

BÁO CÁO CHUYÊN ĐỀ · PHIÊN BẢN 1.0

Sở Khoa học và công nghệ Hải Phòng

Khung quản trị, quản lý dữ liệu, kiến trúc dữ liệu

(

Chuyển đổi phương thức quản lý hành chính sang quản trị quốc gia hiện đại dựa trên dữ liệu — kiến tạo hệ sinh thái tài chính số thống nhất, an toàn và thông minh.

Người trình bày: ThS. Bùi Tiến Sỹ - Trưởng phòng Quản lý dữ liệu và thống kê
Cục Công nghệ thông tin và chuyển đổi số - Bộ Tài chính

Hải phòng · 2026

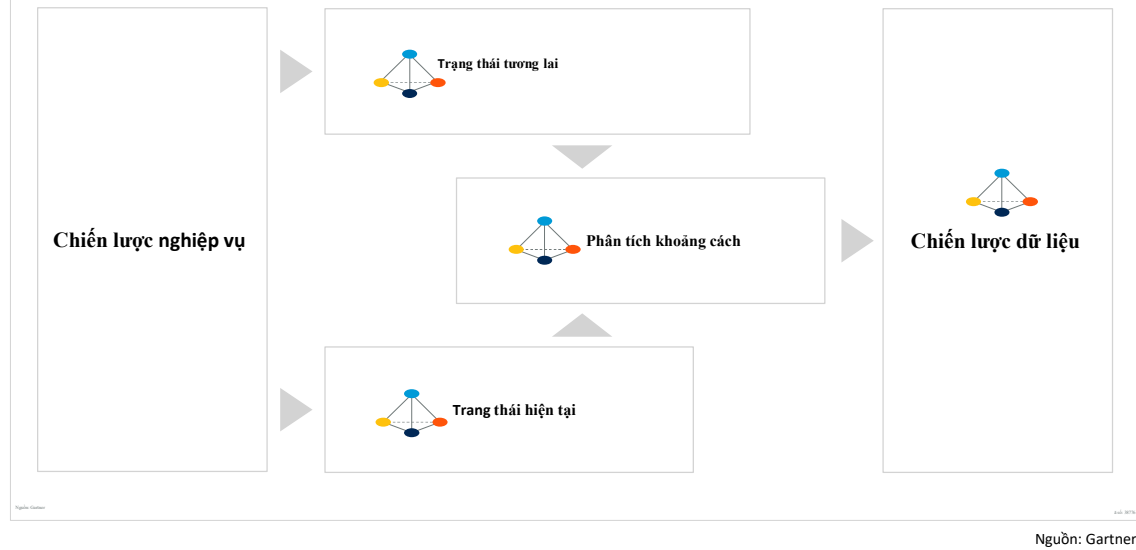


PHƯƠNG PHÁP LUẬN

Quản trị dữ liệu số

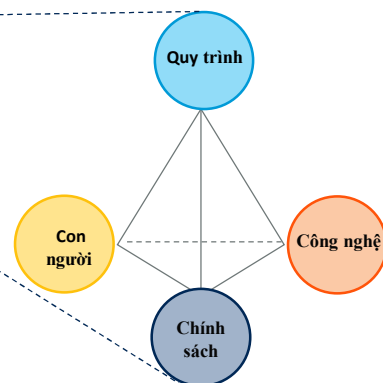
Kiến trúc dữ liệu | Quản trị dữ liệu | Từ điển dữ liệu

Chiến lược dữ liệu phụ thuộc vào các tài liệu tiên quyết



Dữ liệu cung cấp là đa chiều

- Bốn khía cạnh cần được xem xét
- Chúng nên được xem xét đánh giá riêng lẻ và trong bất kỳ sự kết hợp nào
- Bốn khía cạnh này áp dụng cho mọi thứ:
 - Các điều kiện tiên quyết
 - Công việc chuẩn bị
 - Chiến lược dữ liệu



Các thành phần trong Chiến lược Dữ liệu



Các cấp độ chuyển dịch số trong chính phủ

(Bởi Gartner)

	E-Government		Open	Data-Centric	Fully Digital	Smart
Maturity Level	01 Initial	02 Developing	03 Defined	04 Managed	05 Optimizing	
Value Focus	Compliance, efficiency	Transparency and openness	Constituent value	Transformation	Sustainability	
Channel Strategy	Portal	Government as a platform	Nongovernment channels	Truly multichannel	Automation replaces portals	
Leadership	CIO/CTO	CDO	Departments	CIO and departments	CIO _{plus}	
Technology Focus	Service-oriented architecture	Open data, open service	Open any data	Things as data	Smart machines	
Sourcing Strategy	Mixed	Reinsourced, cloud first	Multisourced	Partner-sourced	Outsourced	
Key Metrics	% services online	% open data	Number of data-driven services	% data from things	% decrease of services	

Các cấp độ chuyển dịch số trong chính phủ

(Theo mô hình đánh giá của Gartner)

	Chính phủ điện tử	Chính phủ mở	Trọng tâm dữ liệu	Số hóa toàn diện	Thông minh
Cấp độ trưởng thành	01. Khởi tạo	02. Phát triển	03. Xác lập	04. Quản lý	05. Tối ưu
Trọng tâm giá trị	Tuân thủ, hiệu quả	Minh bạch và cởi mở	Giá trị cho người dân	Chuyển đổi toàn diện	Phát triển bền vững
Chiến lược kênh	Cổng thông tin (Portal)	Chính phủ như nền tảng	Kênh phi chính phủ	Đa kênh thực sự	Tự động hóa thay Portal
Vai trò lãnh đạo	Giám đốc CNTT (CIO)	Giám đốc Dữ liệu (CDO)	Các Sở, Ban, Ngành	CIO phối hợp Sở, Ngành	CIO mở rộng (CIOplus)
Trọng tâm công nghệ	Kiến trúc hướng dịch vụ	Dữ liệu mở, dịch vụ mở	Mở mọi loại dữ liệu	Vạn vật là dữ liệu (IoT)	Máy móc thông minh (AI)
Chiến lược nguồn lực	Hỗn hợp	Tự chủ, ưu tiên Đám mây	Đa nguồn cung cấp	Khai thác từ đối tác	Thuê ngoài toàn bộ
Chỉ số cốt lõi	% dịch vụ trực tuyến	% dữ liệu được mở	Số lượng dịch vụ từ dữ liệu	% dữ liệu từ thiết bị IoT	% giảm tải dịch vụ cơ học

Các xu hướng chính trong quản lý dữ liệu hiện nay



CÁC XU HƯỚNG CHÍNH TRONG QUẢN LÝ DỮ LIỆU NĂM 2025

1. Kiến trúc Dữ liệu

Định hình thiết kế thích ứng

- Xác định mức độ sẵn sàng cho AI (LLM & GenAI).
- Khám phá định dạng dữ liệu mở và kiến trúc Lakehouse.
- Thiết kế và cung cấp các 'sản phẩm dữ liệu'.
- Nâng cao mô hình dữ liệu cho hiệu quả kinh doanh.

2. Lưu trữ & Chia sẻ Dữ liệu

Nền tảng của tiếp cận & hiệu suất

- Nâng cấp hạ tầng hỗ trợ đa mô hình kiến trúc.
- Áp dụng khung đối chiếu Use Case vào lưu trữ với từng trường hợp sử dụng.
- Giải quyết rắc rối của cơ sở dữ liệu phân tán.
- Phá vỡ 'ốc đảo dữ liệu' (data silos) để quản trị.

2025

3. Quản trị Dữ liệu & Siêu dữ liệu

Thúc đẩy dữ liệu sẵn sàng cho AI

- Nâng cao quản trị D&A, hướng tới giá trị kinh doanh.
- Triển khai Quản lý Dữ liệu Chủ (MDM).
- Tích hợp GenAI vào các sáng kiến chất lượng dữ liệu.
- Mở rộng quản lý siêu dữ liệu (Metadata).

4. Kỹ thuật Dữ liệu

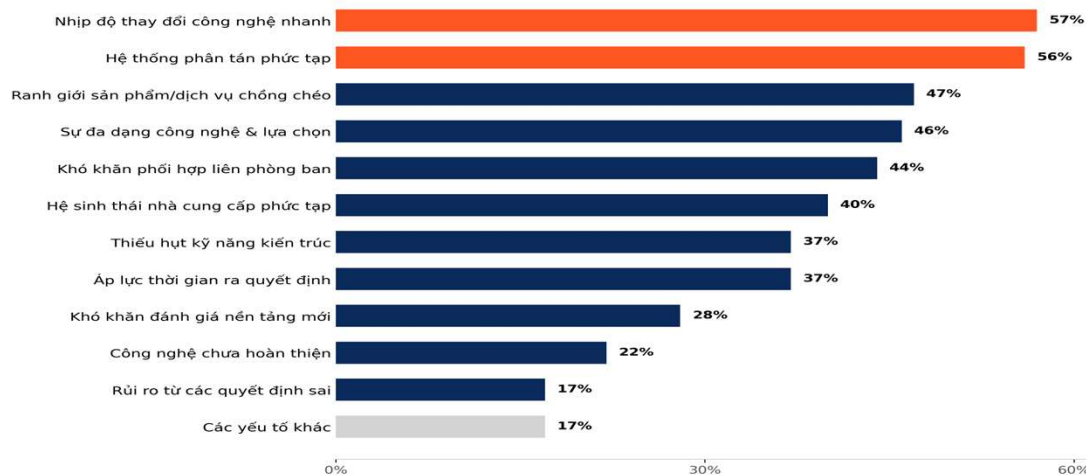
Tăng độ tin cậy và khả năng mở rộng

- Khắc phục thách thức chất lượng trong luồng dữ liệu.
- Điều phối luồng công việc trên nhiều môi trường.
- Xây dựng kiến trúc tích hợp luân chuyển mượt mà.
- Áp dụng 'quan sát dữ liệu' (Data Observability).



Các yếu tố khiến việc đưa ra quyết định về kiến trúc trở nên khó khăn hơn

Những Thách Thức Khi Đưa Ra Quyết Định Kiến Trúc



RESTRICTED DISTRIBUTION

© 2025 Gartner Inc. and/or its affiliates. All rights reserved.

Gartner

7 Trụ cột Bất buộc cho Quản trị Dữ liệu và Phân tích Hiện đại



RESTRICTED DISTRIBUTION

© 2025 Gartner Inc. and/or its affiliates. All rights reserved.

Gartner

Kiến trúc Dữ liệu

Mô hình, nguyên tắc & luồng điều phối dữ liệu toàn ngành

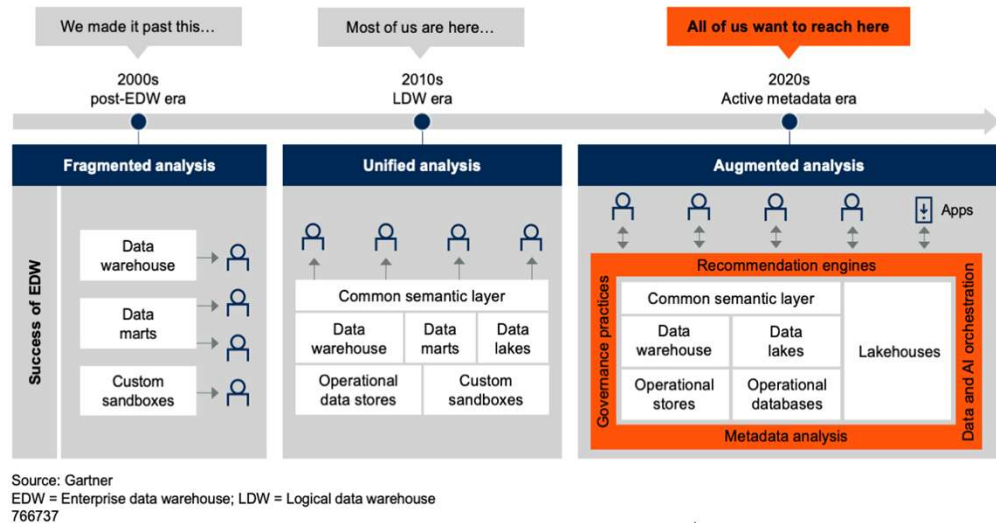
01



Tiến hóa của Kiến trúc dữ liệu

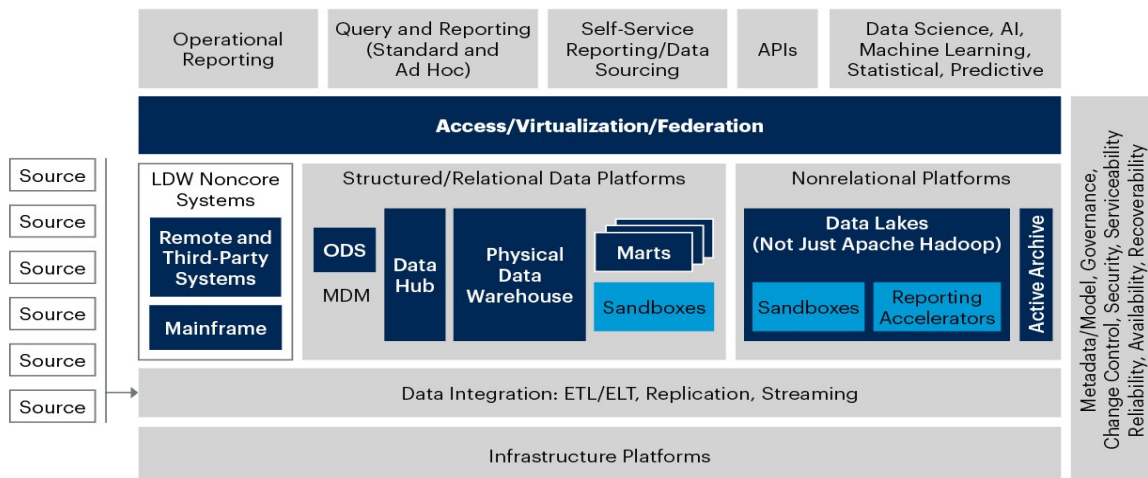
The Evolution of the Data Architecture

Kiến trúc dữ liệu mô tả cấu trúc của các tài sản dữ liệu vật lý và logic cũng như các tài nguyên quản lý dữ liệu của một tổ chức..

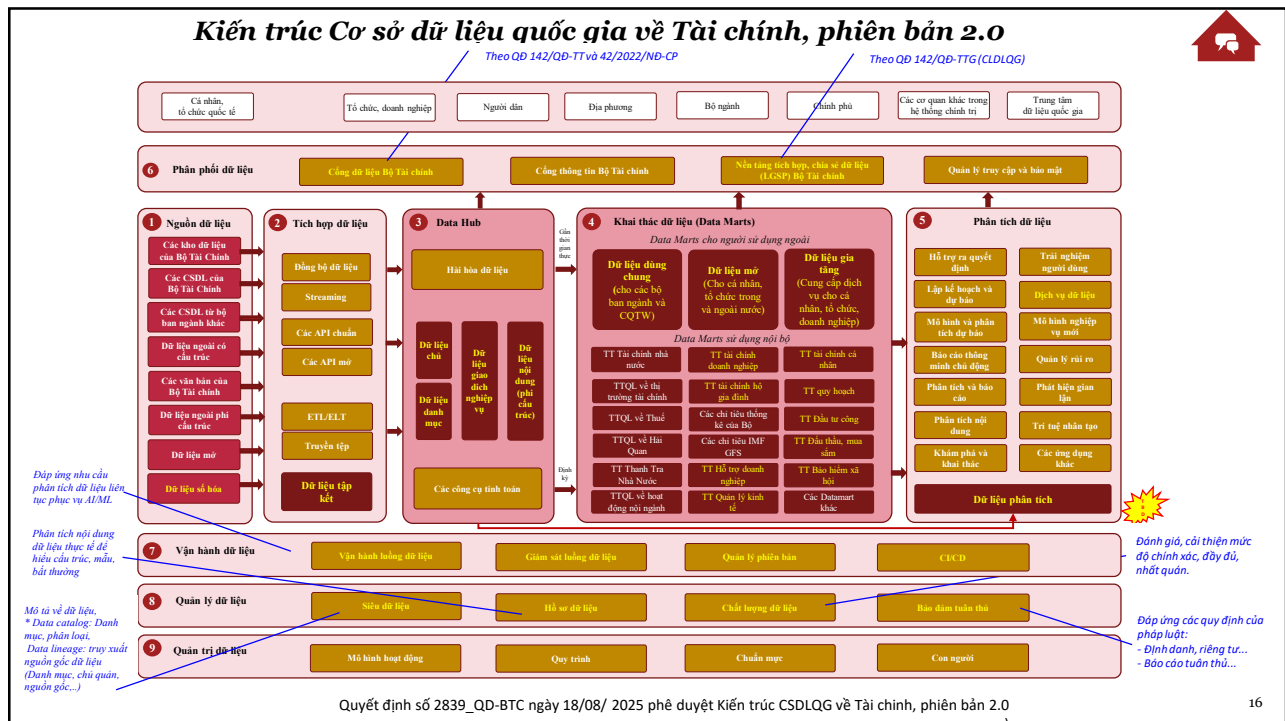
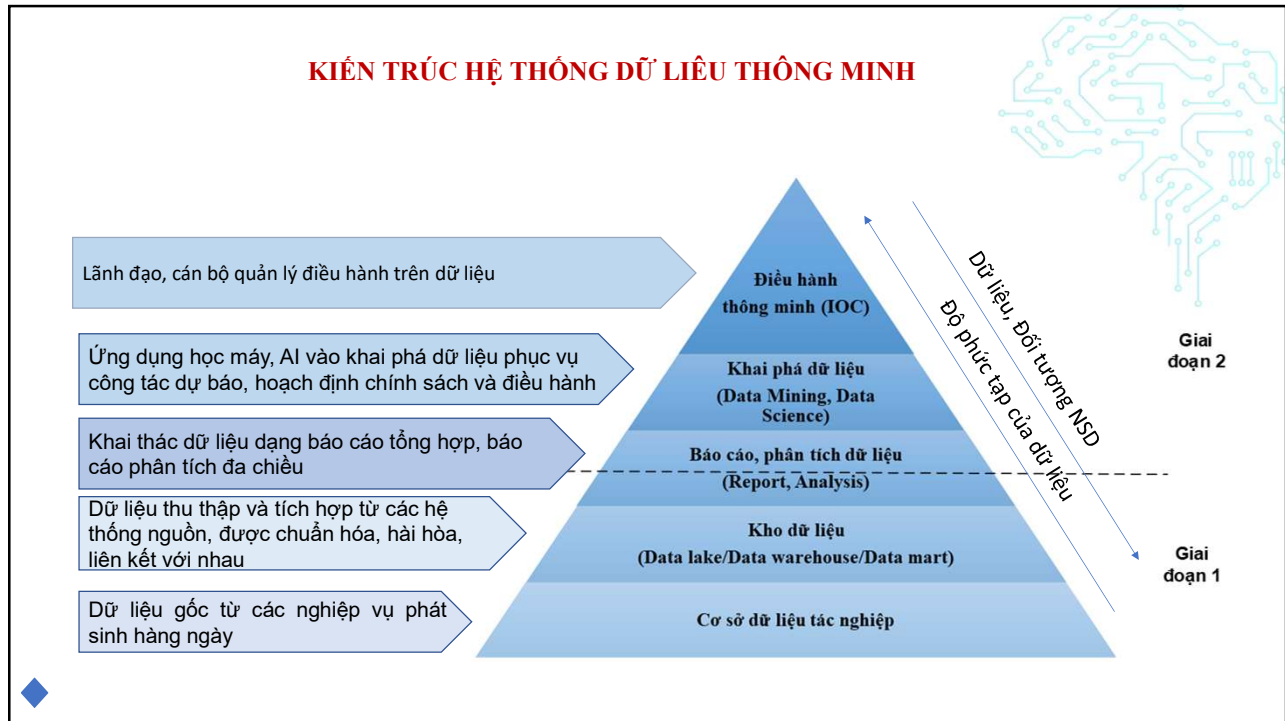


Gartner

High-Level Logical Data Warehouse Architecture



Source: Gartner
719542_C





Chiến lược dữ liệu thành phố Hải Phòng giai đoạn 2026-2030, tầm nhìn đến năm 2045.

