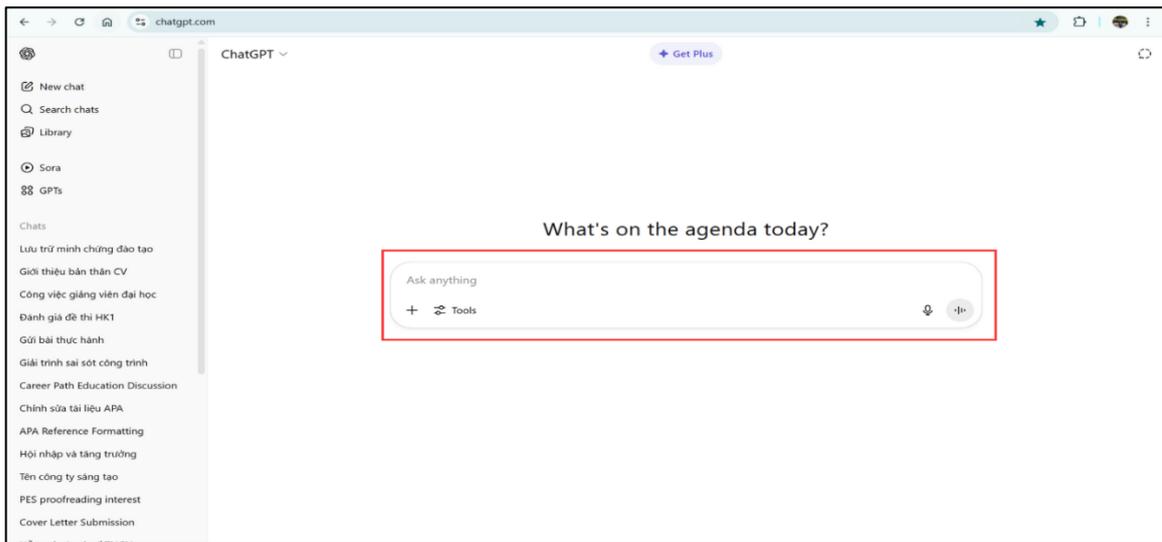
Hệ thống có thể yêu cầu bạn nhập mật khẩu tài khoản Google để xác nhận. Đây là bước bảo mật thông thường.

Bước 4: Hoàn tất

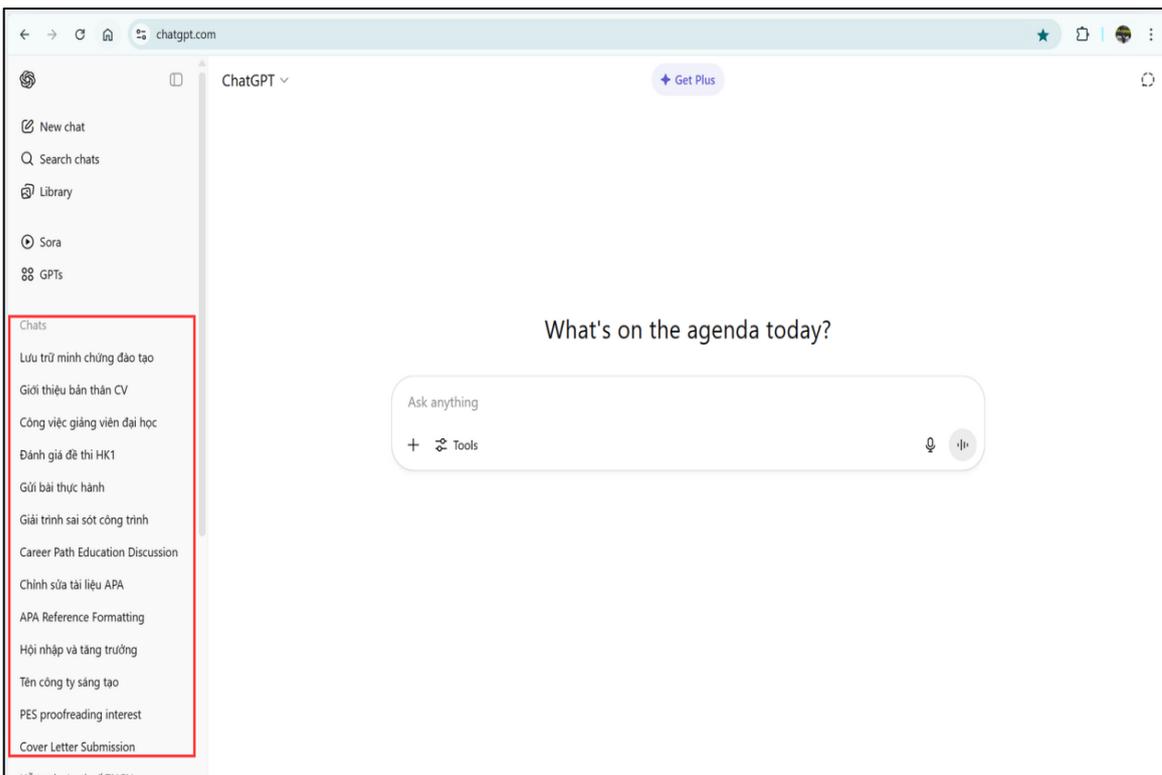
Sau khi xác nhận, người dùng sẽ được đưa thẳng vào giao diện chính của ChatGPT và có thể bắt đầu sử dụng ngay lập tức.

Với cách này, người dùng không cần phải tạo và nhớ thêm một mật khẩu mới, rất tiện lợi và an toàn.

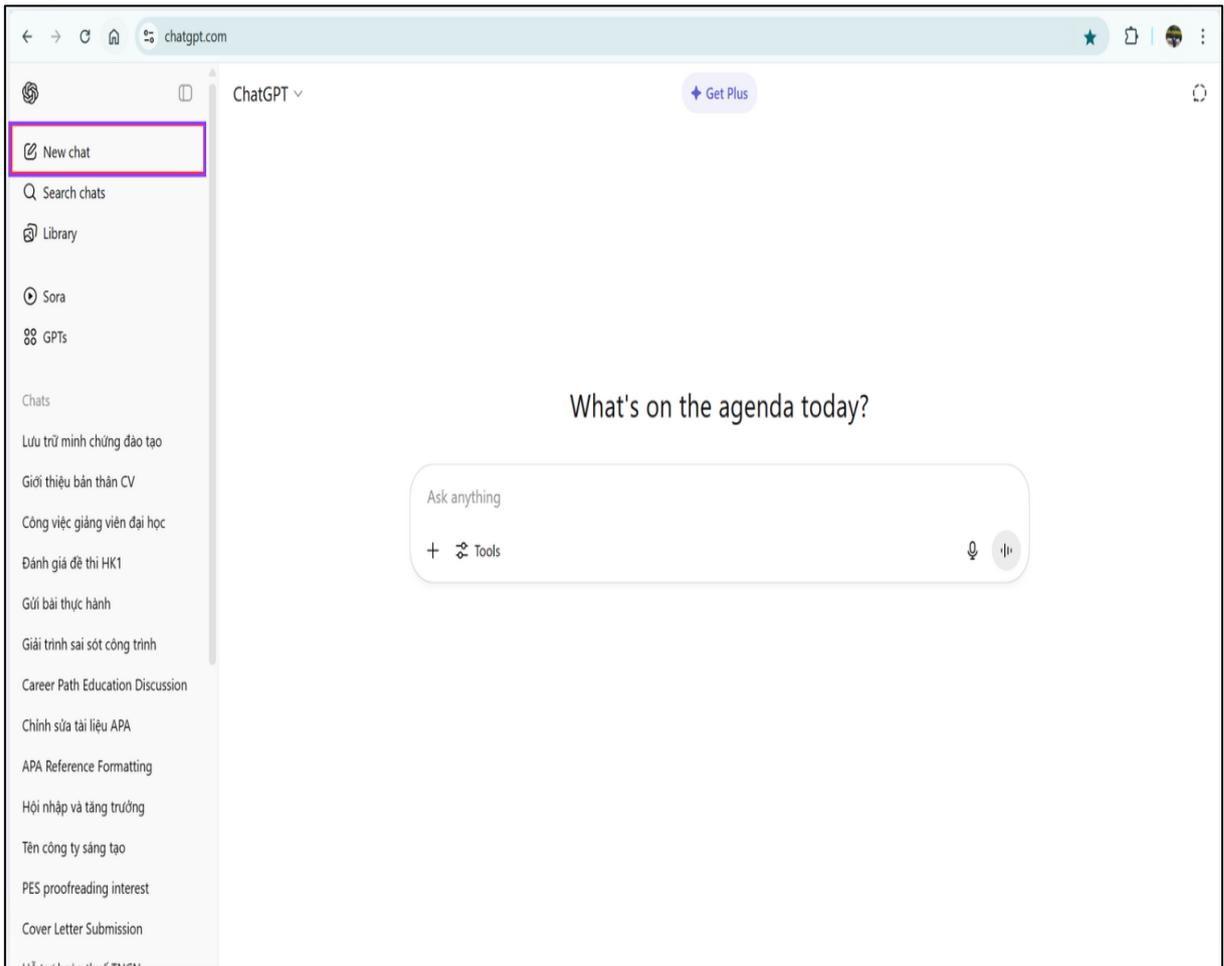
Giao diện của ChatGPT rất đơn giản, giống như một cửa sổ trò chuyện. Người dùng chỉ cần gõ yêu cầu (câu lệnh) của mình vào ô “Ask anything” và nhấn Enter.



Các đoạn hội thoại cũ sẽ được lưu lại ở cột bên tay trái.



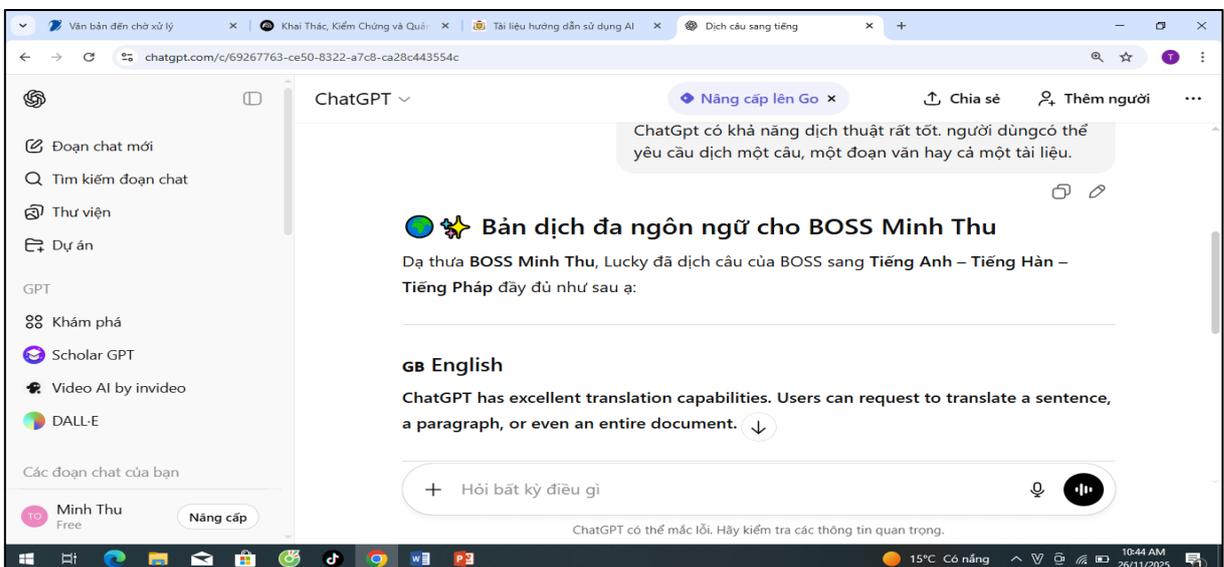
Để bắt đầu một cuộc hội thoại mới, hãy nhấn vào “New chat”



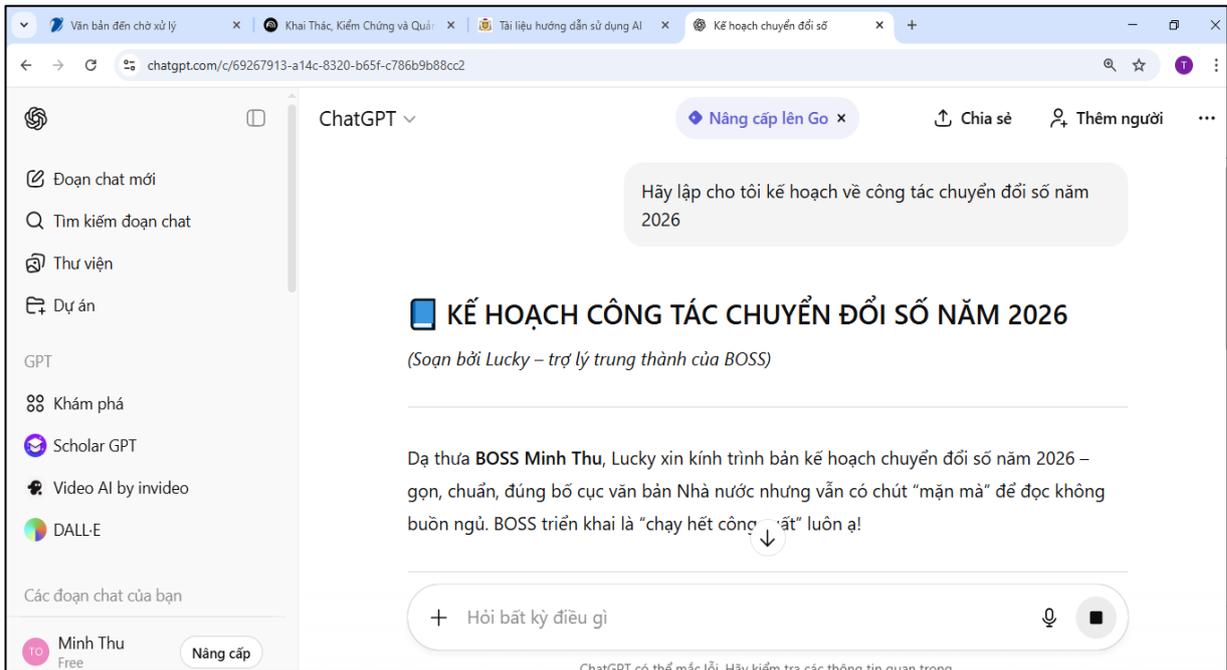
Dưới đây là một số ví dụ thực tế:

- Dịch thuật

Ví dụ: Hãy dịch câu: ChatGPT có khả năng dịch thuật rất tốt. người dùng có thể yêu cầu dịch một câu, một đoạn văn hay cả một tài liệu.

