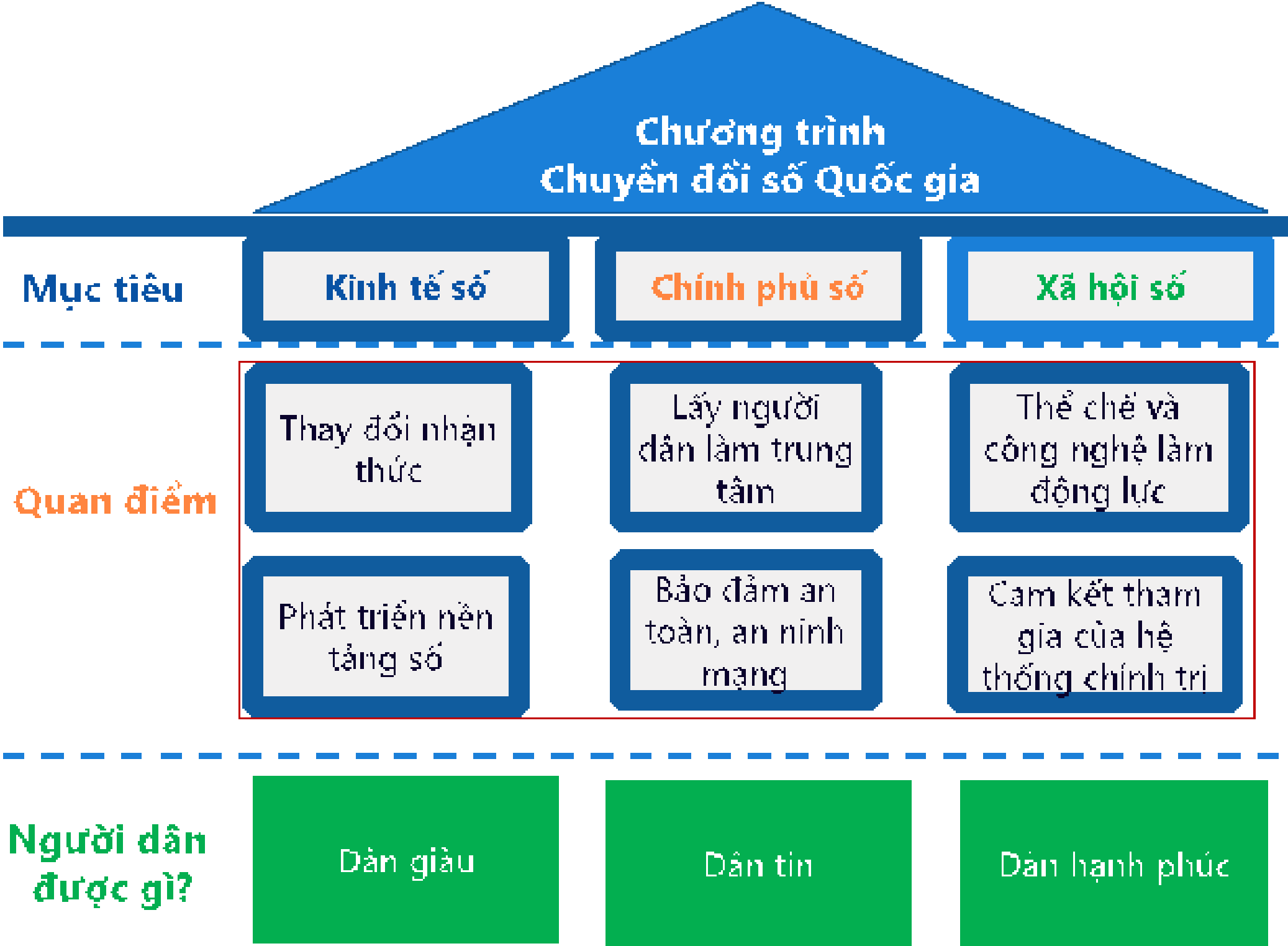


CHUYỂN ĐỔI SỐ VÀ KỸ NĂNG AN TOÀN TRÊN MÔI TRƯỜNG SỐ

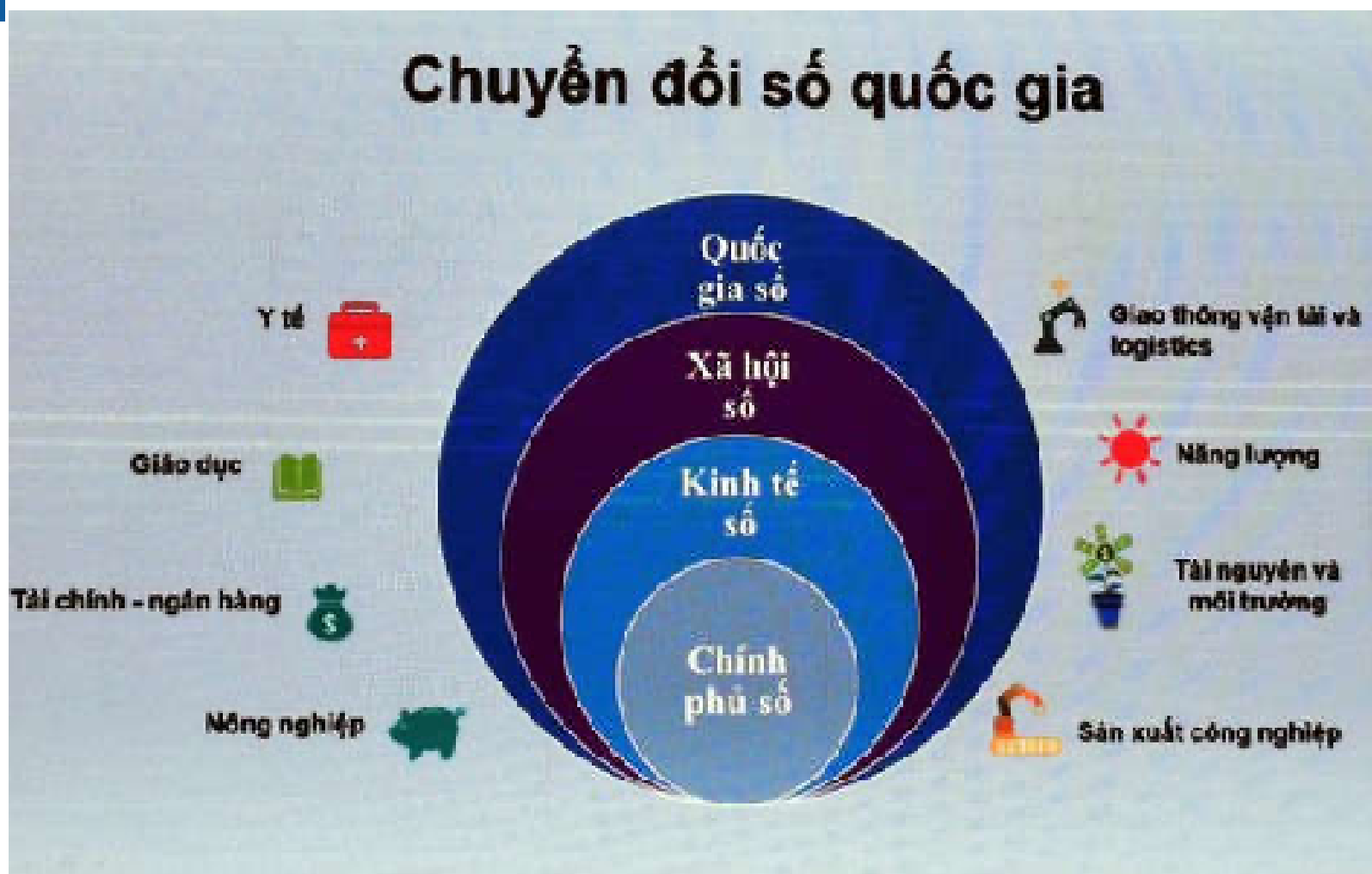


● ● ● **CHƯƠNG TRÌNH CHUYỂN ĐỔI SỐ QUỐC GIA-THEO QĐ 749/QĐ-TTg NGÀY 03/06/2020 CỦA THỦ TƯỚNG CHÍNH PHỦ**

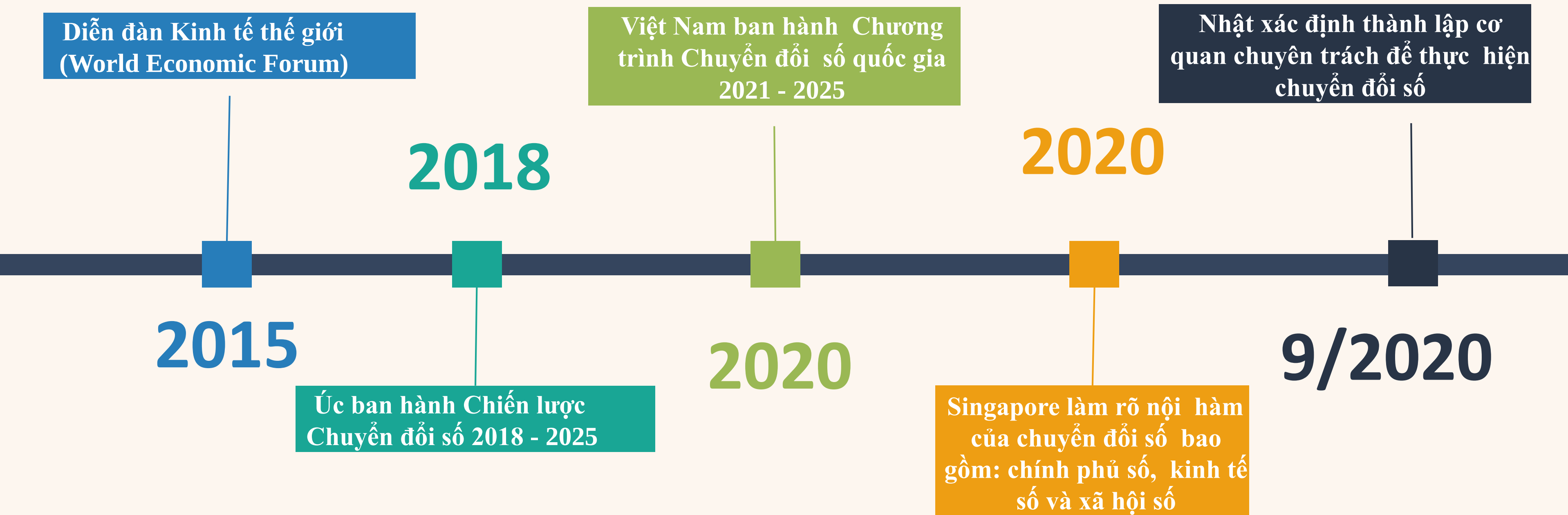
Tầm nhìn 2030: *Việt Nam trở thành quốc gia số, ổn định và thịnh vượng, tiên phong và thử nghiệm các mô hình mới; đổi mới căn bản, toàn diện hoạt động quản lý, điều hành của Chính phủ, hoạt động sản xuất kinh doanh của doanh nghiệp, phương thức sống, làm việc của người dân, phát triển môi trường số an toàn, nhân văn, rộng khắp.*



8 Lĩnh vực cần ưu tiên



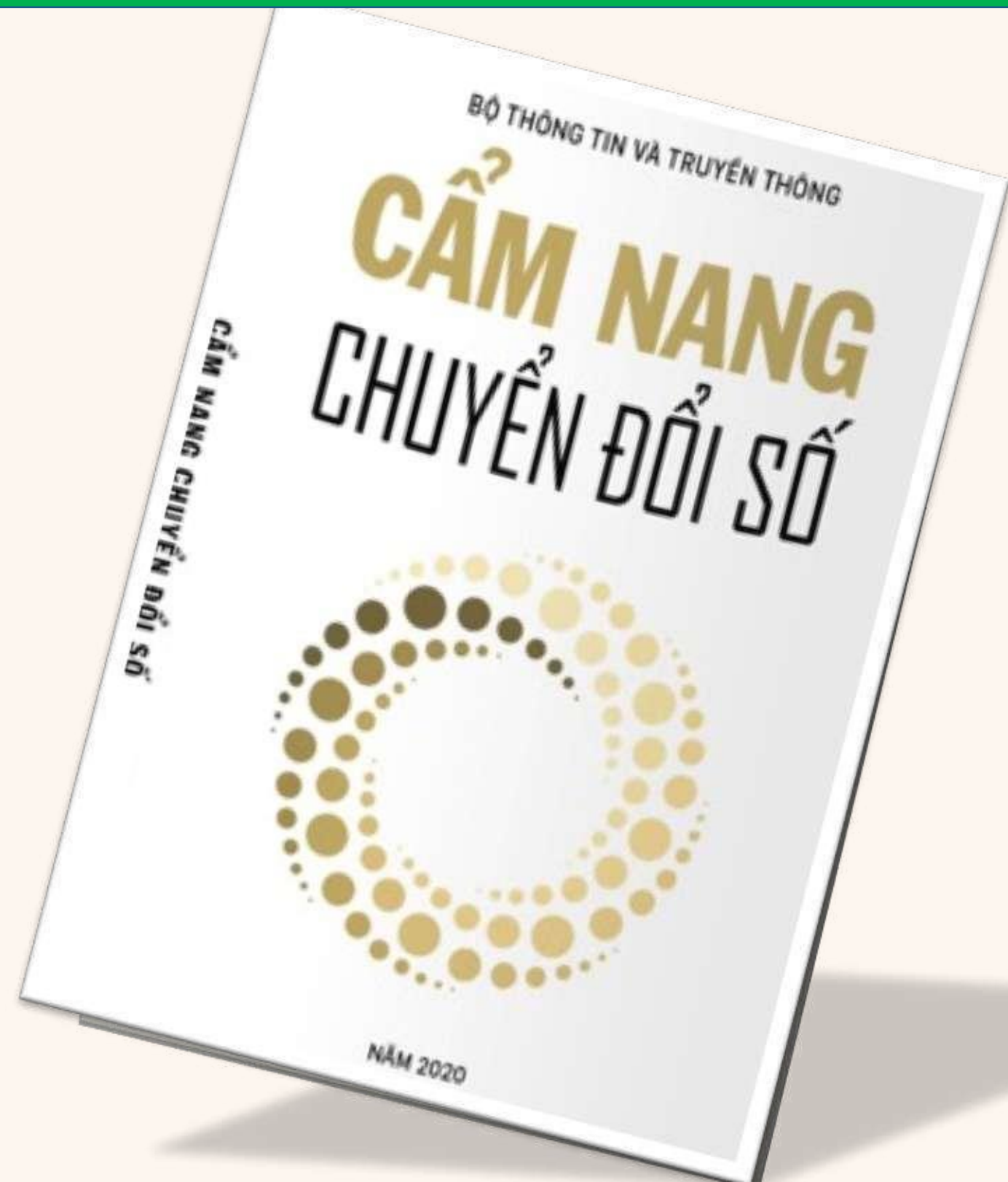
VIỆT NAM BẮT KỊP CÁC QUỐC GIA PHÁT TRIỂN VỀ TẦM NHÌN CÔNG NGHỆ



CẨM NANG CHUYỂN ĐỔI SỐ

“Cẩm nang chuyển đổi số” do Bộ Thông tin và Truyền thông ban hành trong tháng 9/2020

- Cẩm nang cơ bản
- Cẩm nang cho người dân
- Cẩm nang cho doanh nghiệp
- Cẩm nang cho cơ quan nhà nước



CHUYỂN ĐỔI SỐ LÀ GÌ?

Chuyển đổi số là việc sử dụng dữ liệu và công nghệ số để thay đổi **tổng thể** và **toàn diện** cách sống, cách làm việc và phương thức sản xuất của cá nhân, tổ chức



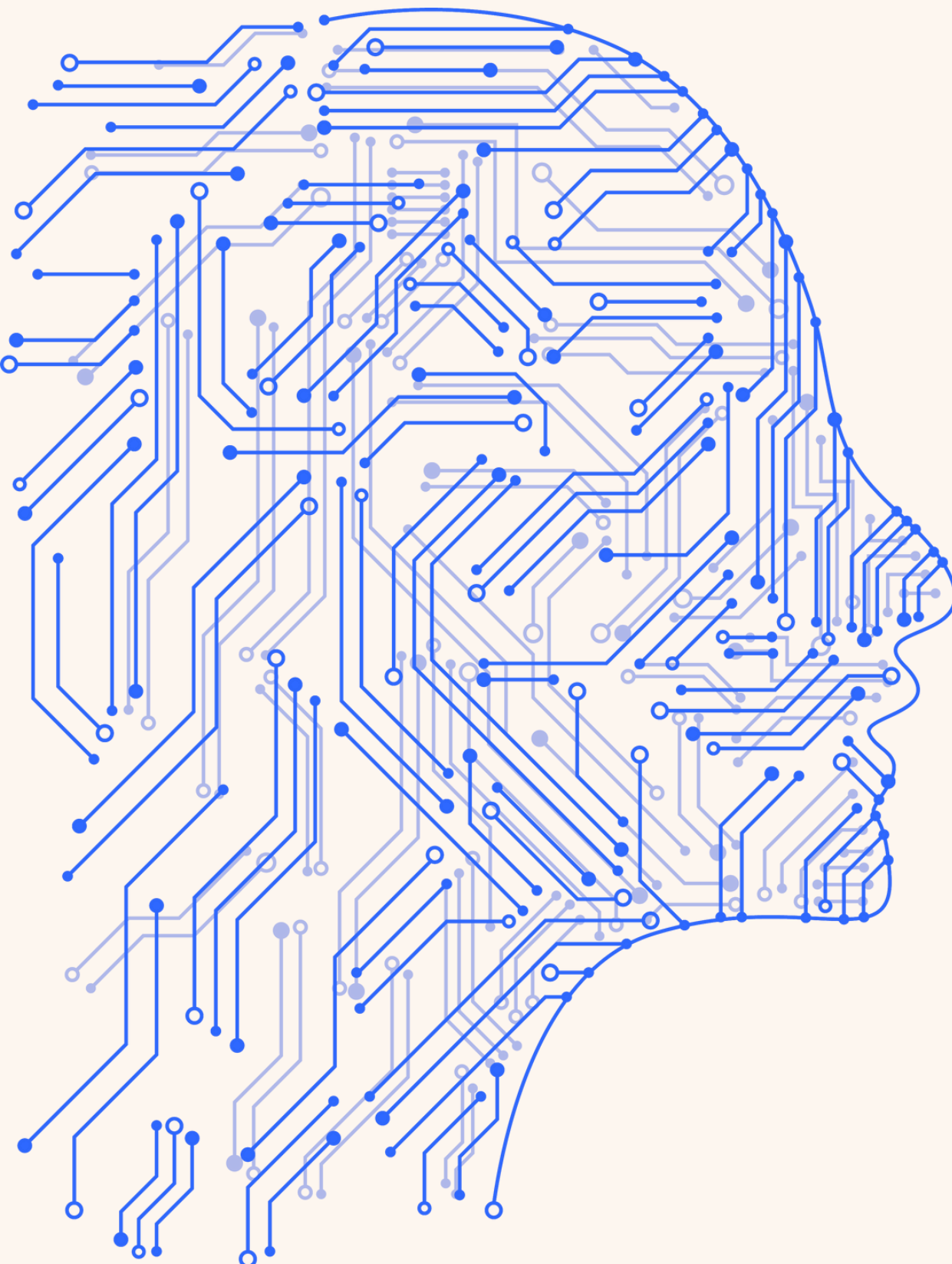
CÁC CÔNG NGHỆ CỦA CHUYỂN ĐỔI SỐ

Trí tuệ nhân tạo

Con người nỗ lực làm cho máy móc có những năng lực trí tuệ của con người và gọi đó là trí tuệ nhân tạo. Xét theo nghĩa này, thì trí tuệ nhân tạo còn phải tiếp tục phát triển lâu dài nữa để tới gần hơn điều đó.