Hà Nội, 2026

Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045



ỦY BAN NHÂN DÂN
THÀNH PHỐ HẢI PHÒNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 5264 /QB-UBND

Hải Phòng, ngày 26 tháng 2 năm 2025

QUYẾT ĐỊNH

Phê duyệt Chiến lược dữ liệu thành phố Hải Phòng đến năm 2030

ỦY BAN NHÂN DÂN THÀNH PHỐ

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Chiến lược dữ liệu thành phố Hải Phòng đến năm 2030 (Chi tiết kèm theo).

Điều 2. Các Sở, ban, ngành thành phố, Ủy ban nhân dân các xã, phường, đặc khu và các cơ quan, đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện Chiến lược dữ liệu thành phố Hải Phòng đến năm 2030; định kỳ rà soát, điều chỉnh, cập nhật nội dung Chiến lược bảo đảm phù hợp với tình hình thực tế và yêu cầu phát triển của thành phố.

Điều 3. Chánh Văn phòng Ủy ban nhân dân thành phố; Thủ trưởng các Sở, ban, ngành thành phố; Chủ tịch Ủy ban nhân dân các xã, phường, đặc khu và các tổ chức liên quan căn cứ Quyết định thi hành.

Quyết định có hiệu lực kể từ ngày ký.

Nơi nhận:

- Như Điều 3;
- Bộ: KHCN, CA, NV;
- VPCP, VPTW Đảng;
- CT, các PCT UBND TP;
- VPTU;
- CVP, các PCVP UBND TP;
- Phòng: VX, NC, TH, XDCT, NNMT, TC, NV&KTGS;

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Xây dựng chiến lược dữ liệu của thành phố Hải Phòng nhằm:

- Hoàn thiện mô hình kiến trúc chuyển đổi số, mô hình tổ chức và quản trị dữ liệu và các giải pháp an ninh mạng, an toàn thông tin dữ liệu của thành phố.
- Đổi mới phương thức chỉ đạo điều hành, nâng cao hiệu quả hoạt động của chính quyền.
- Khai phá hiệu quả tiềm năng của dữ liệu thúc đẩy đổi mới sáng tạo, tạo ra các giá trị mới, với phương châm “Lấy người dân, doanh nghiệp làm trung tâm”.
- Chiến lược dữ liệu của thành phố phù hợp với tầm nhìn và định hướng của quốc gia về phát triển dữ liệu số. Tuân thủ theo Khung Kiến trúc Chính phủ điện tử Việt Nam; Kiến trúc Chính phủ điện tử cấp Bộ; Kiến trúc Chính quyền điện tử của thành phố. Tuân thủ đầy đủ các quy định, hướng dẫn của Chính phủ, các Bộ, ngành, cơ quan Trung ương về quản lý và phát triển dữ liệu số.

Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Các mục tiêu cụ thể đến năm 2030



1. Phát triển hạ tầng dữ liệu

Phát triển, hoàn thiện Trung tâm dữ liệu của thành phố có tính dự phòng, đáp ứng năng lực tính toán, lưu trữ, xử lý dữ liệu lớn, có khả năng kết nối với Trung tâm dữ liệu vùng, khu vực, quốc gia theo quy hoạch của trung ương, phục vụ cho phát triển kinh tế-xã hội của thành phố.

Các Nền tảng điện toán đám mây của thành phố và các Nền tảng ứng dụng trên thiết bị di động Made in Viet Nam đảm bảo sẵn sàng đáp ứng 100% nhu cầu lưu trữ, thu thập, kết nối, chia sẻ dữ liệu của thành phố Hải Phòng, nhu cầu đảm bảo an toàn thông tin, an ninh mạng và bảo mật thông tin theo cấp độ quy định của Luật An toàn thông tin mạng.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Các mục tiêu cụ thể đến năm 2030



2. Dữ liệu số trong phát triển Chính quyền số

- **100%** các CSDL trong danh mục CSDL dùng chung, danh mục CSDL chuyên ngành của thành phố cần ưu tiên triển khai và hoàn thành, tạo nền tảng phát triển Chính quyền số; hoàn thành việc số hóa, cập nhật và đưa vào sử dụng hiệu quả; được kết nối, chia sẻ với Kho dữ liệu dùng chung của thành phố và kết nối, chia sẻ trên phạm vi toàn thành phố.

- Các CSDL dùng chung và chuyên ngành của các Sở, ban, ngành, xã, phường, đặc khu (ngoại trừ các CSDL nghiệp vụ đặc thù) có nhu cầu kết nối, khai thác, tích hợp, chia sẻ thông tin với các CSDL của quốc gia, của thành phố hoặc nhu cầu kết nối, chia sẻ thông tin với nhau, được đáp ứng **100%** yêu cầu thông qua các nền tảng tích hợp, chia sẻ dữ liệu.

- **100%** các cơ quan nhà nước trên địa bàn thành phố thực hiện mở và cung cấp dữ liệu mở đảm bảo chất lượng (không trùng lặp, dư thừa, không tốn công sức và chi phí để xử lý lại dữ liệu, hoặc thu thập lại dữ liệu), đưa vào khai thác sử dụng có hiệu quả, đảm bảo sẵn sàng hỗ trợ, phục vụ cho các hoạt động chỉ đạo điều hành, ban hành chính sách của cơ quan nhà nước và phục vụ phát triển các ứng dụng trí tuệ nhân tạo cho phát triển kinh tế số, xã hội số.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Các mục tiêu cụ thể đến năm 2030

- **100%** hồ sơ, kết quả giải quyết thủ tục hành chính được số hóa; 100% dữ liệu về kết quả thực hiện các thủ tục hành chính được chuyển vào Kho quản lý dữ liệu điện tử của tổ chức, cá nhân để tái sử dụng, chia sẻ theo quy định.
- Tích hợp kết quả xử lý công việc của cán bộ, công chức, viên chức vào phần mềm quản lý văn bản và hồ sơ công việc của từng đơn vị; tỷ lệ áp dụng dữ liệu trong phục vụ quản lý điều hành công việc trên môi trường số, trong kiểm tra, đánh giá, xếp loại cán bộ, công chức, viên chức đạt tối thiểu **70%**.
- Kết hợp khai thác sử dụng dữ liệu và ứng dụng trí tuệ nhân tạo (AI) đối với **100%** thủ tục hành chính có đủ điều kiện cung cấp trực tuyến, nâng cao hiệu quả của bộ máy hành chính nhà nước và cung cấp dịch vụ công phục vụ người dân, doanh nghiệp.
- **100%** các sở, ban, ngành, xã, phường, đặc khu thiết lập được bộ phận phụ trách về dữ liệu; xây dựng và triển khai theo các nội dung chiến lược dữ liệu đã quy định; hàng năm ban hành bổ sung làm giàu danh mục dữ liệu dùng chung, danh mục dữ liệu ngành, danh mục dữ liệu mở; các hoạt động quản trị dữ liệu đã được triển khai thực hiện định kỳ.
- **100%** thủ tục hành chính đủ điều kiện theo quy định của pháp luật được cung cấp dưới hình thức dịch vụ công toàn trình; các Hệ thống thông tin của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội, tổ chức được kết nối Nền tảng định danh và xác thực điện tử để giảm thiểu sự trùng lặp, sai khác thông tin, giảm thiểu chi phí và thời gian, tạo môi trường tin cậy cho các giao dịch trực tuyến của cá nhân.
- 100% cán bộ, công chức, viên chức được đào tạo, tập huấn, bồi dưỡng về tạo lập và quản trị dữ liệu.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Các mục tiêu cụ thể đến năm 2030

3. Dữ liệu số trong phát triển kinh tế số, xã hội số

- Kinh tế số chiếm **40%** tổng sản phẩm trên địa bàn (GRDP)
- Xây dựng và hoàn thành **100%** các bộ dữ liệu ngành nông nghiệp gồm: dữ liệu đất đai, cây trồng, vật nuôi, thủy sản cho các vùng sản xuất nông nghiệp trên địa bàn thành phố phục vụ các hoạt động sản xuất nông nghiệp; hình thành dữ liệu của toàn bộ chuỗi quy trình sản xuất, kinh doanh, chế biến, quản lý giám sát nguồn gốc, cung ứng các sản phẩm nông nghiệp quan trọng, đảm bảo việc cung cấp thông tin minh bạch, chính xác, đẩy mạnh phát triển thương mại điện tử.
- Xây dựng và hoàn thành **100%** các bộ dữ liệu ngành công nghiệp, thương mại và năng lượng, bao gồm: dữ liệu về mạng lưới sản xuất, truyền tải, tiêu thụ; dữ liệu trong lĩnh vực sản xuất công nghiệp, mạng lưới, chuỗi cung ứng sản xuất cơ bản trong các hoạt động công nghiệp từ nguyên liệu thô tới thành phẩm thương mại; dữ liệu về các trung tâm logistics, vận chuyển, kho bãi; dữ liệu về thị trường thương mại, hành vi tiêu dùng, nhu cầu quảng cáo của các nhãn hàng trên thị trường Hải Phòng nhằm tối ưu hóa quá trình sản xuất, tiêu thụ hàng hóa của các đơn vị sản xuất, xây dựng các kênh phân phối hàng hóa hiệu quả và giám sát chặt chẽ nhu cầu thị trường,...



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Các mục tiêu cụ thể đến năm 2030

- **90%** các di sản văn hóa, di tích quốc gia, di tích quốc gia đặc biệt được số hóa, lưu trữ đầy đủ dữ liệu và hình thành thư viện số, di sản số, có hiện diện số trên môi trường mạng để mọi người dân, khách du lịch có thể truy cập, tra cứu tìm hiểu thuận lợi trên môi trường số; **100%** các danh lam thắng cảnh, địa điểm du lịch trên địa bàn thành phố được hoàn thành việc số hóa, lưu trữ và chia sẻ thông tin rộng rãi, kết hợp xây dựng các nền tảng số du lịch đồng bộ để quảng bá, phát triển du lịch Hải Phòng, đưa du lịch thực sự là ngành kinh tế mũi nhọn, phát triển bền vững.

- Hoàn thiện **100%** cơ sở dữ liệu về bảo hiểm xã hội cho người lao động. Dữ liệu chuẩn hóa số lao động điện tử, tích hợp với dữ liệu về học tập suốt đời, dữ liệu về đào tạo nghề (bao gồm cả đào tạo tại trường và đào tạo, tích lũy kinh nghiệm làm việc tại các cơ quan, tổ chức, doanh nghiệp) của người lao động được triển khai, hoàn thiện cho **100%** người lao động đóng bảo hiểm xã hội.

- **100%** các bộ dữ liệu mở về lực lượng, thị trường lao động việc làm, nhu cầu tuyển dụng lao động và yêu cầu trình độ, kỹ năng tương ứng được cung cấp và đảm bảo cập nhật chính xác, kịp thời, làm cơ sở triển khai các giải pháp dự báo nhu cầu, sự biến động về lao động, việc làm; người lao động có thể tiếp cận với dữ liệu về nhu cầu lao động, việc làm của xã hội và được tự động cung cấp gợi ý về danh sách việc làm phù hợp khi bị thất nghiệp.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Các mục tiêu cụ thể đến năm 2030

- Kho học liệu về giáo trình, tài liệu giảng dạy, học tập ngành giáo dục được số hóa, tích hợp với các nền tảng dạy và học trực tuyến đảm bảo hỗ trợ được cho **100%** người học và nhà giáo tham gia có hiệu quả các hoạt động giáo dục trực tuyến; đáp ứng yêu cầu về tài liệu học tập cho toàn bộ chương trình giáo dục phổ thông và tối thiểu **40%** số ngành đào tạo các trình độ của giáo dục đại học.

- **100%** dữ liệu không gian địa lý ngành Nông nghiệp và Môi trường được số hóa, chuẩn hóa và liên thông, chia sẻ cho các cơ quan nhà nước... dưới dạng dịch vụ bản đồ và có thể chia sẻ cho các hệ thống thông tin của những lĩnh vực có sử dụng dịch vụ dữ liệu không gian địa lý kết nối, khai thác sử dụng.

- **100%** dữ liệu giám sát, quan trắc tự động việc xả thải của các khu công nghiệp, các điểm nóng về ô nhiễm môi trường được đảm bảo đáp ứng nhu cầu kết nối về trung tâm giám sát tập trung của ngành Nông nghiệp và Môi trường theo thời gian thực, phục vụ việc phân tích đưa ra các cảnh báo khi có nguy cơ về sự cố môi trường.

- **100%** dữ liệu về hạ tầng giao thông công cộng và phương tiện giao thông, dữ liệu về kho, bãi và các trung tâm logistics được số hóa, cập nhật kịp thời, hỗ trợ giải quyết tốt những vấn đề khó khăn, vướng mắc của ngành giao thông và đáp ứng được nhu cầu xây dựng chuỗi cung ứng giao nhận - kho vận và logistics.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Các mục tiêu cụ thể đến năm 2030

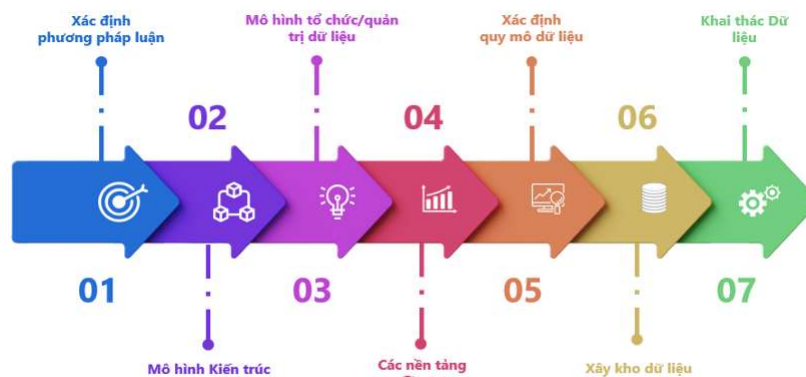
- **95%** các dữ liệu về y tế được xây dựng, tổ chức phù hợp với định hướng phân cấp quản lý từ thành phố đến các xã, phường, đặc khu để phát triển, hoàn thiện cơ sở dữ liệu của thành phố về y tế và các cơ sở dữ liệu chuyên ngành y tế.

- Phát triển thị trường dữ liệu, hoàn thành thí điểm, thử nghiệm **01** sàn giao dịch dữ liệu tạo môi trường mua bán, trao đổi dữ liệu có sự giám sát đảm bảo an toàn, tuân thủ quy định của pháp luật; phát triển các dịch vụ dữ liệu (tổng hợp, phân tích, dân nhân dữ liệu,...) để tạo thêm nhiều cơ hội việc làm cho người dân, nhất là người có hoàn cảnh khó khăn và người khuyết tật; xuất khẩu tri thức của lao động Phòng ra nước ngoài dựa trên các công việc mới với dữ liệu.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Quy trình chuyển đổi số của thành phố

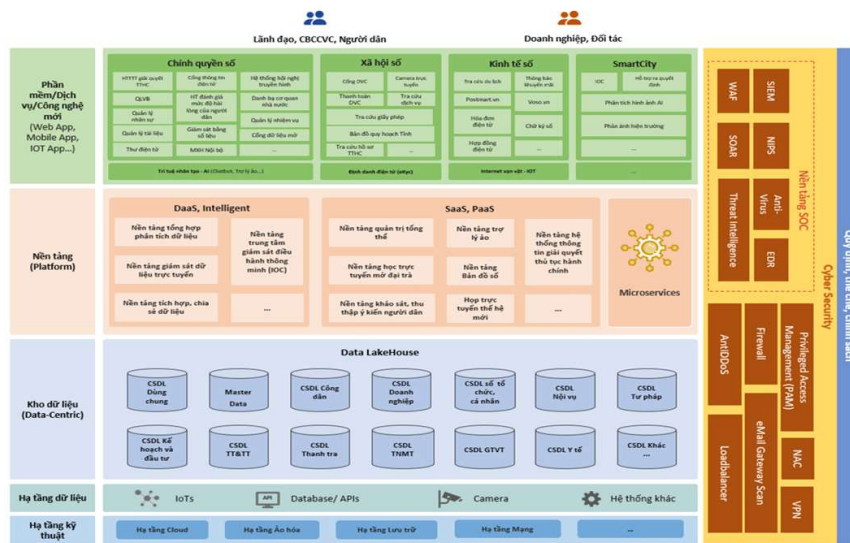


H01: Mô hình tổng quan quy trình thực hiện chuyển đổi số



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

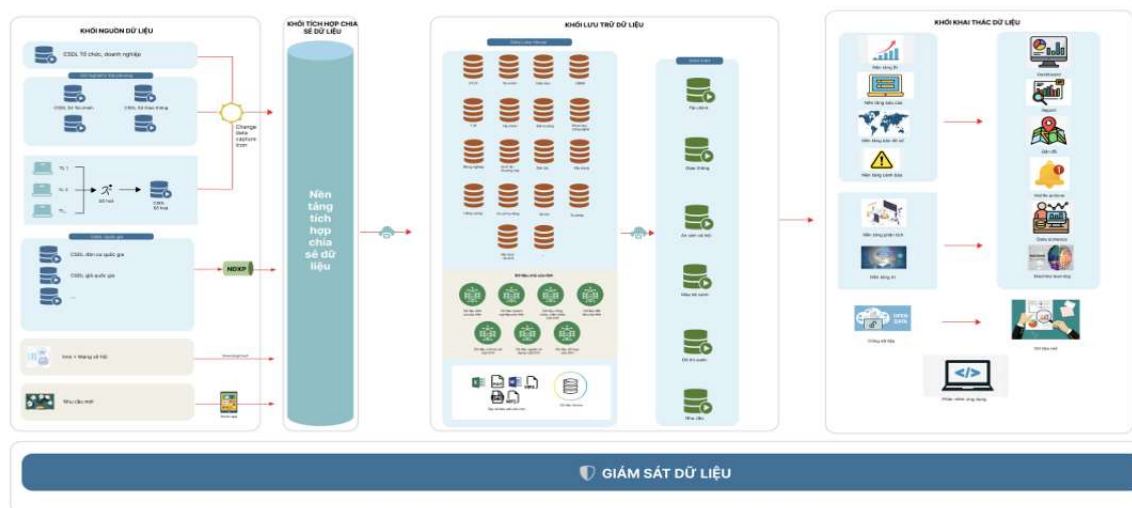
Mô hình kiến trúc chuyển đổi số chung cho thành phố



