CHƯƠNG TRÌNH PHỔ CẬP KỸ NĂNG SỐ

DÀNH CHO NGƯỜI DÂN

BÀI 6. ĐẢM BẢO AN TOÀN VÀ BẢO MẬT THÔNG TIN DỮ LIỆU TRÊN MÔI TRƯỜNG SỐ

MỤC LỤC

BÀI 6. ĐẢM BẢO AN TOÀN VÀ BẢO MẬT THÔNG TIN, DỮ LIỆU TRÊN MÔI TRƯỜNG SỐ

THÔNG TIN TỔNG QUAN

❖ Thời lượng

- Thời lượng lý thuyết: 02 Tiết.

- Thời lượng thực hành: 02 Tiết.

❖ **Hình thức dạy học**

- Trực tuyến kết hợp trực tiếp.

❖ **Đối tượng học**

- Người dân có nhu cầu nâng cao kỹ năng cơ bản và cần ứng dụng công nghệ số vào các hoạt động cá nhân và công việc hàng ngày.
- Yêu cầu: Người dân đã nắm vững các kỹ năng số cơ bản về sử dụng thiết bị, Internet.

❖ **Mục tiêu bài học**

Sau khi hoàn thành bài 6, người học có khả năng:

- Nắm được tầm quan trọng của việc bảo mật thông tin và dữ liệu cá nhân trên không gian số.
- Hiểu được các rủi ro phổ biến (như lừa đảo, mã độc) và hậu quả của việc mất an toàn thông tin.
- Nhận biết các loại hình tấn công mạng và thủ đoạn lừa đảo phổ biến trên mạng xã hội, email, tin nhắn.
- Biết cách sử dụng mật khẩu an toàn, thiết lập và quản lý mật khẩu mạnh, sử dụng xác thực hai yếu tố (2FA).
- Biết cách cài đặt quyền riêng tư, quản lý quyền truy cập ứng dụng và thiết lập các biện pháp bảo vệ thiết bị cơ bản.
- Có ý thức thận trọng, cảnh giác với các thông tin yêu cầu cung cấp dữ liệu cá nhân và các liên kết, tập tin lạ trên môi trường số.
- Có ý thức thường xuyên kiểm tra, cập nhật các biện pháp bảo mật cho thiết bị và tài khoản cá nhân.

NỘI DUNG BÀI HỌC

6.1. Bảo vệ thiết bị

6.1.1. Các quy tắc an toàn cơ bản khi thao tác với thiết bị số

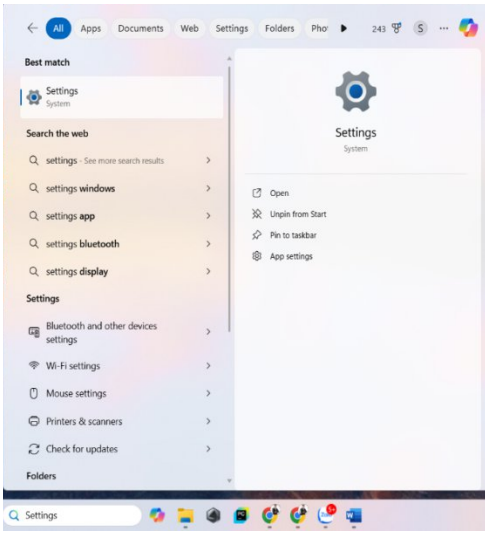
6.1.1.1.Cập nhật phần mềm và công cụ bảo mật tích hợp

Trong thời đại công nghệ số, các thiết bị như điện thoại thông minh, máy tính bảng, hay laptop không chỉ là công cụ liên lạc và làm việc mà còn lưu trữ nhiều thông tin cá nhân quan trọng như tài khoản ngân hàng, ảnh gia đình, hoặc tài liệu công việc.

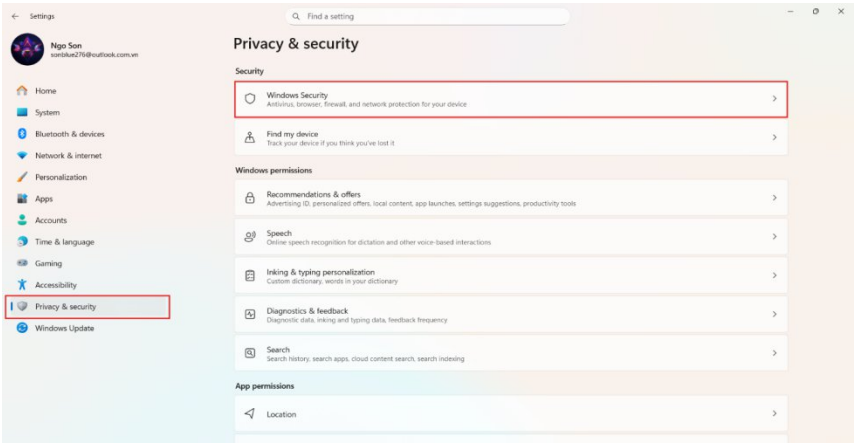
Tuy nhiên, những thiết bị này dễ bị tấn công bởi virus, phần mềm độc hại (malware), hoặc các chiêu trò lừa đảo trực tuyến (phishing), có thể gây mất dữ liệu, đánh cắp thông tin, hoặc làm hỏng thiết bị.

Virus và phần mềm độc hại là các chương trình được thiết kế để xâm nhập vào thiết bị, gây hại như làm chậm máy, xóa dữ liệu, hoặc đánh cắp thông tin cá nhân. Trên Windows đã được tích hợp sẵn phần mềm Windows Security (Windows Defender Antivirus), vì vậy có thể dễ dàng thực hiện việc quét virus mà không cần cài thêm phần mềm bên ngoài. Các bước tiến hành quét virus như sau:

- **Bước 1:** Tại thanh tìm kiếm của Windows, ta gõ **Settings**

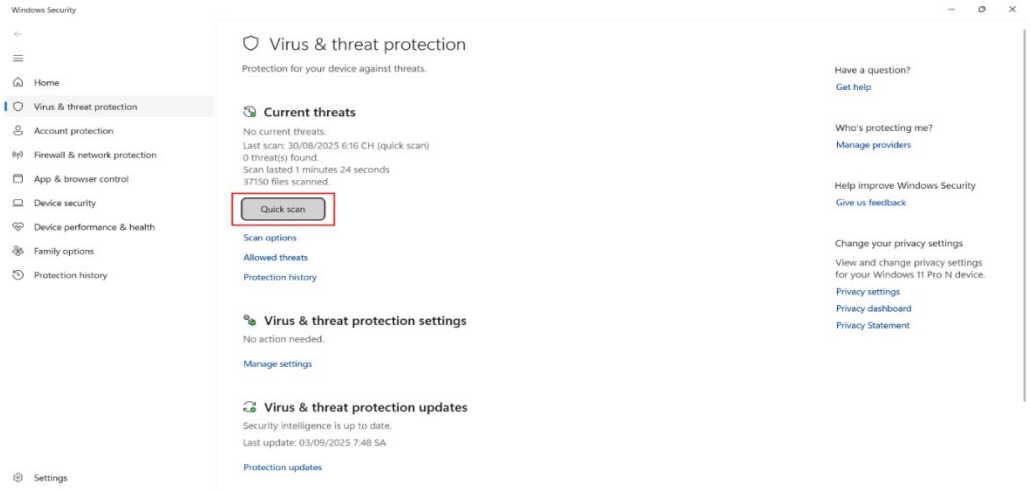


- **Bước 2:** Tại thanh menu bên trái chọn **Privacy & security**>**Windows Security**