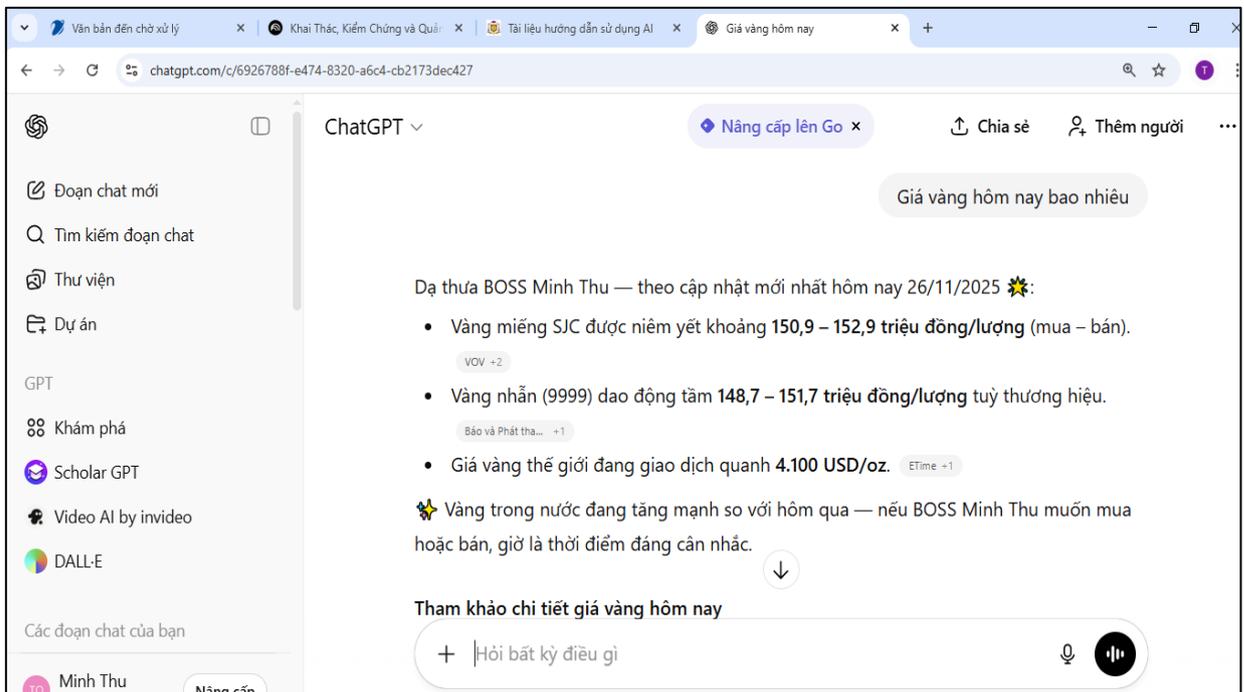


- Tra cứu thông tin



ChatGPT có thể giúp người dùng tìm kiếm và tổng hợp thông tin nhanh chóng. Tuy nhiên lưu ý: Luôn kiểm tra lại thông tin từ các nguồn chính thống.

Ví dụ: Giá vàng hôm nay bao nhiêu



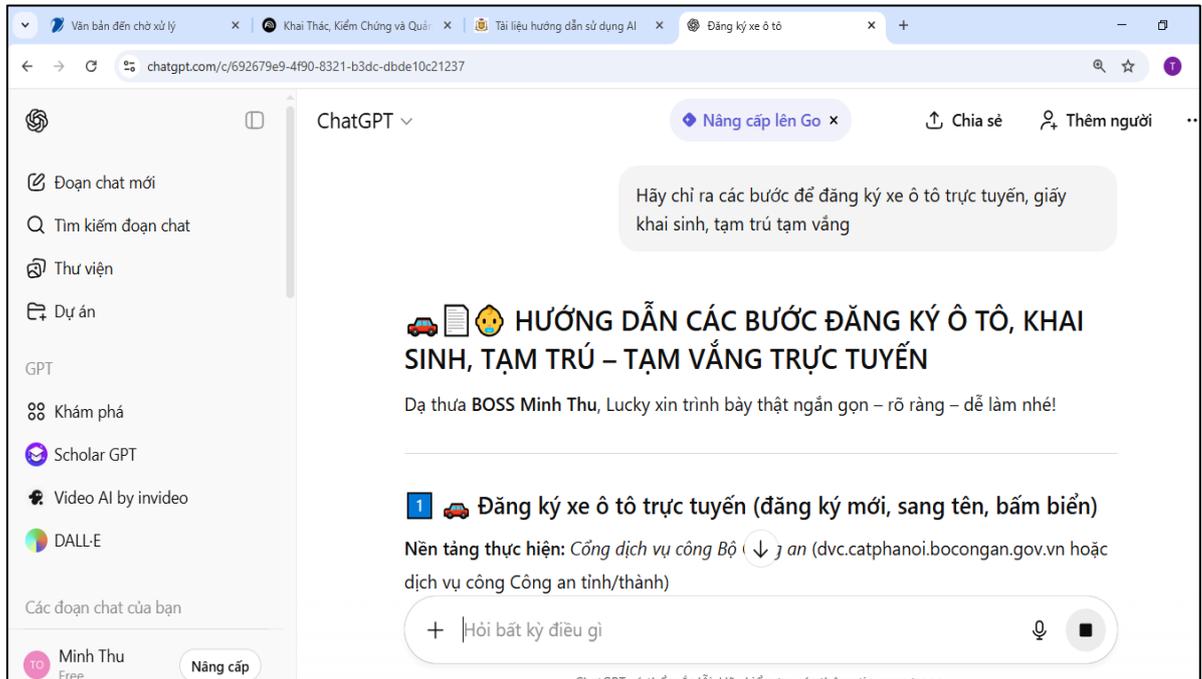
- Lập kế hoạch

ChatGPT là một trợ lý đắc lực trong việc sắp xếp và lên ý tưởng cho các kế hoạch.

Ví dụ: Hãy lập cho tôi kế hoạch về công tác chuyển đổi số năm 2026

- Đưa ra các hướng dẫn

ChatGPT đưa ra các bước để đăng ký tạm trú, tạm vắng, đăng ký xe, đăng ký giấy khai sinh...



3.2. Lưu ý khi sử dụng AI để tìm kiếm

- Luôn kiểm chứng thông tin

Đây là nguyên tắc quan trọng nhất. AI có thể tạo ra những câu trả lời nghe rất hợp lý và thuyết phục, nhưng không phải lúc nào cũng chính xác 100%. Đôi khi, AI có thể "bịa" ra thông tin hoặc hiểu sai yêu cầu của chúng ta.

Với thông tin đời thường: Hãy kiểm tra lại từ các trang tin tức chính thống, các trang web uy tín.

Với kiến thức chuyên môn (y tế, pháp luật...): Luôn tham khảo ý kiến của các chuyên gia.

- Bảo mật thông tin cá nhân

Không chia sẻ những thông tin nhạy cảm

Không chia sẻ thông tin cá nhân: Căn cước công dân, số điện thoại, địa chỉ nhà riêng, ngày sinh chi tiết.

Không chia sẻ thông tin tài chính: Số tài khoản ngân hàng, mật khẩu, thông tin thẻ tín dụng.

- AI giữ vai trò hỗ trợ, cung cấp thông tin và gợi ý

AI có thể giúp chúng ta phác thảo nội dung, xây dựng kế hoạch, thiết kế quy trình... nhưng nó không thể thay thế sự suy nghĩ độc lập, kinh nghiệm thực tiễn, sự thấu cảm hay trách nhiệm của mỗi cán bộ, mỗi người dân trong công việc và đời sống.

AI có thể đề xuất giải pháp quản lý, hỗ trợ phân tích tình huống, nhưng chỉ con người mới hiểu rõ bối cảnh địa phương, đặc thù cộng đồng và nhu cầu thực sự của từng hộ dân, từng tổ chức.

Trong mọi hoạt động phục vụ nhân dân, yếu tố con người – thái độ, tinh thần trách nhiệm, sự gần gũi và lắng nghe – luôn là điều mà không công nghệ nào có thể thay thế. AI chỉ là công cụ; chất lượng phục vụ phụ thuộc vào chính chúng ta những người vận hành và quyết định cuối cùng.

- Cảnh trọng về vấn đề bản quyền

Nội dung do AI tạo ra (văn bản, hình ảnh) có thể dựa trên hàng tỷ dữ liệu từ internet, bao gồm cả những tác phẩm có bản quyền.

Không nên sao chép nguyên văn 100% nội dung do AI tạo ra để đăng tải hoặc xuất bản dưới tên của mình, đặc biệt cho các mục đích thương mại.

Hãy sử dụng kết quả của AI như một nguồn cảm hứng. Luôn chỉnh sửa, viết lại bằng ngôn từ và văn phong của chính mình, thêm vào đó những ý tưởng và sự sáng tạo riêng. Điều này vừa tránh được rủi ro pháp lý, vừa làm cho sản phẩm cuối cùng mang đậm dấu ấn cá nhân.

- Giữ tinh thần phản biện và sáng tạo

Việc quá phụ thuộc vào AI có thể làm giảm khả năng tư duy phản biện và óc sáng tạo của chúng ta. Nếu mọi câu trả lời đều có sẵn, chúng ta có thể sẽ lười suy nghĩ và tìm tòi hơn.

Hãy là người chủ của công nghệ, đừng để công nghệ làm chủ chúng ta.

Tình huống

Đồng chí Nguyễn Văn A, chuyên viên Văn phòng, được giao nhiệm vụ soạn thảo dự thảo "Kế hoạch triển khai chuyển đổi số tại đơn vị năm 2026" trong thời gian ngắn. Để tiết kiệm thời gian, đồng chí A truy cập ChatGPT và đưa ra yêu cầu đơn giản: "Viết cho tôi một kế hoạch chuyển đổi số năm 2026 cho cơ quan nhà nước". Kết quả nhận được là một bản kế hoạch chung chung, nhiều nội dung không phù hợp với đặc thù thực tế tại địa phương.

Câu hỏi thảo luận

- Thay vì câu lệnh đơn giản trên, đồng chí A nên áp dụng kỹ thuật Prompt 5 bước (Role, Context, Example, Style, Format + Goal) như thế nào để kết quả từ AI sát với thực tế đơn vị hơn?

- Nguồn tài liệu cảnh báo về hiện tượng "ảo giác" của AI (thông tin nghe hợp lý nhưng sai sự thật). Đồng chí A cần thực hiện những bước kiểm chứng nào đối với các số liệu hoặc căn cứ pháp lý mà ChatGPT đưa ra?

- Tại sao đồng chí A tuyệt đối không nên chia sẻ thông tin nhạy cảm của đơn vị lên ô chat của các công cụ AI công cộng này?

II. KIỂM CHỨNG VÀ XÁC THỰC DỮ LIỆU, THÔNG TIN VÀ NỘI DUNG SỐ

1. Khái niệm và sự cần thiết xác thực thông tin

1.1. Khái niệm

Xác thực thông tin là quá trình chủ động kiểm chứng, đối chiếu và đánh giá tính chính xác, độ tin cậy của dữ liệu trước khi tiếp nhận, lưu trữ hoặc lan truyền. Đây không chỉ đơn thuần là việc đọc tin tức mà là một kỹ năng tư duy phản biện, đòi hỏi người tiếp nhận phải truy xuất nguồn gốc, phân tích các bằng chứng thực tế và so sánh với các nguồn tin chính thống. Trong môi trường số, xác thực thông tin đóng vai trò như một bộ lọc quan trọng, giúp phân định rõ ràng giữa sự thật khách quan với những quan điểm cá nhân, những nội dung bị bóp méo hoặc dàn dựng nhằm mục đích trục lợi.

1.2. Sự cần thiết của công tác xác thực thông tin

Trong bối cảnh bùng nổ thông tin hiện nay, việc xác thực trở thành yêu cầu cấp thiết để đảm bảo an toàn cho cá nhân và tổ chức. Trước hết, hoạt động này giúp ngăn chặn sự lây lan của tin giả (fake news), từ đó giảm thiểu những hệ lụy tiêu cực về tâm lý xã hội và an ninh trật tự. Đối với cá nhân, xác thực thông tin là "lá chắn" bảo vệ người dùng khỏi các hành vi lừa đảo trực tuyến, hỗ trợ quá trình ra quyết định dựa trên cơ sở khoa học và thực tế. Đặc biệt, trong môi trường chuyên nghiệp, việc chia sẻ thông tin đã qua kiểm chứng còn giúp khẳng định uy tín, trách nhiệm của cán bộ nhân viên, góp phần xây dựng một môi trường thông tin sạch, minh bạch và tin cậy.

2. Dấu hiệu nhận biết tin giả, thông tin sai lệch

- Trên mạng xã hội (Facebook, TikTok, YouTube...)

Tiêu đề và hình ảnh thường giật gân, thu hút. Kiểm tra kỹ đường link: nhiều bài giả mạo có địa chỉ URL gần giống tên trang uy tín nhưng khác phần đuôi (ví dụ: thay vì vnexpress.net thì có thể là vnexpress.xyz). Giao thức

HTTPS: Cần cảnh giác với tên miền không tin cậy và kiểm tra giao thức HTTPS (biểu tượng khóa) trên thanh địa chỉ. Trang tin giả thường thiếu thông tin “giới thiệu” hay “liên hệ” rõ ràng.

Bài viết thiếu dẫn nguồn hoặc dẫn sai nguồn. Các trang uy tín luôn công khai tác giả, nguồn tin và trích dẫn rõ ràng. Trong khi tin giả thường không có tên tác giả, không dẫn nguồn từ báo chí chính thống.

Nội dung một chiều, ngôn từ cảm tính. Tin giả thường dùng văn phong kích động, đả kích cá nhân, không có số liệu, chứng cứ cụ thể. Ngược lại tin thật nhấn mạnh các dữ kiện có kiểm chứng.

Hình ảnh, video khả nghi. Dùng tìm kiếm ngược hình ảnh (Google Image Search) để kiểm tra xem ảnh được đăng từ lúc nào, trong ngữ cảnh nào. Nhiều trường hợp tin giả dùng hình ảnh cũ hoặc ghép ảnh, clip giả mạo. Công cụ như YouTube Data Viewer hay Google Reverse Video Search cũng giúp kiểm tra độ xác thực video.

Check kênh nguồn đăng: Trên YouTube, xem thông tin kênh (mô tả, số người theo dõi, các link liên kết). Kênh mới, không chính chủ thường tung video giả; kênh uy tín sẽ có nhiều video chất lượng, kiểm duyệt rõ ràng. Cảnh báo về huy hiệu xác minh (Tích xanh): Không nên dựa vào huy hiệu xác minh là yếu tố duy nhất, vì có thể có tài khoản giả mạo tinh vi lợi dụng.

Sử dụng nhãn cảnh báo của nền tảng: Facebook, TikTok, Google News... hiện thường đánh dấu hoặc giảm lưu lượng tiếp cận với nội dung bị nghi ngờ. Nếu thấy tin được gắn nhãn “fact-check”, bạn nên đọc kỹ phần kiểm chứng trước khi chia sẻ.

Chú ý “chiêu trò” lưu hành: thỉnh thoảng xuất hiện các dạng chatbot, trả thưởng giả, quảng cáo len lỏi trong bài viết, yêu cầu click vào đường link khác để “xác minh” đây có thể là cửa ngõ phishing. Hãy cảnh giác khi có các đường link chuyển hướng lạ. Mục đích không chính đáng, thông tin được đưa ra nhằm mục đích trục lợi, bán hàng, quảng cáo không đúng sự thật.