Nhưng xét theo nghĩa hẹp hơn, là trí tuệ nhân tạo nhằm “tăng cường năng lực trí tuệ của con người”, thì đã có những bước tiến lớn trong vòng 2 thập kỷ vừa qua.

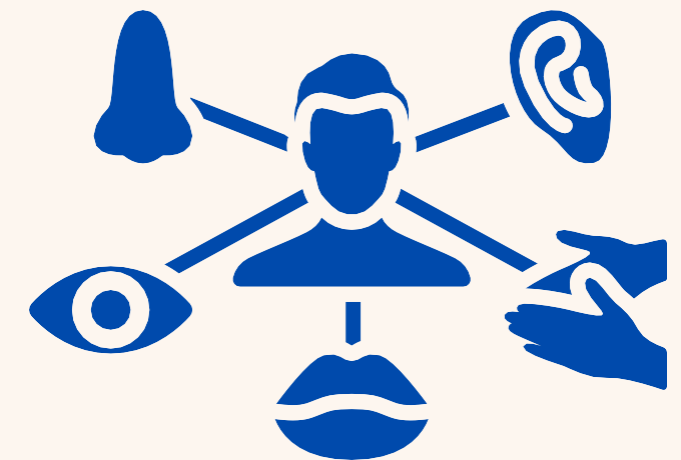
Có thể ví trí tuệ nhân tạo như là hệ thần kinh của con người.



INTERNET VẠN VẬT

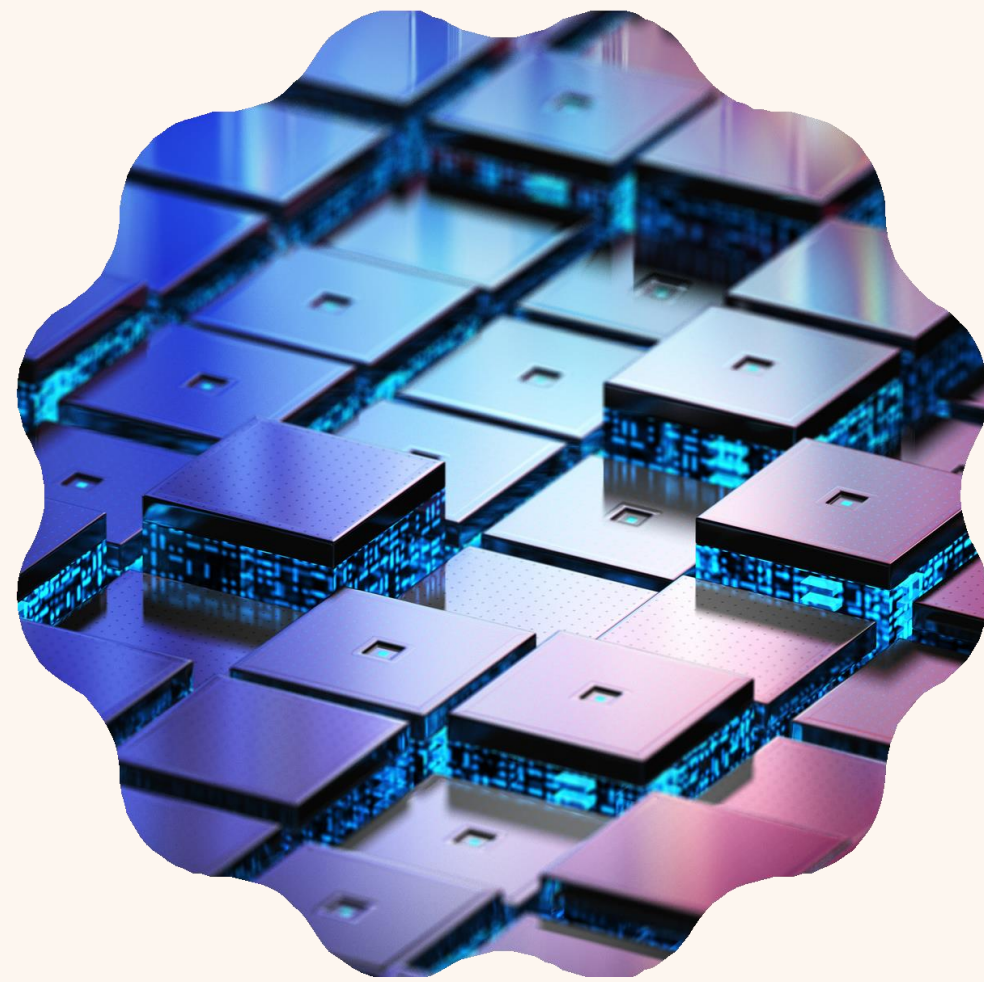
- INTERNET OF THING (IOT)

- Internet vạn vật (IoT) là một công nghệ nền tảng của cuộc Cách mạng công nghiệp lần thứ tư.
- Internet vạn vật là mạng lưới kết nối vạn vật với nhau
- Có thể ví Internet vạn vật như là các giác quan của con người.



DỮ LIỆU LỚN

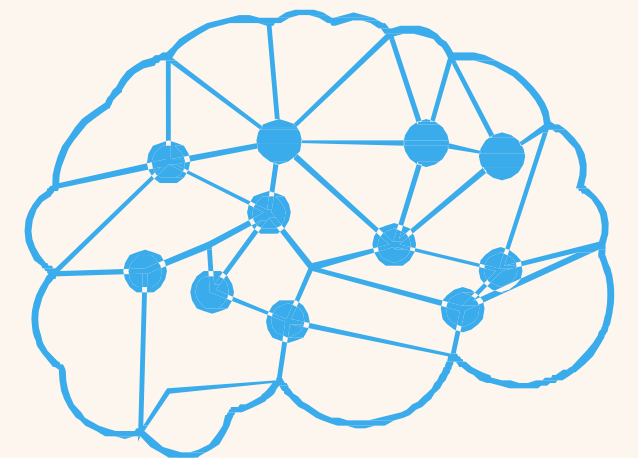
Dữ liệu được sinh ra từ hàng tỷ điện thoại thông minh, thiết bị cảm biến kết nối vạn vật và hoạt động của con người trên môi trường mạng.



Công nghệ số hiện nay cho phép xử lý, phân tích trong khoảng thời gian ngắn hơn rất nhiều để trích rút ra thông tin, tri thức hoặc đưa ra quyết định một cách phù hợp.

Công nghệ số hiện nay chủ yếu xử lý và phân tích dữ liệu phi cấu trúc. Dữ liệu phi cấu trúc chiếm tới **70-80%**, do vậy, chứa nhiều thông tin hơn dữ liệu có cấu trúc.

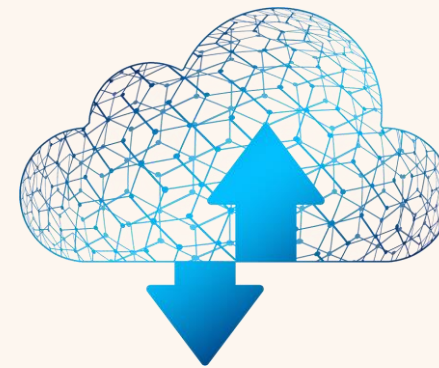
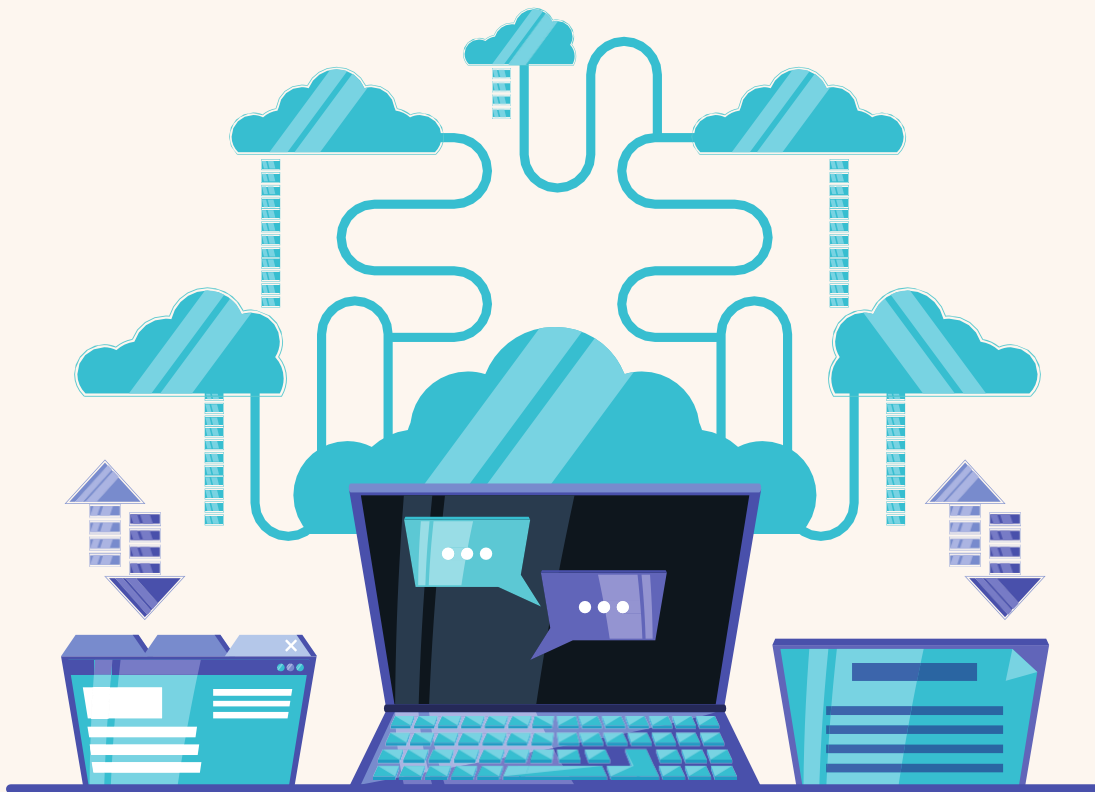
Có thể ví dữ liệu lớn như bộ não của con người.



ĐIỆN TOÁN ĐÁM MÂY

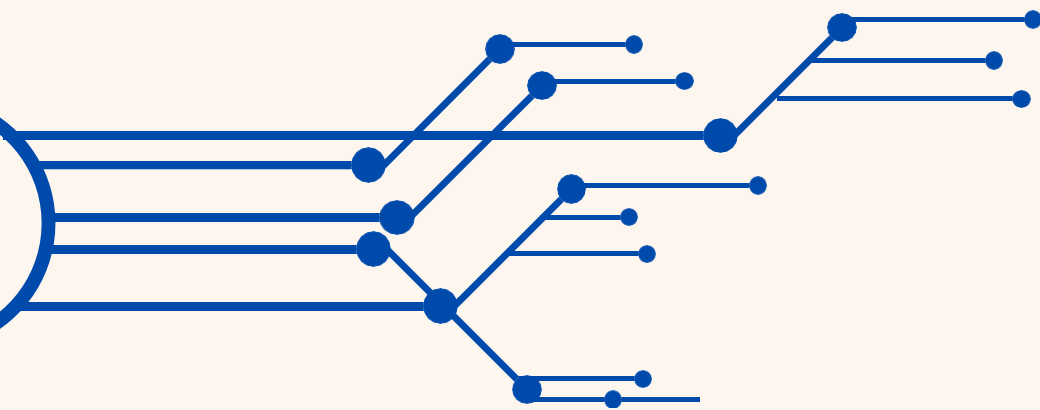
Điện toán đám mây là công nghệ cho phép năng lực tính toán nằm ở các máy chủ ảo, gọi là đám mây trên Internet của các nhà cung cấp thay vì trong máy tính gia đình và văn phòng trên mặt đất, để mọi người kết nối, sử dụng như là dịch vụ khi họ cần.

Điện toán đám mây cũng giống như điện lưới.



Có thể ví điện toán đám mây như là cơ bắp của con người.





CÔNG NGHỆ CHUỖI KHỐI

Là một chuỗi dữ liệu phân tán trên mạng, gồm các khối thông tin được liên kết với nhau bằng mã hóa và mở rộng theo thời gian.

Vì phân tán nên không ai có thể kiểm soát toàn bộ

Vì liên kết nên sự sửa đổi nào đều để lại dấu vết, chống chối bỏ



Vì mã hóa nên bảo mật

Vì tất cả yếu tố như vậy nên bảo đảm sự an toàn, tin cậy và minh bạch

Các giao dịch trong mạng chuỗi khối diễn ra tự động mà không cần bên thứ ba chứng nhận. Công nghệ chuỗi khối sẽ giảm dần và xóa bỏ vai trò của trung gian trong các giao dịch.

Định nghĩa nêu hai ý cơ bản của chuyển đổi số.



“Chuyển đổi số là quá trình tự thay đổi cách sống và cách làm việc trên môi trường thực - số”



Chuyển đổi số là một quá trình tự thay đổi về cách sống (của cá nhân và cộng đồng) và cách làm việc (của cá nhân, tổ chức và doanh nghiệp).



Hai là thay đổi để thích nghi và khai thác các cơ hội của môi trường thực-số.

VÍ DỤ

Công chức, cán bộ, công chức trước đây dùng internet không nhiều



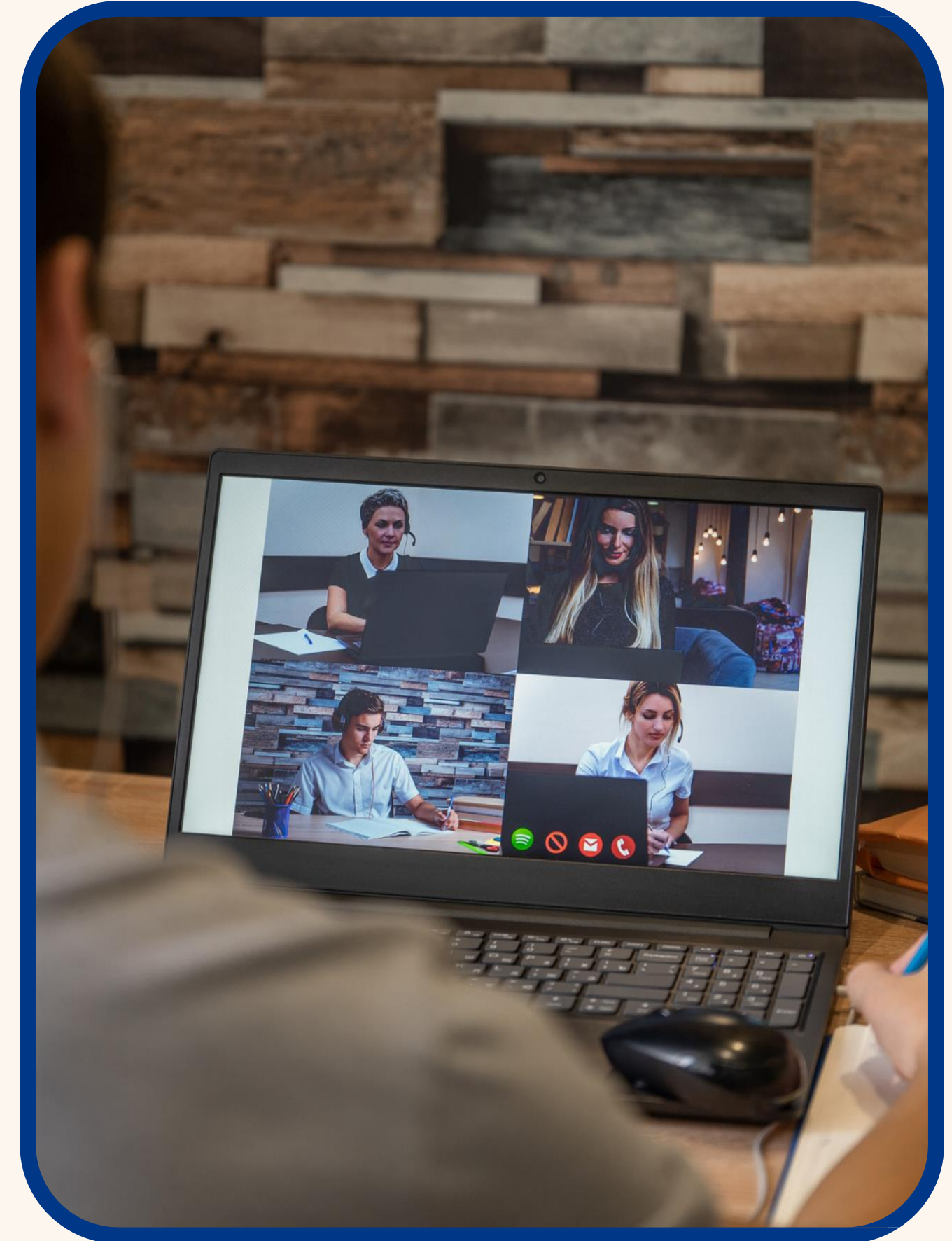
Bây giờ thì khi đến văn phòng ngay lập tức chúng ta ngồi vào cái hệ thống làm việc ở trên mạng.