H02: Mô hình kiến trúc chuyển đổi số của thành phố

Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

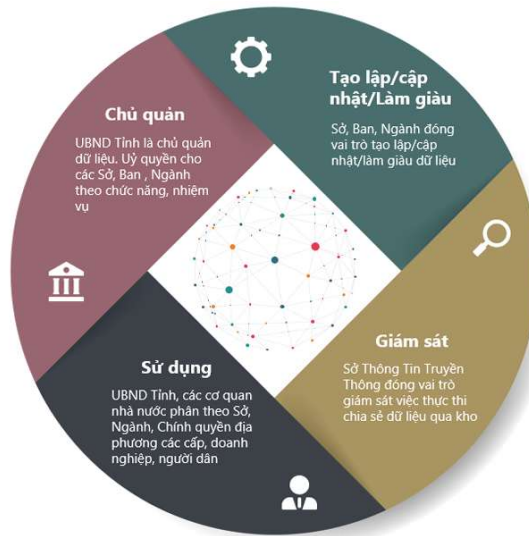
Mô hình tổ chức/quản trị dữ liệu



H03: Mô hình tổ chức dữ liệu của thành phố

Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Mô hình tổ chức/quản trị dữ liệu



H04: Mô hình quản trị dữ liệu của thành phố

Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Nhiệm vụ trọng tâm



Các Sở, ban, ngành thành phố; địa phương ưu tiên xây dựng, nâng cấp, hoàn thiện hệ thống CSDL và ứng dụng chuyên ngành để hình thành CSDL thống nhất, chia sẻ dùng chung; tránh tình trạng cát cứ dữ liệu trong mỗi cơ quan, đơn vị, địa phương; liên thông, tích hợp với các hệ thống thông tin, CSDL chuyên ngành đảm bảo theo các quy định, quy chuẩn, hướng dẫn của các Bộ, ngành chủ quản.

Giải pháp thực hiện

- Xây dựng cơ chế, chính sách
- Tổ chức bộ máy
- Tuyên truyền, bồi dưỡng, tập huấn kỹ năng
- Nghiên cứu, hợp tác phát triển
- Giải pháp tài chính
- Đo lường, giám sát, đánh giá triển khai



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Tổ chức thực hiện



1. Ban Chỉ đạo của thành phố về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06

Chỉ đạo toàn diện việc tổ chức triển khai thực hiện Chiến lược dữ liệu thành phố Hải Phòng đến năm 2030; định kỳ kiểm tra, đôn đốc, đánh giá kết quả thực hiện; chỉ đạo việc rà soát, điều chỉnh, cập nhật nội dung Chiến lược bảo đảm phù hợp với tình hình thực tế và yêu cầu phát triển của thành phố. Chỉ đạo các cơ quan, đơn vị, địa phương phối hợp, chia sẻ dữ liệu và triển khai các nhiệm vụ, dự án liên quan đến phát triển, quản trị và khai thác dữ liệu.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Tổ chức thực hiện



2. Sở Khoa học và Công nghệ

a) Là cơ quan đầu mối, theo dõi, đôn đốc việc triển khai thực hiện Chiến lược dữ liệu, thực hiện vai trò quản lý hạ tầng, giám sát, thực thi việc kết nối, chia sẻ dữ liệu theo Mô hình quản lý dữ liệu.

b) Chủ trì, phối hợp các ngành, địa phương rà soát, cập nhật các danh mục CSDL dùng chung của thành phố, triển khai tích hợp các dữ liệu chủ, dữ liệu dùng chung của thành phố.

d) Chủ trì, phối hợp với các đơn vị tổ chức tập huấn, bồi dưỡng chuyên môn về phát triển, quản lý, quản trị, phân tích dữ liệu và khai thác dữ liệu cho cán bộ công chức, viên chức phụ trách CNTT của các ngành, địa phương.

đ) Tổ chức các hội nghị, hội thảo, các hoạt động tuyên truyền về phát triển dữ liệu số.

e) Phối hợp với các đơn vị công bố danh mục danh mục CSDL chuyên ngành, danh mục các dịch vụ chia sẻ dữ liệu, dữ liệu mở trên Cổng dữ liệu của thành phố. Hướng dẫn, hỗ trợ các Sở, ban, ngành thành phố triển khai danh mục dữ liệu, phát triển danh mục CSDL chuyên ngành, tích hợp CSDL chủ, CSDL dùng chung về Kho dữ liệu dùng chung của thành phố, khai thác các nền tảng tạo lập, quản lý dữ liệu.

g) Theo dõi, tổng hợp tình hình triển khai của các Sở, ban, ngành thành phố, UBND các xã, phường, đặc khu; báo cáo UBND thành phố; chủ động nắm bắt các khó khăn, vướng mắc có khả năng ảnh hưởng đến chất lượng, tiến độ của Chiến lược dữ liệu và phối hợp với các đơn vị tìm phương án giải quyết, báo cáo UBND thành phố xem xét, quyết định.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Tổ chức thực hiện



3. Công an thành phố

Phối hợp với các Sở, ngành, địa phương trong việc bảo đảm an toàn, an ninh dữ liệu, bảo mật hệ thống thông tin và phòng ngừa, phát hiện, xử lý các hành vi vi phạm liên quan đến dữ liệu.

Phối hợp với các đơn vị chức năng thuộc Bộ Công an để thực hiện việc kết nối, chia sẻ thông tin từ Cơ sở dữ liệu quốc gia về dân cư với Kho dữ liệu dùng chung của thành phố theo quy định, bảo đảm việc khai thác, sử dụng dữ liệu đúng mục đích, đúng phạm vi và tuân thủ quy định về bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước.

4. Sở Tài chính

a) Hàng năm, căn cứ khả năng cân đối ngân sách, tham mưu cho UBND thành phố về kinh phí triển khai Chiến lược dữ liệu.

b) Sở Tài chính là cơ quan đầu mối chủ trì, phối hợp với Sở Khoa học và Công nghệ và các sở, ngành, địa phương thúc đẩy, hỗ trợ doanh nghiệp trên địa bàn thực hiện phát triển dữ liệu.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Tổ chức thực hiện



5. Các Sở, ban, ngành thành phố

a) Chủ trì xây dựng danh mục hệ thống thông tin, danh mục CSDL chuyên ngành, danh mục các dịch vụ chia sẻ dữ liệu chuyên ngành, danh mục các nhu cầu cần dự đoán, dự báo.

b) Chủ trì xây dựng chi tiết Danh mục dữ liệu phát triển ngành, lấy đó làm thước đo để triển khai các hệ thống/phần mềm; hướng đến ứng dụng các công nghệ phân tích, xử lý dữ liệu lớn vào phân tích các bài toán bằng dữ liệu của ngành mình.

c) Triển khai các hệ thống thông tin quản lý chuyên ngành thống nhất trên toàn thành phố, từ Sở, ban, ngành thành phố đến các xã, phường, đặc khu và các sở ngành có liên quan.

d) Chủ trì, phối hợp với UBND các xã, phường, đặc khu và các đơn vị có liên quan triển khai số hóa, tạo lập CSDL chuyên ngành đảm bảo sau khi dữ liệu hoàn thiện đến đâu thì đưa vào hệ thống thông tin chuyên ngành đến đó, dữ liệu luôn được cập nhật.

đ) Phối hợp với Sở Khoa học và Công nghệ tham mưu, đề xuất với UBND thành phố về những thay đổi quy định dữ liệu ngành để làm cơ sở cập nhật Chiến lược dữ liệu hằng năm.

e) Phối hợp với Sở Khoa học và Công nghệ về việc tổ chức các hội thảo chuyên sâu về phân tích, xử lý dữ liệu trong ngành, lĩnh vực của cơ quan mình.



Chiến lược dữ liệu TP. Hải Phòng giai đoạn 2026-2030, tầm nhìn 2045

Tổ chức thực hiện



6. Ủy ban nhân dân các xã, phường, đặc khu

a) Phối hợp cùng các Sở, ban, ngành thành phố trong việc triển khai các hệ thống thông tin chuyên ngành và số hóa, tạo lập CSDL chuyên ngành (thống nhất và xuyên suốt từ cấp xã đến cấp Sở, ngành).

b) Đề xuất nhu cầu về phân cấp, phân quyền dữ liệu để phục vụ công tác quản lý, chỉ đạo.

c) Tổ chức các hội nghị, hội thảo tuyên truyền, tập huấn về phát triển dữ liệu số tại địa phương.

d) UBND các xã, phường, đặc khi cân đối nguồn để đảm bảo kinh phí thực hiện các nhiệm vụ phân cấp, phân quyền dữ liệu phục vụ công tác quản lý, chỉ đạo điều hành./.



*Thank
you*





Quản trị và điều hành qua các bộ chỉ số

PHẦN 3

Kiến thức Nâng cao

Quản trị và Điều hành qua các Bộ chỉ số

Mục tiêu: Cán bộ xã hiểu rõ đóng góp của cấp cơ sở vào các bộ chỉ số đánh giá năng lực điều hành của tỉnh

PCI & DDCI

PAR / SIPAS

PAPI

PII

DTI

5 Bộ Chỉ số Quản trị Điều hành

01

PCI & DDCI

Năng lực cạnh tranh cấp tỉnh

02

PAR Index & SIPAS

Cải cách hành chính & Hải lòng dân

03

PAPI

Hiệu quả quản trị & hành chính công

04

PII

Đổi mới sáng tạo cấp địa phương

05

DTI

Chuyển đổi số

Cấp xã là mắt xích quan trọng trong toàn bộ chuỗi chỉ số này — thái độ, minh bạch, và chuyển đổi số cấp cơ sở ảnh hưởng trực tiếp đến kết quả tỉnh

01 PCI & DDCI — Chỉ số Năng lực Cạnh tranh

💡 PCI không chỉ là chỉ số của cấp tỉnh — cấp xã đóng góp trực tiếp!



Thái độ phục vụ

Cán bộ Một cửa cấp xã thân thiện, nhiệt tình, chuyên nghiệp



Chi phí thời gian

Giảm thời gian xử lý hồ sơ, trả kết quả đúng hạn, không gây chậm trễ



Tính minh bạch

Công khai niêm yết thủ tục, phí lệ phí, thời gian giải quyết đầy đủ



Sự năng động

Chủ động hỗ trợ doanh nghiệp/HTX, sáng tạo trong phục vụ

DDCI đánh giá cấp sở/ngành/địa phương — kết quả tốt tại Bộ phận Một cửa cấp xã góp phần nâng hạng DDCI địa phương

02 PAR Index & SIPAS — Cải cách Hành chính & Hải lòng Người dân



Chỉ số Cải cách Hành chính — đo lường mức độ CCHC của địa phương qua các tiêu chí:

- Công tác chỉ đạo điều hành CCHC
- Chất lượng thủ tục hành chính
- Xây dựng và tổ chức thực hiện văn bản QPPL
- Hiện đại hóa hành chính (ứng dụng CNTT)

Chỉ số Hải lòng của Người dân — khảo sát trực tiếp dân về:

- Tiếp cận dịch vụ (địa điểm, giờ làm việc)
- Thủ tục hành chính (đơn giản, dễ hiểu)
- Năng lực, thái độ cán bộ tiếp nhận
- Kết quả giải quyết và thời gian trả

Mỗi người dân đến Bộ phận Một cửa là một cơ hội để nâng điểm SIPAS và PAR Index cho toàn xã!

03 PAPI — Hiệu quả Quản trị và Hành chính Công cấp tỉnh



04 PII — Chỉ số Đổi mới Sáng tạo cấp địa phương

Vai trò của Cấp Xã

Cấp xã là tuyến đầu cung cấp dịch vụ công và hỗ trợ đổi mới sáng tạo cho người dân và doanh nghiệp/HTX tại địa phương.



Hỗ trợ đăng ký sản phẩm OCOP



Xây dựng thương hiệu địa phương



Đưa sản phẩm lên sàn thương mại điện tử

Chuỗi Hỗ trợ Đổi mới Sáng tạo

1

Nhận diện sản phẩm tiềm năng

Rà soát sản phẩm nông nghiệp, thủ công mỹ nghệ địa phương

2

Hỗ trợ đăng ký OCOP

Hướng dẫn hồ sơ, kết nối với các đơn vị tư vấn chứng nhận

3

Xây dựng thương hiệu

Hỗ trợ thiết kế bao bì, nhãn mác, logo, câu chuyện sản phẩm

4

Đưa lên sàn số

Hướng dẫn đăng ký PostMart, Shopee, TikTok Shop...

05 DTI — Chỉ số Chuyển đổi Số cấp Địa phương

Mô hình đánh giá CDS cấp xã gồm 3 trụ cột: Chính quyền số — Kinh tế số — Xã hội số



Hồ sơ trực tuyến

Tăng tỷ lệ DVC mức 3-4 và toàn trình



Thanh toán số

Hướng dẫn dân thanh toán phí online



Chữ ký số cá nhân

Hỗ trợ người dân đăng ký & sử dụng



VNeID

Hỗ trợ kích hoạt tài khoản định danh

Mối liên hệ hữu cơ:

Cải thiện DTI + PII → Cải thiện PAR Index + SIPAS → Nâng hạng PCI

Tóm tắt & Thông điệp Cốt lõi

PCI/DDCI

Thái độ phục vụ và minh bạch tại Một cửa cấp xã ảnh hưởng trực tiếp đến môi trường kinh doanh toàn tỉnh.

PAR/SIPAS

Mỗi giao dịch tại Bộ phận Một cửa là cơ hội để nâng điểm hài lòng của người dân.

PAPI

Dân chủ cơ sở thực chất, minh bạch tài chính và phản hồi kiến nghị kịp thời là nền tảng quản trị tốt.

PII

Cấp xã hỗ trợ OCOP, thương mại điện tử là cầu nối đổi mới sáng tạo cho kinh tế địa phương.

DTI

Cán bộ xã là mắt xích quyết định nâng tỷ lệ hồ sơ trực tuyến, thanh toán số và VNeID.

"Cấp xã mạnh — tỉnh mạnh — đất nước phát triển"

TỔNG QUAN HỆ THỐNG

Trung Tâm Điều Hành Thông Minh (IOC) Thành Phố Hải Phòng

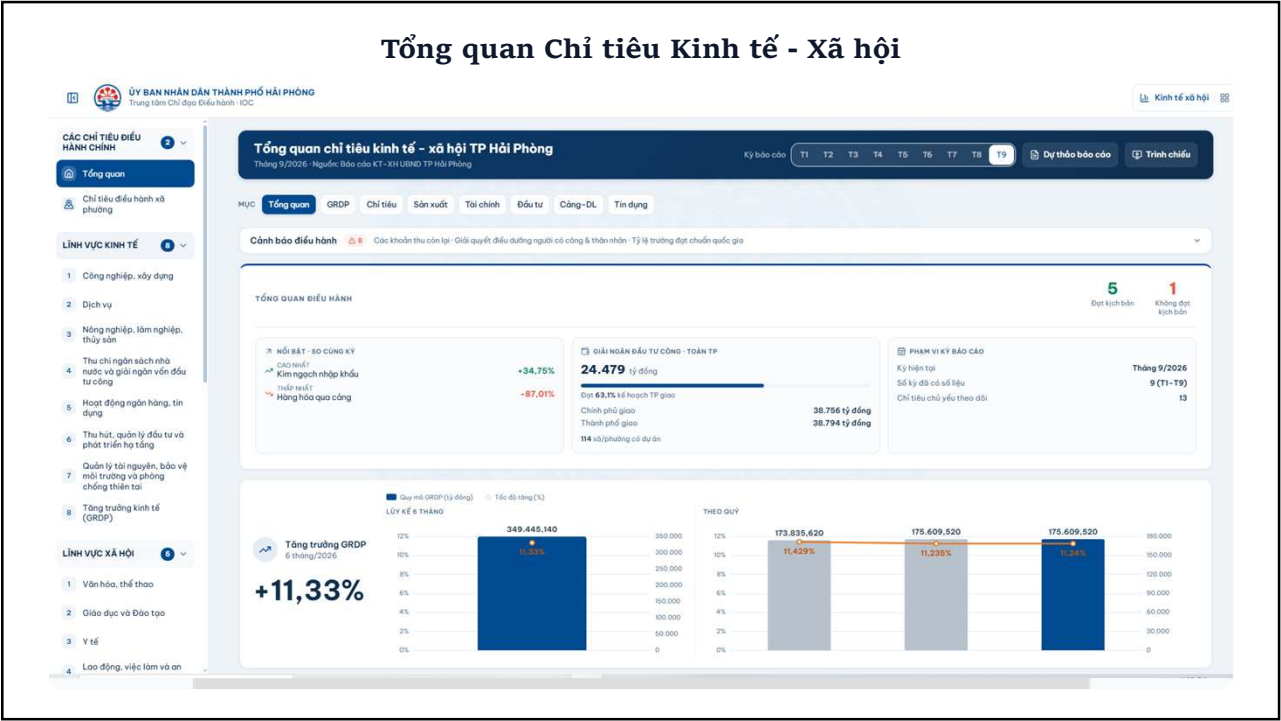
Đã có **22 bộ chỉ số** phục vụ công tác chỉ đạo, điều hành trực tiếp cho lãnh đạo thành phố.