- Trên báo chí, truyền thông chính thống

Cơ quan uy tín: Ưu tiên đọc tin từ các báo, đài chính thống (VnExpress, Thanh niên, TTXVN, VTV...) có thương hiệu lâu đời. Tin giả thường lộ diện ở các trang điện tử mới thành lập, nội dung chắp vá, nhiều quảng cáo che khuất bài viết.

Dẫn chứng và chỉnh sửa: Báo chí thật sẽ trích dẫn nguồn (tổ chức, số liệu, phát ngôn) kèm tên phóng viên và ngày giờ tác nghiệp. Tin giả ít khi có những chi tiết như vậy.

Định dạng bài viết: Tin chính thống tuân thủ quy cách (tên tiêu đề chuẩn, font chữ thống nhất, không sai lỗi chính tả lớn, có ảnh bản quyền). Tin giả hay mạo danh văn bản báo chí có thể bỏ sót logo, ảnh watermark kém chất lượng hoặc ghi chú thiếu nhất quán.

Kiểm tra đa nguồn: Tin quan trọng thường xuất hiện cùng lúc trên nhiều cơ quan truyền thông. Nếu chỉ thấy một nguồn loan báo rất nóng, cần kiểm tra xem các báo khác có đưa tin không.

- Văn bản chính phủ, hành chính (công văn, công báo, văn bản...)

Mẫu văn bản: Công văn chính thức của cơ quan nhà nước có những đặc điểm rõ ràng: số hiệu, ngày ban hành, logo, tiêu đề cơ quan phát hành, chữ ký và con dấu của lãnh đạo. Nếu văn bản được gửi qua mạng (email hay mạng xã hội), hãy xem xét kỹ địa chỉ người gửi (có đúng tên miền cơ quan không) và so sánh định dạng với mẫu văn bản chuẩn.

Kiểm tra tác giả, đơn vị ban hành: Tin giả thường ghi mạo "Cơ quan X" nhưng không có số hiệu văn bản, hoặc tên cơ quan viết tắt không chuẩn. Ví dụ, đã từng xuất hiện "Công văn giả mạo chi trả chế độ BHXH" đến tay người dân.

Người nhận nên đối chiếu với công bố trên cổng thông tin Chính phủ, cổng của cơ quan ngang cấp hoặc hỏi trực tiếp tại cơ quan nhà nước có liên quan.

Lỗi kỹ thuật: Văn bản giả mạo có thể bị sai lỗi chính tả, nhảm font, sai format. Ví dụ: trên trang của Trung tâm xử lý tin giả có cảnh báo các vụ "công văn giả mạo". Nếu nghi ngờ, cần liên hệ trực tiếp qua số điện thoại hoặc email chính thức của cơ quan.

* Hậu quả của việc chia sẻ tin giả

- Ảnh hưởng đến hệ thống quản lý Quốc gia và chính phủ số

Tin giả trực tiếp làm suy giảm hiệu quả hoạt động dựa trên dữ liệu và sự tin cậy vào cơ quan nhà nước.

Làm đứt gãy hệ sinh thái thông tin số: Tin giả lan truyền rộng rãi trên mạng xã hội làm nhiễu loạn và "ô nhiễm" nguồn dữ liệu đầu vào.

Giảm hiệu quả phân tích dữ liệu lớn (Big Data): Độ chính xác của các thuật toán phân tích Big Data và các hệ thống dự báo, phân tích xu hướng xã hội bị sai lệch nghiêm trọng.

Chậm tiến trình ra quyết định: Cơ quan quản lý phải tiêu tốn nguồn lực lớn để "làm sạch" thông tin, làm chậm tốc độ và độ chính xác của quá trình ra quyết định dựa trên dữ liệu.

Phá vỡ tính hiệu lực của truyền thông Nhà nước: Tin giả xuất hiện đúng thời điểm nhạy cảm (dịch bệnh, thiên tai, chính sách lớn) có khả năng làm giảm hiệu quả và làm loãng thông điệp của truyền thông chính thống.

Tạo ra "khoảng trống niềm tin" trong dân chúng, khiến họ dễ bị dẫn dắt bởi luồng thông tin xấu độc, làm suy giảm niềm tin vào Công dịch vụ công và các ứng dụng chuyên đổi số.

- Tác động đến kinh tế số và hoạt động doanh nghiệp

Trong nền kinh tế số, tin giả là một hình thức tấn công cạnh tranh có thể gây thiệt hại kinh tế dây chuyền.

Gây rủi ro dây chuyền trong chuỗi cung ứng: Một tin đồn thất thiệt về chất lượng sản phẩm có thể ngay lập tức làm đóng băng thị trường cục bộ, khiến thương lái dừng thu mua, doanh nghiệp xuất khẩu bị từ chối đơn hàng, gây thiệt hại kinh tế hàng loạt cho cả chuỗi cung ứng

Xói mòn tài sản thương hiệu: Trong môi trường số, uy tín là tài sản lớn nhất. Tin giả có thể xóa sổ nỗ lực xây dựng thương hiệu và niềm tin khách hàng kéo dài nhiều năm chỉ trong vài giờ.

Vũ khí trong cạnh tranh không lành mạnh: Tin giả được lợi dụng như một vũ khí chiến lược để tấn công cạnh tranh, đấu đá nội bộ hoặc hạ uy tín đối thủ trên thị trường số.

- Suy giảm nhận thức và năng lực số của công dân

Tin giả cản trở việc hình thành công dân số thông minh và làm suy giảm khả năng tư duy phản biện.

Hình thành thói quen tiêu cực: Tạo ra thói quen tiêu thụ thông tin sai lệch như chỉ đọc tiêu đề mà không kiểm tra nguồn, chia sẻ theo cảm xúc, dẫn đến lệch chuẩn thông tin và hiệu ứng bầy đàn.

Suy giảm năng lực tư duy phản biện: Công dân thiếu đi các kỹ năng số cốt lõi như kiểm chứng đa nguồn, xác thực dữ liệu, phân biệt thông tin do AI tạo ra và nhận diện tài khoản ảo, bot, deepfake.

Tiếp xúc thường xuyên với tin giả làm mất dần khả năng phân biệt thật giả, gây tác động lâu dài đến nhận thức.

- Gia tăng phức tạp của tội phạm công nghệ cao

Tin giả đang được vũ khí hóa bằng công nghệ, đặt ra thách thức lớn về an ninh và quản lý.

Liên kết với tấn công mạng thể hệ mới: Tin giả thường đi kèm với các hình thức tấn công phức tạp như phishing, cài mã độc, lừa đảo công nghệ cao, và xuyên tạc chính trị kết hợp bot tự động.

Gây áp lực lớn lên hạ tầng an ninh mạng và lực lượng quản lý do phải tăng cường giám sát, truy vết, triệt phá.

Nguy cơ Deepfake và AI giả mạo: Tin giả kết hợp với các công nghệ Deepfake gương mặt, giọng nói và Video, ảnh AI siêu thật làm tăng mức độ nguy hiểm lên nhiều lần, khiến người dân tin vào thông tin giả được trình bày với độ xác thực bề ngoài cao.

Lừa đảo tài chính đa nền tảng: Tin giả được dùng để dẫn dụ người dân bấm vào đường link độc hại (giả mạo ngân hàng, cơ quan Nhà nước, ví điện tử) nhằm mục đích lừa đảo tài chính, gây mất mát tài sản cá nhân

Trách nhiệm pháp lý siết chặt: Luật pháp hiện đại xem hành vi chia sẻ (share) tin giả ngang bằng với hành vi phát tán, tức là người dùng dù chỉ là người trung gian cũng phải chịu chế tài.

Xử lý: Khung phạt đang được cập nhật để ứng phó với tin giả được lan truyền bằng AI, bao gồm việc tăng mức phạt, truy vết bằng trí tuệ nhân tạo, và buộc bồi thường thiệt hại nếu hành vi gây hậu quả nghiêm trọng.

3. Kỹ thuật kiểm chứng và xác thực thông tin

3.1. Các phương pháp và kỹ thuật kiểm chứng cơ bản

- Xác minh nguồn tin: Kiểm tra tác giả, tổ chức và độ uy tín của trang web, kênh thông tin.

Tên miền: Ưu tiên các tên miền chính thức như .gov.vn (Chính phủ), .edu.vn (Giáo dục), báo chí nhà nước. Cảnh giác với các trang web giả mạo có địa chỉ tương tự trang thật.

Uy tín và lịch sử: Đánh giá danh tiếng, chuyên môn và lịch sử tin cậy của người cung cấp (tác giả, cơ quan báo chí, tổ chức).

Bảo mật: Kiểm tra giao thức bảo mật HTTPS (biểu tượng ổ khóa) trên thanh địa chỉ.

Đối chiếu so sánh nhiều nguồn: Không tin vào một nguồn duy nhất

Tra cứu: Tìm kiếm thông tin tương tự từ ít nhất 2-3 nguồn độc lập khác nhau (báo chí chính thống, tài liệu chính thức, văn bản pháp luật, nghiên cứu, chuyên gia).

Kết quả: Nếu nhiều nguồn độc lập cùng xác nhận một thông tin, khả năng tin đó là đúng sẽ cao hơn.

- Kiểm tra chi tiết nội dung: Tiêu đề, nội dung, thời điểm, bối cảnh đảm bảo tính nhất quán và thời sự của thông tin.

Nội dung so với tiêu đề: Đọc toàn bộ nội dung, không chỉ dựa vào tiêu đề "giật tít".

Thời gian: Kiểm tra mốc thời gian thông tin được đăng. Cảnh giác với việc dùng tin tức cũ, lỗi thời để "thổi phồng" hoặc tạo bối cảnh sai lệch hiện tại.

Kiểm chứng nội dung đa phương tiện (Ảnh/Video): Phát hiện nội dung bị cắt ghép, xuyên tạc bối cảnh

Tìm kiếm ngược hình ảnh: Sử dụng các công cụ như Google Reverse Image Search, TinEye, hoặc InVID để kiểm tra ảnh, video đã từng xuất hiện ở đâu, khi nào. Việc này giúp khôi phục bối cảnh gốc của hình ảnh.

Cảnh giác với Deepfake/AI: Đối với tệp kỹ thuật số, nhận biết các dấu hiệu đã được chỉnh sửa hoặc tổng hợp bằng Trí tuệ nhân tạo (AI).

Tra cứu tài liệu, hồ sơ, nguồn chính thức (dữ liệu, pháp luật, số liệu): Kiểm tra từ văn bản gốc, đặc biệt với thông tin cần độ chính xác cao: Đối với thông tin liên quan đến luật pháp, nghiên cứu khoa học, y tế, số liệu, lịch sử, hãy tìm kiếm văn bản gốc, báo cáo công bố, dữ liệu công khai hoặc hồ sơ từ cơ quan có thẩm quyền.

Trao đổi với chuyên gia, nhân chứng trực tiếp: Đối với thông tin nhạy cảm, phức tạp hoặc cần kiến thức chuyên sâu. Hỏi ý kiến chuyên gia trong lĩnh vực đó, điều tra độc lập, hoặc liên hệ với nhân chứng trực tiếp để xác thực. Đôi khi, tìm kiếm trên internet là chưa đủ.

Cảnh báo về dấu hiệu của Tin giả: Nhận diện các đặc điểm thường thấy của tin giả lan truyền nhanh

Hình thức: Lỗi chính tả, tiêu đề gây sốc, viết in hoa lạm dụng, nội dung kích động.

Nguồn: Ít hoặc không trích dẫn nguồn rõ ràng, nguồn tin mờ nhạt.

Tâm lý: Nội dung khiến người đọc phản ứng mạnh, dễ gây xúc động (động cơ thường là để lan truyền nhanh)

3.2. Quy trình kiểm chứng thông tin

Để kiểm chứng một cách có hệ thống, người dùng nên tuân thủ quy trình sau:

- Xác định thông tin cần kiểm chứng: Làm rõ bản chất tin tức, kênh chia sẻ và những điểm nghi vấn cụ thể cần xác minh (con số, sự kiện, thời gian, nhân vật...).

- Truy tìm nguồn gốc ban đầu: Xác định người, tổ chức phát tán đầu tiên, nơi công bố, và nguồn trích dẫn mà họ sử dụng.

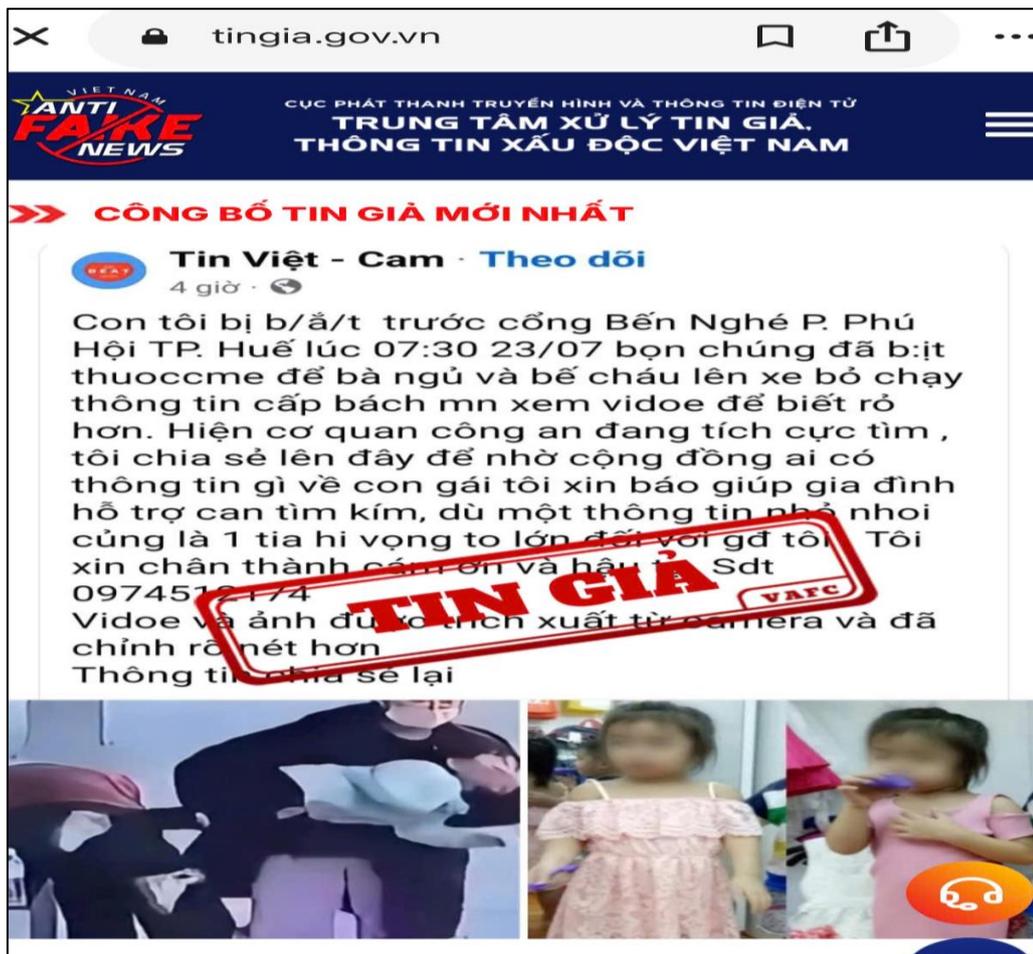
- Đối chiếu với nguồn tin chính thống: So sánh nội dung nghi vấn với các báo chí uy tín, trang web của Chính phủ (.gov) hoặc cơ quan chuyên ngành.