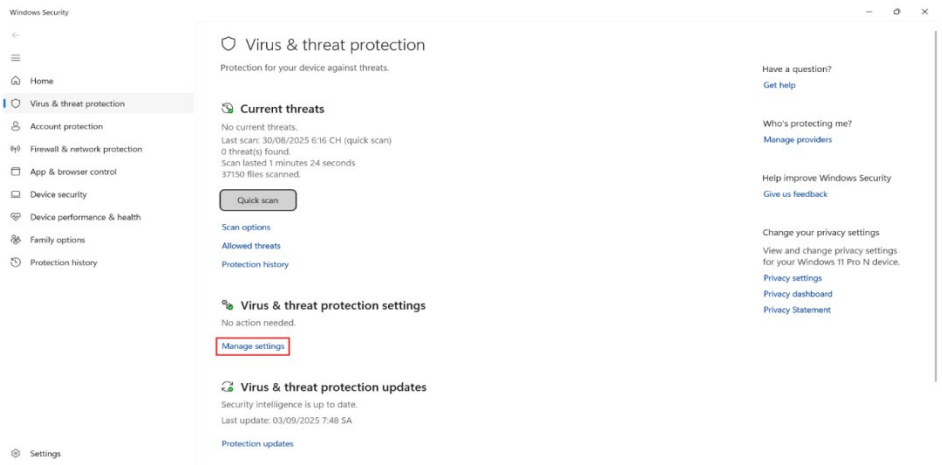


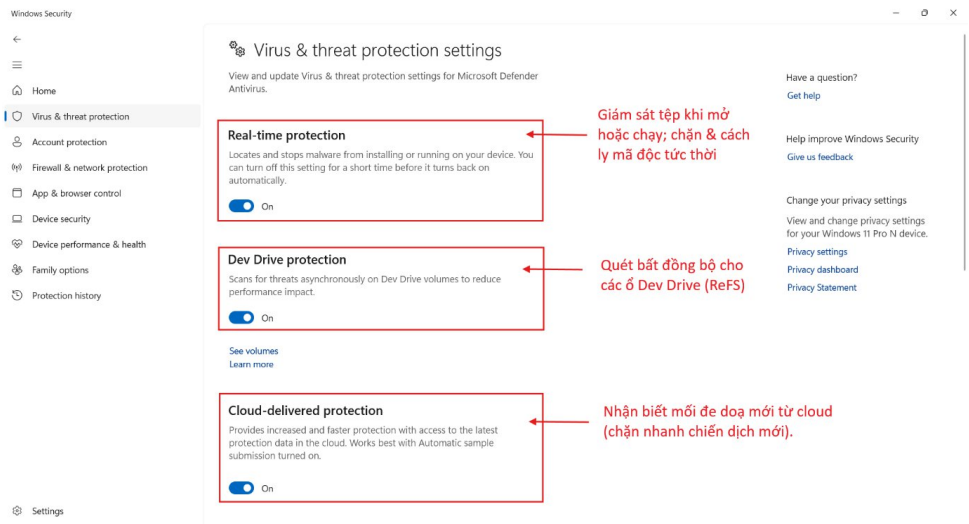
- **Bước 3:** Chọn **Virus & threat protection**

- **Bước 4:** Tại giao diện của **Virus & threat protection** chọn **Quick scan** để tiến hành quét nhanh



- **Bước 5:** Cấu hình thời gian tự động quét virus hoặc quét theo thời gian thực trong mục **Virus & threat protection setting**>**Manage setting**





❖ Cập nhật phần mềm- Tường chắn bảo mật vững chắc

Để đảm bảo thiết bị luôn được bảo vệ, hãy thực hiện các bước sau để cập nhật tự động cho hệ điều hành và ứng dụng của bạn:

Hệ điều hành	Hướng dẫn chi tiết
Windows	1. Mở Windows Update: Nhấn vào nút StartàCài đặt (biểu tượng bánh răng) àCập nhật và Bảo mậtàWindows Update. 2. Thiết lập: Đảm bảo hệ thống đang ở trạng thái Đã bật và kiểm tra các cài đặt nâng cao để cho phép tự động tải xuống. Lưu ý: Windows thường tự động cập nhật, bạn chỉ cần đảm bảo máy tính được kết nối Internet và khởi động lại khi có thông báo yêu cầu.
macOS	1. Mở cập nhật phần mềm: Nhấn vào menu Apple (góc trên bên trái) àTùy chọn hệ thống (System Settings/Preferences) àCài đặt chung (General) àCập nhật phần mềm (Software Update). 2. Thiết lập: Nhấn vào Nâng cao (Advanced) và đảm bảo các tùy chọn tự động cập nhật (Tự động kiểm tra cập nhật, Tải về khi có sẵn, Cài đặt tệp dữ liệu hệ thống) đều được bật.
Android	1. Cập nhật hệ điều hành: Vào Cài đặtàHệ thống (hoặc Thông tin điện thoại) àCập nhật phần mềm. Kiểm tra và thiết lập chế độ *Tự động tải xuống qua Wi-Fi*. 2. Cập nhật ứng dụng: Mở ứng dụng Google Play Storeà Nhấn vào biểu tượng Hồ sơ (góc trên bên phải) àCài đặtàƯu tiên mạngàTự động cập nhật ứng dụngàChọn Chỉ qua Wi-Fi.
iOS	1. Cập nhật hệ điều hành (iOS): Vào Cài đặtàCài đặt chungàCập nhật phần mềm. Trong mục này, chọn Tự động cập nhật và bật cả hai tùy chọn Tải về bản cập nhật iOS và Cài đặt bản cập nhật iOS. 2. Cập nhật ứng dụng: Vào Cài đặtàApp StoreàBật tùy chọn Cập nhật ứng dụng.
Trình duyệt web	Trình duyệt web (Chrome, Edge, Firefox, Safari) là cửa ngõ bạn dùng để vào mạng. Việc cập nhật chúng là cực kỳ quan trọng. Hầu hết các trình duyệt hiện đại đều tự cập nhật.

	Hành động kiểm tra: Mở trình duyệt àNhấn vào menu (thường là ba dấu chấm hoặc ba gạch) à Chọn Trợ giúp (Help) àGiới thiệu về [Tên Trình duyệt] (About [Browser Name]). Trình duyệt sẽ tự động kiểm tra và cập nhật nếu cần.

❖ **Sử dụng tường lửa và phần mềm chống virus**

- ***Quản lý tường lửa***

Tường lửa hoạt động như một người gác cổng, quyết định dữ liệu nào được phép vào và ra khỏi máy tính của bạn. Cả Windows và macOS đều có tường lửa tích hợp sẵn, bạn chỉ cần đảm bảo nó luôn được bật.