Giao diện Hệ sinh thái Điều hành Thông minh

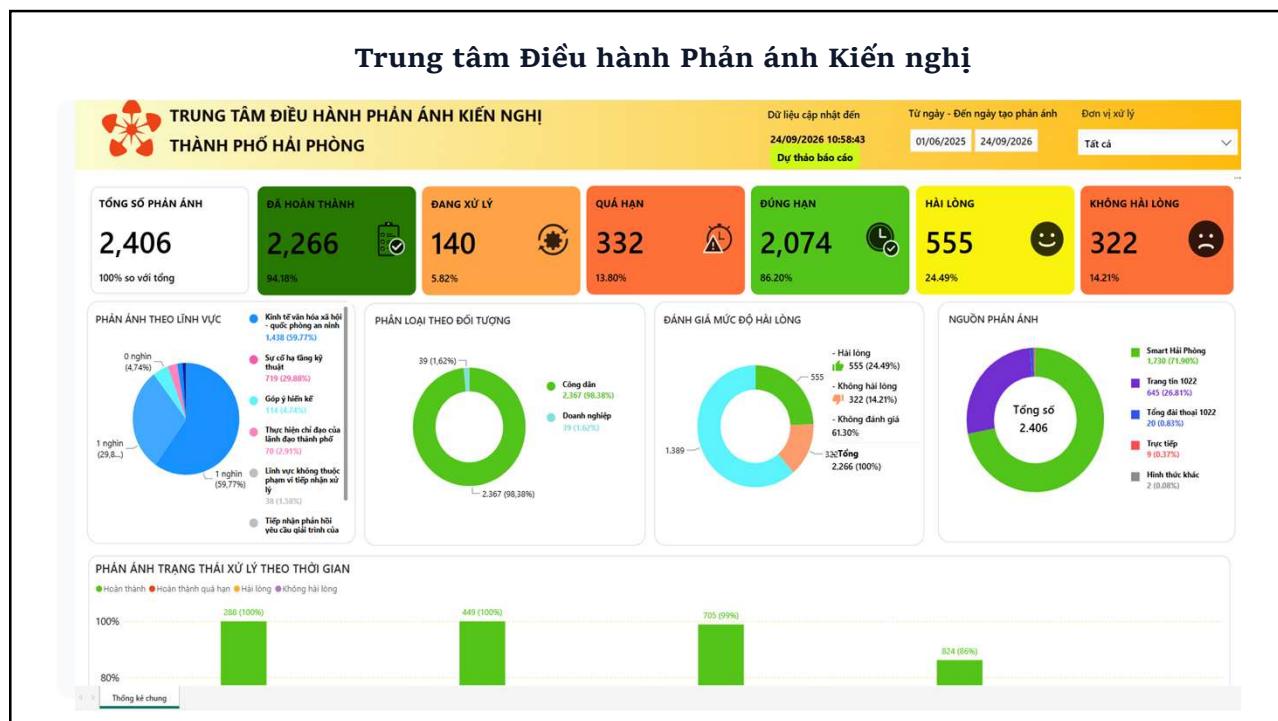


Các Phân hệ Quản lý và Dữ liệu Chuyên ngành





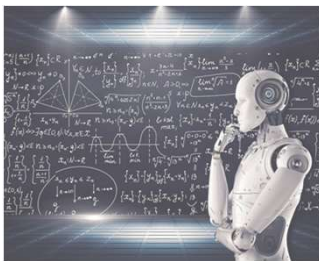
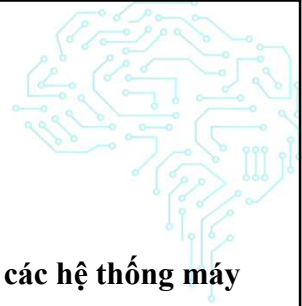
Trung tâm Điều hành Phản ánh Kiến nghị



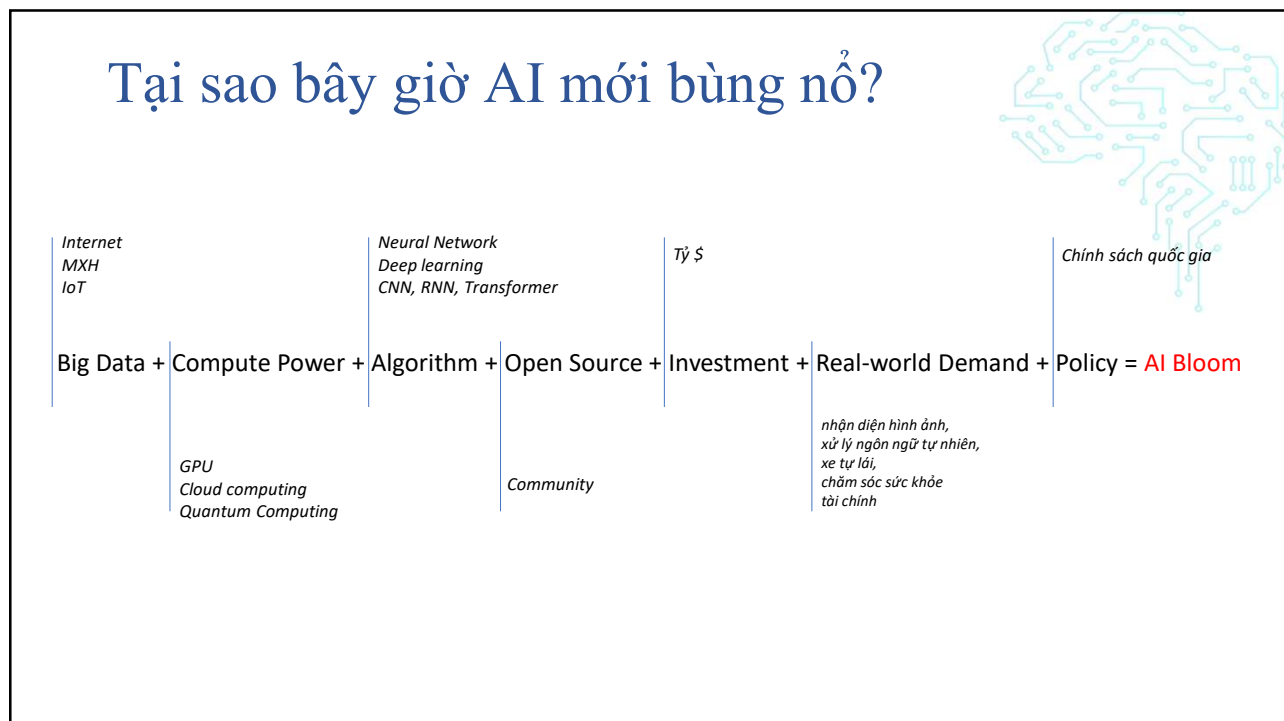
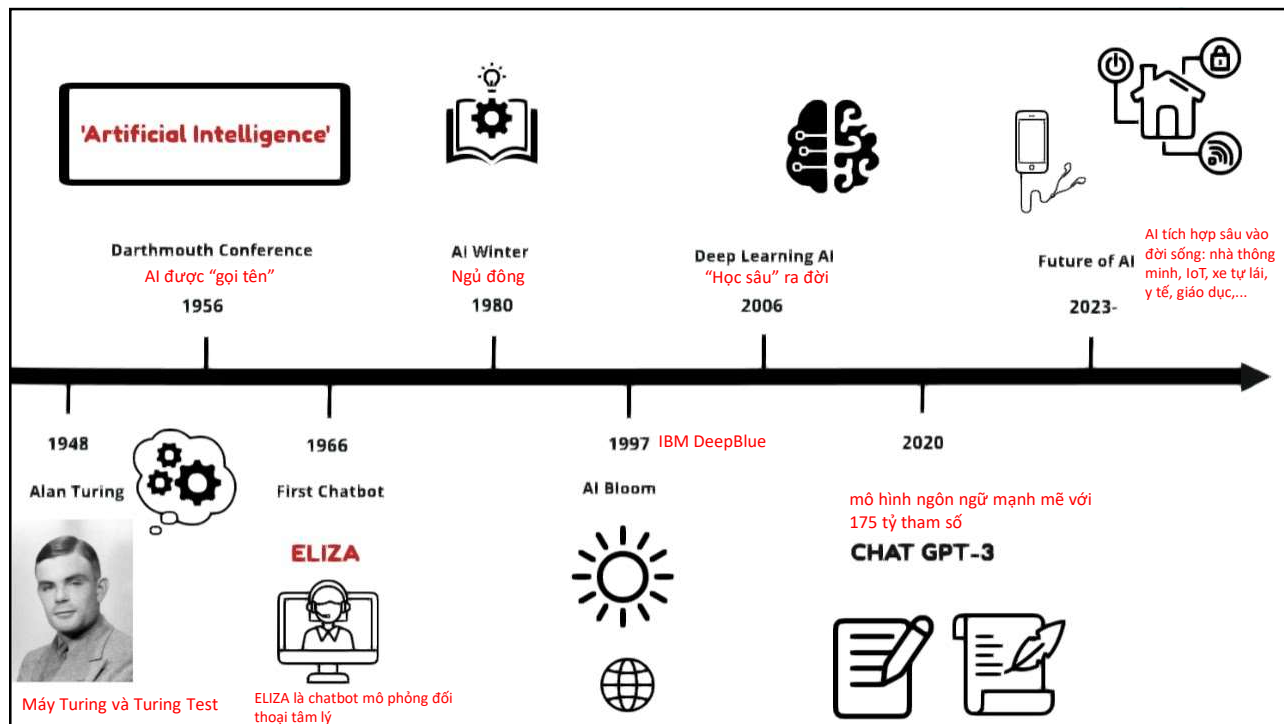


Trí Tuệ Nhân Tạo

Trí tuệ nhân tạo



Trí tuệ nhân tạo đề cập đến **khả năng của các hệ thống máy tính** thực hiện các **nhiệm vụ** liên quan đến trí thông minh của con người, như **học tập, suy luận, giải quyết vấn đề, nhận thức và đưa ra quyết định**.



BÁO CÁO THỊ TRƯỜNG · AI

Xu hướng đầu tư AI toàn cầu

Giai đoạn bùng nổ hạ tầng quy mô nghìn tỷ USD — vốn tập trung cực mạnh vào một số ít công ty lớn và lab frontier, doanh thu bắt đầu xuất hiện để biện minh cho chi tiêu.

\$2,59

nghìn tỷ USD

Tổng chi tiêu AI toàn cầu 2026

 **47% so với 2025**

Cập nhật đến cuối tháng 7/2026

Quy mô tổng thể

Chi tiêu AI năm 2026 ở mức nghìn tỷ USD, hạ tầng chiếm phần lớn

\$2,59 nghìn tỷ

Tổng chi tiêu AI 2026

▲ 47% so với 2025 · Gartner (5/2026)

\$1,43 nghìn tỷ

Hạ tầng AI

Hơn 45% tổng chi tiêu AI

\$6,37 nghìn tỷ

Chi tiêu IT toàn cầu

▲ 14,2% · phần lớn do AI thúc đẩy

\$497 tỷ

Hạ tầng AI (IDC)

▲ 56% · server, chip, networking

Chi tiêu AI trong tổng chi tiêu IT toàn cầu 2026

Hạ tầng AI

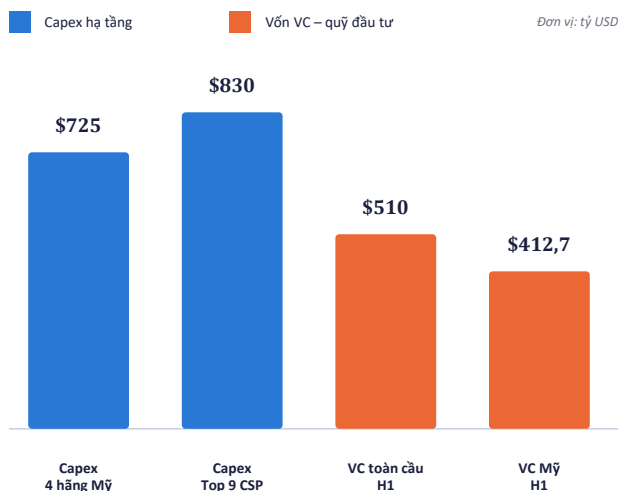
Tổng AI \$2,59T

Tổng IT \$6,37T

Q1/2026, riêng hạ tầng AI (IDC) đã đạt \$89,7 tỷ. Data center systems tăng 62,5% — mức cao nhất trong các hạng mục IT. Nguồn: Gartner, IDC.

Hai dòng chảy vốn chính

Capex của hyperscalers và vốn VC rót vào các lab AI



Capex của hyperscalers – Chi phí đầu tư các công ty công nghệ hàng đầu ~\$700–830 tỷ (2026)

- 4 hãng Mỹ ~\$725 tỷ (▲77%); Top 9 CSP toàn cầu ~\$830 tỷ.
- Lũy kế 2024–2026 đang tiến tới \$1.000 tỷ.

Vốn VC / funding lab AI ~\$510 tỷ (H1/2026)

- AI chiếm hơn 70% VC toàn cầu; riêng Mỹ ~\$412,7 tỷ, AI chiếm 86%.
- OpenAI + Anthropic một mình chiếm ~43% funding startup toàn cầu.

Những xu hướng nổi bật

Sáu chuyển động định hình dòng vốn AI hiện nay



Chuyển từ model sang hạ tầng

Chỉ tiêu chủ yếu vào data center, GPU/TPU, điện, bộ nhớ HBM, mạng — không còn chỉ là phần mềm/model.



Mỹ áp đảo

Chiếm phần lớn private investment và hạ tầng; Trung Quốc dựa nhiều vào hỗ trợ nhà nước.



Doanh thu bắt đầu hiện diện

Doanh thu AI của hyperscalers đã vượt chi phí khấu hao trong vài quý gần đây, dù biên còn mỏng.



Áp lực dòng tiền

Capex tăng nhanh hơn free cash flow → nhiều hãng phải vay nợ, phát hành cổ phiếu, dùng leasing/JV.



Kiến trúc chuyển dịch

Server ARM-based đang vượt x86 trong phân khúc AI accelerated computing.



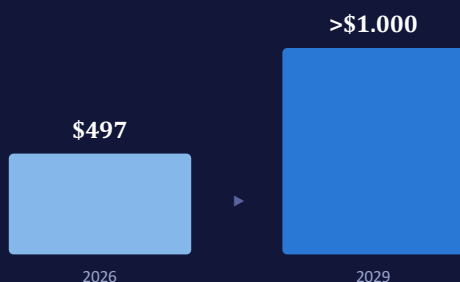
Sovereign AI & địa chính trị

Các quỹ quốc gia và dự án lớn như Stargate (\$500 tỷ) tham gia mạnh vào cuộc đua hạ tầng.

TRIỂN VỌNG NGẮN – TRUNG HẠN

2026–2027 vẫn là giai đoạn xây dựng công suất mạnh

Dự báo hạ tầng AI (IDC) — tỷ USD



Bức tranh tổng thể

- Quy mô nghìn tỷ USD, tăng trưởng nhanh trên mọi hạng mục hạ tầng.
- Tập trung cực cao vào một số ít hyperscaler và lab frontier.
- Doanh thu generative AI bắt đầu xuất hiện để biện minh cho chi tiêu.
- Áp lực dòng tiền và địa chính trị là hai biến số cần theo dõi.

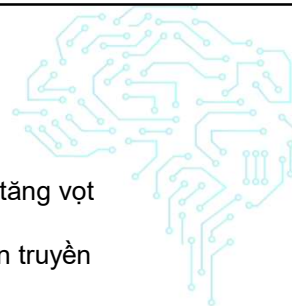
Nhu cầu năng lượng cho các trung tâm dữ liệu tại Mỹ được dự báo sẽ tăng vọt +253% so với mức năm 2026, đạt kỷ lục 194 gigawatt vào năm 2035.

Một gigawatt tương đương với công suất của một lò phản ứng hạt nhân truyền thống đơn lẻ.

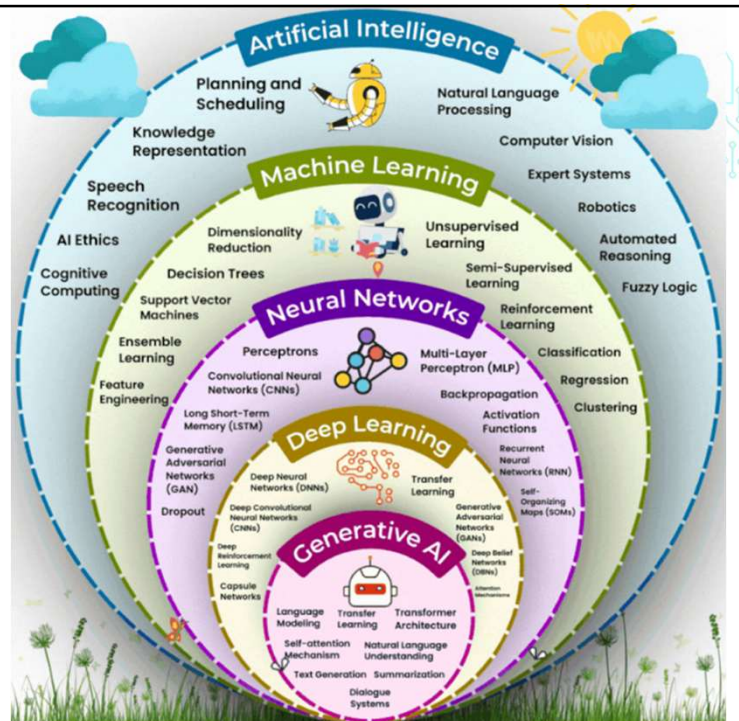
Do đó, các trung tâm dữ liệu dự kiến sẽ chiếm khoảng ~20% tiêu thụ điện của Mỹ vào năm 2035, tăng từ ~6% hiện nay.

Để hình dung rõ hơn, các trung tâm dữ liệu được ước tính sẽ tiêu thụ khoảng ~12% điện năng của Mỹ vào năm 2030.

Điện năng là nút thắt cổ chai tiếp theo của AI.



- Trí tuệ nhân tạo (Artificial Intelligence - AI)
- học máy (Machine Learning - ML)
- học sâu (Deep Learning - DL),
- học tăng cường (Reinforcement Learning - RL),
- xử lý ngôn ngữ tự nhiên (Natural Language Processing - NLP),
- thị giác máy tính (Computer Vision - CV),
- AI tạo sinh (Generative AI),
- transformer,
- GPT (Generative Pre-trained Transformer),
- mô hình ngôn ngữ lớn (Large Language Model - LLM),
- học không giám sát (Unsupervised Learning),
- học có giám sát (Supervised Learning),
- học bán giám sát (Semi-supervised Learning),
- học chuyển giao (Transfer Learning),
- học một lần (One-shot Learning),
- học ít lần (Few-shot Learning),
- học không lần (Zero-shot Learning),
- AI giải thích được (Explainable AI - XAI),
- AI đa phương thức (Multimodal AI),
- AI biên (Edge AI).
- ...