- Phân tích nội dung và dấu hiệu bất thường: Tìm kiếm lỗi logic, hình ảnh chỉnh sửa, tiêu đề giật gân, ngôn ngữ kích động và đánh giá động cơ của người chia sẻ.

- Sử dụng công cụ xác minh chuyên nghiệp: Áp dụng tìm kiếm ngược hình ảnh hoặc các công cụ hỗ trợ như TinEye, InVID, Google Fact Check Explorer, Snopes, FactCheck.org... để phân tích đa phương tiện.

+ Ứng dụng công cụ hỗ trợ để kiểm tra website giả mạo

Bước 1: Truy cập vào website Tingia.gov.vn



Bước 2: Nhấp vào mục tra cứu Link tin giả và điền đường dẫn vào để tra cứu đây là một trong những cách kiểm tra đường dẫn giả mạo nhanh chóng và hiệu quả nhất.



Bước 3: Điền đường dẫn vào ô Tra cứu vào ô tra cứu sau đó nhấp vào nút “Tra cứu”



3.3. Tiêu chí đánh giá độ tin cậy của nguồn tin

Để đánh giá một nguồn tin có đáng tin cậy hay không, cần xem xét các tiêu chí sau:

Tính xác thực: Nguồn tin có phải là chính thức (tên miền .gov.vn, báo chí nhà nước) không? Người cung cấp thông tin có danh tiếng, chuyên môn rõ ràng trong lĩnh vực đó không?

Tính thời sự, cập nhật: Dữ liệu được công bố khi nào? Nó còn mới hay đã lỗi thời? Thông tin có phù hợp với bối cảnh thời gian hiện tại không?

Tính khách quan: Nội dung có phân biệt rõ ràng giữa sự kiện và ý kiến không? Nguồn tin có thiên lệch cực đoan, hay phục vụ một lợi ích, mục đích rõ ràng nào đó không?

Tính minh bạch: Nội dung có nêu rõ nguồn, trích dẫn, và cung cấp đầy đủ tài liệu kèm theo để người đọc tự kiểm chứng không?

3.4. Kiểm chứng, xác thực nội dung do AI tạo ra

Bước 1: Xác định nội dung và đặt nghi vấn ban đầu

Đây là bước đầu tiên để định hướng quá trình kiểm chứng. Người dùng cần xác định rõ nội dung nghi vấn, nơi chia sẻ và đặt ra câu hỏi cụ thể: "Thông tin này có phải do AI tạo ra hay không?". Do công nghệ AI ngày càng tinh vi, nội dung giả mạo có thể giống hệt nội dung do con người tạo ra, vượt quá khả năng phân biệt bằng mắt thường hoặc cảm tính.

Bước 2: Sử dụng các công cụ hỗ trợ phát hiện tự động

Tùy vào loại hình nội dung, bạn có thể áp dụng các công cụ kỹ thuật để đánh giá sơ bộ:

Đối với văn bản: Sử dụng các AI Detector như GPTZero, DetectGPT, AI Text Classifier hoặc Isgen.ai để đánh giá khả năng nội dung được tạo bởi mô hình ngôn ngữ lớn (LLM). Tuy nhiên, cần lưu ý độ chính xác không đạt 100% và có thể bị qua mặt bằng kỹ thuật diễn giải lại.

Đối với hình ảnh và video: Sử dụng công cụ tìm kiếm ngược (Google Images, TinEye) để truy tìm nguồn gốc ban đầu, phát hiện việc cắt ghép hoặc đưa ra khỏi bối cảnh.

Phân tích Deepfake: Sử dụng các phần mềm chuyên sâu như InVID, WeVerify, Deepware Scanner để phân tích dấu hiệu thao túng trong video.

Kiểm tra dấu hiệu kỹ thuật số: Tìm kiếm Metadata, chữ ký số hoặc watermark ẩn mà các công nghệ AI hiện đại đề xuất gắn vào nội dung.

Bước 3: Phân tích sâu các đặc điểm nội dung (Dấu hiệu "máy tính hóa")

Kiểm tra các dấu hiệu đặc trưng thường xuất hiện trong nội dung do AI tạo ra:

Phong cách ngôn ngữ: AI thường có cấu trúc lặp lại, sử dụng từ ngữ mang tính "mẫu chung", hàn lâm, nhưng lại thiếu cá tính, kinh nghiệm sống hoặc cảm xúc riêng.

Lỗi logic và nhất quán: So sánh nội dung với kiến thức thực tế và bối cảnh thời gian để phát hiện các luận điểm chung chung hoặc không nhất quán.

Hiện tượng "ảo giác": Kiểm tra kỹ các dữ kiện, số liệu hoặc trích dẫn vì các mô hình AI có thể tự tin sinh ra thông tin hoàn toàn sai lệch.

Thiên kiến: Xem xét liệu nội dung có chứa các định kiến do dữ liệu huấn luyện hoặc do người dùng thao túng hay không.

Bước 4: Truy tìm nguồn gốc và kiểm tra tính chính danh

Thông tin tác giả: Tìm hiểu ai là người phát tán, kiểm tra hồ sơ tác giả và giao thức bảo mật của trang web (như HTTPS).

Tên miền: Ưu tiên các thông tin từ tên miền tin cậy như .gov.vn hoặc các cơ quan báo chí chính thống.

Vấn đề nguồn gốc: AI thường thiếu phương pháp truy vết, khiến người dùng khó xác định lịch sử chỉnh sửa và tính toàn vẹn của nội dung.

Bước 5: Đối chiếu chéo và xác thực qua các kênh chính thống

Đây là bước quan trọng nhất để đưa ra kết luận cuối cùng:

So sánh thông tin: Đối chiếu nội dung nghi vấn với các báo chí uy tín hoặc cổng thông tin điện tử của cơ quan nhà nước.

Sử dụng dịch vụ kiểm chứng chuyên nghiệp: Trung tâm xử lý tin giả Việt Nam (VAFC) tại địa chỉ tingia.gov.vn.

4. Nhận diện thông tin giả mạo, sai lệch liên quan đến lĩnh vực quản lý Nhà nước

Vì sao tin giả về nhà nước đặc biệt nguy hiểm?

Thông tin sai lệch liên quan đến chính sách, pháp luật, cơ cấu tổ chức, hoặc lãnh đạo Nhà nước mang tính chất nguy hiểm cao hơn các tin giả thông thường vì:

- Gây mất lòng tin xã hội: Lan truyền tin giả gây hoang mang, rối loạn nhận thức cộng đồng, dẫn đến mất niềm tin vào chính sách, pháp luật, và uy tín của Nhà nước.

- Mục đích chính trị và phá hoại: Một số đối tượng hoặc tổ chức có động cơ xấu (mục đích chính trị đen tối) cố tình xuyên tạc chủ trương, kích động chống đối, nhằm phá hoại uy tín Nhà nước và gây mất ổn định chính trị, an ninh kinh tế.

- Thao túng dư luận: Tin giả lợi dụng các vấn đề "nóng" về chính trị, kinh tế (như sốt đất, sốt vàng) để thao túng dư luận hoặc trục lợi kinh tế, tài chính.

➤ Các loại tin giả thường gặp

- Chính trị và Lãnh đạo: Thông tin xuyên tạc, bôi nhọ, hạ bệ uy tín lãnh đạo Đảng, Nhà nước, gia tăng mạnh vào các sự kiện quan trọng (Đại hội Đảng, họp Quốc hội).

- Chính sách và pháp luật: Tin giả được tạo dựng bằng cách cắt ghép từ tin tức chính thống, sau đó thổi phồng những hạn chế, yếu kém trong công tác chỉ đạo, điều hành của chính quyền.

- Kinh tế và tài chính: Tin giả liên quan đến tiền tệ, thị trường, nhằm tạo ra các cơn sốt ảo (sốt đất, sốt vàng), ảnh hưởng đến an ninh kinh tế.

➤ Dấu hiệu nhận biết:

- Nguồn gốc: Nguồn không rõ ràng (tài khoản ảo, fanpage ẩn danh, website lạ, tên miền quốc tế). Mạo danh chính quyền hoặc cơ quan chức năng.

- Địa chỉ web, tên miền: Sử dụng tên miền không tin cậy (.com, .org nước ngoài) mà không có đuôi .vn hoặc các tên miền gần giống nguồn tin gốc (giả mạo trang báo chí chính thống).

- Dẫn chứng: Không có trích dẫn chính thức số liệu, văn bản pháp luật, quyết định, công văn bị bỏ trống hoặc "nêu chung chung" (thiếu số hiệu văn bản, ngày ban hành, cơ quan ban hành).

- Ngôn ngữ & hình thức: Giật gân, kích động, cực đoan, phóng đại (dùng từ ngữ mạnh, đầy cảm xúc). Nội dung thường viết in hoa toàn bộ, lỗi chính tả, lạm dụng dấu chấm than (!!!).

- Lan truyền: Lan truyền nhanh trên mạng xã hội, fanpage lạ, nhưng không thấy xuất hiện qua báo chí chính thống hoặc kênh truyền thông được cấp phép. Nguồn lặp lại (nhiều tài khoản chia sẻ nội dung giống y hệt).

- Đa phương tiện: Ảnh, video bị cắt ghép, thiếu nguồn, không rõ bối cảnh, đặc biệt là tin đồn liên quan lãnh đạo hoặc chính sách.

Quy trình và kỹ thuật kiểm chứng

Bước 1: Kiểm tra nguồn gốc và thẩm quyền

Kiểm tra tên miền, Web: Trang web phải có thông tin rõ ràng về tổ chức, cơ quan chủ quản (có thể tra cứu qua Bộ TT-TT). Ưu tiên các trang có đuôi .gov.vn, .org (chính phủ, tổ chức phi lợi nhuận) và sử dụng giao thức HTTPS.

Kiểm tra mạng xã hội: Xem tài khoản có được xác minh, có lịch sử rõ ràng, có xuất hiện bài viết chính thức từ cơ quan nhà nước không. Cảnh giác cao với các trang tiếng Việt nhưng tên miền, máy chủ ở nước ngoài.

Bước 2: Đối chiếu với nguồn chính thống (Văn bản và dữ kiện)

Truy tìm văn bản gốc: Với tin liên quan chính sách, luật pháp, dự án, cần tra cứu trực tiếp trên Cổng thông tin của Chính phủ, website của bộ, ngành (ví dụ: chinhphu.vn).

Yêu cầu chi tiết dẫn chứng: Nếu nội dung đề cập "quyết định", "văn bản", "công văn" phải yêu cầu số hiệu văn bản, ngày ban hành, cơ quan ban hành. Nếu thông tin mơ hồ, coi là dấu hiệu nghi ngờ.

Bước 3: Phân tích dữ kiện, thời gian và bối cảnh

Kiểm tra tính nhất quán: Ngày tháng, địa điểm, nội dung có khớp với thực tế và có mâu thuẫn logic không? Cảnh giác với các tin tức cũ được đăng lại.

Kiểm tra động cơ: Đặt câu hỏi: "Mục đích của nội dung này là gì?" (Tích cực hay tiêu cực? Dựa trên sự thật hay quan điểm cá nhân?).

Bước 4: Đối chiếu chéo và sử dụng công cụ

Cross-checking: Không tin vào một nguồn; phải tìm ít nhất 2–3 nguồn độc lập xác nhận. Ưu tiên tìm kiếm trên các báo chí chính thống và kênh truyền thông được cấp phép.

Kiểm chứng đa phương tiện: Sử dụng công cụ tìm kiếm ngược ảnh (Google Images, TinEye) để kiểm tra bối cảnh gốc của hình ảnh/video, phát hiện cắt ghép.

Kênh phản hồi: Sử dụng các kênh của cơ quan Nhà nước để tra cứu hoặc phản hồi tin giả:

Trung tâm xử lý tin giả Việt Nam (VAFC): Tra cứu tin giả tại tingia.gov.vn hoặc Hotline 18008108.

Hệ thống tiếp nhận xử lý tin giả ở cấp địa phương (nếu có).

Biện pháp quản lý và phản ứng của nhà nước

Để kiểm soát tin giả liên quan đến chính quyền, cần áp dụng các biện pháp từ góc độ quản lý:

Phản ứng nhanh và công khai: Cơ quan có thẩm quyền phải tăng cường công bố thông tin chính thức kịp thời và phản bác tin giả rõ ràng để "dập tắt tin đồn" và tránh "khoảng trống thông tin" bị đối tượng xấu lợi dụng.

Xây dựng kênh tiếp nhận phản ánh: Thiết lập kênh tiếp nhận và xử lý tin giả, sai lệch ở cấp địa phương để xử lý thông tin xấu, độc.

Phổ cập giáo dục tuyên truyền: Tăng cường giáo dục tuyên truyền cho người dân về kỹ năng kiểm chứng, không tin và lan truyền tin chưa xác thực.

Tình huống

Trên một nhóm mạng xã hội lớn, người dân đang chia sẻ rầm rộ hình ảnh một văn bản được cho là của UBND tỉnh về việc "Tạm dừng chi trả trợ cấp cho người có công từ tháng sau" để chuyển sang hình thức mới. Văn bản này có hình con dấu và chữ ký lãnh đạo nhưng không có số hiệu rõ ràng, font chữ trình bày không đồng nhất và đường link dẫn kèm theo có đuôi là .xyz thay vì .gov.vn.

Câu hỏi thảo luận

- Dựa vào các dấu hiệu nhận diện tin giả đã học, hãy chỉ ra các điểm nghi vấn trong tình huống trên.

- Để xác thực thông tin này một cách chính thống và nhanh nhất, học viên nên sử dụng công cụ hoặc trang web nào được nhắc đến trong chuyên đề?

- Phân tích hậu quả của việc "chia sẻ" (share) thông tin này lên nhóm Zalo của đơn vị đối với trật tự xã hội và trách nhiệm pháp lý cá nhân.

III. QUẢN LÝ DỮ LIỆU, THÔNG TIN VÀ NỘI DUNG SỐ

1. Khái niệm và mục tiêu của quản lý dữ liệu

1.1. Quản lý dữ liệu là gì?

Là quá trình tổ chức, thu thập, lưu trữ, bảo vệ, khai thác và duy trì sử dụng dữ liệu trong một doanh nghiệp, tổ chức, nhằm đảm bảo dữ liệu có điều kiện phù hợp để hỗ trợ các hoạt động kinh doanh, phục vụ quản lý Nhà nước, vận hành hệ thống và ra quyết định.