Tỷ lệ hoạt động của con người trên môi trường số ngày càng nhiều hơn và khi hoạt động trên môi trường số ngày càng nhiều hơn, con người có xu hướng thay đổi hành vi khi mà thay đổi môi trường.



Khi chúng ta thay đổi môi trường sống ngay lập tức là chúng ta thay đổi đến hành vi.



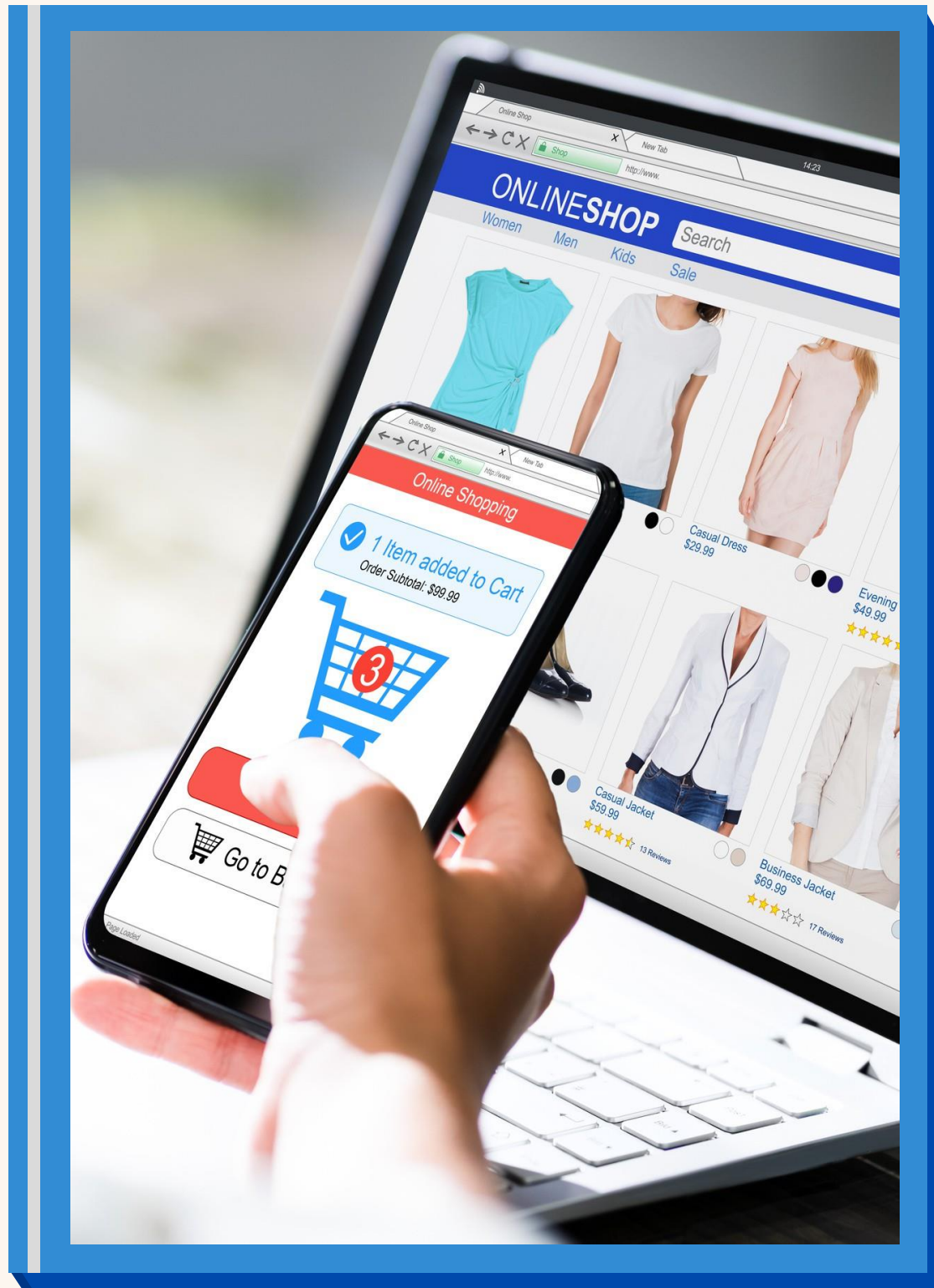
VÍ DỤ

CHUYỂN ĐỔI SỐ ĐÃ THAY ĐỔI TẤT CẢ HÀNH VI CỦA CHÚNG TA.

Trước đây chúng ta phải ra chợ mới mua được đồ cần thiết.



Bây giờ dễ dàng mua sắm trên sàn thương mại điện tử và được vận chuyển đến tay nhanh chóng.





VÍ DỤ

Trước đây các hãng taxi truyền thống họ kinh doanh và họ bán dịch vụ vận tải, con người ra đường thấy taxi thì vậy.

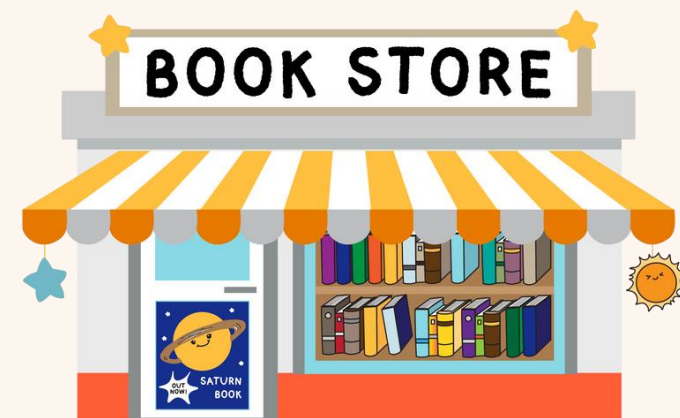


Giai đoạn sau các hãng taxi vẫn bán dịch vụ vận tải nhưng con người có thể gọi điện qua tổng đài, có thể đặt taxi qua ứng dụng.

Trong chuyển đổi số, Grab không còn bán dịch vụ vận tải nữa, mà bán dịch vụ kết nối giữa người có khả năng cung cấp dịch vụ và người có nhu cầu.



Trước đây bán những cuốn sách bằng bản cứng



Ứng dụng công nghệ thông tin,
bán đĩa CD

Chuyển đổi số bán dịch vụ truy cập
vào kho thông tin của họ.



VÍ DỤ



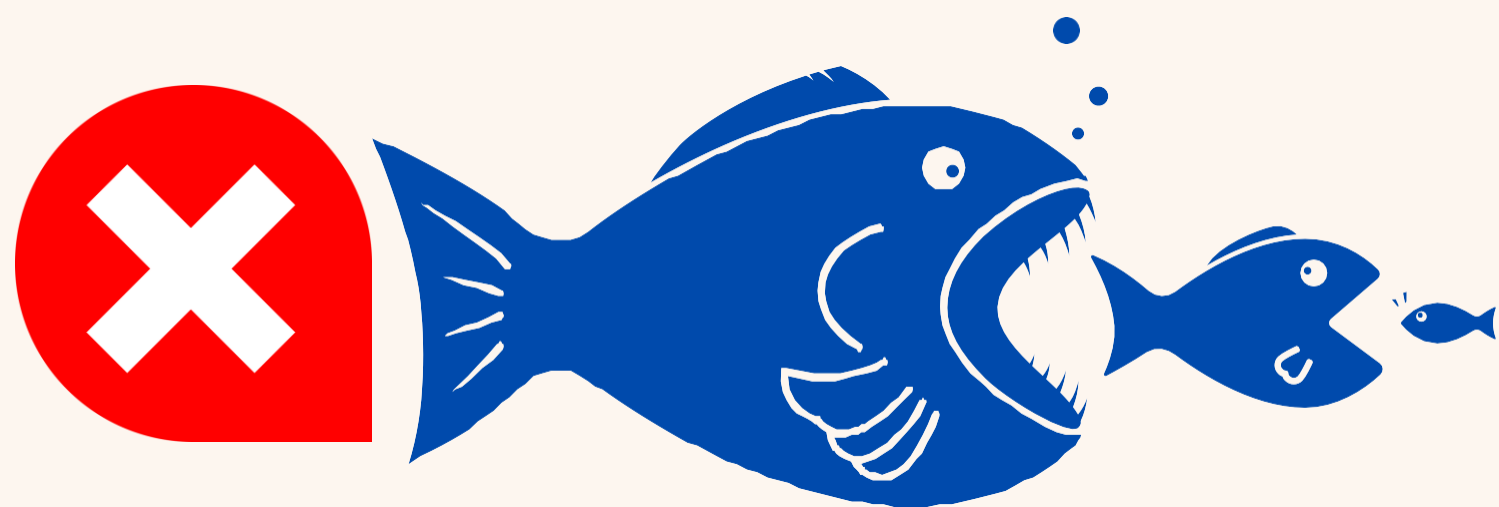


Chuyển đổi số là chuyển đổi từ một ngôi trường cũ sang một môi trường mới và khi điều đó xảy ra nó sẽ tạo ra những sự khác biệt.

SỰ KHÁC BIỆT TRONG CHUYỂN ĐỔI SỐ LÀ GÌ?

Đó chính là sự khác biệt giữa người nhanh và người chậm, ai chuyển đổi lên môi trường số nhanh thì người ấy có nhiều lợi thế. Và chuyển đổi chậm thì mất lợi thế.

Vì vậy thì chúng ta vẫn nói giai đoạn cách mạng công nghệ 4.0 hiện nay không phải cá to nuốt cá nhỏ, chúng ta thấy rất nhiều cá to bị chết vì không chuyển đổi kịp.



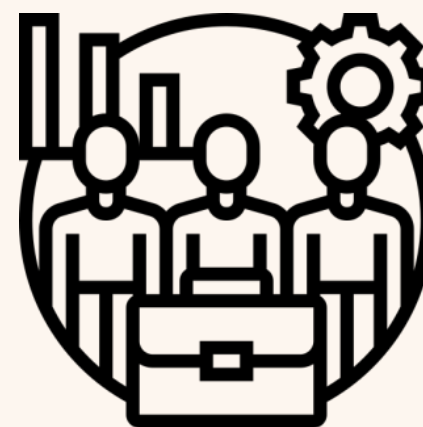
CHUYỂN ĐỔI SỐ ĐEM LẠI LỢI ÍCH GÌ CHO NGƯỜI DÂN



Chuyển đổi số giúp người dân bình đẳng về cơ hội tiếp cận dịch vụ, đào tạo, tri thức, qua đó giúp thu hẹp khoảng cách số thông qua việc phát triển chính phủ số, kinh tế số và xã hội số.



Chính phủ số nhờ dữ liệu số và công nghệ số thấu hiểu người dân hơn, vì vậy, cung cấp dịch vụ số tốt hơn, chăm sóc người dân tốt hơn.



Kinh tế số cho phép mỗi người dân có thể tiếp cận toàn bộ thị trường một cách nhanh chóng theo cách chưa từng có.



Chuyển đổi số có thể giúp xóa nhòa khoảng cách địa lý, mang đến cơ hội bình đẳng cho người dân về tiếp cận dịch vụ, mang lại một loạt những tiến bộ lớn về chất lượng cuộc sống. Người dân có thể sống khỏe mạnh hơn nhờ các hình thức chăm sóc y tế kịp thời, vui vẻ hơn với các hình thức giải trí đa dạng và an toàn hơn.

CHUYỂN ĐỔI SỐ LÀ VIỆC CỦA AI?



Với một tổ chức,

Vì là sự thay đổi, nên trước tiên đó là việc của **lãnh đạo, của người đứng đầu**, vì nếu không thì không ai dám làm và có thể làm.

Vì là tổng thể và toàn diện nên đó là việc của **tất cả mọi thành viên** trong tổ chức.

Xét cho cùng, chuyển đổi số là phục vụ **người dân**.
Mỗi người dân trở thành công dân số thì chuyển đổi số mới thành công.

Do vậy, chuyển đổi số mang ý nghĩa của một cuộc cách mạng toàn dân.

Khi **toàn dân cùng tham gia**, họ sẽ tìm ra công nghệ số phù hợp, sẽ tìm ra cách giải phù hợp và vì thế chuyển đổi số sẽ thành công.





IHANOI

Ứng dụng iHanoi hướng tới là 1 siêu ứng dụng, là kênh tương tác số thu hẹp khoảng cách giữa người dân, doanh nghiệp với chính quyền. Với mục tiêu lấy người dân, doanh nghiệp làm trung tâm, ứng dụng cung cấp 5 nhóm chức năng chính:

- Các tính năng giúp người dân, doanh nghiệp có thể dễ dàng tương tác trực tuyến với chính quyền.
- Cập nhật thông tin toàn diện, đa dạng về tình hình kinh tế, xã hội của Hà Nội. Cập nhật các thông báo, cảnh báo quan trọng từ cơ quan chính quyền.
- Tích hợp các dịch vụ, tiện ích phục vụ đời sống người dân, doanh nghiệp.
- Mạng xã hội giúp người dân tương tác với người dân; người dân tương tác với doanh nghiệp; người dân, doanh nghiệp tương tác với chính quyền.

Đối tượng sử dụng

- Lưu trữ các thông tin, tài liệu cá nhân để phục vụ việc chia sẻ dữ liệu với các cơ quan chính quyền khi cần



Cán bộ, công chức



Người dân



Doanh nghiệp





TẢI ỨNG DỤNG IHANOI

CÔNG DÂN SỐ THỦ ĐÔ



iHanoi ra mắt với sứ mệnh là kênh tương tác số thu hẹp khoảng cách giữa chính quyền với người dân, các doanh nghiệp đang hoạt động kinh doanh trên địa bàn thành phố Hà Nội. Ứng dụng mang tới những thông tin hữu ích, cung cấp các tiện ích đô thị thông minh tới người dân ở mọi khía cạnh cuộc sống, gồm: Giao thông, y tế, giáo dục, môi trường, đất đai, nông nghiệp...

CÔNG DÂN SỐ THỦ ĐÔ



Tên ứng dụng iHanoi được hình thành từ sự kết hợp giữa chữ "i" và tên địa danh Thủ đô "Hà Nội" mang đến nhiều ý nghĩa. Chữ "i" trong iHanoi không chỉ đại diện cho các khái niệm như interconnect (kết nối), interactive (tương tác), information (thông tin), intelligent (thông minh), integration (tích hợp) mà còn thể hiện tính individual (cá nhân), innovation (đổi mới). "i" cũng có nghĩa là "tôi" trong tiếng Anh, thể hiện sự kết nối giữa từng người dân với Thành phố, thúc đẩy tinh thần cộng đồng và sự sáng tạo trong việc xây dựng một Hà Nội thông minh và phát triển.

iHanoi không chỉ đơn giản là một tên gọi mà còn là biểu tượng của sự hài hòa giữa công nghệ hiện đại và văn hoá truyền thống của Hà Nội, thể hiện cam kết sử dụng công nghệ tiên tiến nhất để nâng cao chất lượng sống và hài lòng của người dân và du khách.

CÔNG DÂN SỐ THỦ ĐÔ



Với slogan "Chạm để kết nối", nền tảng thể hiện rõ mục tiêu và tính năng của ứng dụng dành cho người dân. Mỗi lần sử dụng và tương tác, từng "chạm" mang đến một kết nối ý nghĩa: từ liên lạc với cơ quan chính quyền, cập nhật tin tức mới nhất của Hà Nội, đến sử dụng các tiện ích đô thị thông minh.

"Chạm để kết nối" không chỉ là một lời kêu gọi hành động mà còn là một tuyên bố về mục tiêu và giá trị cốt lõi của ứng dụng iHanoi, nhấn mạnh sự dễ dàng trong việc tương tác, khả năng kết nối thông tin và các dịch vụ tiện ích. Điều này góp phần góp phần nâng cao chỉ số phục vụ người dân, doanh nghiệp trên địa bàn Thành phố, mang lại nhiều giá trị, lợi ích cho người dân.

CÔNG DÂN SỐ THỦ ĐÔ



Các chức năng trên ứng dụng iHanoi được chia thành các nhóm :

Nhóm 1 - Hanoi Connect: Giúp người dân, doanh nghiệp tương tác với cơ quan chính quyền dễ dàng hơn thông qua tính năng phản ánh và đăng ký tiếp công dân.

Nhóm 2 - Hanoi Life: Cung cấp các tính năng tiện ích đô thị thông minh như theo dõi giao thông, tra cứu tuyến xe, sổ sức khỏe điện tử, thông tin giáo dục, môi trường, du lịch, và thanh toán trực tuyến. Ứng dụng còn cung cấp giải trí thông qua TV360, mang đến sự tiện lợi và thông minh cho cuộc sống hằng ngày tại Hà Nội.