Hệ điều hành	Hướng dẫn chi tiết kiểm tra và bật tường lửa
Windows	1. Mở bảo mật: Nhấn vào nút StartàGõ tìm kiếm "Windows Security" (Bảo mật Windows) à Mở ứng dụng. 2. Kiểm tra trạng thái: Chọn Tường lửa & Bảo vệ mạng (Firewall & network protection). 3. Đảm bảo bật:Nếu thấy biểu tượng có dấu tick xanh và dòng chữ "Firewall is on" (Tường lửa đang bật) là an toàn. Nếu thấy cảnh báo, hãy nhấp vào để bật lại Tường lửa.
macOS	1. Mở cài đặt: Nhấn vào menu Apple (góc trên bên trái) àCài đặt Hệ thống (System Settings). 2. Kiểm tra tường lửa:Chọn mục Mạng (Network) hoặc Quyền riêng tư & Bảo mật (Privacy & Security) àTìm Tường lửa (Firewall). 3. Đảm bảo bật: Gạt nút gạt để đảm bảo Tường lửa đang ở trạng thái Bật (On).

- ***Quản lý phần mềm chống virus***

Hệ điều hành	Hướng dẫn chi tiết kiểm tra Sử dụng phần mềm chống Virus
Windows (Sử dụng Windows Defender)	1. Kiểm tra trạng thái: Mở ứng dụng Windows Security (Bảo mật Windows). 2. Chọn mục bảo vệ Virus: Chọn Bảo vệ khỏi virus và mối đe dọa (Virus & threat protection). 3. Kiểm tra bảo vệ: Đảm bảo Bảo vệ Thời gian thực (Real-time protection) đang ở trạng thái Bật (On). 4. Quét thiết bị: Bạn nên thỉnh thoảng nhấp vào Quét Nhanh (Quick Scan) để kiểm tra các khu vực dễ bị tấn công trên máy tính.
macOS	macOS có các cơ chế bảo mật tích hợp sâu như Gatekeeper và

	XProtect giúp chống lại mã độc. Người dùng macOS thường không bắt buộc phải cài đặt thêm phần mềm chống virus của bên thứ ba, nhưng vẫn nên: 1. Kiểm tra tệp tải về: Chỉ tải ứng dụng từ App Store hoặc các nhà phát triển đã được xác minh. 2. Thực hiện quét: Nếu cần thiết, bạn có thể sử dụng các phần mềm quét mã độc miễn phí uy tín (ví dụ: Malwarebytes) để kiểm tra thêm.
Điện thoại (Android/iOS)	Lưu ý: Trên điện thoại, việc cài đặt thêm phần mềm diệt virus không phổ biến bằng máy tính. 1. Android: Luôn sử dụng Google Play Protect (đã tích hợp sẵn trong Google Play Store) để quét ứng dụng. 2. iOS: Apple App Store có quy trình kiểm duyệt nghiêm ngặt, chỉ cần đảm bảo bạn không bẻ khóa (Jailbreak) thiết bị và chỉ tải ứng dụng từ App Store chính thức.

- ***Quy tắc an toàn khi lựa chọn phần mềm chống virus***
  - ✔ **Ưu tiên đã tích hợp sẵn:** Đối với máy tính, hãy tận dụng tối đa các công cụ bảo mật có sẵn trong hệ điều hành (như Windows Defender).
  - ✔ **Chọn lọc:** Nếu muốn sử dụng phần mềm bên thứ ba, hãy chọn các thương hiệu uy tín (ví dụ: Kaspersky, Norton, Bitdefender, Malwarebytes, Avast).
  - ✔ **Luôn cập nhật:** Dù bạn dùng phần mềm nào, hãy đảm bảo rằng cơ sở dữ liệu virus của nó luôn được cập nhật liên tục để nhận diện các loại mã độc mới nhất.

6.1.1.2. Một số quy tắc cơ bản khi sử dụng thiết bị và không gian số

a) Không cắm USB, ổ cứng hay thiết bị lạ vào máy tính khi chưa kiểm tra

Thận trọng là trên hết. Tuyệt đối không cắm USB không rõ nguồn gốc, không đáng tin cậy vào các máy tính chứa dữ liệu quan trọng. Nếu phải cắm USB lạ thì nên kiểm tra nội dung của một USB đó trước khi sử dụng bằng cách sử dụng một máy tính riêng biệt, cũ, không kết nối mạng và không chứa bất kỳ thông tin nhạy cảm nào.

Vô hiệu hóa Autorun: Tính năng Autorun (tự động chạy) trên Windows cho phép các chương trình trên thiết bị lưu trữ ngoài tự khởi động khi được kết nối, đây là một

cửa ngõ lây nhiễm virus phổ biến. Người dùng nên vô hiệu hóa tính năng này trong cài đặt hệ điều hành để tăng cường bảo mật.

Sử dụng thủ thuật phím Shift: Đây là một mẹo đơn giản nhưng hiệu quả. Bằng cách nhấn và giữ phím **Shift** trong khi cắm USB vào máy tính, bạn có thể tạm thời ngăn chặn tính năng Autorun, không cho các tệp độc hại có cơ hội tự thực thi.

Thực hiện quy trình quét virus: Luôn quét USB trước khi sử dụng bằng một phần mềm diệt virus uy tín (như Windows Defender có sẵn trên Windows). Hoặc thay vì nhấp đúp trực tiếp vào biểu tượng ổ USB trong "This PC", hãy truy cập nó một cách an toàn thông qua cây thư mục ở khung điều hướng bên trái của File Explorer. Thao tác này giúp tránh kích hoạt các tệp autorun.inf độc hại.

b) Sử dụng mạng Wi-Fi an toàn

Wi-Fi an toàn là những wifi được mã hoá mạnh, có mật khẩu phức tạp hoặc đã tắt tính năng WPS (Tính năng giúp kết nối nhanh). Wifi ở nhà hoặc văn phòng của bạn được cài đặt riêng để sử dụng được coi là các Wifi an toàn. Nhưng Wi-Fi công cộng ở quán cà phê, công viên hoặc sân bay thường không bảo mật, dễ bị hacker "nghe lén" và đánh cắp thông tin như tài khoản ngân hàng hoặc mật khẩu. Để tránh rủi ro, bạn chỉ kết nối Wi-Fi công cộng khi thật cần thiết, và nên dùng VPN (một ứng dụng bảo vệ như ExpressVPN miễn phí cơ bản) để mã hóa dữ liệu. Tại nhà, hãy đặt mật khẩu Wi-Fi phức tạp (kết hợp chữ, số và ký tự đặc biệt) và thay đổi định kỳ để tránh bị người lạ có thể xâm nhập kết nối được vào Wifi của gia đình. Nếu dùng điện thoại, có thể tắt tính năng tự động kết nối Wi-Fi để tránh tự kết nối với mạng lạ. ***Lưu ý rằng, khi làm việc quan trọng như chuyển tiền online, tốt nhất dùng dữ liệu di động (3G/4G/5G) thay vì Wi-Fi công cộng.***

6.1.2. Thiết lập và quản lý mật khẩu an toàn

6.1.2.1. Kỹ thuật tạo mật khẩu mạnh

Mật khẩu yếu hoặc dễ đoán là nguyên nhân chính khiến nhiều người bị hack tài khoản hoặc mất dữ liệu. Tội phạm mạng thường sử dụng các công cụ tự động để thử các mật khẩu phổ biến (như "123456", "password") hoặc dựa vào thông tin cá nhân (như ngày sinh, tên) để truy cập trái phép. Một mật khẩu mạnh, kết hợp chữ cái, số, và ký tự đặc biệt và đảm bảo độ dài, sẽ khó bị bẻ khóa hơn, giúp bảo vệ thiết bị và tài khoản trước các mối đe dọa như lừa đảo trực tuyến (phishing) hoặc phần mềm độc hại. *Kaspersky* (2025)(Kaspersky Team, 2025)nhấn mạnh rằng mật khẩu mạnh cần dài ít nhất 12 ký tự và không chứa thông tin cá nhân dễ đoán như tên hay ngày sinh.