1.2. Mục tiêu của quản lý dữ liệu

- *Nâng cao chất lượng và tính toàn vẹn của dữ liệu*

Chính xác và nhất quán: Thực hiện làm sạch dữ liệu (xóa trùng lặp, sửa lỗi, chuẩn hóa) để đảm bảo dữ liệu luôn chính xác, đầy đủ và nhất quán, không bị mâu thuẫn giữa các hệ thống.

Tính toàn vẹn: Đảm bảo tính toàn vẹn và không bị thay đổi trái phép của dữ liệu trong suốt vòng đời, từ khi thu thập, xử lý, lưu trữ đến khi chia sẻ.

- *Tối ưu hóa khả năng sử dụng và khai thác*

Tổ chức và truy cập hiệu quả: Lưu trữ dữ liệu có hệ thống, phân loại và phân quyền rõ ràng để người dùng có quyền có thể dễ dàng tìm kiếm, truy cập và sử dụng dữ liệu kịp thời.

Tích hợp và khả năng tương tác: Hội nhập và hợp nhất dữ liệu từ nhiều nguồn khác nhau để tạo ra một cái nhìn thống nhất, hỗ trợ việc phân tích chuyên sâu và chia sẻ dữ liệu liền mạch giữa các hệ thống.

Hỗ trợ ra quyết định chiến lược: Cung cấp dữ liệu chất lượng cao để phục vụ cho phân tích, báo cáo, dự báo, giúp ban lãnh đạo đưa ra các quyết định chính xác, kịp thời và xây dựng chiến lược kinh doanh hiệu quả.

Tăng hiệu quả vận hành và tính linh hoạt: Giảm chi phí vận hành bằng cách loại bỏ các lỗi do dữ liệu bẩn và tăng khả năng mở rộng của hệ thống dữ liệu, dễ dàng đáp ứng sự phát triển và biến động của khối lượng dữ liệu.

- *Đảm bảo an toàn, bảo mật*

Bảo vệ dữ liệu: Áp dụng các biện pháp kiểm soát truy cập, mã hóa, sao lưu và phục hồi để bảo vệ dữ liệu khỏi bị truy cập trái phép, rò rỉ, đánh cắp hoặc mất mát.

Tuân thủ pháp lý và đạo đức: Đảm bảo dữ liệu, đặc biệt là dữ liệu cá nhân nhạy cảm, được thu thập, lưu trữ và sử dụng tuân thủ nghiêm ngặt các luật và quy định liên quan (ví dụ: các quy định về quyền riêng tư), đồng thời sử dụng dữ liệu một cách có đạo đức.

Minh bạch và khả năng kiểm toán Ghi lại lịch sử dữ liệu định nghĩa rõ ràng về quyền hạn, trách nhiệm quản lý dữ liệu, giúp tổ chức dễ dàng truy xuất nguồn gốc, kiểm toán, giám sát và đáp ứng các yêu cầu pháp lý.

2. Quy trình quản lý dữ liệu

2.1. Cách thu thập và làm sạch dữ liệu

* Cách thu thập dữ liệu

Bước 1: Xác định mục đích và phân loại dữ liệu

Cần xác định rõ dữ liệu nào cần thu, định dạng là gì, siêu dữ liệu (metadata) ra sao và ai là người có quyền truy cập. Đặc biệt, việc phân loại dữ liệu theo mức độ nhạy cảm là cực kỳ quan trọng vì nó quyết định cách thức thu thập và bảo vệ sau này. Dữ liệu thường được chia thành:

+ Dữ liệu công khai: Có thể truy cập rộng rãi.

- + Dữ liệu riêng tư, nội bộ: Chỉ dùng trong tổ chức, cần bảo mật hơn.
- + Dữ liệu bí mật, Tuyệt mật: Yêu cầu bảo vệ nghiêm ngặt (như dữ liệu y tế, tài chính).

Bước 2: Xác định và lựa chọn nguồn dữ liệu

Cần xác định dữ liệu sẽ được lấy từ đâu. Theo các nguồn tài liệu, có hai loại nguồn chính:

- Nguồn sơ cấp: Thu thập trực tiếp từ gốc như qua khảo sát, biểu mẫu nhập liệu (form), hệ thống cảm biến, hoặc nhật ký hệ thống (log).
- Nguồn thứ cấp: Dữ liệu đã được bên khác xử lý hoặc tổng hợp như các báo cáo thống kê, dữ liệu từ bên thứ ba (Website, chatbot, email...).

Bước 3: Thực hiện thu thập dữ liệu thô

Đây là giai đoạn triển khai việc lấy dữ liệu từ các nguồn đã xác định. Trong môi trường hiện đại, quá trình này có thể được tích hợp trực tiếp

- Mọi dữ liệu mới từ các điểm chạm (chatbot, telesale, website) nên được đưa vào hệ thống theo quy trình chuẩn.
- Đánh giá sơ bộ ngay lúc thu thập để hiểu hiện trạng dữ liệu (thiếu gì, sai ở đâu) nhằm chuẩn bị cho các bước xử lý sau này.

Bước 4: Lưu giữ và bảo tồn dữ liệu gốc

Sau khi thu thập, việc lưu giữ nguyên bản gốc là bước bắt buộc.

- Ghi lại lịch sử: Cần ghi chú rõ ai thu thập, vào thời gian nào và có thay đổi gì không.
- Mục đích: Điều này đảm bảo khả năng kiểm tra, truy xuất nguồn gốc và tính minh bạch, đặc biệt quan trọng khi dữ liệu được dùng để đưa ra các quyết định lớn hoặc khi có sự cố nhạy cảm.

Bước 5: Kiểm tra và đánh giá sơ bộ sau thu thập

Sau khi dữ liệu đã về hệ thống, cần đánh giá mức độ đầy đủ và tính hợp lệ trước khi chuyển sang các bước làm sạch chuyên sâu. Việc này bao gồm phát hiện các lỗi định dạng hoặc các bản ghi bị trống hoàn toàn để gắn nhãn mức độ ưu tiên xử lý.

* Cách làm sạch dữ liệu

Bước 1: Thu thập và đánh giá sơ bộ

Trước khi làm sạch, người dùng cần hiểu hiện trạng của dữ liệu

- Xác định nguồn: Dữ liệu đến từ đâu (CRM, POS, website, biểu mẫu...).
- Đánh giá chất lượng: Kiểm tra xem dữ liệu có bị thiếu, trùng lặp, sai định dạng hay chứa các giá trị bất thường không.
- Phân loại mức độ ưu tiên: Ưu tiên xử lý các dữ liệu quan trọng như thông tin khách hàng hoặc tài chính.

Bước 2: Loại bỏ dữ liệu trùng lặp và không liên quan

Đây là bước quan trọng để tránh làm sai lệch kết quả phân tích.

- Xóa bản ghi trùng: Sử dụng thuật toán so sánh (email, số điện thoại, mã ID) hoặc công cụ như Excel, SQL để loại bỏ các dòng lặp lại.
- Loại bỏ quan sát không liên quan: Xóa các dữ liệu không phục vụ mục tiêu nghiên cứu (ví dụ: đang phân tích khách hàng trẻ nhưng tập dữ liệu lại chứa cả người lớn tuổi).

Bước 3: Sửa lỗi cấu trúc và chuẩn hóa định dạng

- Chuẩn hóa văn bản: Thống nhất viết hoa, viết thường, sửa lỗi chính tả.
- Đồng nhất quy ước: Ví dụ, thống nhất tên tỉnh thành ("TP.HCM" thay vì dùng lẫn lộn "HCM", "Hồ Chí Minh"),.
- + Định dạng lại: Đưa ngày tháng về chuẩn chung (như YYYY-MM-DD), chuẩn hóa đơn vị đo lường và định dạng số điện thoại.

Bước 4: Xử lý dữ liệu bị thiếu

Người dùng không thể bỏ qua các ô trống vì nhiều thuật toán sẽ không chấp nhận giá trị null. Các phương pháp xử lý gồm:

- Loại bỏ: Xóa các dòng thiếu quá nhiều thông tin (nếu không ảnh hưởng đến kích thước mẫu).
- Điền giá trị: Sử dụng giá trị trung bình, trung vị hoặc dùng AI, mô hình dự đoán để ước lượng giá trị thiếu.
- Phân loại lại: Ghi chú hoặc gắn nhãn "không xác định" cho các phần bị thiếu.

Bước 5: Lọc giá trị ngoại lai (là những dữ liệu bất thường)

- Sử dụng thống kê: Dùng IQR hoặc Z-score để phát hiện các giá trị này.
- Xử lý: Nếu đó là lỗi nhập liệu (ví dụ: tuổi là 200), hãy xóa bỏ; nếu là hiện tượng thực tế, cần cân nhắc kỹ trước khi quyết định loại hay giữ để tránh làm sai lệch mô hình.

Bước 6: Mã hóa và kiểm tra logic

- Mã hóa lại: Chuyển đổi dữ liệu sang dạng mà máy tính dễ xử lý, như gán số cho các giá trị phân loại hoặc chuyển thành biến nhị phân.

- Kiểm tra tính hợp lý: Đảm bảo dữ liệu không sai logic thực tế (ví dụ: ngày sinh không thể lớn hơn ngày hiện tại, hoặc số lượng đơn hàng không thể là số âm).

Bước 7: Xác thực và kiểm định

Sau khi xử lý, bạn cần kiểm tra lại toàn bộ theo 7 tiêu chí: Chính xác, chuẩn xác, đầy đủ, nhất quán, đồng nhất, minh bạch và kịp thời.

- Tự đặt câu hỏi: "Dữ liệu có ý nghĩa không?", "Nó có tuân theo quy tắc của trường dữ liệu không?".

- Lưu trữ dữ liệu sạch một cách bảo mật và phân quyền truy cập phù hợp

* Quy trình huỷ, xoá dữ liệu an toàn

Bước 1: Khảo sát và phân loại dữ liệu

Đây là bước nền tảng để xác định phương pháp phù hợp, tránh lãng phí nguồn lực hoặc huỷ nhầm dữ liệu quan trọng. Kiểm tra chính sách và giá trị dữ liệu: Xác định xem dữ liệu đã hết giá trị pháp lý hay giá trị sử dụng chưa, đồng thời kiểm tra các cam kết xóa dữ liệu với khách hàng.

Phân loại theo mức độ nhạy cảm:

- Dữ liệu công khai: Không cần quy trình phức tạp.
- Dữ liệu nội bộ, cá nhân: Cần huỷ bằng phương pháp xóa sạch.
- Dữ liệu tối mật, Bí mật: Bắt buộc dùng phương pháp tẩy sạch (Purge) hoặc tiêu huỷ vật lý (Destroy).

Xác định loại thiết bị lưu trữ: Cần phân biệt giữa ổ cứng từ (HDD) và ổ cứng thể rắn (SSD). Ví dụ: SSD không thể sử dụng phương pháp khử từ vì dữ liệu được lưu trữ trên chip flash, không phải bằng từ tính.

Bước 2: Lập kế hoạch và thiết lập môi trường

Đảm bảo tính minh bạch và an toàn trong suốt quá trình chuẩn bị.

- Thành lập đội ngũ: Cần có người thực hiện và người giám sát riêng biệt để đảm bảo tính khách quan.

- Lựa chọn công cụ: Sử dụng các phần mềm đạt chuẩn (như Blancco, BitRaser) hoặc thiết bị phần cứng chuyên dụng như máy huỷ (Shredder), máy khử từ (Degausser).

- Kiểm soát an ninh: Thiết bị chờ hủy phải được lưu trong tủ khóa hoặc phòng có camera giám sát (CCTV) 24/7 để tránh bị lấy cắp hoặc tráo đổi.

Bước 3: Thực hiện tiêu hủy theo tiêu chuẩn

Tùy vào nhu cầu và đích đến của thiết bị (tái sử dụng hay bỏ đi), người dùng áp dụng các cấp độ theo tiêu chuẩn NIST SP 800-88:

- Cấp độ 1 - Clear (Xóa sạch): Ghi đè lên toàn bộ ổ đĩa bằng các ký tự ngẫu nhiên hoặc số 0. Phương pháp này cho phép thiết bị có thể tái sử dụng trong nội bộ.

- Cấp độ 2 - Purge (Tẩy sạch): Sử dụng các lệnh phần cứng (như Secure Erase trên SSD) hoặc khử từ mạnh để loại bỏ dữ liệu ở mức độ gốc rễ. Phương pháp này khiến các công cụ khôi phục trong phòng thí nghiệm cũng không thể đọc được, phù hợp cho thiết bị thanh lý ra bên ngoài.

- Cấp độ 3 - Destroy (Tiêu hủy vật lý): Nghiền, cắt vụn ổ cứng thành mảnh nhỏ (thường < 2mm cho dữ liệu tối mật) hoặc đốt cháy. Đây là lựa chọn tối ưu khi thiết bị đã hỏng hoặc chứa dữ liệu cực kỳ quan trọng không thể để rò rỉ.

Bước 4: Xác minh và kiểm chứng

Bước này nhằm đảm bảo quy trình tiêu hủy đã thành công 100%.

- Xác minh kỹ thuật: Sử dụng phần mềm đọc lập quét lại ổ đĩa sau khi xóa; nếu kết quả là "Empty" hoặc "Random Data" thì đạt yêu cầu.

- Xác minh mẫu : Với số lượng lớn, chọn ngẫu nhiên 5-10% thiết bị để kiểm tra chuyên sâu.

- Chứng nhận: Nếu thuê dịch vụ ngoài (như HTI Services hay DataSpan), họ phải cung cấp Chứng nhận tiêu hủy dữ liệu (Certificate of Destruction - CoD) kèm mã số seri của từng thiết bị.

Bước 5: Hoàn thiện hồ sơ và báo cáo

Lưu trữ bằng chứng phục vụ kiểm toán hoặc giải trình pháp lý.

- Hồ sơ bao gồm: Thông tin chi tiết thiết bị (loại, số Serial), phương pháp thực hiện (ví dụ: ghi đè 3 lần), nhân sự tham gia và bằng chứng hình ảnh (ảnh chụp thiết bị đã bị nghiền nát hoặc báo cáo "Success" từ phần mềm).

+ Cách xóa dữ liệu trên điện thoại di động

Mở ứng dụng "Ảnh" (hoặc "Thư viện"). Lướt xem ảnh và video. Nhấn giữ vào bức ảnh/video bạn muốn xóa. Bạn có thể chọn nhiều ảnh/video cùng lúc. Bấm vào biểu tượng "Thùng rác" (hoặc "Xóa"). Xác nhận xóa.

Lưu ý: Ảnh/video thường sẽ chuyển vào "Thùng rác" hoặc "Đã xóa gần đây" trong 30 ngày trước khi bị xóa vĩnh viễn. Bạn nên vào đó xóa hẳn để giải phóng dung lượng ngay lập tức.

- Xóa tài liệu không cần thiết:

Mở ứng dụng "Tập của tôi" (hoặc "Quản lý tập"). Tìm đến các file không cần thiết (ví dụ: file cài đặt APK đã dùng xong, tài liệu cũ không còn giá trị). Nhấn giữ vào file muốn xóa, rồi bấm biểu tượng "Thùng rác" (hoặc "Xóa"). Xác nhận xóa.