CÔNG DÂN SỐ THỦ ĐÔ



Nhóm 3 - Hanoi News: Cập nhật tin tức từ Hà Nội và cung cấp thông tin cảnh báo, tin tức kinh tế, xã hội qua các báo điện tử.

Nhóm 4 - Sáng kiến, góp ý: Hỗ trợ người dân gửi ý tưởng, sáng kiến đóng góp cho việc phát triển Thủ đô.

Bên cạnh đó, ứng dụng iHanoi còn có tính năng Hanoi Chat - cung cấp trò chuyện trực tuyến, giúp người dân tương tác với nhau, các doanh nghiệp và cơ quan chính quyền. Người dùng có thể trò chuyện 1:1, tạo nhóm trò chuyện, gọi video call, chia sẻ hình ảnh, file, danh thiếp, vị trí hiện tại

DANH SÁCH CÁC CHỨC NĂNG CHÍNH

- TẢI ỨNG DỤNG IHANOI
- ĐĂNG KÝ TÀI KHOẢN
- QUÊN MẬT KHẨU
- XÁC THỰC TÀI KHOẢN
- TẠO PHẢN ÁNH HIỆN TRƯỜNG
- TẠO PHẢN ÁNH THỦ TỤC HÀNH CHÍNH
- TẠO PHIẾU ĐĂNG KÝ TIẾP CÔNG DÂN
- HƯỚNG DẪN CẤP QUYỀN THÔNG BÁO
- SỔ SỨC KHOẺ ĐIỆN TỬ



9:41

Đăng nhập

Số điện thoại

Mật khẩu

Quên mật khẩu?

Đăng nhập

Bạn chưa có tài khoản? Đăng ký ngay

Bước 1: Ở màn hình Đăng nhập, chọn Đăng ký ngay

9:41

Đăng ký

Số điện thoại

Tiếp tục

Bằng việc đăng ký tài khoản, bạn đồng ý với Điều khoản sử dụng và Chính sách bảo mật của iHanoi.

Bước 2: Nhập số điện thoại cá nhân

9:41

Xác thực số điện thoại

Nhập mã xác thực vừa được gửi tới số 0988777666

Tiếp tục

Không nhận được mã? (60s)

Từ tin nhắn 111 111

1 2 3
4 5 6
7 8 9
0

Bước 3: Nhập OTP được trả về số điện thoại

9:41

Vui lòng nhập các thông tin theo yêu cầu để hoàn tất việc đăng ký tài khoản.
Lưu ý: Nhập đúng họ tên thật để đảm bảo thông tin trao đổi với chính quyền được chính xác & minh bạch.

Họ và tên

Nhập họ và tên

Nơi ở hiện tại

Chọn quận/huyện Chọn phường/xã

Mật khẩu

Nhập mật khẩu

Nhập lại mật khẩu

Nhập lại mật khẩu

Tối thiểu 8 ký tự.
Bao gồm chữ hoa, chữ thường, số & ký tự đặc biệt.

Hoàn tất

Bước 4: Nhập các thông tin theo yêu cầu

ĐĂNG KÝ TÀI KHOẢN

9:41

Đăng nhập

Số điện thoại

Mật khẩu

Quên mật khẩu?

Đăng nhập

Bạn chưa có tài khoản? Đăng ký ngay

Bước 1: Ở màn hình Đăng nhập, chọn Quên mật khẩu

9:41

Quên mật khẩu

Vui lòng nhập số điện thoại bạn đã sử dụng để đăng ký tài khoản

Nhập số điện thoại

Tiếp tục

Bước 2: Nhập số điện thoại đã đăng ký tài khoản

9:41

Xác thực số điện thoại

Nhập mã xác thực vừa được gửi tới số 0988777666

Tiếp tục

Không nhận được mã? (60s)

From Messages
111 111

1 2 3
4 5 6
7 8 9
0

Bước 3: Nhập OTP được trả về số điện thoại

9:41

Tạo mật khẩu mới

Mật khẩu mới

Nhập lại mật khẩu mới

Tối thiểu 8 ký tự.
Bao gồm chữ hoa, chữ thường, số & ký tự đặc biệt.

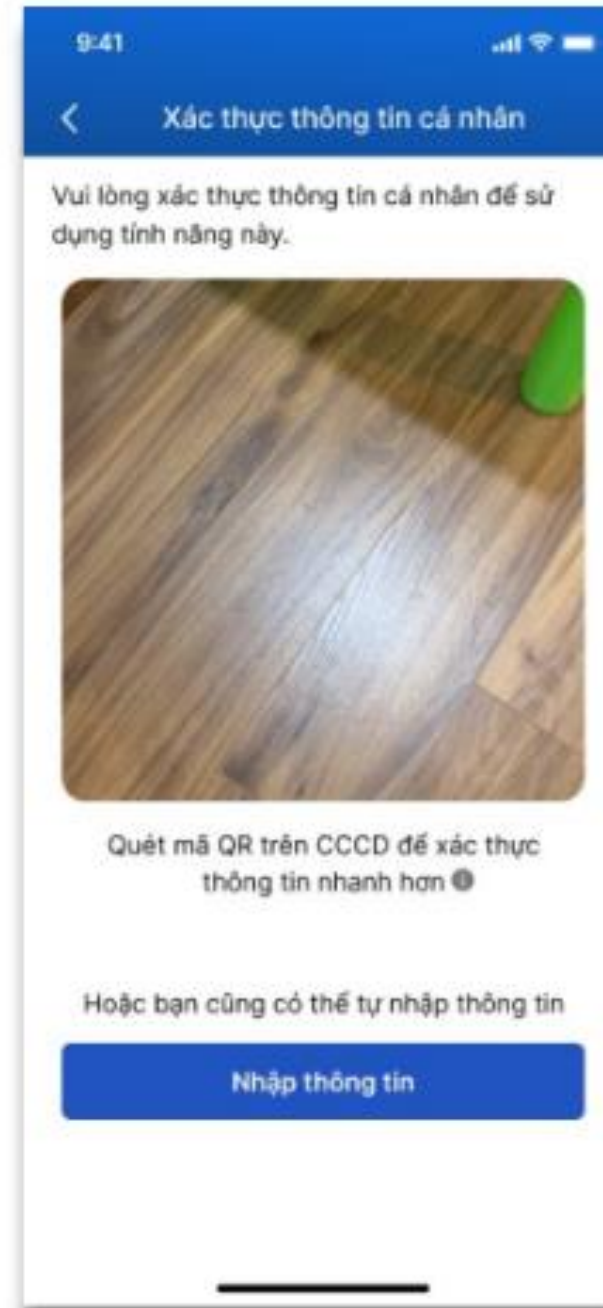
Tiếp tục

Bước 4: Tạo mật khẩu mới

QUÊN MẬT KHẨU



Bước 1: Ở màn hình Xác thực thông tin, chọn Cho phép truy cập để cấp quyền truy cập camera



Bước 2: Quét mã QR trên CCCD



Bước 3: Chọn xác thực thông tin

XÁC THỰC TÀI KHOẢN



Bước 1: Đọc giới thiệu về chức năng, chọn Tôi đã hiểu

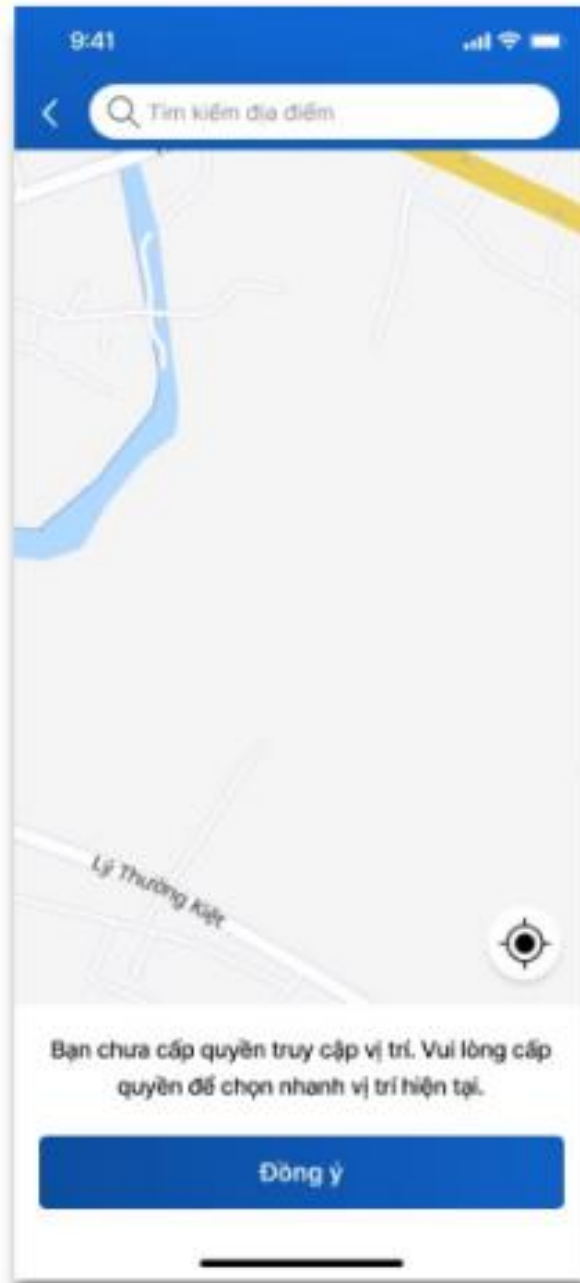


Bước 2: Ở màn danh sách phản ánh, Chọn Tạo phản ánh

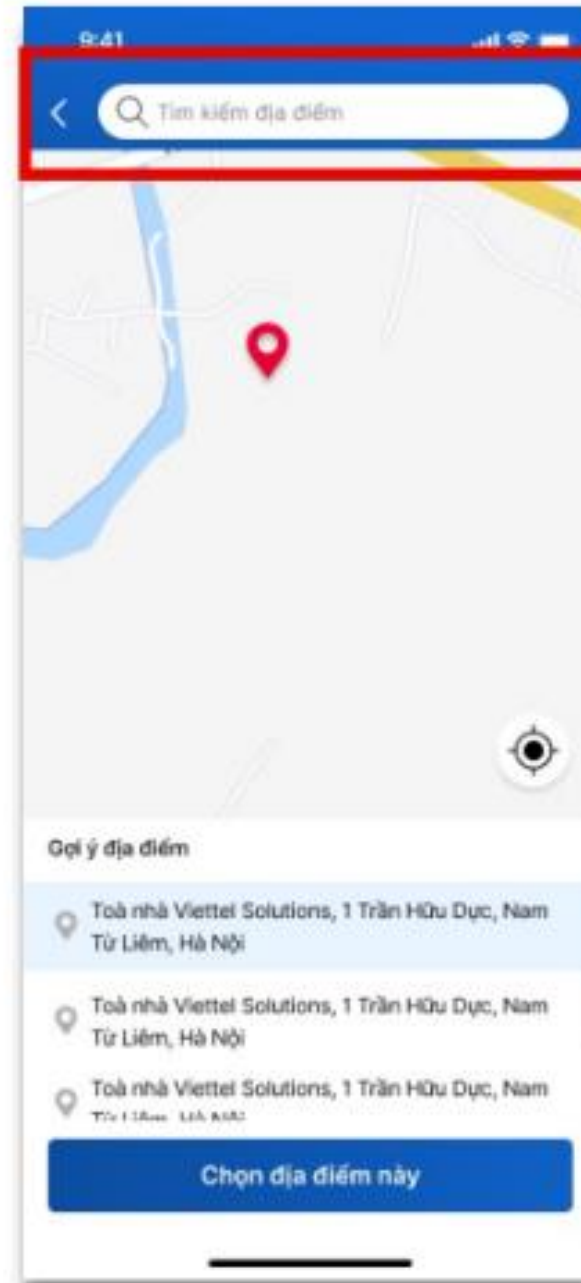


Bước 3: Nhập các thông tin theo yêu cầu (Các thông tin bắt buộc nhập gồm địa điểm phản ánh, nội dung, ảnh/video)

TẠO PHẢN ÁNH HIỆN TRƯỜNG



Trường hợp chưa cấp quyền định vị, chọn Đồng ý để cấp quyền truy cập vị trí hiện tại của người dùng

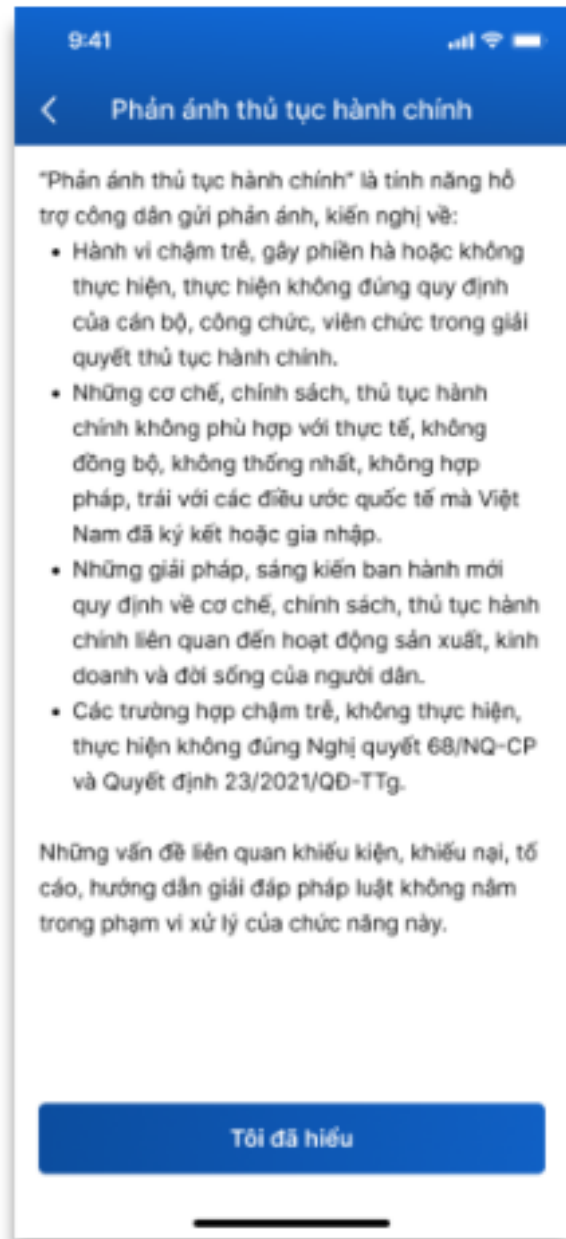


Trường hợp đã cấp quyền định vị, chọn địa điểm phản ánh ở danh sách gợi ý địa điểm



Nhập từ khoá để tìm kiếm địa điểm phản ánh

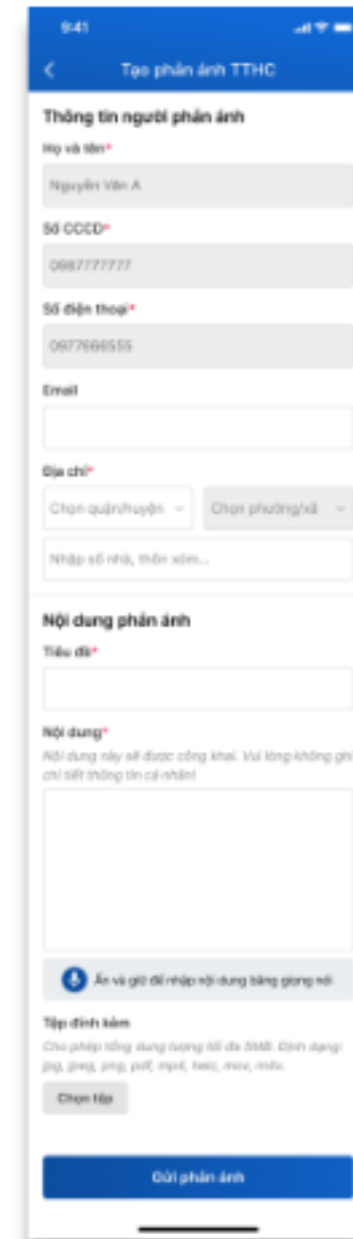
TẠO PHẢN ÁNH HIỆN TRƯỜNG



Bước 1: Đọc giới thiệu về chức năng, chọn Tôi đã hiểu



Bước 2: Chọn vào biểu tượng tạo Phản ánh TTHC

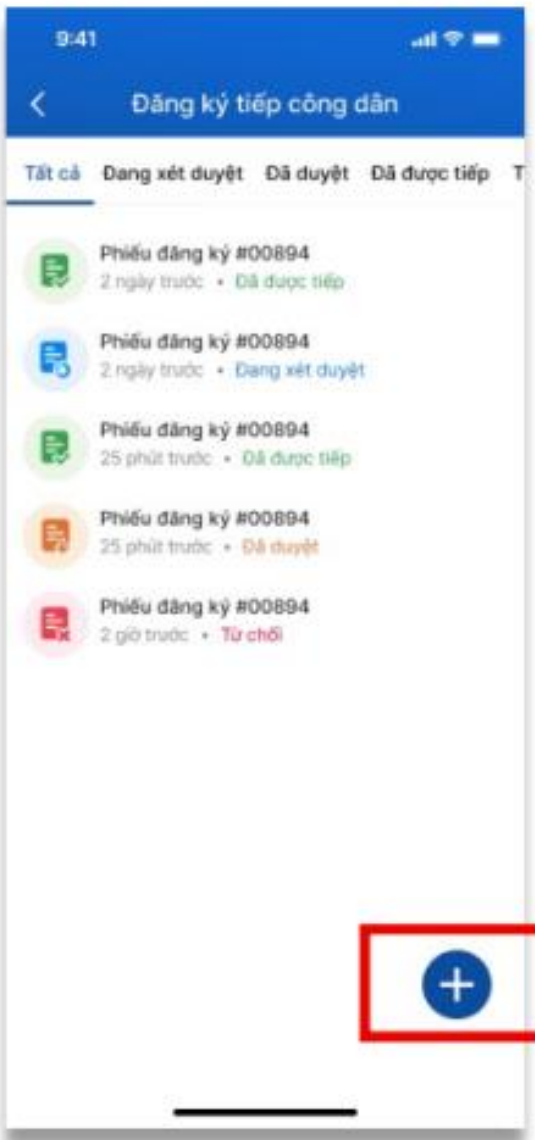


Bước 3: Nhập các thông tin theo yêu cầu (các thông tin bắt buộc nhập gồm Địa chỉ, tiêu đề, nội dung)