Ngoài ra, việc không sử dụng cùng một mật khẩu cho nhiều tài khoản và thường xuyên thay đổi mật khẩu cũng giảm nguy cơ bị tấn công.

Mật khẩu mạnh là một chuỗi ký tự được thiết kế để chống lại các cuộc tấn công dò mật khẩu, dù là bằng phần mềm tự động hay bằng cách phán đoán thủ công. Nó giống như một chiếc chìa khóa có thiết kế độc nhất và phức tạp, khiến kẻ gian không thể dễ dàng sao chép hay bẻ gãy. Một mật khẩu được xem là mạnh khi hội tụ đủ các đặc điểm cốt lõi sau :

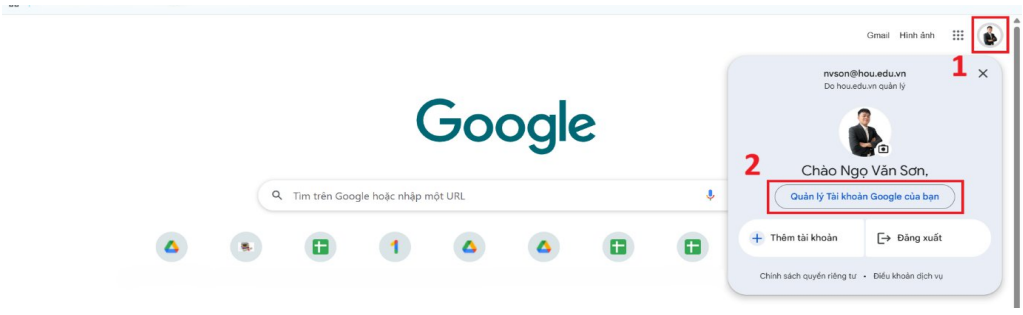
Độ dài: Mật khẩu càng dài thì càng an toàn. Độ dài tối thiểu được khuyến nghị là 12 ký tự, và tốt nhất là từ 14-16 ký tự trở lên. Mỗi ký tự được thêm vào sẽ làm tăng số lượng tổ hợp mà kẻ tấn công phải thử lên theo cấp số nhân, khiến việc bẻ khóa trở nên cực kỳ tốn thời gian và gần như bất khả thi.

Độ phức tạp: Một mật khẩu mạnh phải là sự kết hợp của ít nhất bốn loại ký tự khác nhau: chữ viết hoa (A, B, C), chữ viết thường (a, b, c), chữ số (1, 2, 3) và các ký tự đặc biệt (ví dụ:!, @, #, $, %). Sự đa dạng này phá vỡ các quy tắc và mẫu hình thông thường, làm cho các thuật toán dò mật khẩu trở nên kém hiệu quả.

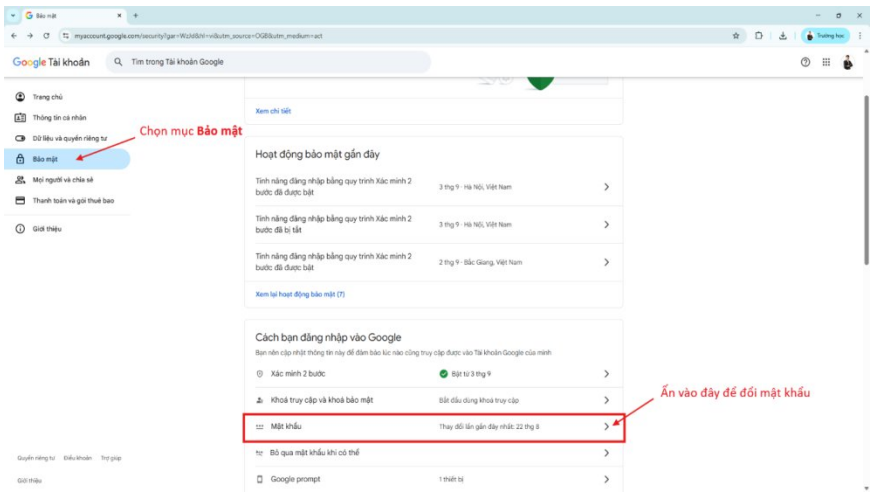
Ví dụ, thay vì dùng “Lan2000” (dễ đoán), hãy dùng “Lan@2023!khoMatkhau”. Bạn cũng nên sử dụng các công cụ quản lý mật khẩu (như LastPass hoặc trình duyệt Google Chrome) để lưu trữ an toàn mật khẩu phức tạp. Trên thiết bị, hãy đặt mật khẩu màn hình khóa (PIN, hình vẽ, hoặc mật khẩu chữ) để ngăn người lạ truy cập. Nếu nghi ngờ mật khẩu bị lộ, hãy thay đổi ngay lập tức. Các bước dưới đây sẽ hướng dẫn bạn cách đặt và quản lý mật khẩu trên Google Drive.

Các bước thực hiện để tạo/đổi mật khẩu mạnh trên tài khoản Google:

Bước 1: Mở trình duyệt Google Chrome. Tại giao diện chính của trang, bạn thực hiện ấn vào biểu tượng **Avatar** → Chọn **Quản lý tài khoản Google của bạn**.

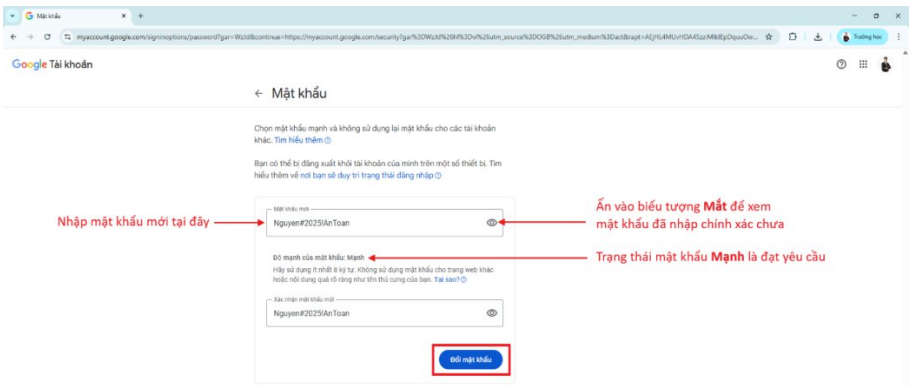


Bước 2: Ở cột trái, chọn **Bảo mật**. Kéo xuống phần **Cách bạn đăng nhập vào Google** → bấm mục **Mật khẩu**

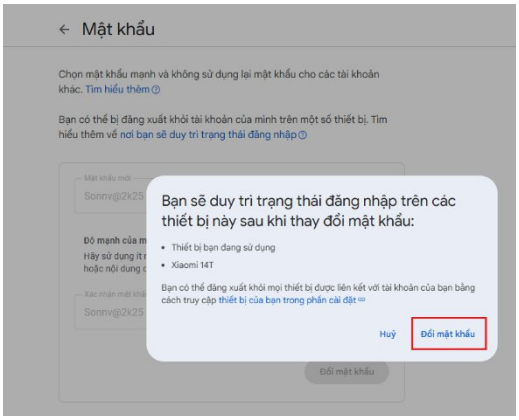


Bước 3: Màn hình yêu cầu nhập **Mật khẩu hiện tại** → gõ mật khẩu đang dùng → bấm **Tiếp theo**