- Gỡ bỏ ứng dụng không dùng đến: Vào "Cài đặt" trên điện thoại. Chọn "Ứng dụng" (hoặc "Quản lý ứng dụng" / "Apps"). Lướt xem danh sách ứng dụng.

Chọn ứng dụng bạn muốn gỡ bỏ, rồi bấm "Gỡ cài đặt" (hoặc "Uninstall"). Xác nhận gỡ cài đặt.

2.2. Tổ chức và lưu trữ dữ liệu

* Cách tổ chức dữ liệu

Bước 1: Lựa chọn phương pháp tổ chức dữ liệu phù hợp

- Sử dụng cơ sở dữ liệu (CSDL): Đây là phương pháp phổ biến và tối ưu nhất hiện nay. Dữ liệu được tổ chức theo mô hình quan hệ, cho phép các bảng liên kết với nhau, giúp kiểm soát sự trùng lặp, đảm bảo tính nhất quán và nâng cao chất lượng dữ liệu thông qua các cơ chế sàng lọc của Hệ quản trị cơ sở dữ liệu.

- Sử dụng bảng dữ liệu: Phù hợp với dữ liệu nhỏ, ít người dùng và xử lý đơn giản (ví dụ: dùng MS Excel). Tuy nhiên, phương pháp này dễ gây sai sót khi dữ liệu lớn (lên tới 88% bảng tính có lỗi) và khó liên kết giữa các tập,.

- Sử dụng tập tin: Phương pháp truyền thống này gặp nhiều bất cập như thừa dữ liệu, thiếu nhất quán và khó khăn trong việc tiếp cận hay bảo mật.

Bước 2: Thiết lập cấu trúc lưu trữ khoa học

- Cấu trúc thư mục: Nên phân loại thư mục theo nhóm, chủ đề, dự án, phòng ban hoặc năm,.

- Phân cấp hợp lý: Chia dữ liệu thành các thư mục lớn (như Documents, Pictures, Work) và các thư mục con chi tiết hơn. Tuy nhiên, không nên chia quá sâu, giới hạn từ 3-4 cấp thư mục là phù hợp để tránh phức tạp.

- Phân loại theo tính chất: Cần tách biệt dữ liệu dựa trên độ nhạy cảm (công khai, nội bộ, bí mật) và định dạng (có cấu trúc hoặc phi cấu trúc như ảnh, video, log) để có cách bảo mật và lưu trữ riêng biệt.

Bước 3: Quy tắc đặt tên tệp và thư mục

- Ngắn gọn và mô tả: Tên phải phản ánh rõ nội dung bên trong.
- Định dạng chuẩn: Không dùng ký tự đặc biệt, dấu tiếng Việt hay khoảng trắng; sử dụng dấu gạch dưới (_) hoặc gạch ngang (-) để ngăn cách.
- Thông tin bắt buộc trong tên tệp: Nên bao gồm ngày tháng (định dạng YYYY-MM-DD hoặc YYYYMMDD), mã dự án, nội dung và số phiên bản (ví dụ: v01, v02, final).
- Tính duy nhất: Đảm bảo tên file là duy nhất trong thư mục để tránh việc ghi đè hoặc nhầm lẫn dữ liệu.

Bước 4: Quản lý nội dung và Metadata (Siêu dữ liệu)

Đề dữ liệu có giá trị sử dụng lâu dài và chi tiết, cần chú trọng:

- Quản lý Metadata: Ghi chú rõ nguồn gốc, thời gian tạo, người nhập liệu và định nghĩa các biến/đơn vị đo lường trong mỗi tệp dữ liệu để người khác có thể hiểu và sử dụng lại.
- Chuẩn hóa dữ liệu: Thống nhất định dạng ngày tháng, đơn vị tính, mã số và tên gọi trong toàn bộ tổ chức để tránh sai sót khi hợp nhất hoặc phân tích.

Bước 5: Chính sách bảo mật và duy trì hệ thống

Một hệ thống tổ chức dữ liệu đầy đủ không thể thiếu các biện pháp bảo vệ:

- Phân quyền truy cập: Thiết lập quyền hạn dựa trên vai trò, chỉ cho phép đúng người tiếp cận đúng dữ liệu vào đúng thời điểm.
- Sao lưu (Backup): Thực hiện sao lưu định kỳ và có kế hoạch phục hồi sau sự cố để giảm thiểu rủi ro mất mát dữ liệu.
- Quy trình quản lý: Lập quy định rõ ràng về việc thu thập, chia sẻ và xóa dữ liệu, đồng thời kiểm tra chất lượng định kỳ.
- Đào tạo nhân sự: Nâng cao nhận thức của nhân viên về các quy chuẩn nhập liệu và lưu trữ để toàn bộ tổ chức vận hành đồng bộ.

*** Cách lưu trữ dữ liệu**

- Phân loại dữ liệu cần ưu tiên lưu trữ

Trước khi bắt đầu, chúng ta cần xác định những gì thực sự quan trọng để tránh lãng phí không gian lưu trữ

+ Dữ liệu cá nhân: Hình ảnh, video gia đình, tài liệu cá nhân cần được lưu trữ thường xuyên vì nếu mất đi sẽ không thể khôi phục lại.

+ Dữ liệu công việc: Các hợp đồng, biên bản, chứng từ quan trọng cần lưu trữ kỹ để làm bằng chứng hoặc xem lại khi cần.

+ Hệ điều hành và phần mềm: Sao lưu toàn bộ hệ thống giúp tiết kiệm thời gian cài đặt lại khi máy tính gặp sự cố.

- Các phương thức lưu trữ phổ biến

- Lưu trữ vật lý (Offline): Đây là cách lưu trữ dữ liệu trực tiếp vào các thiết bị phần cứng.

+ Ổ cứng SSD: Có tốc độ đọc ghi rất cao, bền bỉ, chống va đập tốt, phù hợp để chạy hệ điều hành và phần mềm.

+ Ổ cứng HDD: Giá thành rẻ trên mỗi GB, dung lượng lớn, phù hợp để lưu trữ "kho dữ liệu" không lò như video, ảnh hoặc làm bản sao lưu lâu dài.

+ USB và thẻ nhớ: Nhỏ gọn, dễ di chuyển dữ liệu giữa các máy tính, nhưng dung lượng thường thấp và tuổi thọ có hạn nếu xóa, ghi quá nhiều.

- Lưu trữ đám mây (Online/Cloud Storage)

Dữ liệu được lưu trên máy chủ từ xa, cho phép bạn truy cập từ bất kỳ thiết bị nào có Internet,. Các dịch vụ phổ biến bao gồm:

+ Google Drive: Miễn phí 15GB, tích hợp tốt với hệ sinh thái Google (Gmail, Docs).

+ OneDrive: Miễn phí 5GB, tích hợp sâu vào Windows và bộ Office (Word, Excel).

+ iCloud: Miễn phí 5GB, dành riêng và tối ưu nhất cho người dùng hệ sinh thái Apple (iPhone, Mac).

+ Dropbox: Miễn phí 2GB, nổi bật với khả năng đồng bộ hóa cực nhanh và ổn định.

+ Zalo Cloud: Tiện lợi cho người dùng Việt Nam để lưu trữ file trong các hội thoại chat mà không chiếm bộ nhớ máy.

- Cách lưu trữ an toàn và hiệu quả

Không có một phương pháp nào là hoàn hảo 100%, vì vậy cách tốt nhất là kết hợp nhiều phương thức:

+ Nguyên tắc kết hợp: Nên sử dụng song song bản sao lưu Online (Đám mây) và Offline (Ổ cứng rời). Ví dụ: Dùng SSD để làm việc hàng ngày, HDD để lưu trữ dữ liệu lớn và Cloud để đồng bộ các file quan trọng cần truy cập mọi nơi.

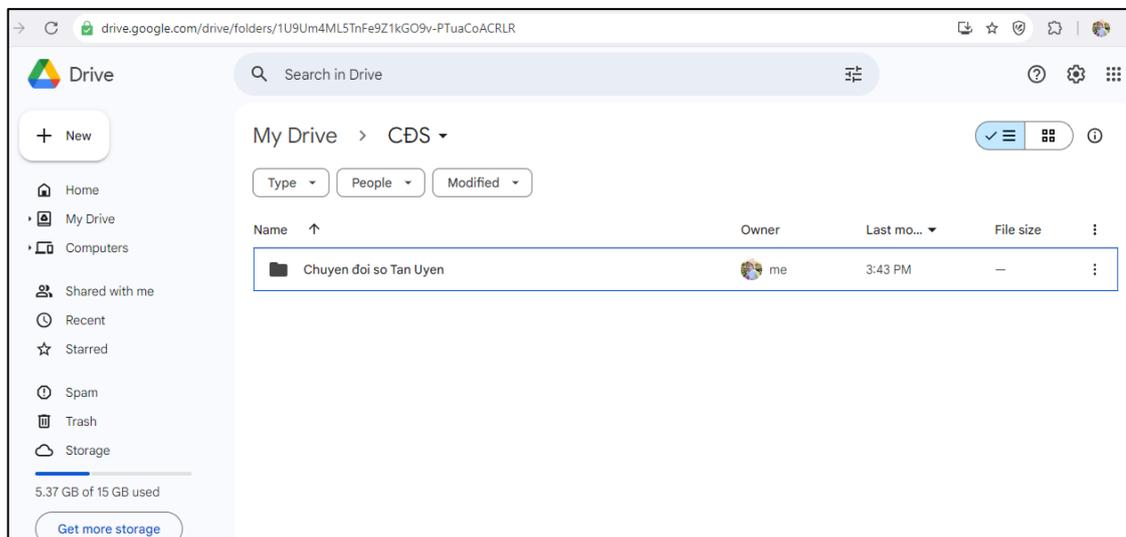
+ Ưu tiên tự động hóa: Tránh việc sao lưu thủ công bằng tay vì dễ quên và tốn thời gian. Hãy sử dụng các tính năng sao lưu tự động (như file history trên Windows, Time Machine trên Mac hoặc tính năng tự động đồng bộ của Google Drive/OneDrive).

+ Duy trì nhiều bản sao: Việc lưu trữ thường xuyên và có nhiều bản sao sẽ giúp giảm thiểu tối đa rủi ro mất trắng dữ liệu khi một thiết bị bị hỏng.

* Cách thức lưu trữ dữ liệu trên đám mây

Bước 1: Tạo tài khoản: Truy cập vào Google, vào địa chỉ [Drive.google.com](https://drive.google.com) hoặc vào nút lệnh các ứng dụng của Google trong tài khoản Gmail, chọn ứng dụng Drive

Bước 2: Nhập tên đăng nhập và mật khẩu gmail đã đăng ký

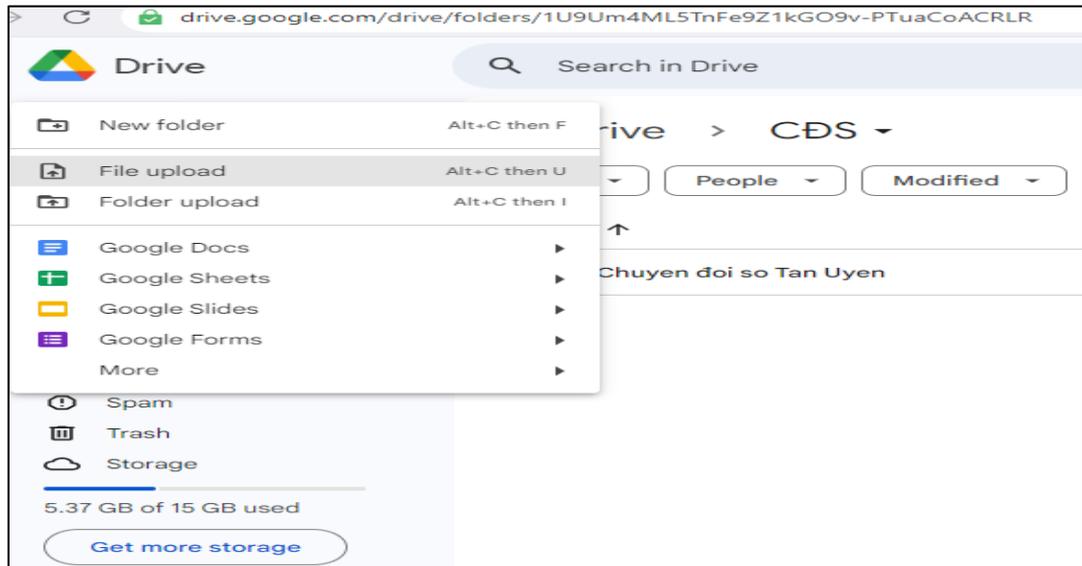


➤ Các tính năng cơ bản trong Google Drive

- New Folder (Tạo thư mục mới): tạo thư mục để phân loại dữ liệu khi tải lên

- File Upload (Tải tệp lên): Chỉ upload tệp tin, tuy nhiên sau này sẽ khó khăn trong quá trình tìm kiếm và quản lý file.

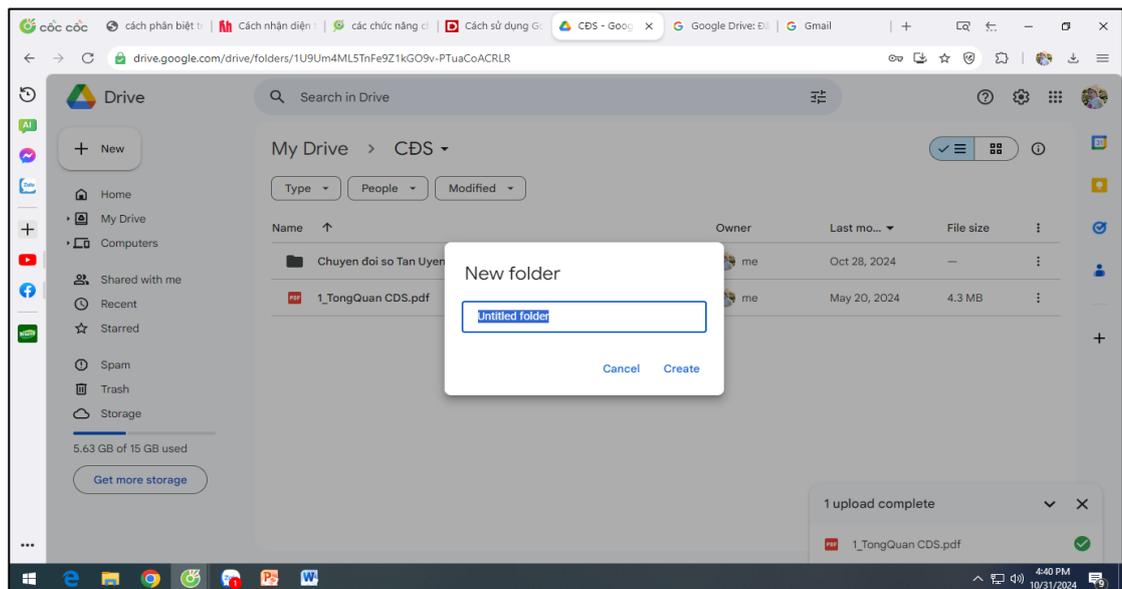
- Folder Upload (Tải thư mục lên): Drive sẽ tải lên thư mục có sẵn trong máy tính. Sau khi tải lên, Drive sẽ chứa một thư mục đầy đủ các tệp tin giống trong máy tính.