Narrow AI

Dùng để hỗ trợ hoặc thực hiện các nhiệm vụ cụ thể

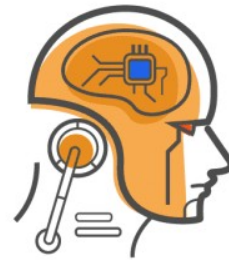
Narrow AI có thể hoạt động rất tốt trong các tác vụ cụ thể như nhận diện hình ảnh, dịch ngôn ngữ, hoặc chơi game cờ vua. Tính hiệu quả và hiệu suất cao là điểm mạnh của loại AI này, nhưng chúng không có khả năng tự học hoặc tự cải thiện.



General AI

Nhận các kiến thức từ một miền và chuyển sang các miền khác

General AI có khả năng học hỏi, tư duy, và tự cải thiện thông qua việc thu thập và phân tích dữ liệu, và có khả năng áp dụng kiến thức từ một lĩnh vực sang lĩnh vực khác. Mục tiêu cuối cùng của General AI là tạo ra một máy tính có thể hiểu, tư duy, và thậm chí có ý thức như con người.

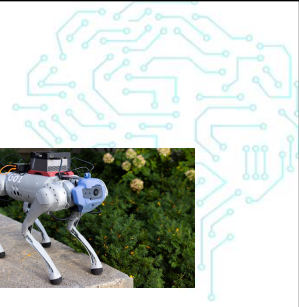


Super AI

Cổ máy thông minh hơn con người rất nhiều

Đây là loại AI mà khả năng thông minh và hiểu biết vượt xa cả trí tuệ của con người. Superintelligent AI có thể tự cải thiện bản thân mình ở một tốc độ nhanh chóng và thậm chí có khả năng tự học và tiến hóa một cách độc lập.

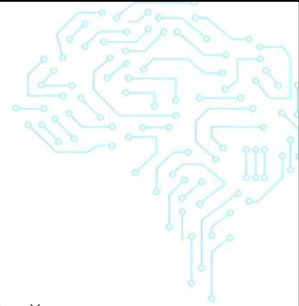
Hình thái AI sẽ thế nào?



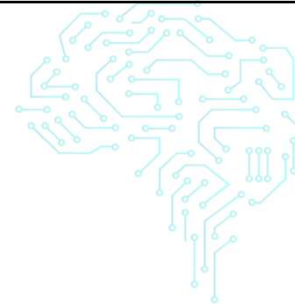
AI is a “New Kind of Species”
AI là một giống loài mới

Con số nổi bật về AI 2025 (1)

- Có 34 triệu hình ảnh được AI tạo ra mỗi ngày
- 71% hình ảnh trên mạng xã hội hiện được tạo ra bởi AI
- Các vụ gian lận Deepfake tăng vọt từ 0,01% lên 6,5% trong vòng 3 năm
- Các ông lớn công nghệ đầu tư 320 tỷ USD vào việc phát triển AI vào năm 2025
- Thị trường dịch vụ AI toàn cầu đạt 243 tỷ USD trong năm nay
- 97% lãnh đạo đầu tư vào AI báo cáo chỉ số ROI (Lợi nhuận đầu tư) tích cực
- 25% doanh nghiệp sẽ triển khai các tác nhân AI trong năm nay

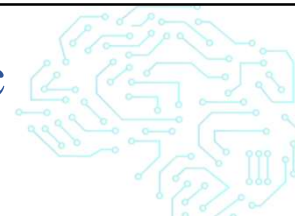


Con số nổi bật về AI 2025 (2)



- Thị trường AI trong lĩnh vực y tế được định giá 38,7 tỷ USD, tăng gấp đôi kể từ năm 2023
- Khoảng cách áp dụng: 81% người lao động vẫn chưa sử dụng công cụ AI
- Sự khác biệt về niềm tin: Ấn Độ (77%) và Trung Quốc (72%), chấp nhận AI, Mỹ chỉ 32%
- Trung tâm dữ liệu tiêu thụ 5% năng lượng của Mỹ, tăng gấp đôi vào năm 2030
- AI nâng cấp trải nghiệm di động với 30% smartphone mới tích hợp Gen AI
- 50% doanh nghiệp chọn sử dụng AI tích hợp giải pháp mã nguồn mở
- Gần 50% lãnh đạo công nghệ tích hợp AI hoàn toàn vào chiến lược kinh doanh, nhưng chỉ 30% áp dụng toàn diện

Ứng dụng AI trong cơ quan nhà nước



ỨNG DỤNG TỰ ĐỘNG HÓA Ở SỐ CÔNG ĐOẠN TRONG CÁC BỘ, NGÀNH, ĐỊA PHƯƠNG, BAO GỒM:



Nghiệp vụ xuất nhập cảnh



Quản lý đô thị



Số hóa dữ liệu tiếng nói, văn bản



Thu thập số liệu tự động, giám sát, cảnh báo, dự báo các lĩnh vực khí tượng, thủy văn, tài nguyên nước....



Các cải tiến về chính sách đầu tư và quản lý nhà nước



Các đề án xây dựng thành phố thông minh

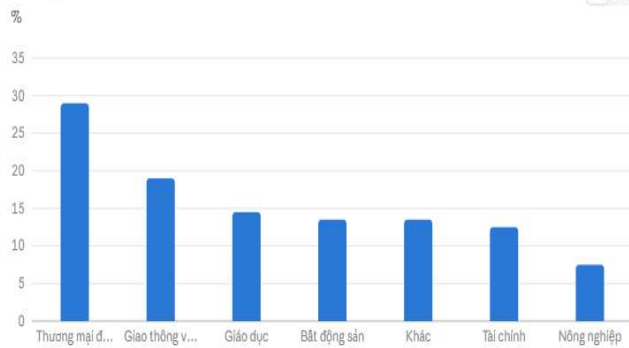


Các đề án Chuyển đổi số quốc gia và Chính phủ điện tử

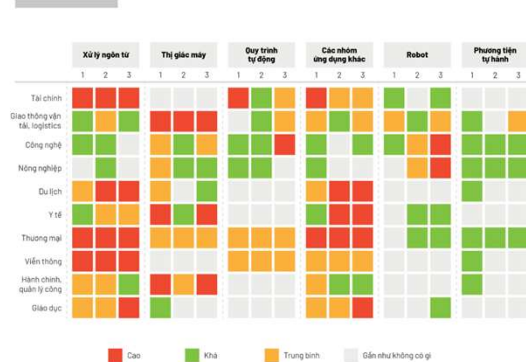
Ứng dụng AI trong Kinh tế - Xã hội



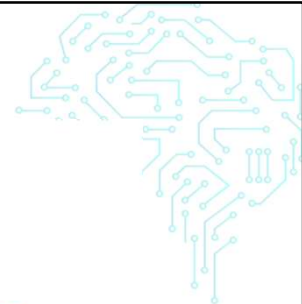
Tỷ trọng theo lĩnh vực (%)



Thực trạng về dữ liệu, nguồn cung và nhu cầu TTNT trong các ngành kinh tế xã hội.



Ứng dụng AI trong Kinh tế - Xã hội



MỘT SỐ ỨNG DỤNG TRONG KINH TẾ XÃ HỘI



Tài chính ngân hàng
Chatbot, phát hiện gian lận và rửa tiền, hỗ trợ quyết định tín dụng



Thương mại
Sàn thương mại điện tử, ứng dụng nhận dạng mã sản phẩm, ứng dụng sinh trắc học trong thanh toán điện tử



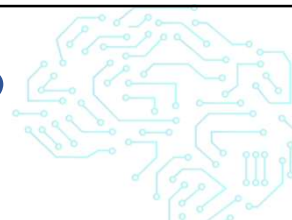
Giao thông vận tải & Logistics
Trạm thu phí không dừng, trung tâm giám sát điều hành giao thông đường bộ, hệ thống logistics thông minh, taxi công nghệ ứng dụng TTNT



Y tế
Hàng loạt sản phẩm robot thông minh trong hỗ trợ cán bộ y tế tại Bệnh viện

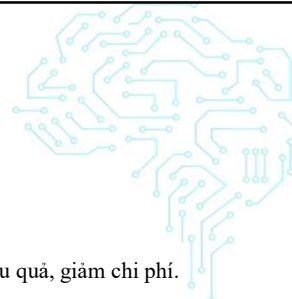
<https://vjst.vn/hien-trang-ung-dung-tri-tue-nhan-tao-o-viet-nam-25450.html>

Mối liên hệ giữa AI và Chuyển đổi số



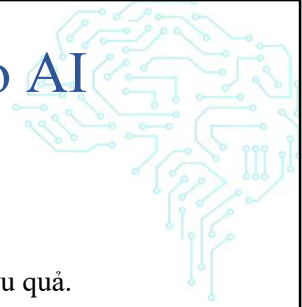
Yếu tố	Trí tuệ nhân tạo (AI)	Chuyển đổi số
Bản chất	Công nghệ mô phỏng trí tuệ con người để máy móc học và ra quyết định.	Quá trình ứng dụng công nghệ để thay đổi cách tổ chức vận hành, cung cấp dịch vụ.
Vai trò trong CDS	Là công cụ, nền tảng giúp xử lý dữ liệu lớn, tự động hóa, tối ưu quy trình.	Là mục tiêu và quá trình tổ chức ứng dụng AI (và các công nghệ khác) để đổi mới.
Tác động	Giúp CDS diễn ra thông minh, hiệu quả và có chiều sâu hơn.	Tạo ra môi trường và dữ liệu phù hợp để AI phát huy hiệu quả.

Cách AI thúc đẩy chuyển đổi số



- Tự động hóa quy trình
 - AI giúp thay thế các công việc thủ công, lặp đi lặp lại → nâng cao hiệu quả, giảm chi phí.
- Ra quyết định dựa trên dữ liệu (data-driven)
 - AI xử lý và phân tích dữ liệu lớn để đưa ra gợi ý, dự báo hỗ trợ lãnh đạo và nhân viên.
- Cá nhân hóa dịch vụ
 - Trong thương mại điện tử, giáo dục, y tế... AI giúp cung cấp trải nghiệm phù hợp với từng người dùng.
- Cảnh báo và phòng ngừa rủi ro
 - AI phát hiện gian lận, bất thường trong tài chính, an ninh mạng, y tế...

Cách Chuyển đổi số tạo điều kiện cho AI



- Số hóa dữ liệu và quy trình
 - Dữ liệu số là —nhiên liệu để AI học và vận hành hiệu quả.
- Hạ tầng công nghệ hiện đại
 - Chuyển đổi số thúc đẩy đầu tư vào cloud, IoT, hệ thống thông minh — điều kiện cho AI hoạt động.
- Văn hóa tổ chức hướng đổi mới
 - Tạo môi trường chấp nhận công nghệ mới, chấp nhận rủi ro và học hỏi liên tục.

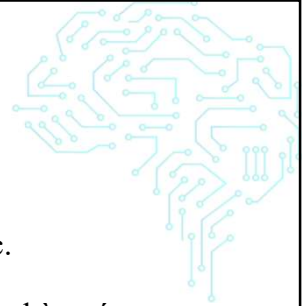




Ứng Dụng Trí Tuệ Nhân Tạo Trong Công Sở

Mục tiêu

1. Nắm bắt được các loại hình công cụ AI phổ biến.
2. Biết cách sử dụng các công cụ AI cơ bản để tối ưu hóa công việc.
3. Nhận diện được tiềm năng và lợi ích khi áp dụng AI vào quản lý nhà nước.



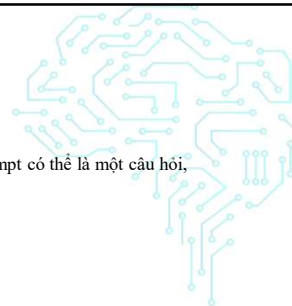
Nội dung

1. Cách viết Prompt hiệu quả
2. Gemini Deep Research – Chuyên gia nghiên cứu tự trị
3. NotebookLM – Thư viện số cục bộ và rà soát thể chế nội bộ
4. Gemini Canvas – Phác thảo, tinh chỉnh và Trực quan hóa nội dung
5. Phân tích Dữ liệu và Dự báo



(1) Ra lệnh (prompt) cho AI

- Prompt là một câu lệnh hoặc yêu cầu mà người dùng nhập vào để giao tiếp với các mô hình AI như ChatGPT. Prompt có thể là một câu hỏi, một chỉ dẫn, hoặc đoạn văn bản mô tả mà người dùng mong muốn AI phản hồi lại.
- Prompt = lời nhắc / yêu cầu / chỉ dẫn mà bạn gửi cho AI để nhận được câu trả lời như mong muốn.



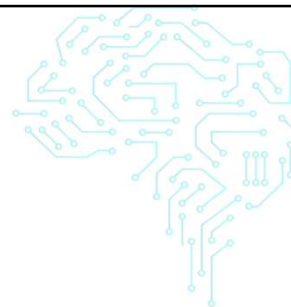
Mục đích	Prompt đơn giản	Prompt hiệu quả
Bản chất	Tóm tắt đoạn này	Tóm tắt đoạn văn dưới đây thành 3 gạch đầu dòng dễ hiểu cho học sinh lớp 9
Viết bài	Viết bài về chuyển đổi số	Bạn là Giám đốc chương trình chuyển đổi số với 10 năm kinh nghiệm triển khai. Viết một bài trình bày về vai trò của chuyển đổi số trong quản lý nhà nước, dài khoảng 500 từ, sử dụng các ví dụ để minh họa.
Dịch thuật	Dịch đoạn này sang tiếng Anh	Dịch đoạn văn sau sang tiếng Anh học thuật, giữ nguyên sắc thái nghiêm túc.

(1) Cách viết Prompt hiệu quả

Công thức Prompt hiệu quả

Vai trò – Ngữ cảnh – Mục tiêu – Đầu Ra

- **Vai trò:** Bạn là giám đốc chương trình chuyển đổi số tỉnh Phú Thọ với 10 năm kinh nghiệm thiết kế, triển khai các hệ thống tài chính công
- **Ngữ cảnh:** Bạn cần viết một đề án **Chuyển đổi số** cho bài toán **Quản trị rủi ro và Bảo mật**.
- **Mục tiêu:** Đề án Chuyển đổi số cần có các Nội dung gồm:
 - 1. Phân tích hiện trạng và Bối cảnh;
 - 2. Mục tiêu của đề án;
 - 3. Kiểm tra Giải pháp công nghệ;
 - ...
- **Đầu ra:** Đề án được viết không quá 9000 từ, có cấu trúc rõ ràng. Sử dụng văn phong khoa học dễ hiểu.



BỘ KHOA HỌC VÀ CÔNG NGHỆ CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số 557 /BKHCN-CĐSQG Hà Nội, ngày 31 tháng 09 năm 2025

V/v hướng dẫn một số nguyên tắc chung đối với công chức, viên chức và người lao động trong cơ quan nhà nước sử dụng các mô hình ngôn ngữ lớn (chatbot AI) phục vụ công việc

Kính gửi:

- Các Bộ, Cơ quan ngang bộ, Cơ quan thuộc Chính phủ;
- UBND các tỉnh, thành phố trực thuộc Trung ương.

Căn cứ Nghị định số 55/2025/NĐ-CP ngày 02/03/2025 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Khoa học và Công nghệ;

Thực hiện chức năng quản lý nhà nước về hoạt động nghiên cứu khoa học, phát triển công nghệ và đổi mới sáng tạo, đáp ứng yêu cầu thực tiễn trong ứng dụng công nghệ Trí tuệ nhân tạo trong các cơ quan nhà nước,

Bộ Khoa học và Công nghệ hướng dẫn một số nguyên tắc chung đối với công chức, viên chức và người lao động trong cơ quan nhà nước sử dụng các mô hình ngôn ngữ lớn (chatbot AI) phục vụ công việc (Phiên bản 1.0).

Bộ Khoa học và Công nghệ đề nghị các Quý Cơ quan tham khảo Tài liệu hướng dẫn, triển khai phù hợp với yêu cầu thực tiễn trong việc sử dụng chatbot AI phục vụ công việc.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc, đề nghị Quý Cơ quan liên hệ với Cục Chuyển đổi số quốc gia, Bộ Khoa học và Công nghệ để được hỗ trợ.

Trân trọng./.

Nơi nhận:

- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Đức Long;
- Lưu: VT, CĐSQG.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG


Phạm Đức Long

Công văn số 557/BKHCN-CĐSQG ngày 31/3/2025 hướng dẫn **một số nguyên tắc chung** đối với công chức, viên chức và người lao động trong cơ quan nhà nước sử dụng các mô hình ngôn ngữ lớn (chatbot AI) phục vụ công việc.

BỘ KHOA HỌC VÀ CÔNG NGHỆ

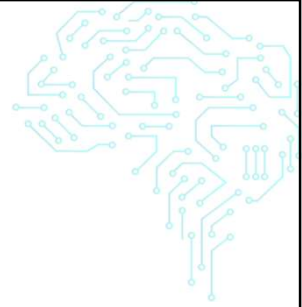
**Nguyên Tắc Sử Dụng Chatbot AI
Trong Cơ Quan Nhà Nước**

Hướng dẫn chuẩn hoá hành vi sử dụng các mô hình ngôn ngữ lớn (LLM) phục vụ công việc hiệu quả và an toàn.

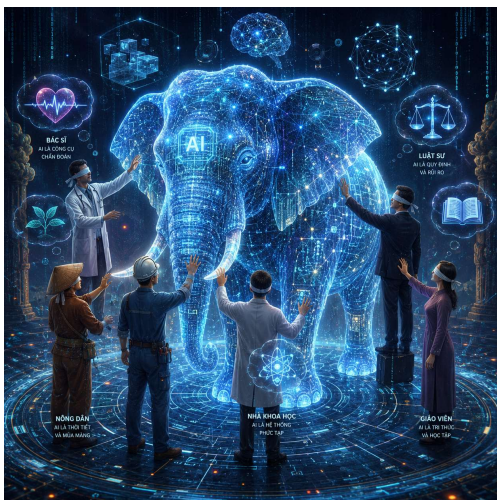
Quyết định: 557/BKHCN-CĐSQG
Ban hành: 31/03/2025
Phiên bản: 1.0

Demo Cách sử dụng AI để đọc tài liệu

- NotebookLM
- Gemini với Email / Tài liệu / Bảng tính ...