Bước 4: Nhập mật khẩu mới. Ở ô **Mật khẩu mới**, nhập mật khẩu bạn muốn đặt.Ở ô **Xác nhận mật khẩu mới**, nhập lại y hệt mật khẩu mới để xác nhận.Có biểu tượng **con mắt** ở mỗi ô: bấm để **hiện/ẩn** ký tự, giúp tránh gõ sai.Ngay bên dưới có dòng **Độ mạnh của mật khẩu**; cố gắng để hiện **Mạnh**



Bước 5: Xác nhận đổi mật khẩu.Bấm Đổi mật khẩu.Hộp thoại sẽ hiện các thiết bị đang giữ trạng thái đăng nhập (ví dụ điện thoại của bạn). Bấm tiếp Đổi mật khẩu để hoàn tất.



Bên cạnh việc đặt mật khẩu mạnh thì thói quen **thay đổi mật khẩu định kỳ** cũng là một kỹ năng bảo vệ thông tin an toàn. Bằng cách đặt mật khẩu mới sau một khoảng thời gian nhất định (ví dụ: 3–6 tháng), người dùng có thể hạn chế khả năng kẻ xấu khai thác mật khẩu đã bị rò rỉ mà bản thân chưa hay biết. Bên cạnh việc thay đổi thường xuyên, mật khẩu mới cần tuân thủ nguyên tắc an toàn:

- Không sử dụng lại mật khẩu cũ hoặc những mật khẩu dễ đoán như ngày sinh, số điện thoại.
- Tạo mật khẩu dài ít nhất 12 ký tự, kết hợp chữ hoa, chữ thường, số và ký hiệu đặc biệt.
- Cân nhắc sử dụng trình quản lý mật khẩu tự động (password manager) để lưu trữ và sinh mật khẩu mạnh.

6.1.2.2. Xác thực đa yếu tố (MFA/2FA)

❖ **Kích hoạt xác thực đa yếu tố**

Xác thực đa yếu tố (MFA) là biện pháp bảo mật mạnh mẽ nhất mà người dùng có thể áp dụng. MFA là việc sử dụng ít nhất hai yếu tố độc lập để xác minh danh tính của bạn. Dù kẻ xấu có lấy được mật khẩu của bạn, chúng vẫn không thể đăng nhập được.

MFA = Yếu tố bạn biết (Mật khẩu) + Yếu tố bạn có (Mã OTP/Sinh trắc học)

Trong đó:

- Mã số sử dụng một lần (OTP) gửi qua tin nhắn SMS (yếu tố CÓ).
- Mã OTP được tạo bởi ứng dụng xác thực. Ví dụ như Google Authenticator, Microsoft Authenticator hoặc được cung cấp bởi các nhà cung cấp dịch vụ khác như ngân hàng.
- Sinh trắc học (Vân tay, khuôn mặt) (yếu tố LÀ)

Hành động BẮT BUỘC: kích hoạt MFA trên tất cả các tài khoản quan trọng của bạn như Gmail, Facebook, Zalo, Ngân hàng.v.v.

❖ **Xác thực hai yếu tố 2FA**

Xác thực hai yếu tố (2FA) là một lớp bảo mật bổ sung giúp bảo vệ tài khoản trực tuyến và thiết bị số như điện thoại thông minh, máy tính bảng, hoặc laptop khỏi bị truy cập trái phép. Ngay cả khi mật khẩu của bạn bị lộ, 2FA yêu cầu một bước xác minh thứ hai, chẳng hạn như mã OTP gửi qua tin nhắn hoặc ứng dụng, để đảm bảo chỉ bạn mới có thể đăng nhập. Phần này sẽ giải thích lý do cần sử dụng 2FA, hướng dẫn cách kích hoạt và sử dụng nó trên các dịch vụ phổ biến, và cung cấp các bước cụ thể để dễ dàng áp dụng, giúp bảo vệ thông tin cá nhân và tài sản an toàn hơn.

Xác thực hai yếu tố bổ sung một lớp bảo vệ bằng cách yêu cầu thêm một yếu tố xác minh, như mã OTP gửi qua SMS, email, hoặc ứng dụng xác thực (như Google Authenticator). Điều này làm tăng độ khó để kẻ xấu truy cập tài khoản, ngay cả khi hacker biết mật khẩu của bạn. *Google* (2025) cũng nhấn mạnh rằng 2FA là một trong những biện pháp hiệu quả nhất để bảo vệ tài khoản Gmail, Google Drive, và các dịch vụ khác (Google - 2FA Guide). Không sử dụng 2FA khiến tài khoản của bạn dễ bị tấn công, đặc biệt với các dịch vụ quan trọng như ngân hàng, email, hoặc ứng dụng nhắn tin như Zalo.

Việc sử dụng đồng thời hai lớp bảo vệ sẽ giúp hạn chế khả năng xâm nhập trái phép ngay cả khi một yếu tố (thường là mật khẩu) bị lộ.

Thông thường, ba nhóm yếu tố xác thực chính được sử dụng trong 2FA bao gồm:

Thứ người dùng biết: Đây là những thông tin chỉ người dùng hợp pháp mới có, chẳng hạn như mật khẩu, mã PIN, hoặc câu hỏi bảo mật được đặt sẵn. Mặc dù yếu tố này rất phổ biến, nhưng lại dễ bị lộ nếu người dùng thiết lập mật khẩu yếu hoặc dùng chung cho nhiều tài khoản.

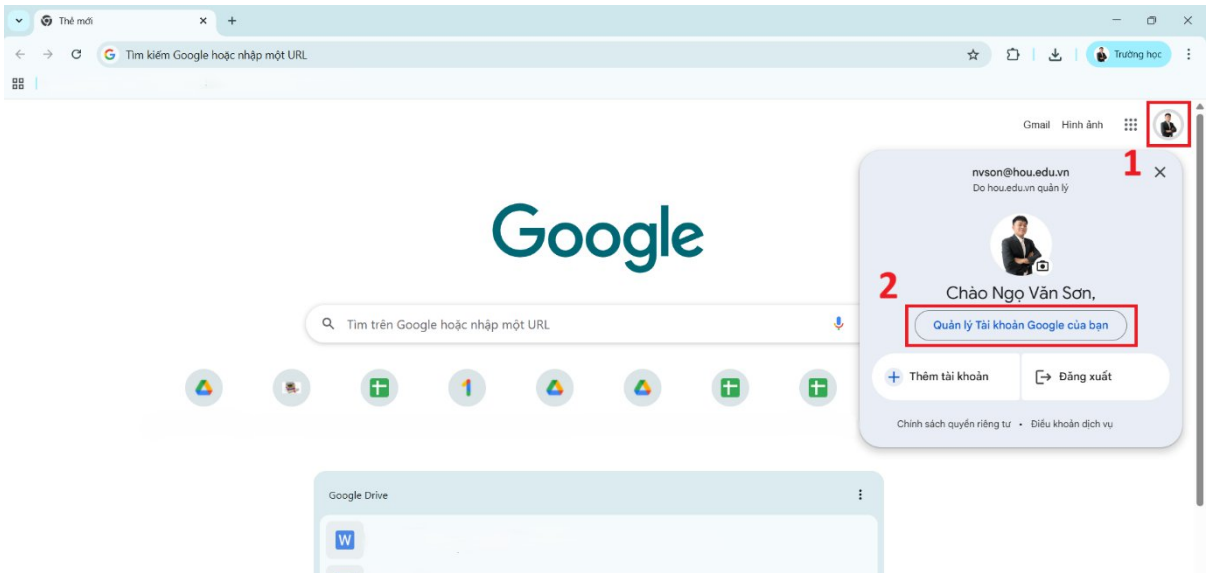
Thứ người dùng sở hữu: Đây là các thiết bị hoặc phương tiện mà người dùng đang nắm giữ, có thể là điện thoại nhận mã OTP qua SMS. Yếu tố này chỉ hoạt động khi người dùng thực sự sở hữu thiết bị tương ứng, làm tăng độ khó cho kẻ tấn công.