➤ Tạo thư mục mới

Nhấp chọn New (Mới) => Chọn New Folder (Thư Mục)

Nhập tên thư mục muốn đặt và chọn Create



➤ Tải thư mục, tập tin từ máy tính lên Google Drive

- Tải thư mục:

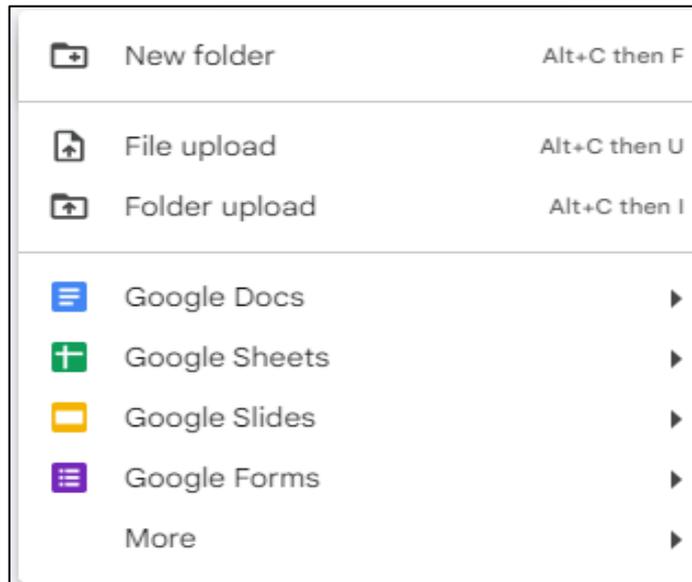
+ Bước 1: Nhấp chọn New (Mới) => Folder upload

+ Bước 2: Tìm đến thư mục cần tải lên => chọn tải lên

- Tải tập tin:

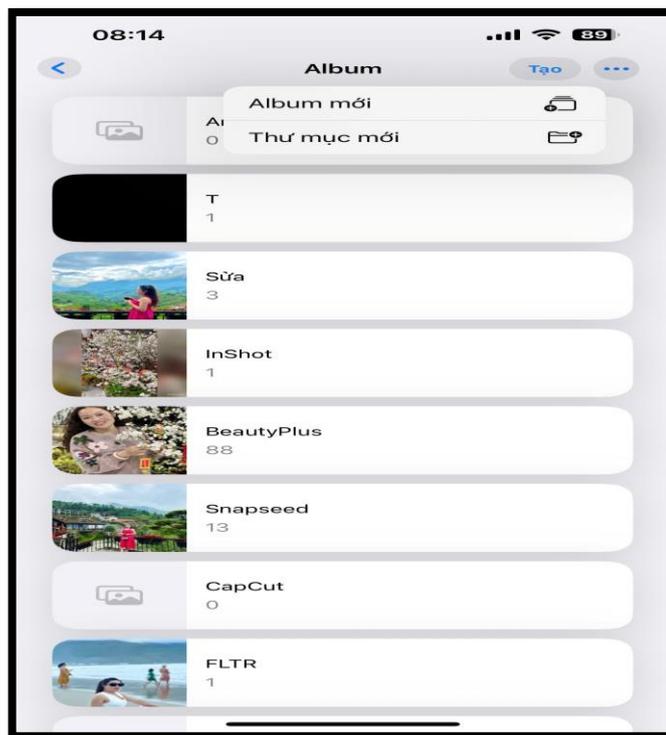
+ Bước 1: Nhấp chọn New (Mới) => File upload

+ Bước 2: Tìm đến thư mục chứa tập tin => chọn tập cần tải lên => chọn tải lên.

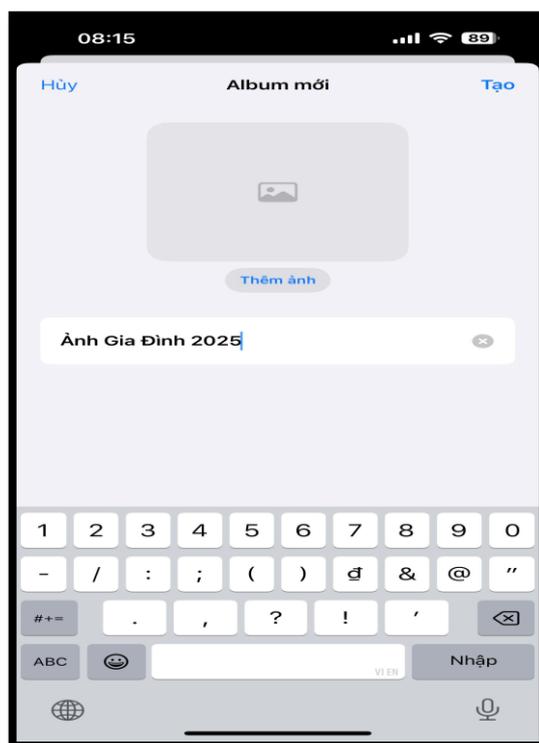


* Cách lưu trữ hình ảnh, video trên điện thoại

Bước 1: Cách tạo Album/Thư mục trong Thư viện ảnh. Mở ứng dụng “Ảnh” hoặc “Thư viện”. Chọn biểu tượng "Album" hoặc "Thư mục ". Bấm "Tạo Album mới" hoặc “Thư mục mới” sau đó ấn “Tạo”.



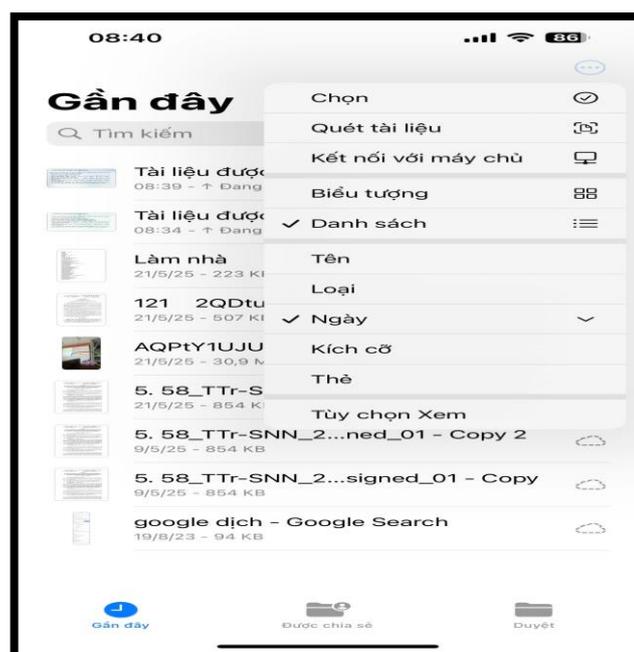
Bước 2: Đặt tên cho Album (ví dụ: "Ảnh Gia đình 2024", "Ảnh Du lịch Đà Lạt"). Chọn những bức ảnh bạn muốn di chuyển vào Album đó.



Bước 3: Sau khi đã tạo được Album chúng ta nhấp vào nút Thêm ảnh sau đó chọn ảnh và nhấp vào nút “Thêm” ảnh của bạn sau đó sẽ được lưu vào Album.

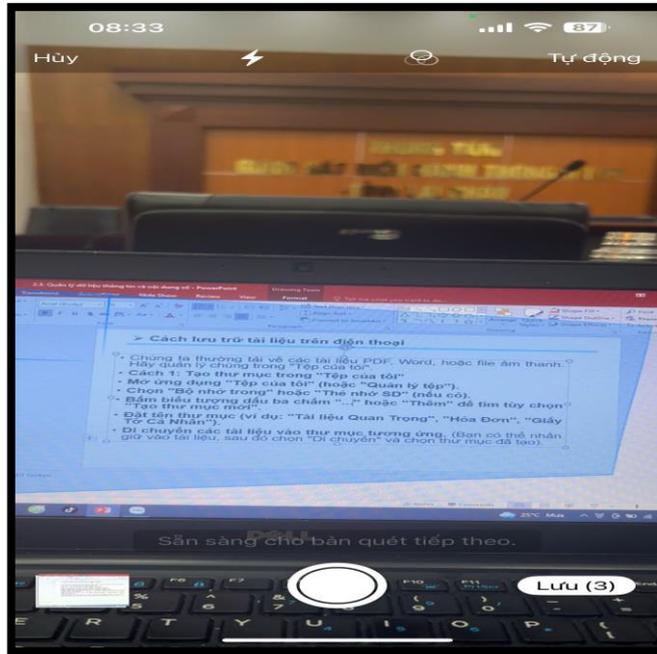
* Cách lưu trữ tài liệu trên điện thoại

Bước 1: Tại thư mục "Tập của tôi" mở ứng dụng "Tập" hoặc “Quản lý Tập”, chọn "Bộ nhớ trong" hoặc "Thẻ nhớ SD" (nếu có).

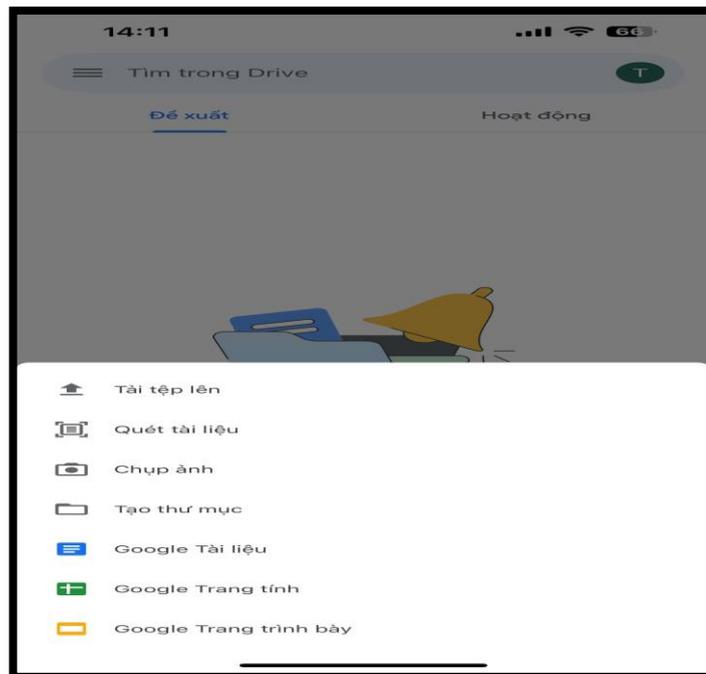


Bước 2: Bấm biểu tượng dấu ba chấm "..." hoặc "Thêm" để quét tài liệu cần lưu trữ sau đó chọn thư mục lưu trữ và bấm “Lưu”. Chọn thư mục để lưu tài

liệu và ấn “Lưu”. Đặt tên thư mục ví dụ: "Tài liệu quan trọng", "Hóa đơn", "Giấy tờ cá nhân".



Bước 3: Đăng nhập tài khoản Google: Tìm và mở ứng dụng Google Drive trên điện thoại. Tải dữ liệu lên: Chọn biểu tượng dấu (+) để tải tệp, thư mục hoặc ảnh/video bạn muốn lưu trữ. Chọn thư mục trên Google Drive để lưu trữ sau đó chờ quá trình hoàn tất.



* Tìm kiếm thông tin đã lưu

Tìm kiếm thông tin trên điện thoại thật đơn giản!

Cách 1: Sử dụng thanh tìm kiếm trong ứng dụng

Trong ứng dụng "Ảnh" (hoặc "Thư viện"): Thường có biểu tượng kính lúp ở góc trên. Bạn có thể gõ tên Album, hoặc thậm chí là từ khóa mô tả ảnh (ví dụ: "hoa", "biển" - nếu ảnh có nhận diện thông minh).

Trong ứng dụng "Tập của tôi" (hoặc "Quản lý tập"): Tương tự, có biểu tượng kính lúp. Bạn gõ tên file hoặc tên thư mục bạn muốn tìm.

Cách 2: Sử dụng thanh tìm kiếm tổng thể của điện thoại

Kéo từ trên màn hình xuống (đối với Android) hoặc vuốt từ giữa màn hình xuống (đối với iPhone) để hiển thị thanh tìm kiếm.

Gõ tên ảnh, tên tài liệu, hoặc từ khóa liên quan. Điện thoại sẽ gợi ý các kết quả từ khắp các ứng dụng.

3. Bảo mật và tuân thủ pháp lý

3.1. Bảo mật dữ liệu

- Các biện pháp bảo mật dữ liệu thiết yếu

Quản lý danh tính và xác thực thiết lập mật khẩu mạnh: Bắt buộc sử dụng mật khẩu độc lập, phức tạp và thực hiện thay đổi định kỳ.

Xác thực đa yếu tố (MFA/2FA): Kích hoạt MFA trên mọi tài khoản nhạy cảm, đặc biệt là các dịch vụ đám mây, để tăng cường lớp bảo vệ thứ hai.

Quản lý tài khoản: Không sử dụng chung tài khoản; thu hồi quyền truy cập ngay lập tức khi nhân sự chuyển vị trí hoặc chấm dứt hợp đồng lao động.

- Mã hóa dữ liệu

Mã hóa dữ liệu tĩnh: Mã hóa dữ liệu khi nó được lưu trữ trên ổ cứng hoặc máy chủ (ví dụ: sử dụng chuẩn AES-256).

Mã hóa dữ liệu truyền tải: Bảo vệ dữ liệu trong quá trình truyền qua mạng (ví dụ: sử dụng giao thức TLS 1.3).

Yêu cầu: Dữ liệu nhạy cảm phải được mã hóa ngay cả trước khi đưa lên các dịch vụ đám mây công cộng.

- Kiểm soát truy cập và phân quyền

Áp dụng cơ chế phân quyền để giới hạn phạm vi thao tác của người dùng.

Nguyên tắc đặc quyền tối thiểu: Cấp cho người dùng, hệ thống các quyền tối thiểu cần thiết để thực hiện công việc.

Kiểm soát truy cập dựa trên vai trò: Phân quyền truy cập dựa trên vai trò công việc và nhóm người dùng, thay vì cấp quyền cá nhân.

- Sao lưu và khôi phục dữ liệu

Đảm bảo tính sẵn sàng và tính toàn vẹn của dữ liệu.

Chiến lược sao lưu 3-2-1: Duy trì 3 bản sao dữ liệu, trên ít nhất 2 loại phương tiện lưu trữ khác nhau, và có ít nhất 1 bản sao lưu ngoại tuyến ngoài cơ sở.

Kiểm tra định kỳ: Thực hiện kiểm tra khả năng khôi phục dữ liệu định kỳ để xác minh tính hiệu quả của quy trình sao lưu.