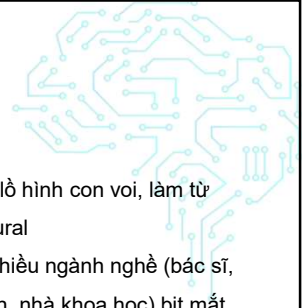


(1) Ví dụ minh họa



Vẽ hình thầy bói xem voi:

- **Chủ thể:** Một thực thể AI khổng lồ hình con voi, làm từ ánh sáng và các đường mạch neural
- **Bối cảnh:** Những người thuộc nhiều ngành nghề (bác sĩ, kỹ sư, luật sư, nông dân, giáo viên, nhà khoa học) bịt mắt, mỗi người chạm vào một phần khác nhau của “con voi AI”
- **Bố cục:** Con voi AI ở trung tâm, những nhân vật đứng vòng tròn xung quanh; phía trên đầu họ xuất hiện các biểu tượng thể hiện cách họ “tưởng tượng AI”
- **Phong cách:** Tranh số concept art, hướng siêu thực (surreal), màu sắc ấn tượng
- **Chi tiết:** Ánh sáng xanh dịu, hiệu ứng dữ liệu, texture hologram, bố cục giàu biểu tượng
- **Cảm xúc:** Suy tư, triết lý, gợi mở



Mẫu prompt hỗ trợ soạn văn bản



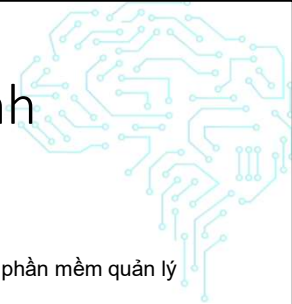
✓ Prompt:

- **Bạn là** chuyên viên hành chính văn phòng. Hãy giúp tôi **soạn một công văn** mời tham dự hội nghị tổng kết năm 2025 dành cho các đơn vị cấp sở. **Định dạng:** Văn bản hành chính theo mẫu chuẩn của Nhà nước.

✓ Kết quả:

- ChatGPT sẽ tạo một công văn có đủ quốc hiệu, tiêu đề, kính gửi, nội dung, thời gian, địa điểm, người ký,...

Mẫu prompt phân tích và ra quyết định



✓ Prompt:

- Tôi là cán bộ quản lý cấp phòng. Hãy giúp tôi phân tích ưu – nhược điểm của việc áp dụng phần mềm quản lý văn bản điện tử trong cơ quan hành chính cấp huyện. Kết quả dạng bảng so sánh.

✓ Kết quả:

- ChatGPT sẽ xuất bảng như:

Phân tích ưu – nhược điểm của việc áp dụng phần mềm quản lý văn bản điện tử trong cơ quan hành chính cấp huyện

Khía cạnh	Ưu điểm	Nhược điểm / Thách thức
Hiệu quả xử lý công việc	Giảm thời gian luân chuyển văn bản giữa các phòng ban; xử lý nhanh hơn so với giấy tờ truyền thống	Nếu quy trình điện tử thiết kế chưa hợp lý có thể phát sinh thao tác rườm rà
Tra cứu và lưu trữ	Tìm kiếm văn bản nhanh theo số, ngày, nội dung, người xử lý	Phụ thuộc vào chất lượng nhập liệu và chuẩn hóa hồ sơ
Giảm chi phí	Giảm chi phí giấy, mực in, chuyển phát, lưu kho hồ sơ	Chi phí đầu tư ban đầu cho phần mềm, máy chủ, chữ ký số
Minh bạch và giám sát	Dễ theo dõi tiến độ xử lý, xác định trách nhiệm cá nhân/phòng ban	Có thể tạo tâm lý "bị giám sát" đối với một số cán bộ
Chỉ đạo điều hành	Lãnh đạo có thể phê duyệt, giao việc từ xa; nắm bắt tình hình theo thời gian	Phụ thuộc vào internet và thiết bị

Mẫu prompt hỗ trợ tổ chức đào tạo



✅ Prompt:

- Tôi là chuyên viên cao cấp với 10 năm kinh nghiệm về chuyển đổi số. Tôi đang xây dựng nội dung buổi tập huấn cho cán bộ xã về chuyển đổi số. Hãy đề xuất cho tôi khung chương trình trong 3 giờ, gồm: nội dung, thời lượng, phương pháp, và ví dụ minh họa thực tế ở Việt Nam. Trình bày dưới dạng bảng.

✅ Kết quả:

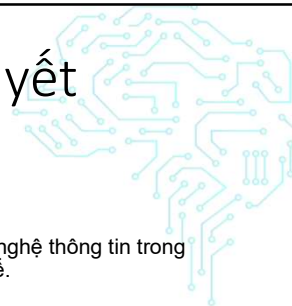
- ChatGPT sẽ tạo bảng chi tiết như sau:

Đề xuất khung chương trình tập huấn 3 giờ

Chủ đề: Chuyển đổi số cho cán bộ cấp xã

STT	Nội dung	Thời lượng	Phương pháp triển khai	Ví dụ minh họa thực tế tại Việt Nam
1	Khai mạc và định hướng	10 phút	Giới thiệu, trao đổi ngắn với học viên	Nêu mục tiêu xây dựng chính quyền số, xã số theo Chương trình Chuyển đổi số quốc gia của Bộ Thông tin và Truyền thông
2	Tổng quan về chuyển đổi số trong cơ quan nhà nước	25 phút	Thuyết trình kết hợp hỏi đáp	Ví dụ về UBND Thành phố Hà Nội triển khai dịch vụ công trực tuyến, hồ sơ điện tử, ký số
3	Vai trò của cán bộ xã trong chuyển đổi số	20 phút	Thảo luận tình huống thực tế	Cán bộ tư pháp xử lý hệ tích điện tử; cán bộ địa chính cấp nhật dữ liệu đất đai; cán bộ một cửa xử lý hồ sơ online
4	Kỹ năng số cơ bản cần có	30 phút	Demo trực tiếp + thực hành nhanh	Sử dụng: - email công vụ - lưu trữ cloud - họp trực tuyến - tra cứu văn bản - bảo mật mật khẩu
5	Sử dụng phần mềm quản lý văn bản và điều hành	25 phút	Minh họa quy trình thực tế	Quy trình tiếp nhận → chuyển xử lý → ký số → lưu trữ văn bản điện tử trên hệ thống điều hành của tỉnh/thị xã/quận

Mẫu Prompt hỗ trợ viết báo cáo / thuyết trình



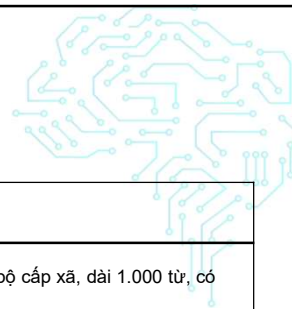
✅ Prompt:

- Bạn là Trưởng phòng Công nghệ. Bạn hãy viết báo cáo tổng kết tình hình ứng dụng công nghệ thông tin trong cơ quan năm 2025. Báo cáo ngắn gọn dưới 2000 từ, có số liệu giả định và kiến nghị cụ thể.

✅ Kết quả:

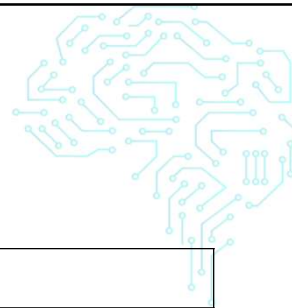
- ChatGPT sẽ tạo một báo cáo tổng kết

Một số mẫu prompt tham khảo



Tình huống	Prompt gợi ý
Viết báo cáo	"Hãy viết báo cáo tổng kết chương trình tập huấn về an toàn thông tin cho cán bộ cấp xã, dài 1.000 từ, có cấu trúc mở bài, nội dung và kết luận."
Tạo slide	"Tạo slide PowerPoint (20 trang) cho chuyên đề 'Ứng dụng AI trong cải cách hành chính', có hình ảnh minh họa và ví dụ thực tiễn Việt Nam."
Tóm tắt chính sách	"Tóm tắt Nghị định số 59/2022/NĐ-CP thành 5 gạch đầu dòng dễ hiểu để phổ biến cho cán bộ xã."
Soạn bài giảng	"Tôi cần một bài giảng 60 phút về chuyển đổi số cấp cơ sở. Hãy giúp tôi soạn nội dung, ví dụ, câu hỏi thảo luận và tài liệu phát tay."
Tạo biểu mẫu	"Tạo biểu mẫu khảo sát mức độ hài lòng của người dân về dịch vụ công trực tuyến, 10 câu hỏi, định dạng Google Form."

Lưu ý khi dùng AI



Nên	Tránh
Đưa vai trò, bối cảnh cụ thể	Câu hỏi quá chung chung
Rà lại nội dung trước khi sử dụng	Sao chép nguyên văn mà không kiểm tra
Yêu cầu tạo tài liệu theo định dạng	Chỉ yêu cầu "giúp tôi với"
Kiểm chứng thông tin pháp lý – chính sách	Dùng ChatGPT như nguồn chính thức

PROMPT HANDBOOK

Báo cáo tổng kết có số liệu thực Thay vì báo cáo chung chung Cơ bản	Tóm tắt văn bản pháp luật cho lãnh đạo Ra quyết định nhanh, không đọc toàn văn Cơ bản
Tóm tắt biên bản họp thành to-do list Sau mỗi cuộc họp, không mất việc Cơ bản	Soạn email từ chối khéo Giữ mối quan hệ tốt khi phải nói không Cơ bản
Sơ sánh 2 lựa chọn để quyết định Mua sắm, chính sách, nhân sự... Nâng cao	Phân tích rủi ro dự án / kế hoạch Trước khi trình lãnh đạo hoặc triển khai Nâng cao
Lập kế hoạch tài chính cá nhân Tối kiệm, chi tiêu, mục tiêu Cơ bản	Soạn CV / tự giới thiệu cho vị trí cụ thể Xin việc, thăng tiến, chuyển ngành Cơ bản
Giải thích vấn đề phức tạp cho người thân Y tế, pháp lý, tài chính, công nghệ Cơ bản	Học một kỹ năng mới trong thời gian ngắn Lộ trình 80/20 cho người bận Nâng cao
Phản biện & cải thiện bài viết của bạn Bài luận, đề án, báo cáo nghiên cứu Nâng cao	Viết bài mạng xã hội thu hút Facebook, Zalo, cho có quan hoặc cá nhân Cơ bản
Soạn kịch bản thuyết trình ngắn (5-10 phút) Hội nghị, báo cáo, pitch ý tưởng Cơ bản	Nhiều vòng lặp cải thiện Khi kết quả AI chưa đạt yêu cầu Power User
Đóng vai chuyên gia phản biện Kiểm tra ý tưởng trước khi cam kết Power User	Tạo template tái sử dụng cho công việc lặp lại Chuẩn hóa quy trình, tiết kiệm thời gian Power User



<https://juhuvn-prompt-handbook.netlify.app/>

An toàn thông tin và bảo vệ dữ
liệu cá nhân trong chuyển đổi số

Nội dung

1

- Cập nhật tình hình an toàn thông tin trong và ngoài nước

2

- Cơ bản về ATTT cho người dùng

3

- Nâng cao nhận thức ATTT cho người dùng
 - An toàn khi sử dụng máy tính cá nhân
 - An toàn khi sử dụng các thiết bị di động
 - An toàn khi sử dụng mạng không dây
 - An toàn khi sử dụng thư điện tử Email
 - An toàn khi sử dụng mạng xã hội
 - An toàn khi duyệt web và thực hiện các giao dịch trực tuyến
 - Phòng tránh các tấn công kiểu lừa đảo (Social Engineering)

Tình hình an toàn thông tin hiện nay

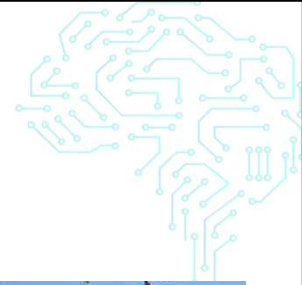
- Con người ngày càng phụ thuộc vào công nghệ thông tin:
 - Không chỉ là Internet với hạ tầng riêng của nó, các hạ tầng quan trọng khác dựa vào Internet trong hoạt động hàng ngày.
 - Sự phụ thuộc và phụ thuộc lẫn nhau ngày càng tăng.

Tình hình an toàn thông tin hiện nay



- Tấn công mạng ngày càng tinh vi và có chủ đích
 - Việt Nam ghi nhận khoảng **552.000 cuộc tấn công mạng trong năm 2025**, trong đó hơn **52% cơ quan và doanh nghiệp bị thiệt hại do tấn công mạng**.
- Dữ liệu trở thành mục tiêu số 1 của tội phạm mạng
 - Riêng quý III/2025 tại Việt Nam ghi nhận: hơn **6,5 triệu** tài khoản cá nhân bị đánh cắp, khoảng **502 triệu bản ghi** dữ liệu bị rò rỉ, gần **4.000** tên miền giả mạo (phishing).
- Ransomware tiếp tục bùng phát mạnh
 - Tại Việt Nam, thiệt hại do ransomware trong nửa đầu năm 2025 ước tính vượt **10 triệu USD**, với hơn **3 terabyte dữ liệu bị mã hóa**. Trên thế giới, số nhóm ransomware hoạt động đã tăng lên hơn **120 nhóm trong năm 2025**.

Tình hình an toàn thông tin hiện nay



- **Con người vẫn là mắt xích yếu nhất:** Mặc dù đầu tư cho an toàn thông tin ngày càng tăng, phần lớn sự cố vẫn bắt nguồn từ:

- click vào email giả mạo,
- lộ mật khẩu,
- tải file độc hại,
- sử dụng AI và cloud không an toàn.

Nghiên cứu gần đây cho thấy phần lớn người dùng vẫn khó phân biệt email lừa đảo do AI tạo ra với email thật.



Chiếc ngựa gỗ thành Troy
(Hy Lạp cổ đại - Thế kỷ 12 TCN)

Tình hình an toàn thông tin hiện nay



- **Email, web và mạng xã hội vẫn là kênh tấn công phổ biến nhất:**

Email phishing tiếp tục là phương thức phát tán mã độc hiệu quả nhất. Các báo cáo năm 2025 cho thấy:

- email vẫn là nguồn phát tán phần lớn mã độc,
- các cuộc tấn công ngày càng sử dụng AI để tạo nội dung lừa đảo tinh vi hơn,
- tấn công qua điện thoại, mạng xã hội và tin nhắn đang gia tăng nhanh chóng.

Tình hình an toàn thông tin hiện nay



- **AI vừa là công cụ hỗ trợ vừa là nguy cơ mới:** Tin tặc đã bắt đầu sử dụng AI để:

- tạo email giả mạo tự nhiên hơn,
- sinh mã độc nhanh hơn,
- tự động dò quét lỗ hổng,
- tạo deepfake để lừa đảo.

Đồng thời, việc cán bộ và nhân viên sử dụng AI không kiểm soát cũng làm tăng nguy cơ rò rỉ dữ liệu nội bộ.

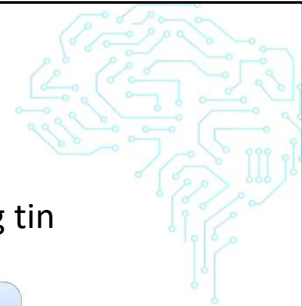
Tình hình an toàn thông tin hiện nay



- **Xu hướng mới: giảm số lượng nhưng tăng mức độ thiệt hại:** Số lượng cuộc tấn công có thể giảm nhẹ nhờ đầu tư bảo mật, nhưng mức độ thiệt hại ngày càng lớn do tin tặc chuyển sang:

- tấn công có chủ đích,
- đánh cắp dữ liệu lâu dài,
- tấn công chuỗi cung ứng,
- gián điệp mạng.

Cơ bản về ATTT cho người dùng



- Mô hình CIA: 3 thuộc tính quan trọng của bảo mật thông tin



Cơ bản về ATTT cho người dùng



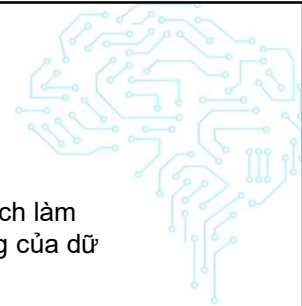
- Một số khái niệm

- An toàn thông tin có nghĩa là phải tổ chức việc xử lý, ghi nhớ và trao đổi thông tin *đảm bảo tính bí mật, toàn vẹn và khả dụng ở mức độ đầy đủ*
- An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin *tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép*
- Đảm bảo an toàn thông tin hiện nay đang là vấn đề quan tâm hàng đầu của xã hội, có ảnh hưởng rất nhiều đến hầu hết các ngành khoa học tự nhiên, kỹ thuật, khoa học xã hội và kinh tế. *Đặc biệt trong kỷ nguyên công nghiệp 4.0.*

Một số thuật ngữ thường gặp

Các loại mã độc:

- **Malware / malicious code / Malicious software (mã độc)**
là một chương trình được chèn bí mật vào hệ thống với mục đích làm ảnh hưởng đến tính bí mật, tính toàn vẹn và/hoặc tính khả dụng của dữ liệu, của ứng dụng hoặc hệ điều hành của nạn nhân.
- **Virus**
là một chương trình máy tính có khả năng tự nhân bản, nhiễm trái phép vào các máy, thiết bị.
- **MacroVirus**
là một loại mã độc sử dụng khả năng lập trình macro của ứng dụng dùng với tài liệu để thực hiện hoặc phát tán.
- **Rootkit**
là một bộ các công cụ dạng phần mềm, có quyền truy cập cấp quản trị được cài đặt vào các hệ thống thông tin và được thiết kế để che dấu sự hiện diện của nó, duy trì quyền truy cập và ẩn các hoạt động mà các công cụ đó thực hiện.



Một số thuật ngữ thường gặp

Các loại mã độc:

- **Ransomware**
là một loại mã độc thực hiện trái phép các tác vụ trên máy nạn nhân và yêu cầu trả tiền chuộc để khôi phục lại như ban đầu. Chủ yếu hiện nay là mã hoá dữ liệu và đòi tiền chuộc.
- **Spyware**
phần mềm được cài bí mật hoặc lén lút vào hệ thống thông tin mà người dùng hoặc chủ của hệ thống không biết
- **Trojan horse**
là một chương trình máy tính có vẻ như hữu dụng, nhưng có chức năng độc hại ẩn giấu bên trong để tránh các cơ chế bảo mật, khai thác các quyền hợp pháp mà nó có từ tính năng công khai.
- **Worm**
một chương trình máy tính tự sao chép, sử dụng cơ chế mạng để tự lan truyền.