Thứ người dùng là: Đây là các yếu tố sinh trắc học được cá nhân hóa cao như dấu vân tay, nhận diện khuôn mặt, quét võng mạc hoặc nhận diện giọng nói. Đây là loại xác thực khó bị làm giả nhất và thường được tích hợp trong các thiết bị hiện đại như điện thoại thông minh, máy tính xách tay hoặc hệ thống cửa ra vào an ninh cao.

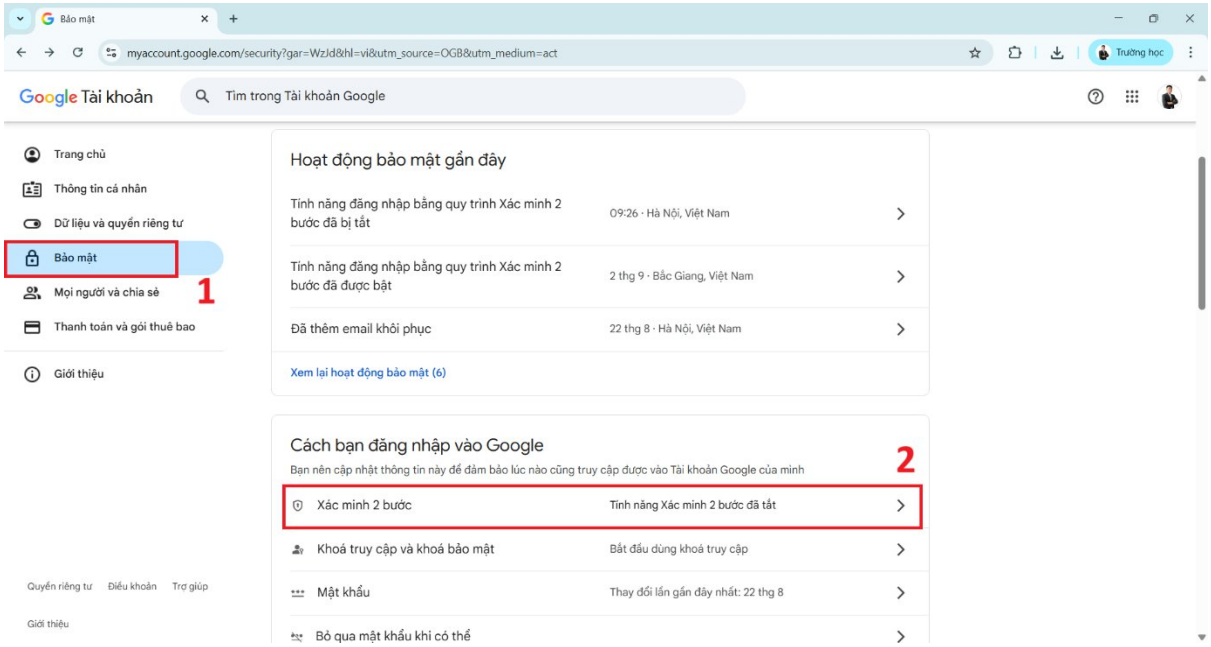
Để bảo vệ tài khoản và thiết bị, bạn nên kích hoạt xác thực hai yếu tố trên tất cả các dịch vụ hỗ trợ, chẳng hạn như tài khoản ngân hàng (Vietcombank, Techcombank), email (Gmail, Outlook), và ứng dụng nhắn tin (Zalo, WhatsApp). 2FA thường yêu cầu bạn nhập mật khẩu (yếu tố thứ nhất) và một mã xác minh (yếu tố thứ hai), có thể là mã OTP gửi qua tin nhắn, email, hoặc được tạo bởi ứng dụng xác thực như Google Authenticator hoặc Microsoft Authenticator. Bạn nên ưu tiên sử dụng ứng dụng xác thực vì chúng an toàn hơn tin nhắn SMS, vốn có thể bị chặn bởi tội phạm mạng. Sau khi kích hoạt, hãy lưu mã khôi phục (recovery code) ở nơi an toàn để sử dụng trong trường hợp mất điện thoại hoặc không nhận được mã OTP. Nếu gặp khó khăn, bạn có thể nhờ người thân hoặc liên hệ hỗ trợ từ dịch vụ (như ngân hàng hoặc Google).

Các bước cụ thể dưới đây sẽ hướng dẫn bạn cách kích hoạt và sử dụng 2FA một cách dễ dàng, dù là người mới sử dụng công nghệ. Sau đây là các bước thực hiện:

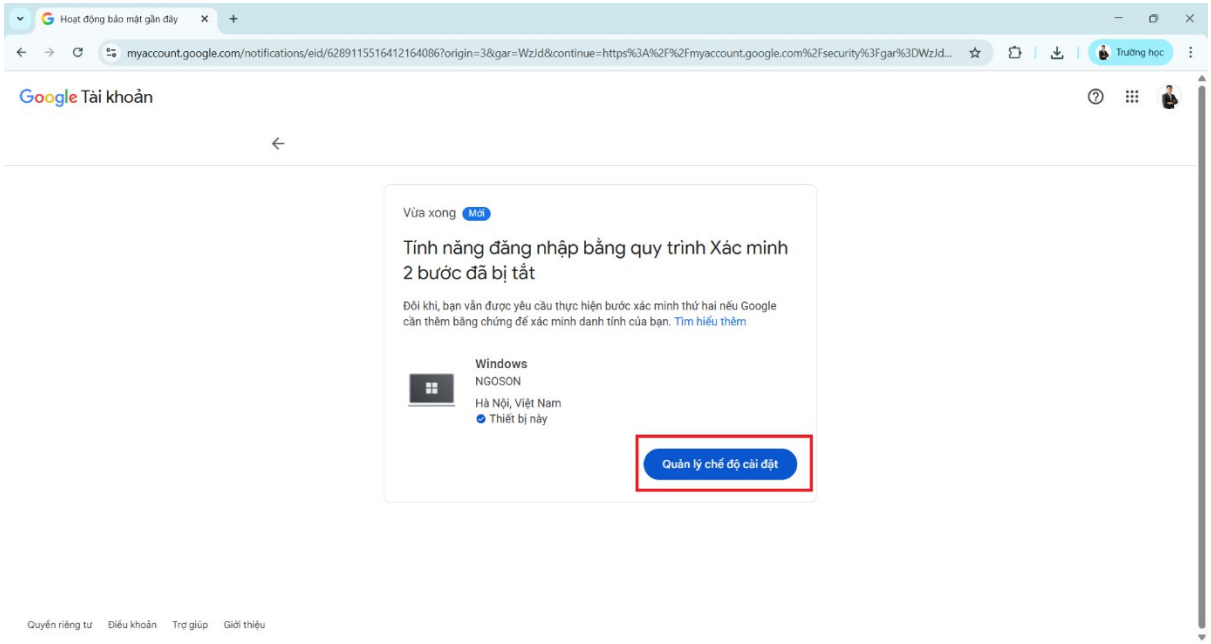
Bước 1: Mở trình duyệt Google Chrome. Tại giao diện chính của trang, bạn thực hiện ấn vào **biểu tượng Avatar** chọn **Quản lý tài khoản Google của bạn**.