- Trách nhiệm an toàn thông tin cá nhân

Mã hóa ổ cứng: Mã hóa ổ cứng máy tính cá nhân (ví dụ: BitLocker trên Windows) để bảo vệ dữ liệu khi thiết bị bị mất hoặc đánh cắp.

An toàn duyệt web: Sử dụng trình duyệt tuân thủ tiêu chuẩn bảo mật, ưu tiên các tính năng như xác thực trang web, chế độ ẩn danh và chặn quảng cáo mã độc hại.

Không cắm thiết bị lạ: Tuyệt đối không cắm các thiết bị lưu trữ ngoại vi (USB) không rõ nguồn gốc vào hệ thống công việc.

3.2. Tuân thủ pháp lý

- Luật An toàn thông tin mạng năm 2015

Quy định về nguyên tắc bảo vệ thông tin cá nhân trên mạng.

Điều 17 (Nguyên tắc bảo vệ thông tin cá nhân trên mạng): Cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật. Cơ quan, tổ chức, cá nhân xử lý thông tin cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý.

Điều 18 (Thu thập và sử dụng thông tin cá nhân): Phải thông báo cho chủ thể về hình thức, phạm vi, mục đích và thời gian lưu trữ thông tin.

- Luật An ninh mạng năm 2018

Tập trung vào việc bảo vệ dữ liệu trên môi trường không gian mạng.

Điều 17: Quy định về phòng, chống hành vi xâm phạm quyền sở hữu trí tuệ, hình ảnh, dữ liệu và thông tin cá nhân trên không gian mạng.

Điều 26: Quy định về việc lưu trữ dữ liệu và đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam đối với các doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet.

- Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân

Đây là văn bản pháp lý quan trọng và chi tiết nhất hiện nay, điều chỉnh trực tiếp các hoạt động liên quan đến dữ liệu cá nhân.

Điều 3 (Giải thích từ ngữ): Định nghĩa rõ về dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm (như tình trạng sức khỏe, quan hệ chính trị, dữ liệu di truyền, vị trí...).

Điều 8 (Quyền của chủ thể dữ liệu): Quy định 11 quyền của cá nhân đối với dữ liệu của mình, bao gồm: quyền được biết, quyền đồng ý, quyền truy cập, quyền chỉnh sửa, quyền xóa dữ liệu và quyền phản đối xử lý dữ liệu.

Điều 9 (Nghĩa vụ của chủ thể dữ liệu): Cá nhân có nghĩa vụ tự bảo vệ dữ liệu cá nhân của mình và tôn trọng dữ liệu của người khác.

Điều 26, 27 & 28: Quy định về hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và chuyển dữ liệu cá nhân ra nước ngoài.

4. Chia sẻ dữ liệu an toàn

- Nguyên tắc trước khi chia sẻ dữ liệu

Tối thiểu hóa dữ liệu: Chỉ chia sẻ phần dữ liệu thực sự cần thiết cho công việc, không sao chép hoặc lưu trữ thêm khi không cần.

Đúng mục đích và thẩm quyền: Chỉ khai thác dữ liệu dựa trên nhu cầu công việc thực tế và chỉ chia sẻ khi được phép, có mục đích rõ ràng.

Kiểm soát quyền truy cập: Xác định rõ người nhận và gán quyền tương ứng (chỉ xem, bình luận, hoặc chỉnh sửa) thay vì cho phép toàn quyền.

- Các phương pháp và công cụ chia sẻ an toàn nhất

+ Đối với nhu cầu nhanh chóng, ẩn danh và miễn phí

Wormhole: Cho phép chia sẻ tập tin lên đến 10GB với tính năng mã hóa đầu cuối (End-to-End). Người nhận có thể tải ngay khi người gửi đang tải lên, giúp tiết kiệm thời gian. Liên kết tự động hết hạn sau 24 giờ.

OnionShare: Một công cụ mã nguồn mở sử dụng mạng Tor để đảm bảo tính riêng tư và ẩn danh tuyệt đối. Dữ liệu được chuyển trực tiếp giữa hai máy tính (ngang hàng) mà không qua máy chủ trung gian.

+ Đối với tập tin quan trọng, mật khẩu hoặc văn bản nhạy cảm

Bitwarden Send: Một tính năng của trình quản lý mật khẩu Bitwarden, cho phép chia sẻ thông tin văn bản, mật khẩu hoặc tài liệu quan trọng. Bạn có thể đặt mật khẩu bảo vệ, hẹn giờ xóa và giới hạn số lượt truy cập.

LastPass: Hỗ trợ chia sẻ thông tin đăng nhập qua email mà người nhận không cần biết mật khẩu gốc của bạn.

+ Đối với lưu trữ đám mây và làm việc nhóm

Mega: Một trong những dịch vụ an toàn nhất với mã hóa đầu cuối. Bạn có thể chia sẻ qua mã QR để chỉ những người cụ thể mới nhận được liên kết.

pCloud: Phù hợp cho các tập tin lớn vì không giới hạn kích thước tải lên và hỗ trợ nhiều nền tảng (Windows, macOS, iOS, Android).

Tresorit & DocSend: Tresorit cung cấp bảo mật tiêu chuẩn Thụy Sĩ, trong khi DocSend cho phép xác minh danh tính người nhận qua email và cập nhật phiên bản mới ngay cả sau khi đã gửi.

- Quy trình thực hiện chia sẻ an toàn

+ Chuẩn bị dữ liệu: Mã hóa tập tin bằng mật khẩu mạnh (sử dụng chuẩn AES-128 hoặc AES-256) trước khi gửi.

+ Chọn kênh truyền: Sử dụng các kênh an toàn như VPN, email mã hóa hoặc các hệ thống chia sẻ nội bộ của cơ quan. Tuyệt đối không sử dụng Wi-Fi công cộng để xử lý dữ liệu.

+ Thiết lập rào cản: Khi gửi link, hãy luôn đặt mật khẩu, thời hạn truy cập (ví dụ: hết hạn sau 24h) và giới hạn quyền tải xuống.

+ Gửi mật khẩu riêng biệt: Bạn có thể gửi tập tin qua email, nhưng hãy gửi mật khẩu giải mã qua một kênh khác (ví dụ: tin nhắn tự xóa như Snapchat) để tăng cường bảo mật.

+ Ghi chép và theo dõi: Lưu lại nhật ký chia sẻ (ai gửi, ai nhận, lúc nào) và chủ động gỡ bỏ các liên kết chia sẻ khi không còn sử dụng.

- Các rủi ro cần tránh

Không chia sẻ qua ứng dụng cá nhân: Tránh sử dụng Zalo cá nhân, Facebook để chuyển dữ liệu công việc quan trọng.

Cẩn thận với Phishing: Luôn kiểm tra kỹ để tránh các cuộc tấn công lừa đảo nhằm lấy mật khẩu tài khoản cloud.

Không dùng link công khai (Public link): Việc mở liên kết không giới hạn sẽ dễ dẫn đến lộ lọt thông tin ra ngoài.

Sao lưu (Backup): Luôn áp dụng mô hình 3-2-1 (3 bản sao, 2 loại lưu trữ, 1 bản ở nơi khác) để tránh mất mát dữ liệu.

5. Phân tích dữ liệu, hỗ trợ ra quyết định

- Khái niệm và bản chất

Ra quyết định dựa trên dữ liệu (Data-driven decision making - DDDM) là quá trình sử dụng các dữ kiện, số liệu và kết quả phân tích để đưa ra các quyết định chiến lược kinh doanh hoặc quản lý phù hợp với mục tiêu đã đề ra. Đây không chỉ là việc chọn công nghệ phù hợp mà còn là quá trình khai thác giá trị từ dữ liệu bằng các phương pháp thống kê và trí tuệ nhân tạo để hỗ trợ lãnh đạo ra quyết định kịp thời, chính xác dựa trên bằng chứng thay vì cảm tính.

- Tầm quan trọng và lợi ích

+ Đưa ra quyết định tự tin và khách quan: Dữ liệu mang tính logic, giúp loại bỏ các yếu tố chủ quan và bản năng, giúp nhà lãnh đạo cam kết hoàn toàn với tầm nhìn chiến lược mà không quá lo lắng về rủi ro.

Nâng cao tính chủ động: Thay vì chỉ phản ứng lại các sự kiện đã xảy ra, phân tích dữ liệu lớn giúp doanh nghiệp xác định cơ hội hoặc phát hiện mối đe dọa (như thiên tai, dịch bệnh, bất thường tài chính) trước khi chúng trở nên nghiêm trọng.

+ Tiết kiệm chi phí: Theo khảo sát, hơn 49% tổ chức nhận thấy giá trị thực tế từ các dự án dữ liệu nhằm giảm chi phí vận hành.

+ Tối ưu hóa quản lý Nhà nước: Giúp chính sách được hoạch định sát thực tế, tăng tính minh bạch và hiệu quả phân bổ ngân sách.

- Quy trình 6 bước ra quyết định hiệu quả

Bước 1: Xác định mục tiêu kinh doanh: Hiểu rõ vấn đề cần giải quyết và các chỉ số hiệu suất chính (KPI) cần đạt được.

Bước 2: Khảo sát và tìm nguồn dữ liệu: Lấy ý kiến từ các bộ phận liên quan để xác định nguồn dữ liệu ưu tiên (như CSDL quốc gia, báo cáo nội bộ, mạng xã hội).

Bước 3: Thu thập và chuẩn bị dữ liệu: Truy cập, làm sạch dữ liệu để loại bỏ trùng lặp và đảm bảo tính tin cậy. Nên ưu tiên nguồn dữ liệu có tác động cao nhưng độ phức tạp thấp để bắt đầu.

Bước 4: Xem và khám phá dữ liệu: Sử dụng các thành phần trực quan như biểu đồ, bản đồ để hiểu các xu hướng và ngoại lệ.

Bước 5: Phát triển thông tin chuyên sâu: Sử dụng tư duy phản biện để đặt câu hỏi và tìm ra các cơ hội hoặc rủi ro thông qua các mô hình phân tích (mô tả, chẩn đoán, dự báo, đề xuất).

Bước 6: Hành động và chia sẻ thông tin: Trình bày kết quả qua các bảng điều khiển (dashboard) động để lãnh đạo ra quyết định nhanh và chia sẻ hiểu biết đó với cộng sự.

- Công cụ hỗ trợ phân tích dữ liệu
- + Công cụ phổ thông: Microsoft Excel, Google Sheets.
- + Công cụ trực quan hóa nâng cao: Power BI, Tableau, Google Data Studio.
- + Công cụ AI và lập trình: ChatGPT, Microsoft Copilot, ngôn ngữ Python (pandas, scikit-learn).
- Yếu tố then chốt để thành công
- + Xây dựng văn hóa dữ liệu: Khuyến khích tư duy phản biện, sự sáng tạo và coi việc sử dụng dữ liệu là chuẩn mực hàng ngày.
- + Đào tạo nhân sự: Nâng cao mức độ thông thạo dữ liệu ở tất cả các cấp độ công việc.
- + Mô hình tự phục vụ (Self-service): Cho phép mọi người truy cập dữ liệu họ cần nhưng vẫn đảm bảo tính bảo mật và quản trị.

Tình huống

Cơ quan cần chuyển một tập tin danh sách lương và thông tin cá nhân (dữ liệu nhạy cảm) cho đơn vị kiểm toán bên ngoài. Một cán bộ đề xuất gửi nhanh qua Zalo cá nhân hoặc tải lên một trang lưu trữ đám mây miễn phí không yêu cầu mật khẩu để đối tác tải về cho tiện.

Câu hỏi thảo luận

- Theo Nghị định 13/2023/NĐ-CP, việc rò rỉ dữ liệu cá nhân nhạy cảm trong tình huống này có thể vi phạm những quyền gì của chủ thể dữ liệu?.
- Để đảm bảo an toàn, hãy xây dựng một quy trình chia sẻ an toàn (sử dụng công cụ mã hóa, đặt mật khẩu, kênh truyền mật khẩu riêng biệt) dựa trên hướng dẫn của chuyên đề.
- Nếu cơ quan cần thanh lý các máy tính cũ đã từng lưu trữ dữ liệu này, bạn sẽ chọn cấp độ tiêu hủy nào theo tiêu chuẩn NIST SP 800-88 (Clear, Purge hay Destroy)? Tại sao?

TÀI LIỆU THAM KHẢO

1. Nguồn:<https://gpquinhon.org/truyen-thong/tai-lieu-huong-dan-su-dung-ai-7061.html>
2. <https://mic.mediacdn.vn/639352410187198464/2024/2/22/cam-nang-phong-chong-tin-gia-1708573604318415362313.pdf>
3. <https://tingia.gov.vn/#:~:text=Image%3A%20H%C3%A0%20N%E1%BB%99i%3A%20Gi%E1%BA%A3%20m%E1%BA%A1o,%C4%91%E1%BB%99%20b%E1%BA%A3o%20hi%E1%BB%83m%20x%C3%A3%20h%E1%BB%99i>
4. <https://dhtn.ttxvn.org.vn/tintuc/hay-tinh-tao-va-luon-nghi-ngo-de-loai-tru-tin-gia-7684#:~:text=C%C3%B3%20ba%20b%C6%B0%E1%BB%9Bc%20c%C6%A1%20b%E1%BA%A3n,ch%C3%AD%20tr%E1%BA%BB%20hay%20di%E1%BB%85n%20%C4%91%C3%A0n>
5. <https://congan.quangninh.gov.vn/thong-bao/tuyen-truyen-pho-bien-phap-luat/tac-hai-cua-tin-gia-tin-sai-su-that-tren-khong-gian-mang-va-cach-phong-tranh-2540.html>
6. <https://mindx.edu.vn/blog/lam-sach-du-lieu>
7. <https://ocd.vn/huong-dan-lam-sach-du-lieu/>
8. <https://htiservices.vn/huy-du-lieu-an-toan-dau-la-phuong-phap-phu-hop/>
9. <http://xdulieu.com/co-so-du-lieu/cs1-khai-quat/kq2-cac-phuong-phap-to-chuc-du-lieu.html>
10. <https://dtsoft.vn/5-cach-luu-tru-du-lieu-an-toan-nhat-hien-nay-cttt144.html>
11. https://ooc.vn/luu-tru-dam-may-cloud-storage/?utm_source=chatgpt.com
12. <https://www.microsoft.com/vi-vn/security/business/security-101/what-is-data-security>
13. <https://fptshop.com.vn/tin-tuc/thu-thuat/7-cong-cu-tot-nhat-de-chia-se-du-lieu-an-toan-voi-bat-ky-ai-141330>
14. <https://www.thegioididong.com/tin-tuc/nhung-phuong-phap-giup-ban-chia-se-tap-tin-mot-cach-an-toan-hon-1150771>
15. https://codegym.vn/blog/phan-tich-du-lieu-la-gi-cac-buoc-phan-tich-du-lieu-hieu-qua-de-ra-quyet-dinh-dung-dan/?utm_source=chatgpt.com
16. <https://base.vn/blog/phan-tich-du-lieu/>
17. <https://www.elcom.com.vn/ra-quyet-dinh-dua-tren-du-lieu-la-gi-loi-ich-va-cach-thuc-hien-1706173088>