TẠO PHẢN ÁNH THỦ TỤC HÀNH CHÍNH



Bước 1: Đọc giới thiệu về chức năng, chọn Tôi đã hiểu

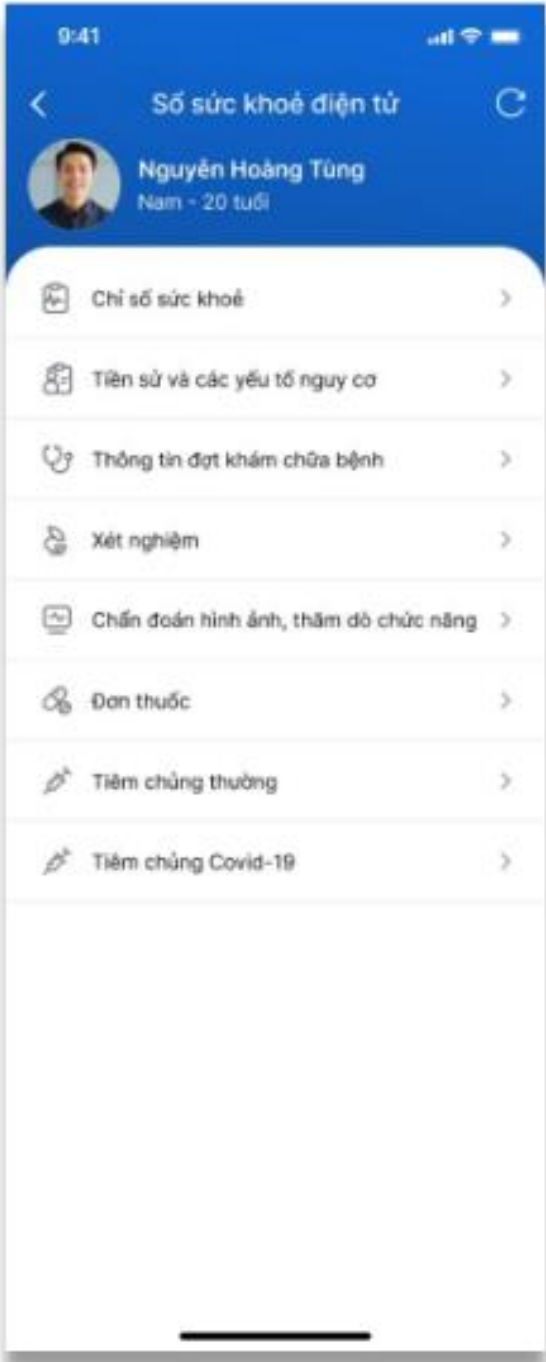


Bước 2: Chọn vào biểu tượng tạo đăng ký tiếp công dân



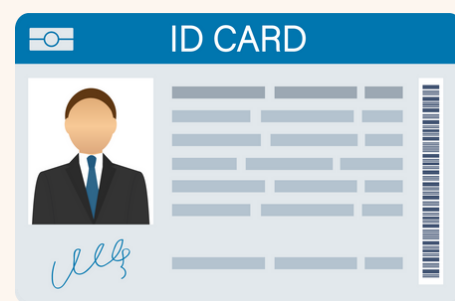
Bước 3: Nhập các thông tin theo yêu cầu (các thông tin bắt buộc nhập gồm người khiếu nại, hình thức tiếp, loại hình tiếp, loại nội dung, địa phương xảy ra sự việc, nội dung trình bày)

ĐĂNG KÝ TIẾP CÔNG DÂN



LÀM GÌ ĐỂ AN TOÀN TRÊN MÔI TRƯỜNG SỐ

Bên cạnh những tác động tích cực to lớn của chuyển đổi số, an toàn thông tin đang trở thành vấn đề nóng bỏng đối với các quốc gia, đặc biệt đối với những quốc gia có tốc độ phát triển công nghệ thông tin nhanh như Việt Nam. Từ đây, dù bạn là ai (giáo viên, học sinh, bác sĩ, kỹ sư... hay cả những chuyên gia an toàn thông tin), **hàng loạt vấn đề phức tạp đã nảy sinh, khi đã sử dụng Internet sẽ phải đối mặt với các nguy cơ mất an toàn thông tin như:**



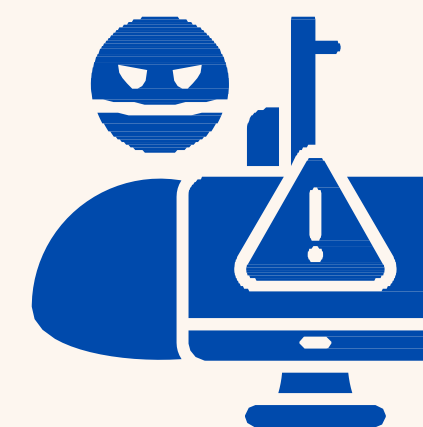
Nguy cơ lộ lọt thông tin cá nhân.



Nguy cơ lừa đảo trực tuyến.



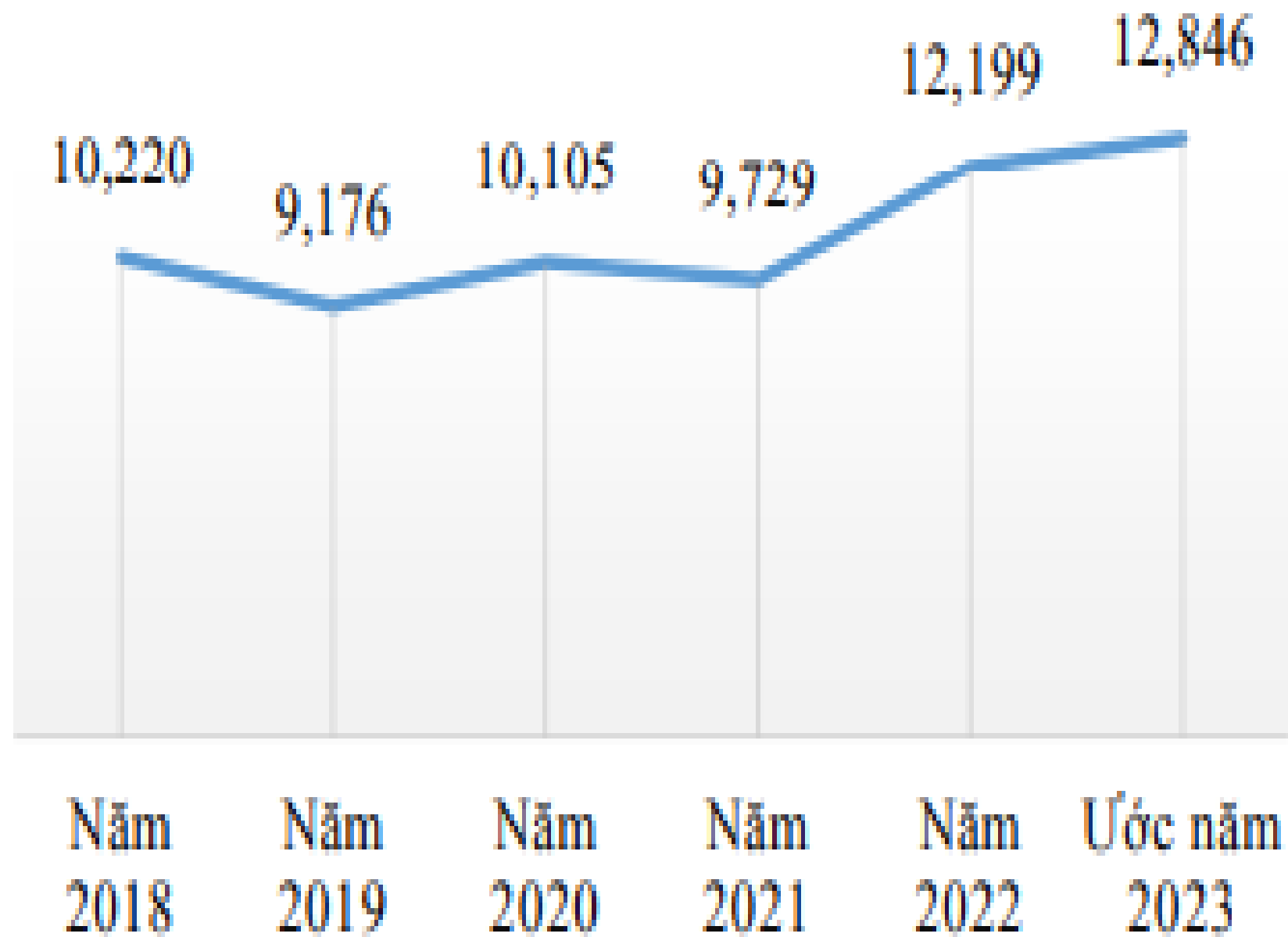
Nguy cơ bị nhiễm mã độc, nghe lén.