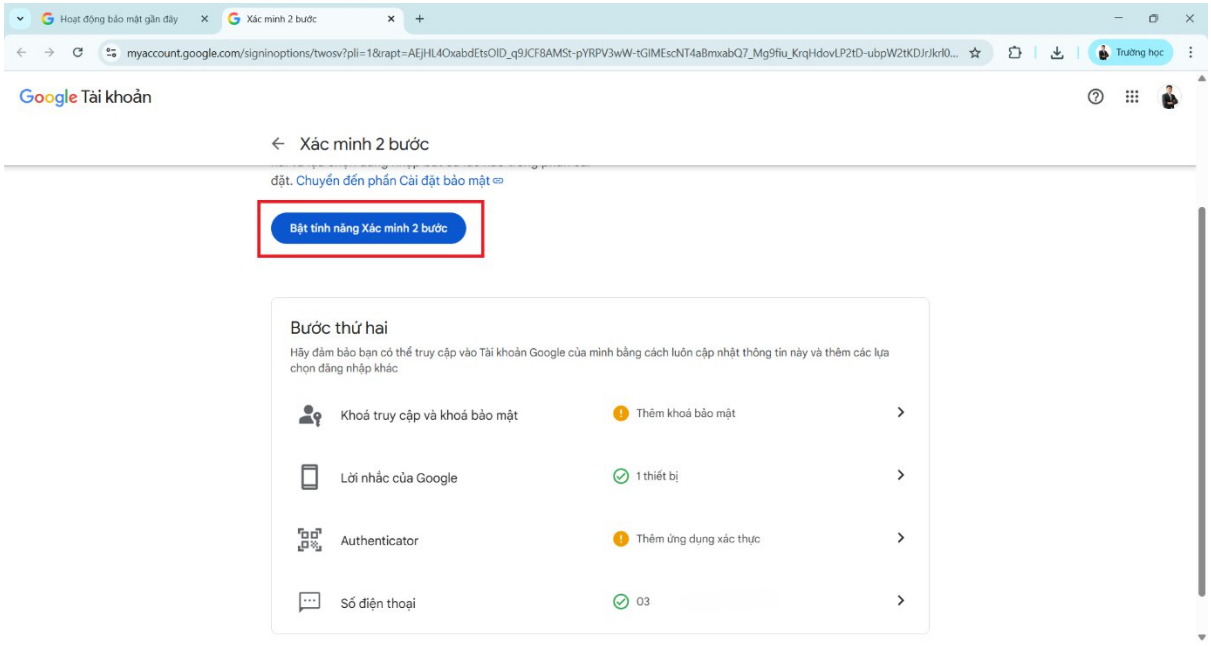
Bước 2: Trong menu bên trái chúng ta chọn **Bảo mật**



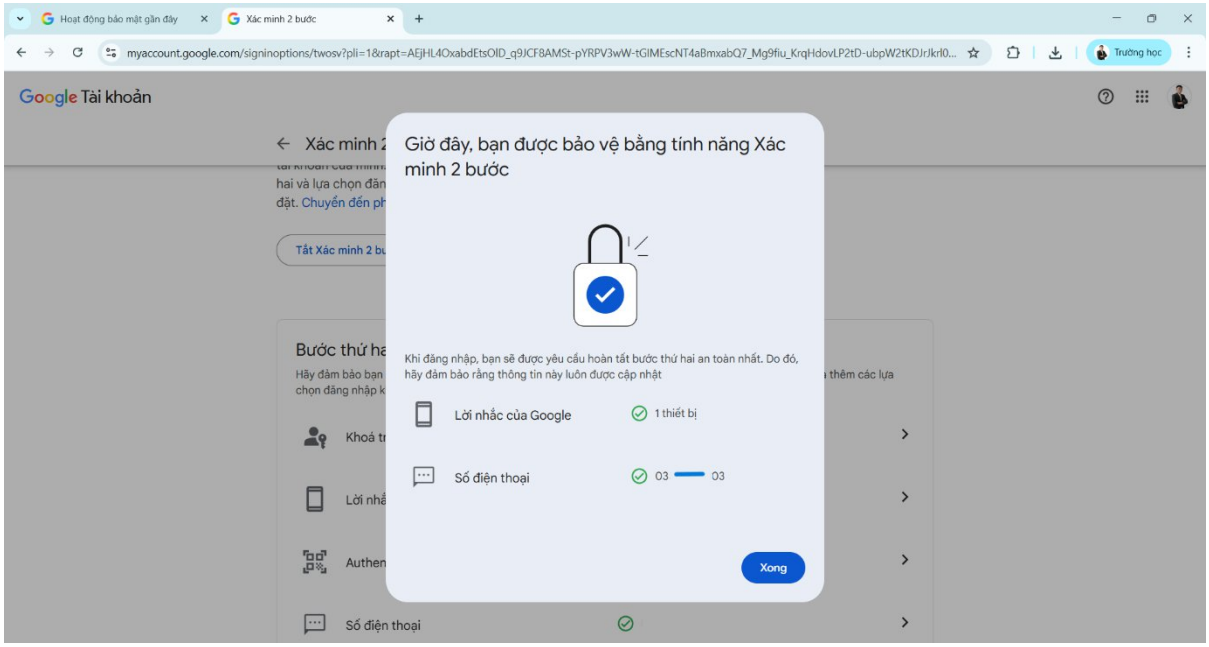
Bước 3: Tại cửa sổ hiện ra, chúng ta tìm dòng nội dung **Xác minh 2 bước**, chúng có thể thấy được trạng thái đã bật tính năng xác minh 2 bước hay chưa.



Bước 4: Nếu tài khoản của bạn chưa bật xác minh 2 bước thì bạn ấn vào **Bật tính năng Xác minh 2 bước**. Để đảm bảo có thể bật tính năng chúng ta cần thêm **Số điện thoại** hoặc **Thiết bị kết nối (lời nhắc của Google)**.



Bước 5: Kiểm tra trạng thái của dịch vụ đã kích hoạt thành công hay chưa, các thông tin xác minh, bổ sung thêm các phương thức xác minh khác nếu cần.



6.1.2.3. Lợi ích và cách sử dụng công cụ quản lý mật khẩu

Phương pháp viết mật khẩu ra giấy hoặc dùng mật khẩu giống nhau cho mọi tài khoản là cực kỳ nguy hiểm. Công cụ quản lý mật khẩu giúp bạn giải quyết vấn đề này.

Tạo mật khẩu mạnh: Tự động tạo ra các mật khẩu phức tạp, ngẫu nhiên. Ví dụ *g&Y%r$7t#9@P!Z^b*.