101

Một số thuật ngữ thường gặp

- **Cyber attack**
nỗ lực để có quyền *truy cập trái phép* vào các dịch vụ, tài nguyên hoặc thông tin của hệ thống máy tính hoặc nỗ lực để xâm phạm tính toàn vẹn của hệ thống
- **Phishing**
một dạng kỹ thuật xã hội trên mạng để đánh lừa cá nhân cung cấp thông tin nhạy cảm
- **APT – Advanced Persistent Threat**
kiểu tấn công sử dụng *nhiều kiểu tấn công qua mạng*, trực tiếp hoặc các hình thức lừa đảo để xâm nhập mục tiêu mà không phát hiện được, tồn tại trong thời gian dài để trộm thông tin.

102

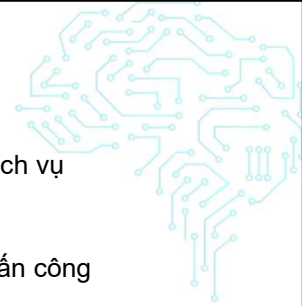
Một số thuật ngữ thường gặp



- **Bot / Zombie**
là một loại mã độc lén cài hoặc bí mật cài vào máy tính kết nối với Internet để *thực hiện các lệnh dưới sự điều khiển và kiểm soát từ xa* của người viết bot
- **Botnet (mạng bot)**
tập hợp các máy tính bị cài mã độc bot và kiểm soát qua mạng.
- **Cyberbullies (bắt nạt mạng)**
là các kẻ dùng công nghệ mới như thư điện tử, tin nhắn tức thời, các trang web, ảnh kỹ thuật số, ... để thực hiện việc quấy rối, bắt nạt người khác trên môi trường mạng
- **Data breach / data leakage (trích dữ liệu trái phép)**
di chuyển trái phép hoặc tiết lộ thông tin nhạy cảm cho đối tượng bên ngoài không được phép xem / biết thông tin.

103

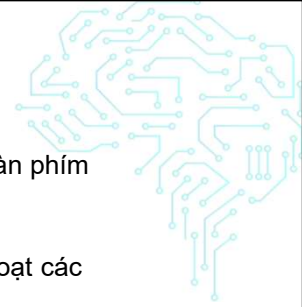
Một số thuật ngữ thường gặp



- **Denial of Service - DoS (từ chối dịch vụ)**
một kiểu tấn công ngăn sử dụng hợp pháp các tài nguyên và dịch vụ theo dạng không đáp ứng được.
- **DDoS (Distributed Denial of Service)**
tấn công từ chối dịch vụ sử dụng nhiều hệ thống để thực hiện tấn công đồng thời.
- **Digital signature (chữ ký số)**
là giá trị được tính từ tiến trình *mã hoá sử dụng khoá riêng* được nối vào dữ liệu, được xem là ký số vào dữ liệu.
- **Electronic signature (chữ ký điện tử)**
bất kỳ dạng điện tử nào được gắn với tài liệu điện tử như là chữ ký.
- **IoT (Internet of Things) Devices**
các thiết bị có sẵn các kết nối với Internet dùng để điều khiển, giám sát, cập nhật thông tin qua mạng Internet.

104

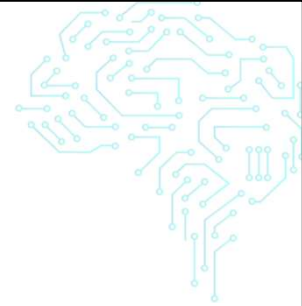
Một số thuật ngữ thường gặp



- **Keylogger**
phần mềm hoặc phần cứng theo dõi bí mật các phím bấm từ bàn phím để giám sát hành động người dùng.
- **Spam**
việc lạm dụng các hệ thống tin nhắn / thư điện tử để gửi hàng loạt các tin nhắn /thư điện tử mà người nhận không mong muốn.
- **Threat (nguy cơ/đe dọa)**
một tình huống hoặc sự kiện chỉ báo khả năng điểm yếu có thể bị khai thác làm ảnh hưởng đến hoạt động của tổ chức, của cá nhân, của xã hội.
- **Vulnerability (điểm yếu / lỗ hổng)**
một điểm yếu chung hoặc cụ thể làm cho tổ chức hoặc các hệ thống thông tin có thể bị khai thác gây ra các nguy cơ / nguy hiểm.

105

Các nguy cơ mất an toàn thông tin



Các kiểu tấn công phổ biến vào người dùng:

- Dùng mã độc: virus, rootkit, botnet, phần mềm chống virus giả mạo, Spyware, ransomware
- Thư điện tử: phishing, spam, thư giả mạo
- Giao dịch trực tuyến
- Dùng kỹ thuật xã hội, wifi công cộng, ...
- Dẫn dụ truy cập các trang web / đường dẫn không an toàn
- Gắn mã độc (thường là trojan) vào các phần mềm hoặc ứng dụng để người dùng tải về và cài đặt
- Xâm nhập máy tính, điện thoại chưa cập nhật các bản vá lỗi hoặc bảo vệ không đủ

Mục đích: trộm thông tin cá nhân, tấn công vào doanh nghiệp.

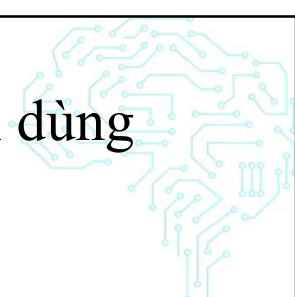
Tại sao cần đảm bảo ATTT cho doanh nghiệp và cá nhân?



- Xu hướng toàn cầu: BYOD – Bring Your Own Device (Dùng thiết bị của riêng bạn) và BYON – Bring Your Own Network (Dùng mạng của riêng bạn).
- Xâm nhập – do thám mạng từ các tổ chức, các chính phủ; tấn công mạng vào các tổ chức, doanh nghiệp và cá nhân
- Phương thức tấn công: sử dụng mạng internet và các kết nối mạng
- Mục tiêu tấn công:
 - **Dữ liệu**
 - **Bí mật kinh doanh** của doanh nghiệp

107

Nâng cao nhận thức ATTT cho người dùng



1. An toàn khi sử dụng máy tính cá nhân
2. An toàn khi sử dụng thiết bị di động
3. An toàn khi dùng mạng không dây
4. An toàn khi sử dụng thư điện tử
5. An toàn khi sử dụng mạng xã hội
6. An toàn khi duyệt web và giao dịch trực tuyến

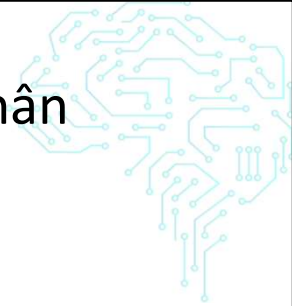
1. An toàn khi sử dụng máy tính cá nhân



• Bản quyền và lợi ích của phần mềm có bản quyền

- 2 loại bản quyền phần mềm: bản quyền thương mại và bản quyền nguồn mở
- Lợi ích sử dụng phần mềm có bản quyền:
 1. Không bị cài cắm các chương trình độc hại => an toàn hơn
 2. Có sự hỗ trợ chính thức của nhà cung cấp: tài liệu, hỗ trợ phát sinh
 3. Được giới thiệu/nâng cấp/sử dụng các tính năng mới (một số)
 4. Được cập nhật các thông tin và các bản vá cho lỗi không ổn định hoặc lỗi bảo mật mới phát hiện
- Để hạn chế vi phạm bản quyền và đảm bảo an toàn:
 1. Không tải, cài đặt các phần mềm, ứng dụng không thực sự cần thiết
 2. Chỉ tải phần mềm từ trang web chính thức của nhà cung cấp
 3. Sử dụng tính năng trial (thử nghiệm) của nhà cung cấp để thử nghiệm và xem nhu cầu thực sự
 4. Không sử dụng các phần mềm bẻ khóa
 5. Không tải và thi hành các trình tạo khóa bản quyền (key generator)

1. An toàn khi sử dụng máy tính cá nhân



• Những điều cần làm khi rời khỏi chỗ làm việc

- khóa màn hình và khi mở lại phải dùng mật khẩu
- laptop cần phải có dây khóa vào bàn hoặc cất vào tủ

• Trước khi kết nối một máy tính mới vào Internet

- Chỉ kết nối vào các mạng an toàn
- Cấu hình và bật firewall (tường lửa của hệ điều hành)
- Cài đặt phần mềm chống virus, chống mã độc và cập nhật dữ liệu mới

1. An toàn khi sử dụng máy tính cá nhân



• An toàn máy tính:

- Cập nhật các phiên bản mới nhất - đặt chế độ tự động cập nhật
- Bảo vệ các thông tin cá nhân: không cho mượn máy, không cung cấp thông tin qua trang web, email, tin nhắn, ...
- Bảo vệ mật khẩu: tạo mật khẩu mạnh và giữ chúng an toàn
 - Độ dài tối thiểu 10 ký tự gồm ký tự, số, ký tự đặc biệt, chữ hoa
 - Không dùng tên, từ, ngày tháng có nghĩa
 - Không dùng chung mật khẩu cho nhiều tài khoản
 - Không chia sẻ mật khẩu qua điện thoại, email, tin nhắn
 - Nếu phải viết mật khẩu để ghi nhớ, phải khoá riêng chúng
- Thiết lập xác thực 2 thành phần cho các tài khoản
- Gỡ bỏ các phần mềm không cần thiết: càng ít phần mềm càng ít nguy cơ
- Chỉ cung cấp thông tin cá nhân qua các trang web có mã hoá
- Sao lưu các tập tin

1. An toàn khi sử dụng máy tính cá nhân



Đảm bảo an toàn khi sử dụng máy tính cá nhân nơi công cộng:

- Chỉ kết nối vào các mạng an toàn (https)
- Cấu hình và bật firewall (tường lửa của hệ điều hành)
- Cài đặt phần mềm chống virus, chống mã độc và cập nhật dữ liệu mới
- Không rời khỏi máy và nếu tạm thời không sử dụng, chuyển sang chế độ khóa màn hình
- Hạn chế sử dụng các thông tin riêng tư hoặc thông tin của doanh nghiệp nơi công cộng
- Không lưu tài khoản & mật khẩu những lần truy cập

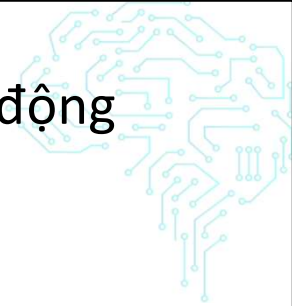
1. An toàn khi sử dụng máy tính cá nhân



Sao lưu và phục hồi dữ liệu:

- Sử dụng Backup (sao lưu) và Recovery (khôi phục) của Windows 10
- Sử dụng Backup and Restore của các bản Windows trước
- **Nên có 1 ổ đĩa di động** để sao lưu các tập tin quan trọng: phòng ngừa sự cố đĩa cứng, máy tính hoặc bị mã hóa
- Sử dụng Google Drive, OneDrive, ...
- Sử dụng các công cụ tích hợp sẵn trên các ổ đĩa di động
- Sử dụng công cụ miễn phí để sao lưu dữ liệu:
<https://allwaysync.com/>

2. An toàn khi sử dụng các thiết bị di động



- Các nguy cơ khi sử dụng các thiết bị di động
- Đảm bảo an toàn khi sử dụng các thiết bị di động
- Xử lý điện thoại không còn sử dụng

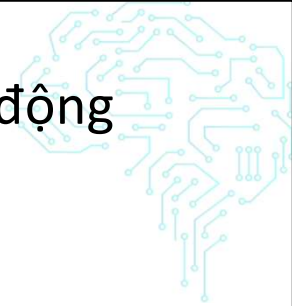
2. An toàn khi sử dụng các thiết bị di động



Các nguy cơ khi sử dụng các thiết bị di động

- Rò rỉ dữ liệu Phần mềm miễn phí thường chèn quảng cáo ...
- Wi-Fi không an toàn wifi công cộng tiềm ẩn nhiều rủi ro.
- Giả mạo mạng hacker có thể tạo các mạng "Free Airport Wifi"
- Tấn công Phishing email hiển thị trên điện thoại thường tối giản
- Phần mềm gián điệp (spyware) "bạn thân/đồng nghiệp/... cài đặt lên"
- Mật mã yếu hoặc dùng không đúng cách
- Xử lý phiên không đúng cách

2. An toàn khi sử dụng các thiết bị di động



Đảm bảo an toàn khi sử dụng các thiết bị di động:

- Giữ điện thoại trong tầm tay, khi không cần dùng nên để trong túi
- Thiết lập mật khẩu sử dụng
- Giữ cho các ứng dụng trong điện thoại luôn cập nhật mới
- Cài đặt ứng dụng chống virus và phát hiện spyware
- Cẩn trọng khi dùng các Wi-Fi công cộng:
 - Đảm bảo mạng là hợp pháp
 - Không thực hiện các hoạt động mua sắm, thanh toán, ...
 - Chỉ sử dụng các trang web https khi phải mua sắm trực tuyến hoặc thanh toán ngân hàng. Nên dùng kết nối 3G/4G của riêng cá nhân
- Sao lưu dữ liệu vào máy tính

2. An toàn khi sử dụng các thiết bị di động



Đảm bảo an toàn khi sử dụng các thiết bị di động:

- Không bấm vào các liên kết trong email hoặc tin nhắn
- Chỉ tải các ứng dụng / phần mềm từ nhà cung cấp chính thức: Apple App Store, Google Play Store
- Xem xét các thiết lập kết nối như bluetooth và khoá khi không dùng
- Khi mua sắm trực tuyến, cẩn thận với các đề nghị “quá tốt” hoặc các đường link kèm theo, hạn chế trả lời các email của người bán (để tránh bị spam hoặc phishing)

2. An toàn khi sử dụng các thiết bị di động



Xử lý điện thoại không còn sử dụng

1. Dùng Factory reset hoặc Hard reset (trả lại thiết lập của nhà sản xuất)
2. Gỡ bỏ SIM, thẻ nhớ
3. Sau khi reset, hãy kiểm tra xem có còn Danh bạ, nhật ký cuộc gọi, tin nhắn, hình ảnh cá nhân, lịch sử tìm kiếm,

2. An toàn khi sử dụng các thiết bị di động

• Hạn chế sử dụng các ổ đĩa di động USB

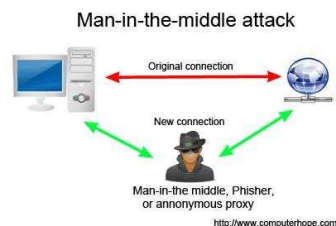
- USB drive là nguồn lây nhiễm lớn nhất virus/ransomware, ..
- Nếu bắt buộc phải dùng thì cần phải quét vi rút
- Tắt tính năng auto-run khi cắm USB
 - (chạy `gpedit.msc`, chọn **Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies > Turn off Autoplay = Enableb trên All drives**)

3. An toàn khi sử dụng mạng không dây (Wifi)

Các rủi ro khi sử dụng mạng không dây:

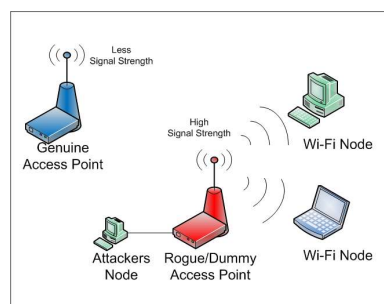
1. Man-in-the-Middle – tấn công trung gian

Tin tặc chặn các gói dữ liệu giữa 2 nạn nhân và truyền qua chúng.



2. Các mạng Wi-Fi giả mạo

Giả các mạng miễn phí, mạng không mật khẩu để người dùng truy cập



3. An toàn khi sử dụng mạng không dây (Wifi)



Lời khuyên khi sử dụng mạng không dây:

- Mạng WiFi công cộng có sử dụng mã hoá WPA2 là an toàn hơn, tránh xa các mạng không mã hoá (không yêu cầu password đăng nhập)
- Hạn chế cung cấp thông tin cá nhân, kể cả các trang web có mã hoá https
- Hãy thoát kết nối khi không dùng, không đặt chế độ lưu và tự động kết nối
- Không dùng chung mật khẩu cho các các trang web
- Lưu ý các cảnh báo trên trình duyệt cho người dùng như trang web gian lận hoặc mã độc
- Một số ứng dụng di động hoặc phần mềm không mã hoá dữ liệu truyền nhận → không sử dụng ứng dụng khi dùng WiFi công cộng. Khi cần thiết, dùng kết nối dữ liệu 3G/4G của điện thoại cá nhân
- Sử dụng VPN để mã hoá các thông tin gửi nhận, kể cả từ các ứng dụng
- Tắt chế độ chia sẻ trong Control Panel hoặc chọn chế độ "Public"

4. An toàn khi sử dụng email



Phòng tránh phishing:

- Thư giả lừa đảo (Phishing scam) là các thông điệp nhằm **lừa người nhận cung cấp thông tin nhạy cảm**, thường giả mạo từ ngân hàng hoặc nhà cung cấp, yêu cầu nhập lại mật khẩu, xác minh thông tin,

Yêu cầu xác thực: Vui lòng xác nhận tài khoản của bạn

DV Dịch vụ khách hàng <bounces+40...> Wednesday, May 20, 2026 at 7:00 AM

To: O cuongnguyen@ibt.ac.vn

DỊCH VỤ BẢO MẬT

YÊU CẦU XÁC THỰC KHẨN CẤP

Xác nhận tài khoản BIDV của bạn

Nhập vào nút bên dưới để xác thực tài khoản và tiếp tục sử dụng dịch vụ ngân hàng trực tuyến.

Kính gửi Quý khách hàng,

Ngân hàng TMCP Đầu tư và Phát triển Việt Nam (BIDV) đã nâng cấp hệ thống bảo mật theo tiêu chuẩn **Smart OTP** và tuân thủ Nghị định 35/2026/NĐ-CP về bảo vệ dữ liệu cá nhân và an toàn giao dịch trực tuyến.

Hệ thống phát hiện hoạt động đăng nhập bất thường từ thiết bị lạ. Để đảm bảo an toàn cho tài khoản của Quý khách, vui lòng **xác nhận quyền truy cập** ngay để tránh tài khoản bị tạm khóa tạm thời.