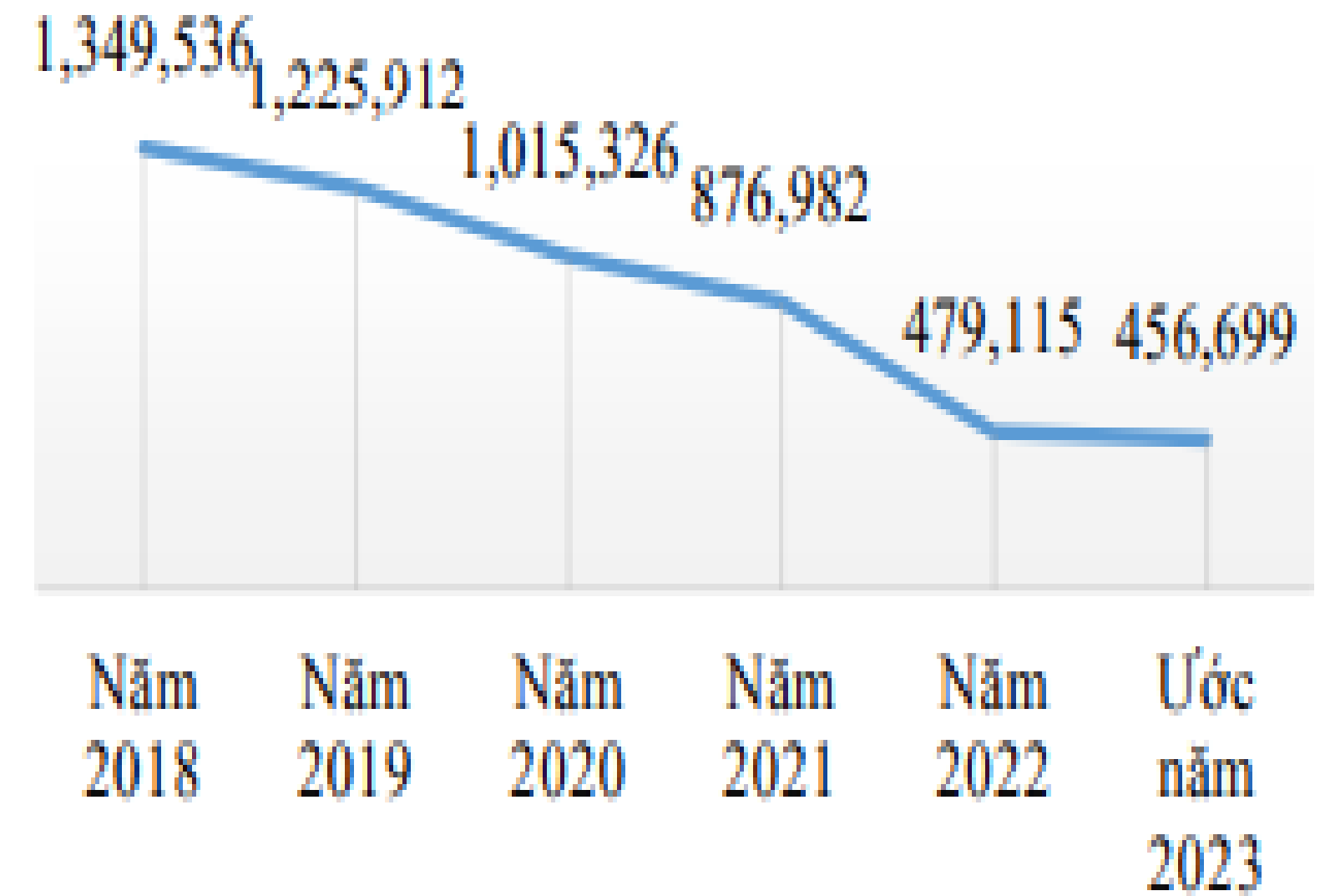
Nguy cơ về tin giả, khủng bố mạng

TÌNH HÌNH AN TOÀN THÔNG TIN

Số lượng cuộc tấn công mạng

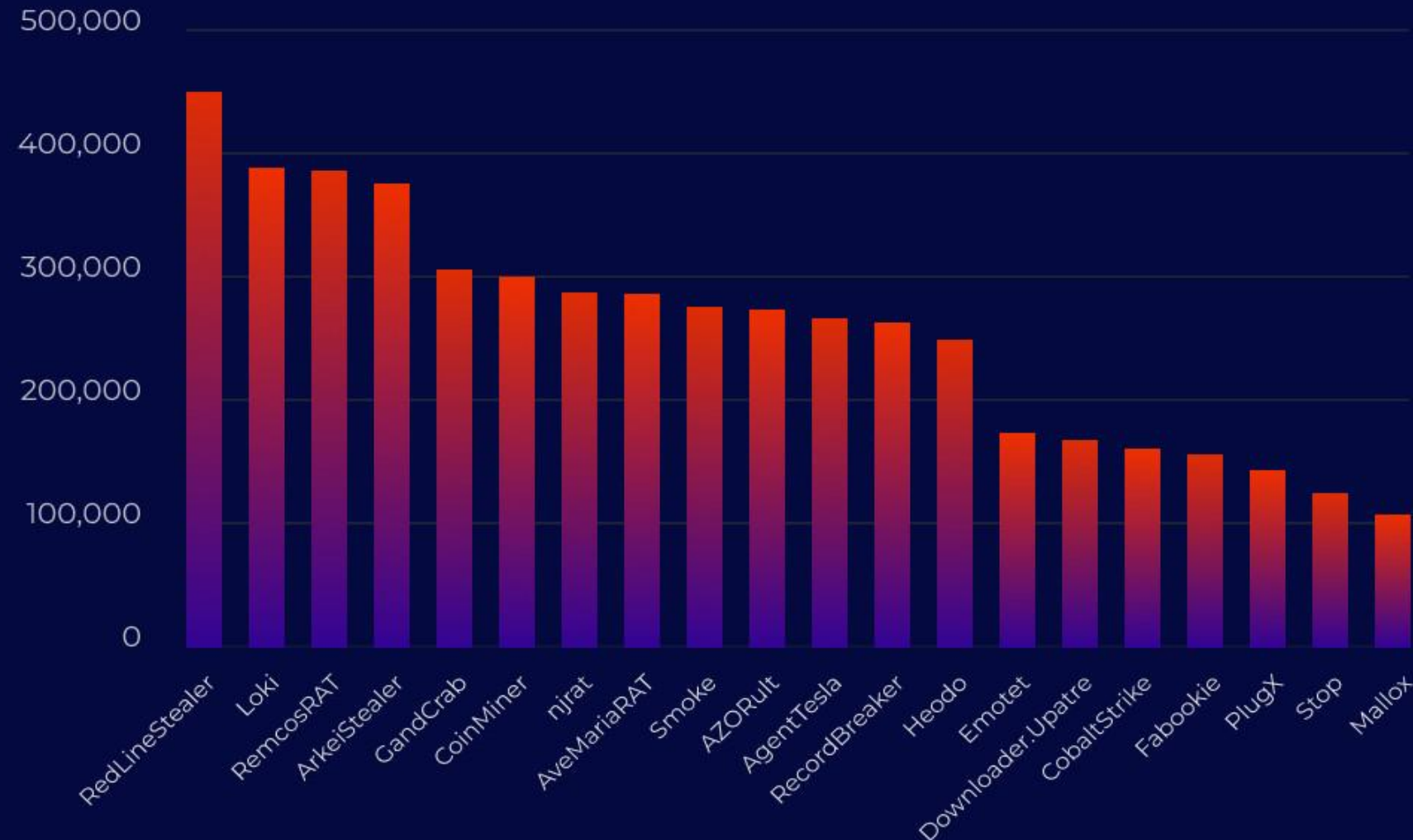


**Số lượng địa chỉ IP của Việt Nam
nằm trong mạng botnet**

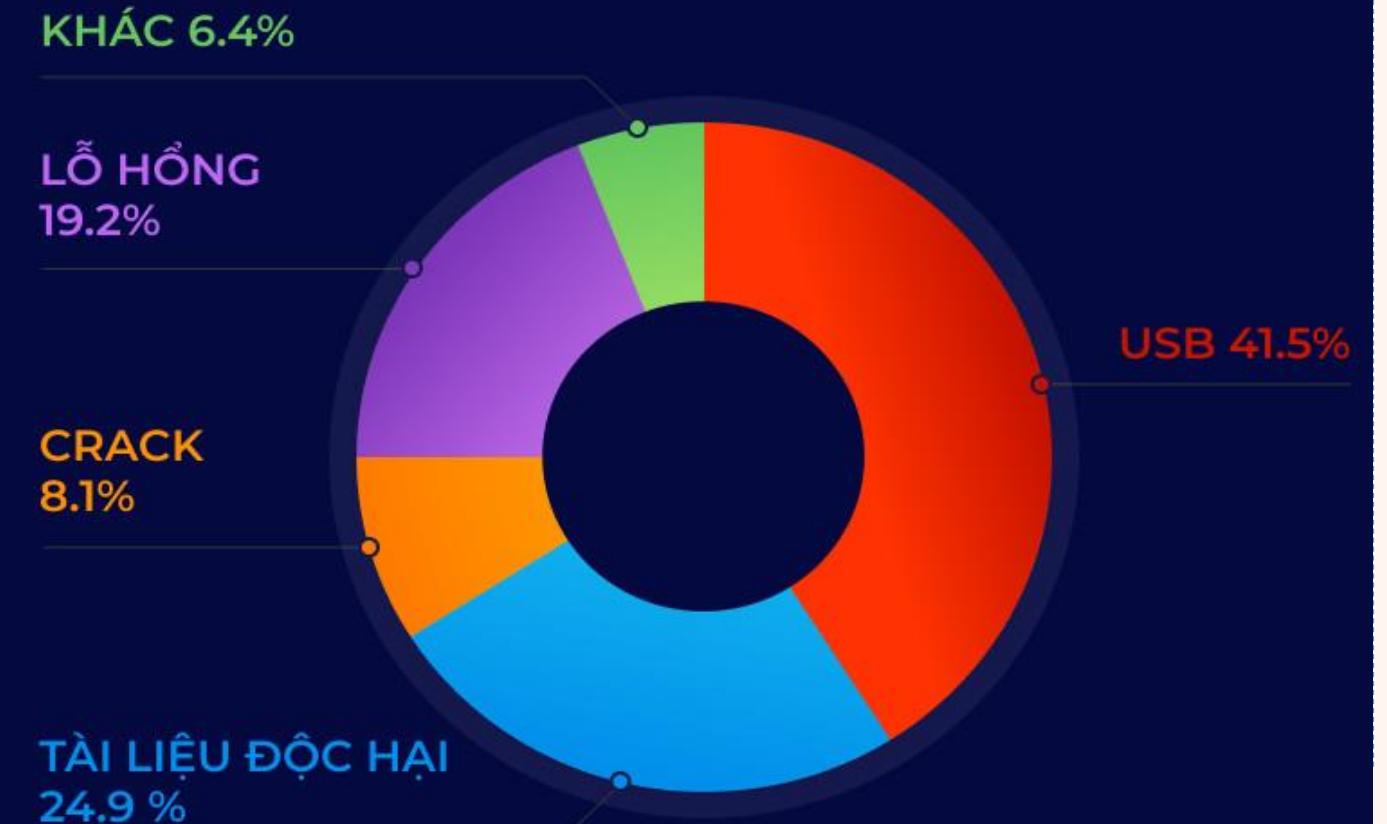


TÌNH HÌNH AN TOÀN THÔNG TIN

TOP 20 DÒNG VIRUS PHỔ BIẾN TẠI VIỆT NAM



CÁC CON ĐƯỜNG LÂY LAN VIRUS PHỔ BIẾN TẠI VIỆT NAM



6,062,715
Số máy bị nhiễm virus

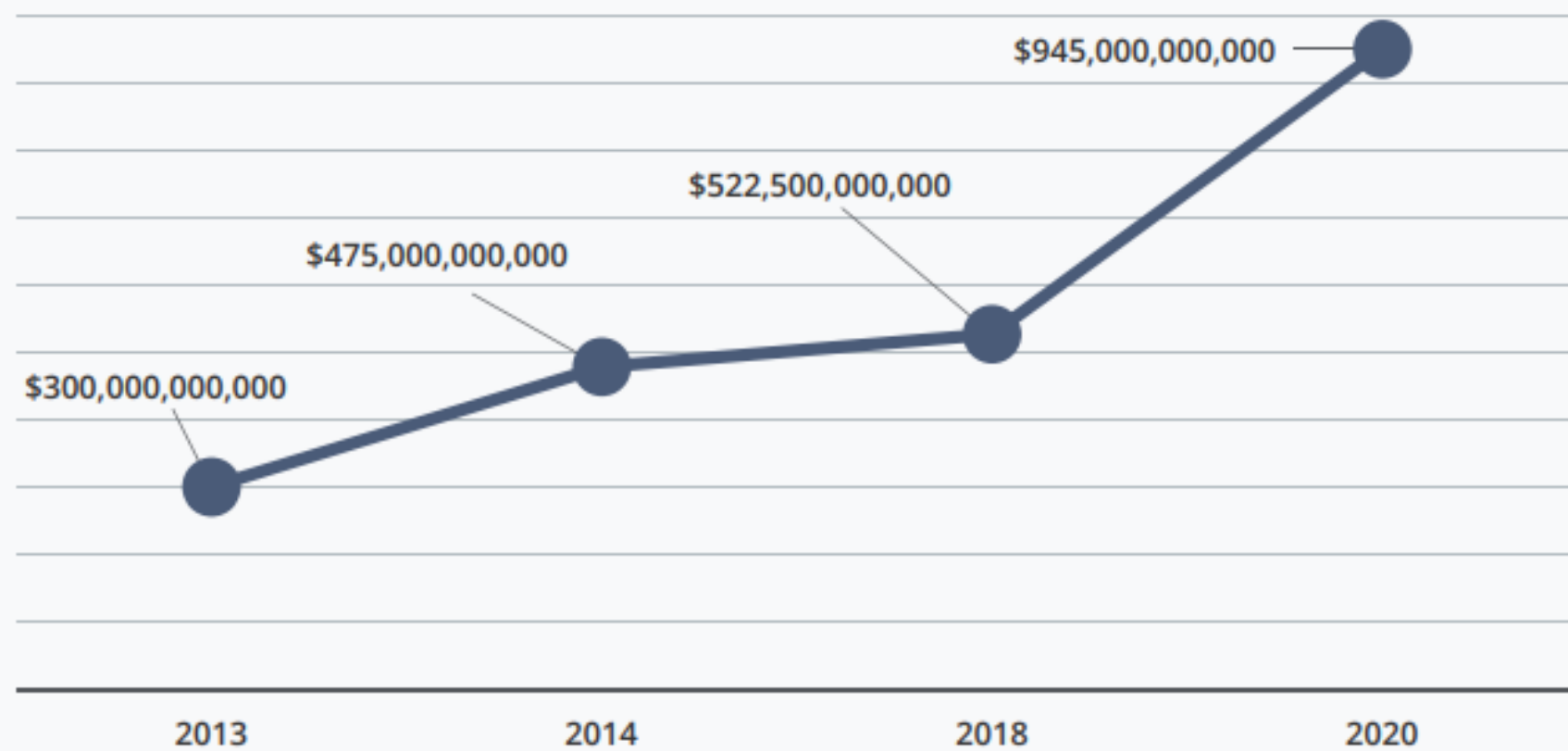
745k+
Số máy bị nhiễm virus
đánh cắp tài khoản

286k+
Số máy bị tấn công
APT

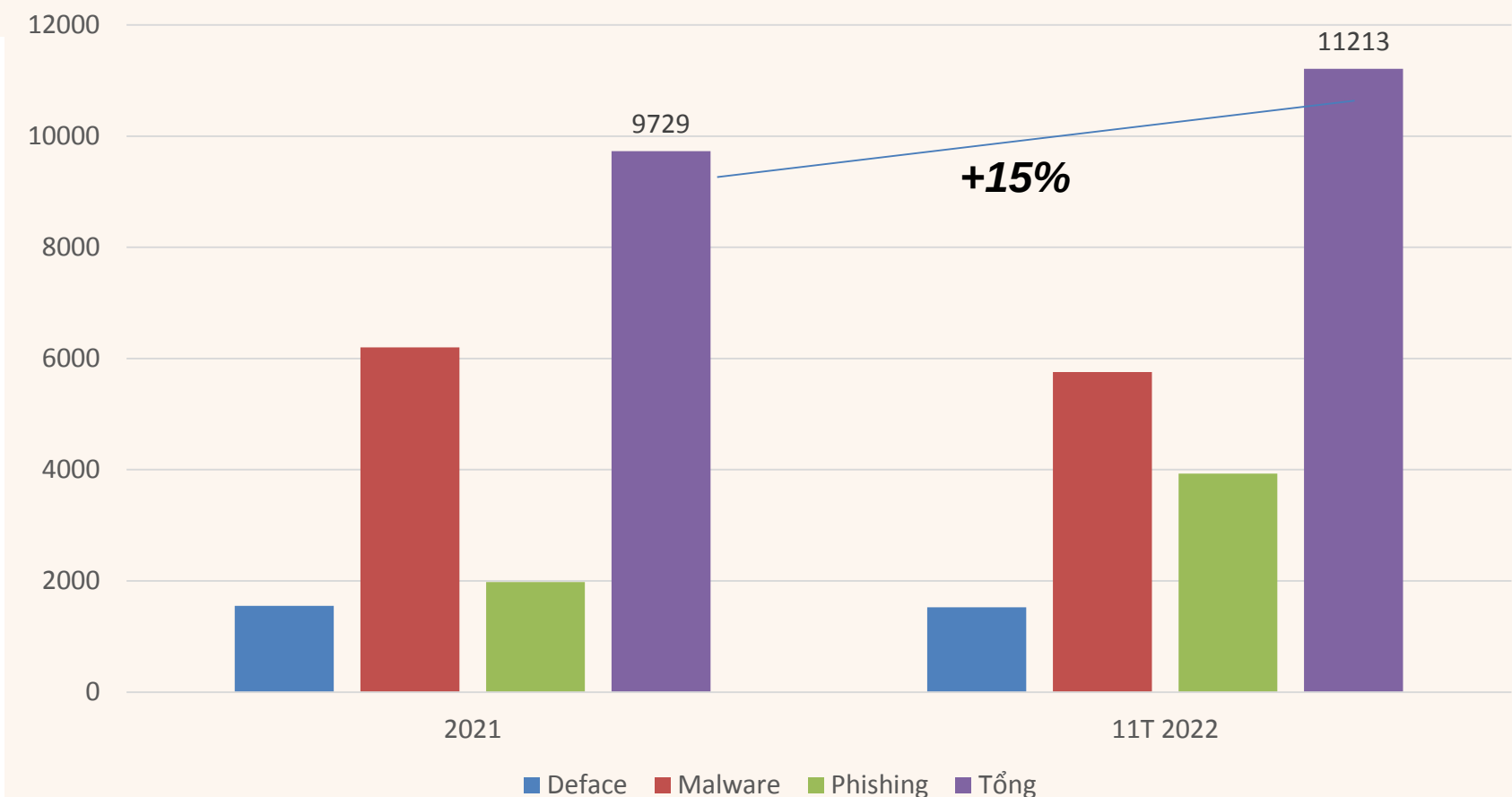
19k+
Số Server
bị tấn công

TÌNH HÌNH AN TOÀN THÔNG TIN

Thiệt hại do tội phạm mạng (**)



Thống kê tấn công vào websites Việt Nam



An toàn mạng đến 2025

DOANH THU (*)

- **352** tỷ USD.
- Tăng trưởng 14,5%/năm.

NHÂN LỰC

06 triệu
gấp 2 năm 2020

ĐỐI TƯỢNG

Đối tượng bị tấn công:
- **2025**: gấp 2,7 lần 2020.
- **2030**: gấp 7,5 lần 2020.

NGUY CƠ

- **3.000** cuộc tấn công/giây
- **12** mã độc/giây
- **70** lỗ hổng mới/ngày

- Tấn công mạng quy mô, chuyên nghiệp
- ATTT chuỗi cung ứng
- Ảnh hưởng của công nghệ, AI
- Bùng nổ thiết bị IoT
- Thiếu hụt nguồn nhân lực ATTT

QUAN ĐIỂM VỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ

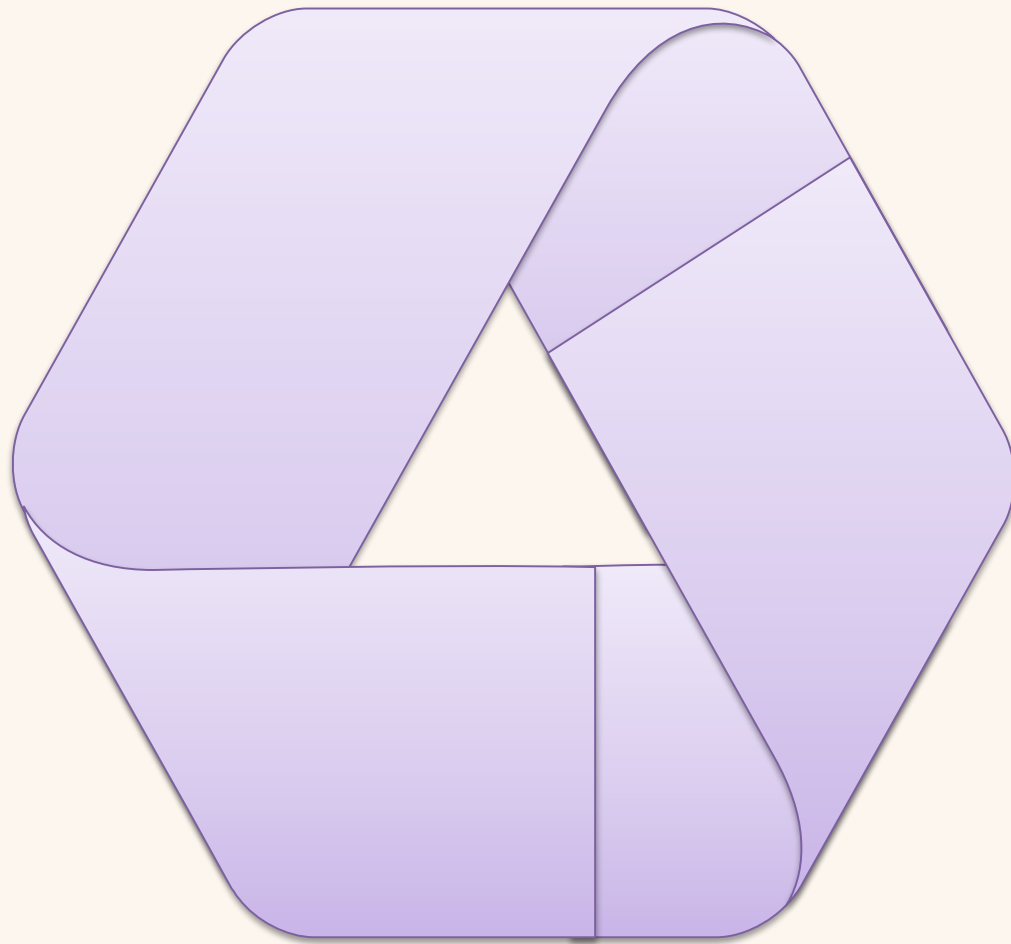


Quyết định 749/QĐ-TTg ngày 03/6/2020 Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030

Bảo đảm an toàn, an ninh mạng là **then chốt** để chuyển đổi số **thành công** và **bền vững**, đồng thời là phần **xuyên suốt**, không thể tách rời của chuyển đổi số.

Mọi thiết bị, sản phẩm, phần mềm, hệ thống thông tin, dự án đầu tư về công nghệ thông tin đều có **cấu phần bắt buộc về an toàn, an ninh mạng** ngay **từ khi thiết kế**.

NỘI DUNG VỀ ĐẢM BẢO AN TOÀN THÔNG TIN TRONG CHUYỂN ĐỔI SỐ



Chỉ thị 02/CT-TTg ngày 26/4/2022 về phát triển chính phủ điện tử hướng tới chính phủ số, thúc đẩy chuyển đổi số quốc gia

Có 04 nội dung cần lưu ý về an toàn thông tin:

1. Hệ thống thông tin cần **triển khai đầy đủ** phương án bảo đảm an toàn thông tin theo cấp độ.
2. Phần mềm nội bộ phải **do đơn vị chuyên nghiệp** phát triển, tuân thủ Khung phát triển phần mềm an toàn DevSecOps
3. Hệ thống thông tin được kiểm tra, đánh giá an toàn thông tin mạng **trước khi đưa vào sử dụng**, khi nâng cấp, thay đổi, định kỳ theo quy định.
4. Hệ thống thông tin được quản lý, vận hành theo **mô hình 4 lớp**

CHIẾN LƯỢC AN TOÀN, AN NINH MẠNG QUỐC GIA



Quyết định 964/QĐ-TTg ngày 10/08/2022 Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

Quan điểm: liên quan chuyển đổi số

- + An toàn, an ninh mạng là trọng tâm của quá trình chuyển đổi số, là trụ cột quan trọng tạo lập niềm tin số và sự phát triển thịnh vượng trong kỷ nguyên số.
- + ATANM là nhiệm vụ trọng yếu, thường xuyên, lâu dài nhằm khởi tạo và duy trì môi trường mạng an toàn, lành mạnh, tin cậy cho các cơ quan, tổ chức, doanh nghiệp và mỗi người dân.
- + Đầu tư cho ATANM là đầu tư cho phát triển bền vững và tạo ra giá trị.

CHIẾN LƯỢC AN TOÀN, AN NINH MẠNG QUỐC GIA



Quyết định 964/QĐ-TTg ngày 10/08/2022 Phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030

Mục tiêu:

c) Hình thành lực lượng bảo đảm an toàn, an ninh mạng tại các bộ, ngành, cơ quan nhà nước, các tổ chức chính trị – xã hội và các tập đoàn, tổng công ty nhà nước; đảm bảo mỗi cơ quan, tổ chức, doanh nghiệp nhà nước có một bộ phận được giao làm nhiệm vụ làm đầu mối, chịu trách nhiệm về công tác bảo đảm an toàn, an ninh mạng. Khuyến khích các doanh nghiệp khác có một đơn vị bảo đảm an toàn, an ninh mạng.

d) Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, UBND tỉnh, thành phố ...thực hiện bảo đảm an toàn, an ninh mạng theo quy định của pháp luật về an toàn thông tin và an ninh mạng.

đ) Bảo vệ hệ thống thông tin của 11 lĩnh vực quan trọng

NÂNG CAO NĂNG LỰC ĐỘI ỨNG CỨU SỰ CỐ



ĐỘI ỨNG CỨU SỰ CỐ

Chỉ thị 18/CT-TTg ngày 13/10/2022 về Đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam

Nguyên tắc: “Ứng cứu sự cố an toàn thông tin mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn thông tin mạng”.

Trách nhiệm các Bộ, ngành, địa phương:

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải **chuyển từ bị động sang chủ động**: sẵn lòng mỗi nguy hại và rà quét lỗ hổng 6 tháng 1 lần; hoàn thành phương án kịch bản ứng cứu sự cố; diễn tập thực chiến 1 lần/năm đối với HTTT từ cấp độ 3 trở lên.
- Kiến toàn lại Đội Ứng cứu sự cố theo hướng **chuyên nghiệp, cơ động, có tối thiểu 05 chuyên gia ATTTM**
- 11 lĩnh vực quan trọng (QĐ 632/QĐ-TTg 2017) cần ưu tiên đảm bảo ATTTM, triển khai mô hình CERT lĩnh vực
- Đội Ứng cứu sự cố được giao các **nhiệm vụ thường xuyên**

TRIỂN KHAI BẢO ĐẢM AN TOÀN TRONG CÁC TỔ CHỨC



Xây dựng và triển khai **“Chương trình đảm bảo ATTT”** của tổ chức:

- Đáp ứng các **yêu cầu luật định**
- **Chiến lược ATTT** phù hợp với chiến lược của doanh nghiệp
- Ban hành **chính sách ATTT**
- Phát triển **Nguồn nhân lực CNTT, ATTT + nâng cao nhận thức ATTT** cho tất cả nhân viên
- **Quản lý rủi ro**
- Triển khai **Quản lý an toàn** theo chuẩn
- Xây dựng và duy trì **Kế hoạch ứng phó**
- Duy trì **vận hành đảm bảo an toàn**
- Triển khai các **Cơ chế bảo vệ cụ thể** - các sản phẩm, giải pháp bảo mật, đảm bảo an toàn

Bảo đảm an toàn thông tin mạng là bảo đảm tính bí mật, tính toàn vẹn, tính chống chối bỏ và tính sẵn sàng của thông tin, trong đó:

Tính bí mật: Bảo đảm thông tin chỉ có thể được truy cập bởi những người có thẩm quyền đối với thông tin.

Ví dụ: một giao dịch tín dụng qua Internet, số thẻ tín dụng được gửi từ người mua hàng đến người bán, và từ người bán đến nhà cung cấp dịch vụ thẻ tín dụng. Hệ thống sẽ cố gắng thực hiện tính bí mật bằng cách **mã hóa** số thẻ trong suốt quá trình truyền tin, giới hạn nơi nó có thể xuất hiện (cơ sở dữ liệu, log file, sao lưu (backup), in hóa đơn...) và bằng việc **giới hạn truy cập** những nơi mà nó được lưu lại. Nếu một bên không được xác thực (ví dụ người dùng không có trong giao dịch, hacker...) lấy số thẻ này bằng bất kì cách nào, thì tính bí mật không còn nữa.



Tính bí mật

rất cần thiết (nhưng chưa đủ) để trì sự riêng tư của người có thông tin được hệ thống lưu giữ.





Tính toàn vẹn: Thông tin không bị sửa đổi làm sai lệch nội dung.

Đảm bảo tính toàn vẹn của thông tin nghĩa là chỉ người có thẩm quyền mới được chỉnh sửa thông tin nhưng không làm thay đổi sự chính xác của dữ liệu. Về điểm này, nhiều người thường hay nghĩ toàn vẹn thông tin chỉ đơn giản bảo đảm thông tin không bị thay đổi là chưa đầy đủ.



Trong an toàn thông tin, toàn vẹn có nghĩa rằng dữ liệu không thể bị chỉnh sửa mà không bị phát hiện. Tính toàn vẹn bị xâm phạm khi một thông điệp bị chỉnh sửa trong giao dịch. Hệ thống thông tin an toàn luôn cung cấp các thông điệp toàn vẹn và bí mật.



Ví dụ: những trường hợp sau **tính toàn vẹn** của thông tin bị phá vỡ như:

- + Trang thông tin bị hacker thay đổi giao diện, điều chỉnh thông tin.
- + Chỉnh sửa trái phép tệp lưu trên máy tính.
- + Do sự cố trên đường truyền mà tính hiệu bị nhiễu hoặc suy hao dẫn đến thông tin không còn chính xác.



Tính khả dụng hay tính sẵn sàng: Bảo đảm những người được cấp quyền có thể truy cập sử dụng thông tin ngay khi có nhu cầu.

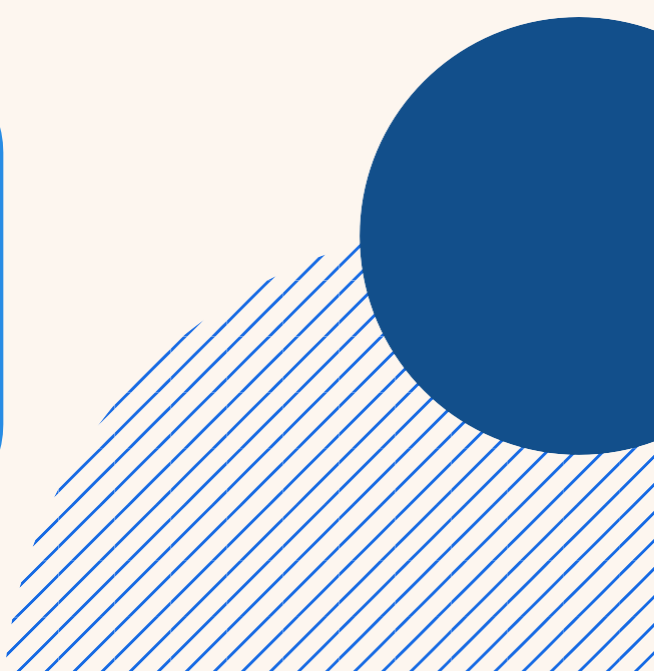


Mọi hệ thống thông tin đều phục vụ mục đích riêng của nó và thông tin phải luôn luôn sẵn sàng khi cần thiết.

Điều đó có nghĩa rằng hệ thống thông tin được thiết lập để lưu trữ và xử lý thông tin, và có một hệ thống các giải pháp an toàn thông tin sử dụng để bảo vệ hệ thống thông tin đó, bảo đảm kênh kết nối phải luôn sẵn sàng và hoạt động chính xác.



Hệ thống có tính sẵn sàng cao hướng đến sự sẵn sàng ở mọi thời điểm, tránh được những rủi ro cả về phần cứng, phần mềm như: sự cố mất điện, hỏng phần cứng, cập nhật, nâng cấp hệ thống thông tin... đảm bảo tính sẵn sàng cũng có nghĩa là tránh được tấn công từ chối dịch vụ.



Tính chống chối bỏ: có nghĩa rằng một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác.



Ví dụ: trong khi giao dịch mua hàng qua mạng, khi khách hàng đã gửi số thẻ tín dụng cho bên bán, đã thanh toán thành công, thì bên bán không thể phủ nhận việc họ đã nhận được tiền, (trừ trường hợp hệ thống không đảm bảo tính an toàn thông tin trong giao dịch).

Tình hình an toàn trên không gian mạng luôn có những **diễn biến phức tạp, khó lường**.

Các cuộc tấn công vào hệ thống mạng công nghệ thông tin **không ngừng tăng** cả về số lượng, cường độ và tính phức tạp.

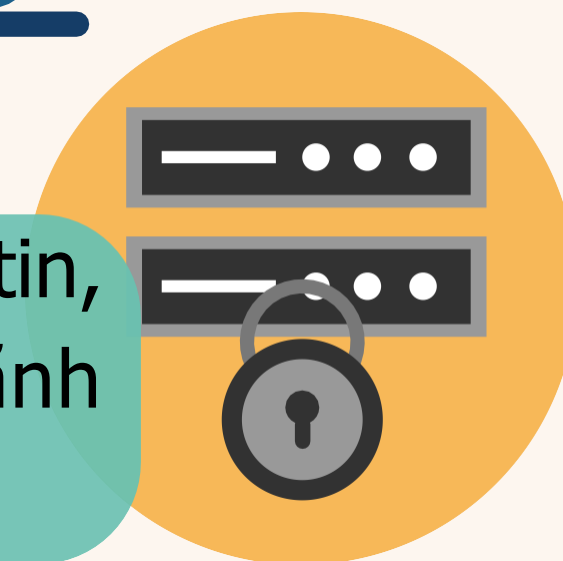
Các nhóm tội phạm mạng ngày một gia tăng với sự hỗ trợ mạnh mẽ của các tổ chức kinh tế, chính trị,... và **nguy cơ chiến tranh mạng** đang hiện hữu, đe dọa hòa bình và an ninh thế giới, chủ quyền quốc gia dân tộc.



Nhiều quốc gia trên thế giới đã **phát triển lực lượng tác chiến mạng**, sẵn sàng tham gia, đối phó với chiến tranh mạng.

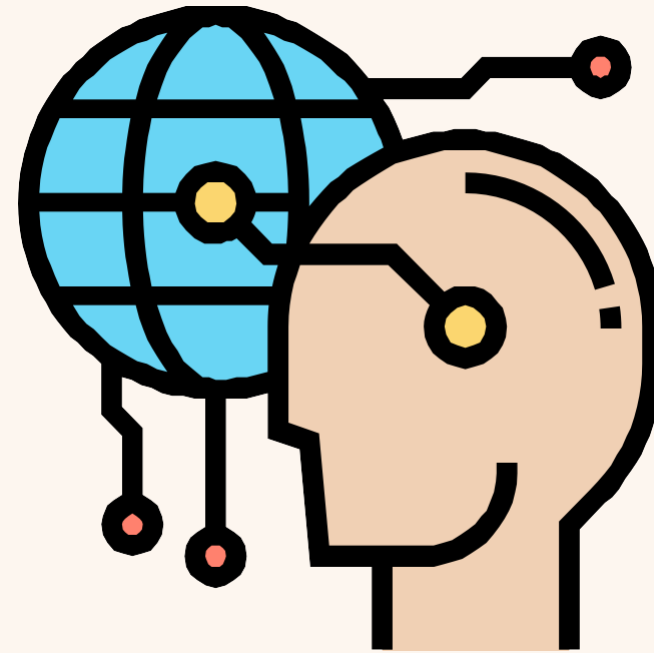


Vì vậy, vấn đề bảo đảm an toàn trên không gian mạng không chỉ là bảo vệ thông tin, hệ thống thông tin mà còn là bảo vệ chủ quyền quốc gia, bảo vệ chủ quyền lãnh thổ, vùng đất, vùng biển, vùng trời... mà còn là chủ quyền trên không gian mạng.



2.1. Một số sự cố tiêu biểu trên không gian mạng thời gian gần đây

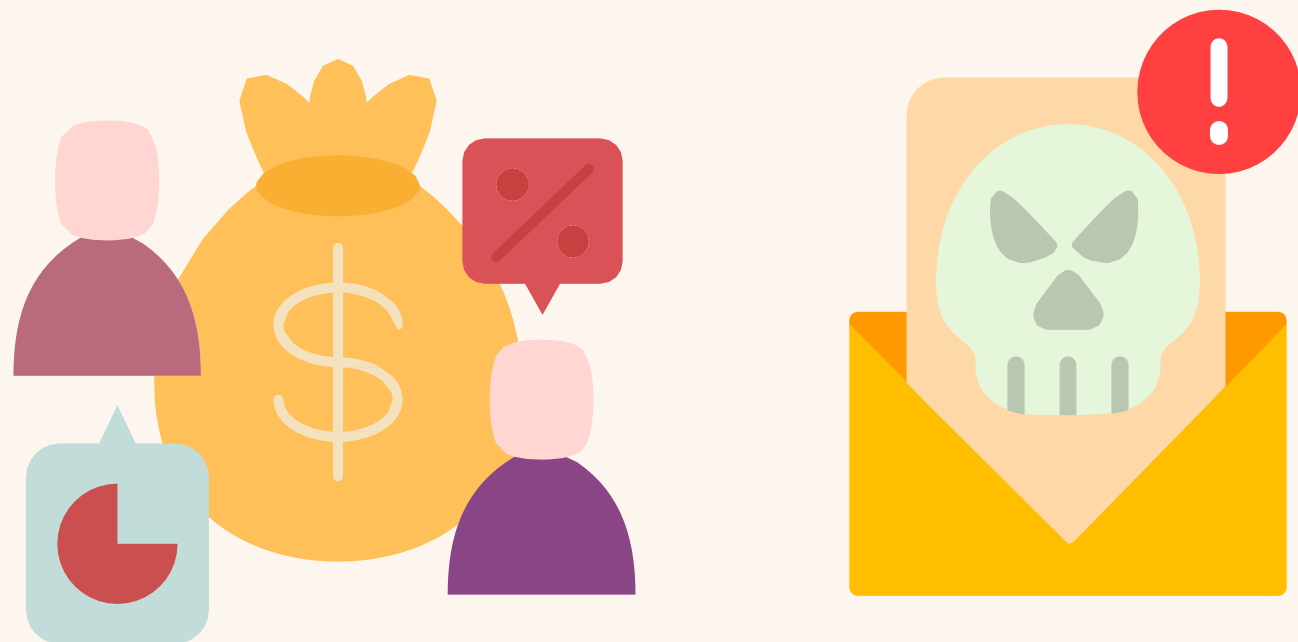
Có thể thấy, không gian mạng mang cơ hội để **phát triển kinh tế - xã hội** nhưng cũng **tiềm ẩn** không ít nguy cơ, rủi ro mất an toàn thông tin mạng. Một quốc gia sẽ không an toàn nếu không gian mạng của quốc gia đó không an toàn. Người sử dụng không gian mạng phải **đối mặt** với nhiều nguy cơ, mỗi đe dọa sẽ dần dẫn đến tình trạng lo sợ và mất niềm tin đối với không gian mạng.



Các cuộc tấn công mạng gây sự cố lớn gần đây như vụ Solar Winds ảnh hưởng đến **16.000** hệ thống thông tin trên toàn thế giới, nạn nhân bao gồm cả các cơ quan quan trọng của Hoa Kỳ như: Bộ Ngoại giao, Bộ An ninh nội địa, Bộ Tài chính.



Hay vụ tấn công bằng **mã độc tổng tiền** (ransomware) vào công ty đường ống nhiên liệu lớn nhất Hoa Kỳ - Colonial Pipeline - làm **ngưng trệ** hoạt động của đường cung cấp nhiên liệu cho hơn 50 triệu khách hàng buộc Tổng thống quốc gia này phải ban hành sắc lệnh hành pháp nhằm tăng cường khả năng phòng thủ không gian mạng.



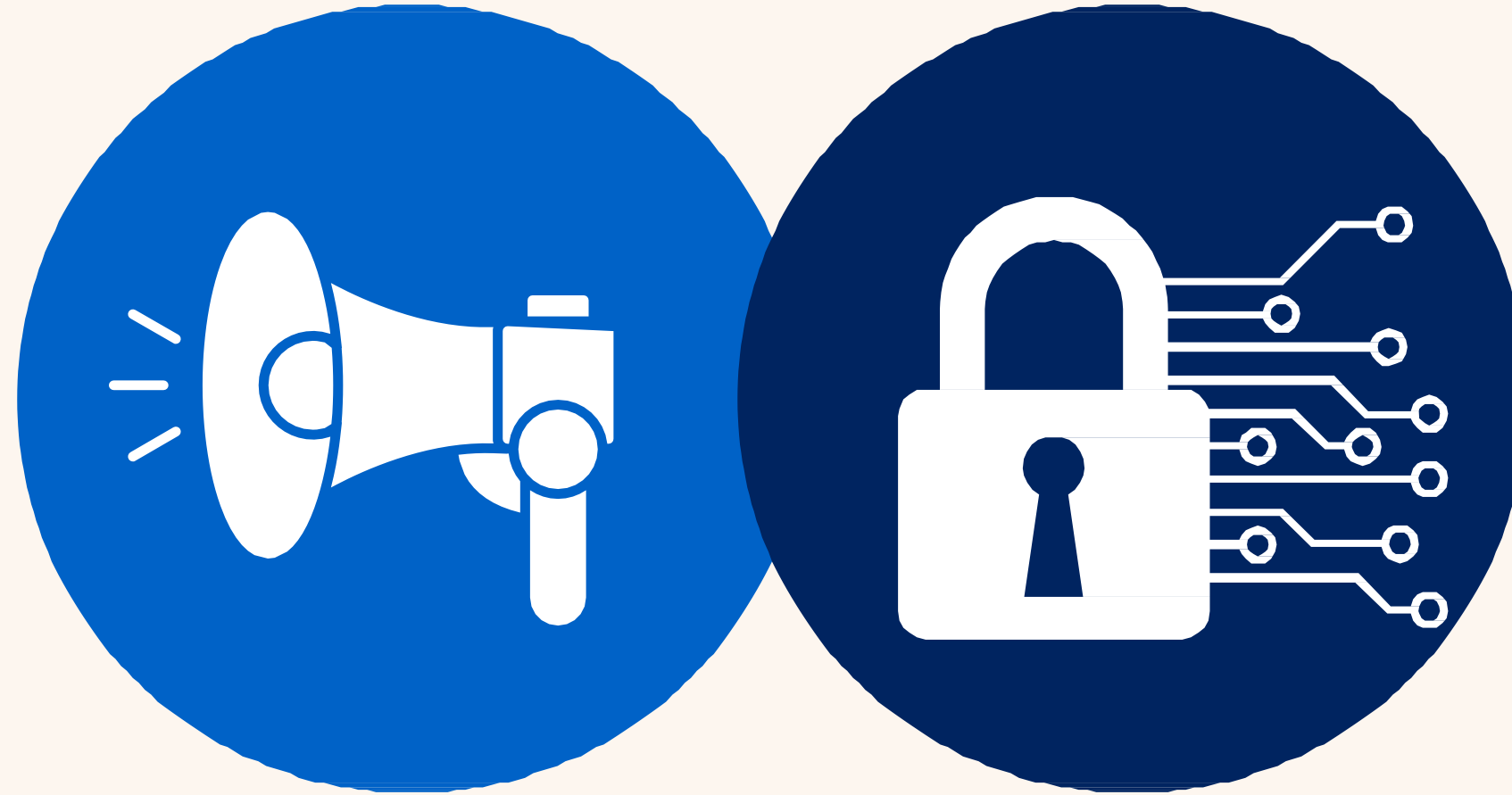
Và mới đây nhất, năm 2022 hơn **1,2 triệu thẻ ngân hàng** trên thế giới bị đánh cắp thông tin. Dữ liệu bị rò rỉ bao gồm **1,2 triệu hồ sơ** có chứa số thẻ, ngày hết hạn, mã bảo mật 3 chữ số được in ở mặt sau của thẻ (CVV), tên chủ thẻ, tên ngân hàng liên quan, địa chỉ đầy đủ, ngày sinh, email và số điện thoại. Quy mô dữ liệu bị đánh cắp trải rộng toàn thế giới.