XÁC THỰC TÀI KHOẢN NGAY

Hướng dẫn xác thực:

- Nhập vào nút **Xác thực tài khoản ngay** ở trên
- Đăng nhập bằng thông tin tài khoản BIDV của bạn
- Nhập mã OTP được gửi qua SMS hoặc ứng dụng **Smart OTP**
- Hoàn tất xác thực để bảo vệ tài khoản

Kết nối an toàn: Giao dịch được mã hóa theo chuẩn TLS 1.3. Thông tin tài khoản của Quý khách được bảo mật tuyệt đối.

Trân trọng cảm ơn Quý khách đã tin tưởng và đồng hành cùng BIDV.

Trân trọng,
Phòng An ninh & Bảo mật Thông tin BIDV

THÔNG BÁO KHẨN CẤP – CẦN HÀNH ĐỘNG NGAY

A Admin-ibt.ac.vn <aivanova@mail.kiap.ru> Yesterday at 4:07 PM

To: O cuongnguyen@ibt.ac.vn

ibt.ac.vn

Bắt đầu từ hôm nay, 5/26/2026 4:38:25 a.m., trang đăng nhập Zimbra Web Client sẽ được cấp nhật như một phần của quá trình nâng cấp hệ thống bảo mật và email quan trọng.

Để tránh bị vô hiệu hóa ngay lập tức và ngăn ngừa mất quyền truy cập vào tài khoản email của bạn, bạn phải xác minh và kích hoạt tài khoản của mình càng sớm càng tốt.

NHẬP VÀO ĐÂY ĐỂ ĐĂNG NHẬP VÀ KÍCH HOẠT

Việc không hoàn tất xác minh này có thể dẫn đến việc tạm ngưng hoặc đình chỉ vĩnh viễn dịch vụ email của bạn.

Cảm ơn bạn đã nhanh chóng giải quyết vấn đề này và đã lựa chọn Zimbra Web Client.

ibt.ac.vn © 2026 Dịch vụ thư tin - Một email đã được gửi đến địa chỉ sau: cuongnguyen@ibt.ac.vn

Zimbra Administration
Security Services Team

Focused Other All v

Saturday, December 15, 2018

KeyBank Relationship Rewards
Nhìn, your November statement is 5,717 points are waiting – redeem th Sat 12/15

Apple
Re: [New-Receipt Purchase] Thanks Sat 12/15

Thursday, December 13, 2018

KeyBank
This is your final chance at \$5,000! Thu 12/13
There's still time to use an eligible K.

Wednesday, December 12, 2018

KeyBank
Enjoy faster online checkouts Wed 12/12
For faster online checkouts, register

Thursday, December 6, 2018

KeyBank
Get twice as many chances at \$5,000! 12/6/2018
Use an eligible KeyBank Mastercard

Re: [New-Receipt Purchase] Thanks for your orders [Your invoice from Apple on Friday, December 14, 2018] (FWD).

Apple <no-toreply.zzeizelresolutions-cares20@xiakoska-cemewes.com> 12/15/2018 4:30 AM

To: support@... Recent-Purchase-Mail-iPhone XS Silicone Case - (PRODUCTRED-033).pdf
Recent-Purchase-Mail-iPhone X... 27.03 KB

Apple

Dear Customer

Your Apple ID, has just been used to purchase iPhone XS Silicone Case - (PRODUCTRED) Bucks \$39.00 on a computer or a device that not previously been used to make purchases.

You may also be receiving this email if you have reset your password since your last purchase.

If you did not make this purchase, or believe someone may have accessed your account, please find the attached file.

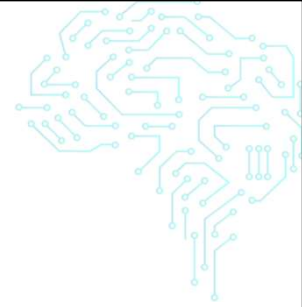
Sincerely,
Apple Support

4. An toàn khi sử dụng email

Gửi và nhận thư điện tử Email an toàn:

- Đặt mật khẩu mạnh, thay đổi thường xuyên và lưu giữ an toàn, không chia sẻ cho người khác
- Không mở các tập tin đính kèm hoặc các liên kết trong mail từ những người không quen
- Khi dùng webmail, đăng thoát (log out) khi sử dụng xong
- Không trả lời thư rác, cẩn thận khi đặt chế độ tự động trả lời
- Không chia sẻ thông tin cá nhân qua email
- Cẩn thận với các email giả mạo ngân hàng hoặc mạng xã hội yêu cầu thay đổi thông tin
- Nên có nhiều email cho các mục đích khác nhau: công việc, mua hàng/giao dịch trực tuyến, lướt web, ...

4. An toàn khi sử dụng email



Đối phó với thư điện tử Email giả mạo, phishing:

- Đừng tin vào tên người gửi được hiển thị
- Chỉ xem chứ đừng bấm – di chuột trên đường link để xem địa chỉ thực
- Kiểm tra lỗi chính tả, cách sử dụng ngôn ngữ
- Xem lời chào có đúng tên của bạn không?
- Cẩn thận với những email yêu cầu thực hiện khẩn cấp
- Xem chữ ký bên dưới
- Đừng bấm vào tập tin đính kèm
- Đừng tin vào tiêu đề (header)
- Đừng tin vào những nội dung bạn đã xem
- Để kiểm tra email header, chép header vào các trang như <http://mxtoolbox.com/EmailHeaders.aspx> hoặc <https://www.whatismyip.com/email-header-analyzer/>

5. An toàn khi sử dụng mạng xã hội



Các rủi ro khi sử dụng mạng xã hội:

- Mạng xã hội là mạng kết nối, khuyến khích mọi người cung cấp nhiều thông tin và kết nối với nhau. **Lợi ích kết nối – thông tin của mạng xã hội là rất lớn.**
- Một số nguy cơ, rủi ro trên mạng xã hội:
 - + Ai cũng có thể tham gia và tạo tài khoản trên các mạng xã hội
 - + Không biết đang giao tiếp với người dùng thật / giả mạo
 - + Thông tin trên mạng do người dùng tự đưa lên, không qua kiểm chứng
 - + Các kẻ tấn công mạng dễ dàng khai thác thông tin và có thể tấn công đồng thời nhiều nạn nhân
 - + Thông tin cá nhân và các quan hệ cá nhân có thể bị phổ biến, khai thác không kiểm soát được, cả thông tin đúng và thông tin không đúng
 - + Các phát biểu cá nhân có thể không phù hợp với cộng đồng

5. An toàn khi sử dụng mạng xã hội



Điển hình: Khai thác dữ liệu người dùng trên Facebook

- Công ty **Cambridge Analytica** đã mua dữ liệu từ Aleksandr Kogan, giảng viên Đại học Cambridge
- Kogan thu thập thông tin dựa trên ứng dụng **thisisyourdigitallife**. Ứng dụng này đòi hỏi người dùng đăng nhập tài khoản Facebook cũng như yêu cầu quyền truy cập hồ sơ, vị trí của họ;
- Dữ liệu này đã từng được một công ty thứ ba sử dụng để tạo nội dung quảng cáo ủng hộ Donald Trump trong cuộc bầu cử Tổng thống Mỹ năm 2016
- Sau khi sự việc được công bố, giá cổ phiếu Facebook cũng lao dốc 7% trong phiên giao dịch ngày 19/3/2018, khiến Zuckerberg mất 5 tỷ USD.

5. An toàn khi sử dụng mạng xã hội



Hạn chế rủi ro và an toàn hơn khi sử dụng mạng xã hội:

- Không nên cung cấp thông tin chi tiết về cá nhân, gia đình
- Giới hạn lượng thông tin mà bạn đăng, hạn chế các thông tin như địa chỉ, đường đi, lịch trình, ... Không cập nhật hoạt động hàng giờ, hàng phút lên mạng
- Lưu ý rằng Internet là nguồn thông tin công cộng, khi đã gửi thì không thể rút lại
- Cẩn thận với người lạ, liên lạc với những người trong danh bạ, không kết bạn với người không quen biết
- Luôn đặt câu hỏi và hoài nghi với mọi thông tin, không trả lời các câu hỏi thăm dò
- Xem xét và kiểm tra các thiết lập riêng tư của cá nhân
- Cảnh giác với các ứng dụng của các bên thứ ba
- Sử dụng mật khẩu mạnh và thường xuyên thay đổi mật khẩu
- Cập nhật các phần mềm, trình duyệt web, trình chống virus mới nhất.

5. An toàn khi sử dụng mạng xã hội



Hạn chế rủi ro và an toàn hơn khi sử dụng mạng xã hội:

- Xác minh lại nếu nhận được tập tin từ bạn bè trên MXH gửi, phòng tránh mã độc và các chương trình độc hại
- Không nên hoặc cẩn trọng khi bấm vào các đường link liên kết trong các bài viết trên MXH
- Cần nhớ số điện thoại, email đăng ký MXH để khôi phục lại tài khoản, mật khẩu khi cần
- Cẩn nhắc trước khi đăng hình ảnh.

6. An toàn duyệt web & giao dịch trực tuyến



Các nguy cơ mất ATTT khi truy cập web và thực hiện các giao dịch trực tuyến:

Khả năng truy cập vào các trang web có ý đồ xấu: đánh cắp thông tin, phán tán mã độc / mã độc mã hóa tổng tiền hoặc các trang web giả mạo là rất cao.

- **Các nguy cơ khi truy cập web:**
 - + Máy không cài đặt các công cụ bảo vệ
 - + Hệ điều hành và các ứng dụng không được cập nhật
- **3 cách phổ biến mà các kẻ tấn công có thể lợi dụng:**
 - + Tạo trang web và email lừa đảo cho các cửa hàng giả mạo, các tổ chức từ thiện – quyên góp sau thiên tai, ...
 - + Khai thác các giao dịch không an toàn, ví dụ không mã hoá để chặn lấy thông tin
 - + Nhắm đến các điểm yếu/lỗ hổng trên máy tính của cá nhân, các hệ thống của doanh nghiệp để khai thác thông tin, cơ sở dữ liệu, ...

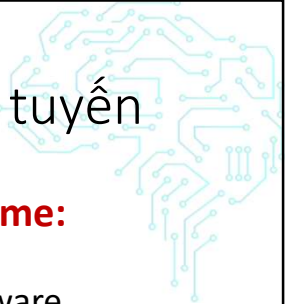
6. An toàn duyệt web & giao dịch trực tuyến



Các nguy cơ mất ATTT khi truy cập web và thực hiện các giao dịch trực tuyến:

- Các nguy cơ độc hại trực tuyến:
 - + Trang web độc hại
 - + Có các kịch bản (script) độc hại
 - + Có các script để tải các chương trình độc hại, và thi hành để trộm dữ liệu từ các giao dịch ngân hàng trực tuyến và các tài khoản mạng xã hội, hoặc thông tin đăng nhập
 - + Tải các trojan về máy
 - + Bị khai thác các lỗ hổng mà các phần mềm bảo vệ không phát hiện được
 - + Các phần mềm quảng cáo: thường đi kèm với phần mềm miễn phí hoặc phần mềm chia sẻ (shareware).

6. An toàn duyệt web & giao dịch trực tuyến



Thiết lập chế độ an toàn trên trình duyệt web Chrome:

- Google Chrome: thiết lập trong Advanced Settings
 - + Cho phép bảo vệ phishing và mã độc (phishing and malware protection): trong phần Privacy
 - + Tắt tìm kiếm tức thời (instant search) để tránh gửi những gì bạn gõ được chuyển đến cho Google
 - + Không đồng bộ (sync) để tránh đồng bộ tài khoản email với Chrome, ngăn các thông tin cá nhân như mật khẩu, dữ liệu tự điển, các tham khảo ... được lưu trên các máy chủ của Google. Nếu cần thực hiện đồng bộ, cần chọn "Encrypted all synced data" và tạo một khóa cho việc mã hóa.

6. An toàn duyệt web & giao dịch trực tuyến

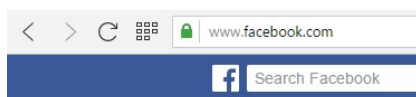
Thiết lập chế độ an toàn trên trình duyệt web Chrome:

- Google Chrome: thiết lập trong Advanced Settings
 - + Thiết lập cấu hình các nội dung: chọn “content settings” trong “Privacy” và thực hiện:
 - Cookies: chọn *“Keep local data only until I quit my browser”* và *“Block third-party cookies and site data”* để đảm bảo cookie sẽ bị xóa khi thoát Chrome và các bên quảng cáo không thể theo dõi bạn bằng cách dùng các cookie của các bên thứ ba
 - JavaScript: chọn *“Do not allow any site to run JavaScript”*
 - Pop-ups: chọn *“Do not allow any site to show pop-ups”*
 - Location: chọn *“Do not allow any site to track my physical location”*
 - + Thiết lập cấu hình mật khẩu và các khuôn dạng: *tắt tự động điền (autofill) và tắt “Offer to save passwords I enter on the web” trong phần “Passwords and forms”*. Việc này giúp ngăn Chrome lưu thông tin đăng nhập, mật khẩu và các thông tin nhạy cảm khác.

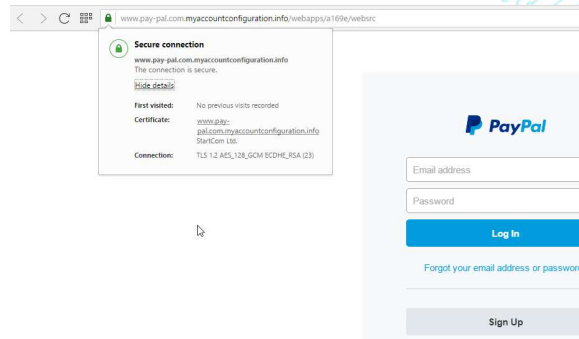
6. An toàn duyệt web & giao dịch trực tuyến

Nhận biết trang web an toàn:

- Luôn kiểm tra URL cẩn thận để không bị chuyển hướng hoặc truy cập vào các trang giả mạo, nhất là các liên kết trong email hoặc khi bấm vào các liên kết trong các quảng cáo. Đây là cách phát hiện một trang giả hay còn gọi là phishing website, giả mạo gần giống các trang web nổi tiếng để thu thập thông tin đăng nhập của bạn. Nhiều trường hợp giả mạo có thể biết được ngay như trong ví dụ ở trang sau nhưng nhiều trường hợp khó nhận biết nếu kẻ giả mạo đăng ký tên miền gần giống, ví dụ www.face-book.com



6. An toàn duyệt web & giao dịch trực tuyến



Trang web giả mạo có chứng chỉ

6. An toàn duyệt web & giao dịch trực tuyến

Những điều cần nhớ khi duyệt web và giao dịch trực tuyến:

1. Luôn sử dụng phần mềm diệt virus có khả năng phát hiện phishing, spyware để đánh cắp thông tin nhạy cảm của bạn
2. Tránh dùng các mạng Wi-Fi công cộng
3. Nếu phải dùng Wi-Fi công cộng, hãy thiết lập một kênh VPN riêng giữa máy tính và Internet để ngăn hacker trộm thông tin
4. Đảm bảo rằng máy tính hoặc điện thoại đã được cập nhật mới nhất cho hệ điều hành
5. Thay đổi mật khẩu thường xuyên và đảm bảo dùng mật khẩu mạnh
6. Đăng ký và sử dụng dịch vụ thông báo giao dịch của tài khoản trên điện thoại
7. Tránh đăng nhập tài khoản ngân hàng trực tuyến qua email
8. Không dùng máy tính công cộng để đăng nhập ngân hàng trực tuyến.

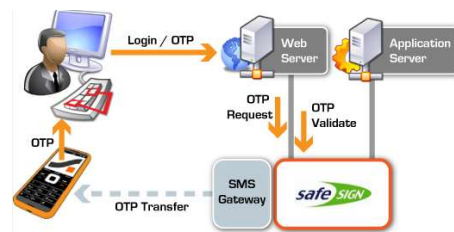
6. An toàn duyệt web & giao dịch trực tuyến

Bổ sung an toàn cho thanh toán trực tuyến:

1. Kiểm tra kỹ người bán là ai, ghi lại thông tin như địa chỉ thực tế, số điện thoại, địa chỉ email, người liên lạc
2. Kiểm tra xem trang web có hợp pháp không: *kiểm tra tên miền, kiểm tra ổ khóa màu xanh lá*



3. Nếu sử dụng USB Token để thanh toán: giữ gìn tránh bị mất, không lộ mã, đảm bảo an toàn trước khi nhập mã



6. An toàn duyệt web & giao dịch trực tuyến

Khái niệm cơ bản về Social Engineering:

- Trong kiểu tấn công social engineering (kỹ thuật xã hội), kẻ tấn công dùng các **kỹ năng xã hội tương tác với đối tượng để có hoặc xâm nhập thông tin** về tổ chức hoặc các hệ thống máy tính của tổ chức.
- Kẻ tấn công thường khiêm tốn, có vẻ đáng kính, tự xưng là một nhân viên mới, người sửa chữa hoặc nhà nghiên cứu, có thể cung cấp thông tin để xác thực. Bằng cách đặt các câu hỏi, người đó có thể thu thập đủ các thông tin cần thiết để xâm nhập mạng của tổ chức. Nếu thu thập không đủ thông tin từ 1 nguồn, họ có thể liên hệ với một nguồn khác trong tổ chức và cung cấp thông tin từ nguồn đầu tiên để tăng sự tin nhiệm.
- **Phishing** là một dạng của Social engineering, sử dụng email hoặc các trang web độc hại để lấy thông tin cá nhân qua việc đóng giả là tổ chức đáng tin cậy.
- Các tấn công lừa đảo phishing cũng thường giả dạng các tổ chức từ thiện, dựa vào các sự kiện trong năm như **thiên tai, bầu cử, ngày lễ**, ...

6. An toàn duyệt web & giao dịch trực tuyến

Những hình thức tấn công Social Engineering phổ biến:

5 loại tấn công phổ biến nhất:

1. **Lừa đảo – Phishing** tạo cảm giác sợ hãi, khẩn cấp để lừa
2. **Mồi – Baiting** Đưa ra lợi ích, giải thưởng, quà để lừa
3. **Vật bồi thường - Quid Pro Quo** đề nghị trao đổi có lợi
4. **Đội lốt người khác – Pretexting** Giả danh công an, sếp, người thân, bạn bè ...
5. **Cống – PiggyBacking** Đi nhờ thẻ thang máy, văn phòng,

Nâng cao nhận thức ATTT cho người dùng

1. An toàn khi sử dụng máy tính cá nhân
2. An toàn khi sử dụng thiết bị di động
3. An toàn khi dùng mạng không dây
4. An toàn khi sử dụng thư điện tử
5. An toàn khi sử dụng mạng xã hội
6. An toàn khi duyệt web và giao dịch trực tuyến