4. Mỗi người cần làm gì để sống an toàn trên môi trường số.

1. Một số kỹ năng bảo đảm an toàn thông tin cá nhân trên môi trường số

Đối với bất kỳ người dùng dù là ai (giáo viên, học sinh, bác sĩ, kỹ sư... hay cả những chuyên gia an toàn thông tin), khi đã sử dụng Internet sẽ phải **đôi mắt** với các nguy cơ mất an toàn thông tin, tuy nhiên nếu mỗi cá nhân có kiến thức và kỹ năng về an toàn thông tin trên môi trường số thì cũng đã **hạn chế** được 80% các nguy cơ này.





Thứ nhất: Nâng cao nhận thức, hiểu biết các nguy cơ, tình huống **mất an toàn thông tin** có thể xảy ra đối với mình, đặc biệt là các nguy cơ đã đề cập trong tài liệu này; từ đó có những **phản xạ** để **nâng cao cảnh giác, đề phòng** tránh khỏi các tình huống mất an toàn thông tin mà nguyên nhân xuất phát từ chính mình;

Thứ hai: Thực hiện **bảo đảm an toàn** cho máy tính, tiết bị di động sử dụng để truy cập Internet: chúng ta cần cài đặt, thiết lập tính năng **bảo mật** có sẵn của thiết bị, và sử dụng thêm một số phần mềm ứng dụng bảo đảm an toàn thông tin (như phần mềm diệt virus);

Thứ ba: Khi sử dụng bất kỳ dịch vụ nào trên Internet (thông qua trình duyệt, hoặc các ứng dụng - app cài đặt trên máy tính, điện thoại) cần phải **tìm hiểu kỹ** thông tin về nhà cung cấp dịch vụ, các tính năng hỗ trợ bảo đảm an toàn thông tin cho người dùng và cách sử dụng các tính năng đó.



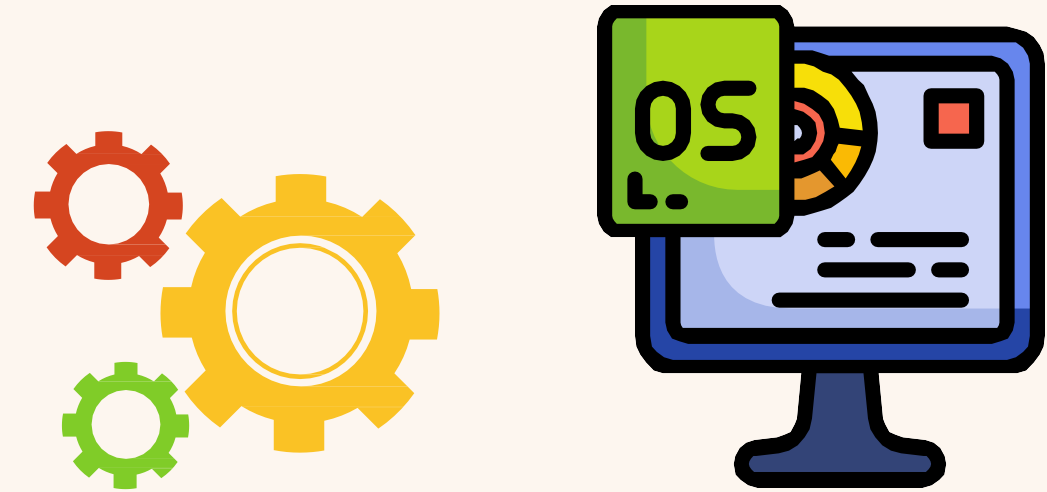
Thứ tư: Tìm hiểu và có sẵn các kênh để có thể hỏi và được **tư vấn, hoặc hỗ trợ xử lý** khi gặp các vấn đề an toàn thông tin trên không gian mạng.



Một số nguyên tắc chung để bảo đảm an toàn thông tin cho thiết bị cá nhân:

Nguyên tắc 1: Cập nhật phần mềm:

Rất nhiều người có suy nghĩ rằng việc **cập nhật phần mềm** sẽ tốn nhiều thời gian và gây phiền nhiễu. Trong một số trường hợp thì đúng là như vậy, nhưng nó vẫn là hình thức **bảo vệ quan trọng** nhất để chống lại các hacker.



Có thể nói, phần mềm hoạt động trên tất cả các loại thiết bị, như:

- Các hệ điều hành **Windows** hoặc **MacOS** cài trên máy tính hoặc máy tính xách tay.
- Các hệ điều hành **Android** hoặc **iOS** được cài đặt trên các thiết bị di động.

Nguyên tắc 2: đặt mật khẩu mạnh:



 Username

 Password

Login

☐ Remember me [Forgot password?](#)

Các trang web và các ứng dụng thường yêu cầu bạn sử dụng **mật khẩu kết hợp** giữa chữ cái và chữ số. Nhưng trên thực tế thì nó **khá dễ dàng** bị bẻ khóa bởi các hacker và đó là lý do tại sao bạn nên cân nhắc sử dụng **cụm mật khẩu** (passphrases) thay vì mật khẩu. Những cụm từ dài nhưng dễ nhớ, đó là hai điều kiện **tiên quyết** để có một mật khẩu mạnh.



Cách tốt nhất để lưu mật khẩu:



Sử dụng trình quản lý mật khẩu.

Viết mật khẩu và giữ nó ở nơi an toàn để đảm bảo bạn không bao giờ mất khả năng truy cập vào trình quản lý mật khẩu của mình.

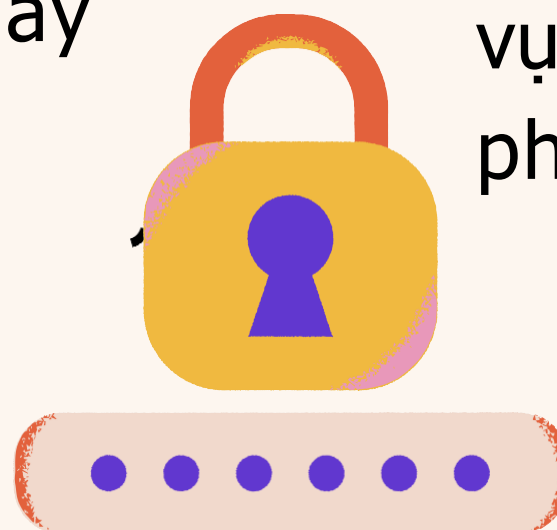
Sử dụng cụm mật khẩu (passphrase).

Sử dụng trình quản lý mật khẩu để tạo và lưu trữ các mật khẩu ngẫu nhiên có độ dài tối thiểu là 08 kí tự.



Theo dõi mật khẩu bị mất:

Cho dù mật khẩu của bạn có mạnh đến mức nào, nó vẫn có thể bị **đánh cắp**. Đó là lý do tại sao điều quan trọng là phải kiểm tra xem mật khẩu của bạn có bị hacker đánh cắp hay không.



Xác thực hai yếu tố:

Để hạn chế hậu quả khi bị mất mật khẩu, bạn có thể sử dụng **cơ chế xác thực hai nhân tố (2 FA)**, đây là một phương pháp bảo mật tương đối mới. Bạn có thể **kích hoạt** xác thực hai nhân tố thông qua các dịch vụ bạn sử dụng, nếu chúng hỗ trợ phương pháp này.



Lưu ý về biểu tượng khóa (nhưng đừng tin tuyệt đối):

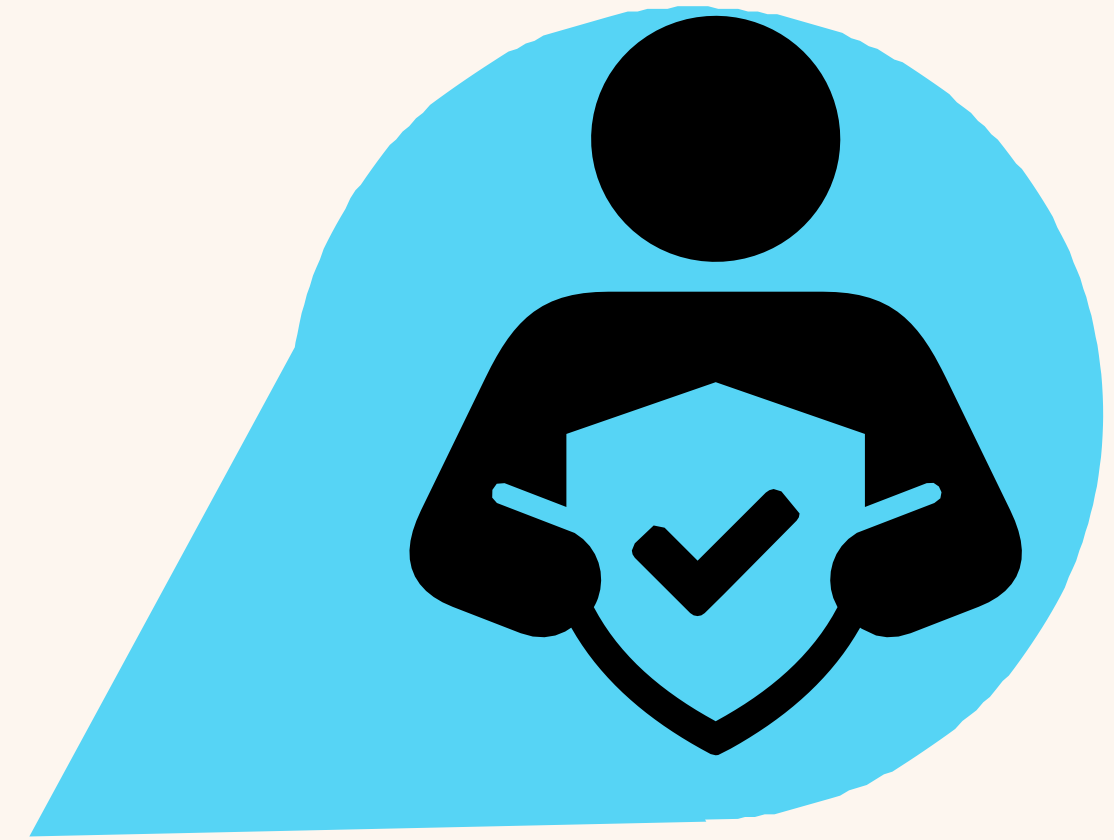
Biểu tượng khóa tại thanh địa chỉ của trình duyệt web cho biết bạn đang **sử dụng kết nối được mã hóa**. Điều này có nghĩa là thông tin bạn đang nhập vào trang web, ví dụ như mật khẩu hoặc thông tin thẻ tín dụng của bạn, sẽ được gửi đi một cách an toàn và **không thể bị chặn** bởi hacker. Vì vậy, hãy nhớ rằng bạn chỉ nhập thông tin nhạy cảm trên các trang web hiển thị biểu tượng khóa này tại thanh địa chỉ. Nếu một địa chỉ trang web bắt đầu bằng **https://**, thì đồng nghĩa đây là địa chỉ an toàn.



Tuy nhiên, cũng lưu ý rằng biểu tượng khóa không có nghĩa là bạn thực sự có thể **tin tưởng trang web** bạn đang truy cập. Rất nhiều trang web lừa đảo cũng sử dụng biểu tượng khóa như vậy để lấy được lòng tin của bạn, qua đó sẽ tìm cách **ăn cắp thông tin** đăng nhập của bạn. Hãy chú ý hơn đến địa chỉ của trang web và kiểm tra lại xem nó có chính xác hay không.

Nguyên tắc 3: Thực hiện sao lưu:

Bảo vệ dữ liệu quan trọng bằng cách **sao lưu** chúng vào ổ cứng ngoài hoặc hệ thống lưu trữ trên hạ tầng đám mây. Trường hợp thiết bị của bạn bị **nhễm phần mềm độc hại hoặc bị truy cập bởi hacker**, dữ liệu của bạn có thể bị hỏng, bị **xóa hoặc mã hóa** đòi tiền chuộc ransomware.



Tuy nhiên, để việc sao lưu, phục hồi dữ liệu **hiệu quả** cần lưu ý một số nội dung sau:

-Đảm bảo thiết bị di động, ổ cứng ngoài sử dụng để sao lưu dữ liệu **tách biệt** với thiết bị đang sử dụng (Không kết nối liên tục qua dây cable vật lý hoặc mạng cục bộ)

-Sử dụng dịch vụ lưu trữ đám mây để lưu trữ một bản sao dữ liệu của mình ở nơi khác qua Internet



Nguyên tắc 4: Nhận biết lừa đảo:

Tấn công lừa đảo là một dạng tấn công phổ biến, tấn công trực diện vào sự thiếu hiểu biết của người dùng. Kẻ tấn công sử dụng các **mánh khóe lôi kéo** những người khác tiết lộ thông tin mà có thể được sử dụng để đánh cắp dữ liệu, truy cập vào hệ thống, truy cập vào điện thoại di động, tiền bạc, hoặc thậm chí thông tin riêng của bạn. Các tấn công như vậy có thể rất đơn giản hoặc rất phức tạp tùy vào mục tiêu, đối tượng tấn công.



Nguyên tắc 5: Hãy cẩn thận với tệp đính kèm và kiểm tra các tập tin bạn không tin tưởng



Tấn công bằng việc cài **mã độc, virus trong các tệp đính kèm** trong thư điện tử là phương thức tấn công phổ biến và **hiệu quả nhất** hiện nay. Không nên tải và mở chạy tệp ngay khi nhận được thư điện tử có tệp đính kèm.

Chú ý tới định dạng tệp và tạo thói quen **quét virus với các tệp đính kèm** trước khi mở chúng, đặc biệt là các tập tin đính kèm có đặt mật khẩu gửi kèm theo nhằm qua mặt các giải pháp bảo vệ ở lớp mạng.

Đặc biệt, cần cẩn trọng đối với những hộp thư có tệp gửi kèm từ những người lạ. Trường hợp người quen, nếu bạn nghi ngờ thì có thể **liên hệ** với người gửi trước khi mở những hộp thư này, bởi một số trường hợp, kẻ lạ đánh cắp hộp thư của một người nào đó để gửi thư lừa đảo.

Nguyên tắc 6: Cảnh giác với WiFi công cộng:

Trong những năm gần đây, mạng không dây ngày càng trở nên phổ biến, giá thành thấp và dễ sử dụng. Người dùng có thể lắp đặt để truy cập mạng không dây tại nhà hoặc sử dụng máy tính xách tay, thiết bị di động thông minh để truy cập tại những nơi công cộng như quán café, sân bay, khách sạn, v.v... Việc sử dụng mạng không dây sẽ rất **tiện lợi và đơn giản** nhưng nó cũng tiềm ẩn rất nhiều nguy cơ mất an toàn thông tin.



- Nếu mạng không dây không được bảo vệ đúng mức, đặc biệt trường hợp máy tính hoặc thiết bị di động của chúng ta chưa cập nhật các **lỗ hổng, điểm yếu** thì kẻ xấu có thể lợi dụng mạng không dây để tìm kiếm các thiết bị đang sử dụng trong mạng để cài cắm mã độc hoặc đánh cắp thông tin.

Nguyên tắc 7: Sử dụng VPN (mạng riêng ảo Virtual Private Network):



VPN là các kết nối mạng được **mã hóa**. Điều này cho phép người dùng từ xa truy cập an toàn từ xa vào các dịch vụ của tổ chức. VPN là một cách để đảm bảo **tính bảo mật** cho “dữ liệu truyền qua” trên một mạng không tin cậy, nhưng chúng cũng cung cấp một số lợi ích khác.

Ví dụ: Một tổ chức có văn phòng ở nhiều địa điểm có thể sử dụng VPN để **cung cấp** cho người dùng từ xa quyền truy cập vào các ứng dụng, dịch vụ hay thư điện tử của công ty, cơ quan qua mạng Internet công cộng.



Nguyên tắc 8: Nhớ thực hiện đăng xuất ứng dụng

Khi thực hiện đăng nhập sử dụng các dịch vụ trên mạng, hay liên kết với các tài khoản ngân hàng để thực hiện giao dịch với thiết bị công cộng, bạn nên **đăng xuất** sau khi sử dụng xong. Việc duy trì kết nối có thể biến bạn trở thành nạn nhân của tội phạm công nghệ thông qua các lỗ hổng bảo mật.