Lưu trữ an toàn: Lưu trữ tất cả các mật khẩu trong một kho mã hóa được bảo vệ bằng mật khẩu duy nhất.

Không cần nhớ: Bạn chỉ cần nhớ một mật khẩu chủ duy nhất.

Gợi ý các công cụ: Các trình quản lý mật khẩu tích hợp sẵn trên thiết bị. Ví dụ như Google password manager, iClound Keychain hoặc các công cụ chuyên dụng như Bitwarden, LastPass.

6.2. Bảo vệ dữ liệu cá nhân và quyền riêng tư

6.2.1. Quản lý thông tin, dữ liệu cá nhân

6.2.1.1. Chia sẻ dữ liệu có trách nhiệm

❖ **Dấu chân kỹ thuật số**

Dấu chân kỹ thuật số – đôi khi được gọi là bóng kỹ thuật số hoặc dấu chân điện tử – dùng để chỉ dấu vết của mọi thứ mà bạn để lại trên internet khi sử dụng các thiết bị và dịch vụ số. Dấu vết bao gồm các trang web mà bạn truy cập, lịch sử tìm kiếm, email bạn gửi và thông tin cá nhân mà bạn đăng ký trực tuyến. Có thể sử dụng dấu chân kỹ thuật số để theo dõi các hoạt động và thiết bị trực tuyến của một người. Dấu chân kỹ thuật số được chia làm hai nhóm chính:

Dấu chân chủ động, là những thông tin bạn tự nguyện chia sẻ trong quá trình sử dụng. Như bài đăng Facebook, bình luận trên diễn đàn, điền thông tin cá nhân vào mẫu trực tuyến, đăng ký một tài khoản mới.

Dấu chân thụ động, là những thông tin được thu thập mà bạn không hề hay biết hoặc không trực tiếp chia sẻ. Như lịch sử duyệt web, vị trí địa lý của bạn khi bạn sử dụng ứng dụng bản đồ hay thông tin về thiết bị bạn đang sử dụng.

Đôi khi, không phải lúc nào cũng rõ ràng bạn đang để lại dấu chân kỹ thuật số. Ví

❖ **Nguyên tắc "tối thiểu hóa dữ liệu"**

Nó đơn giản là việc chỉ chia sẻ những gì thật sự cần thiết, không thừa mứa. Trước khi chia sẻ thông tin nào trên môi trường số, hãy tự hỏi "*Thông tin này có thực sự cần thiết cho dịch vụ/ mục đích này không?*". Nếu câu trả lời là **Không**, thì đừng chia sẻ.

Bảng dưới đây mô tả một số áp dụng thực tế vào đời sống số:

Tình huống thực tế	Hành động của bạn (Tối thiểu hóa)	Thông tin cần tránh cung cấp
Mua hàng Online/Đăng ký	Chỉ cung cấp Tên, Số điện thoại và Địa chỉ giao hàng.	Ngày tháng năm sinh, Số CMND/CCCD, Nơi làm việc,

thành viên		Tình trạng hôn nhân.
Điền Form khảo sát	Chỉ điền các trường có dấu **(*) bắt buộc**. Điền thông tin chung chung vào các trường không bắt buộc (*Optional*).	Thu nhập chi tiết, Số tài khoản mạng xã hội (trừ khi cần), Tên người thân.
Sử dụng mạng xã hội (Facebook, Zalo)	Đặt chế độ **"Chỉ mình tôi"** (Only Me) hoặc **"Bạn bè"** (Friends) cho các thông tin nhạy cảm.	Ảnh chụp giấy tờ tùy thân (CMND/CCCD/Bằng lái), Vé máy bay (có mã vạch), Thông tin trường học của con cái.
Đăng ký Email (Lần đầu)	Sử dụng một Email riêng (Email phụ) cho các dịch vụ không quan trọng hoặc dịch vụ bạn không tin tưởng hoàn toàn.	Số điện thoại di động chính (dùng cho ngân hàng, OTP), Email chính (dùng cho công việc).
Chụp và lưu trữ ảnh	Xóa ngay các ảnh chụp giấy tờ (căn cước, sổ hộ khẩu, hóa đơn) sau khi đã sử dụng xong, không lưu chúng trên thư viện ảnh điện thoại.	Hình ảnh chứa thông tin nhạy cảm đã sử dụng xong.

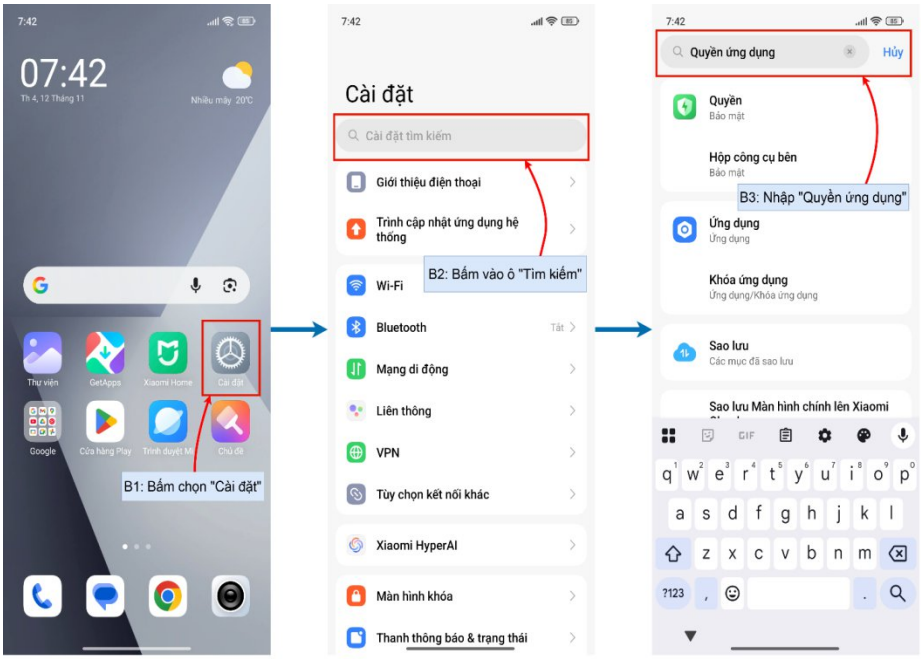
❖ **Kiểm tra và quản lý quyền truy cập ứng dụng**

- ***Hướng dẫn quản lý quyền truy cập trên Android***
  - ✔ *Vào cài đặt***:** Mở ứng dụng Cài đặt (Settings) trên điện thoại của bạn.
  - ✔ *Tìm quản lý quyền***:** Cuộn xuống và tìm mục Bảo mật & Quyền riêng tư (Security & Privacy) hoặc Ứng dụng & Thông báo (Apps & Notifications). Sau đó tìm kiếm Trình quản lý quyền (Permission Manager).
  - ✔ *Kiểm tra từng loại quyền***:** Trình quản lý quyền sẽ liệt kê các loại quyền (Ví dụ: Danh bạ, Vị trí, Máy ảnh, Micro).
  - ✔ *Hành động cụ thể*:
    - Nhấp vào một loại quyền bất kỳ (Ví dụ: Máy ảnh).
    - Bạn sẽ thấy danh sách các ứng dụng được phép sử dụng Máy ảnh.

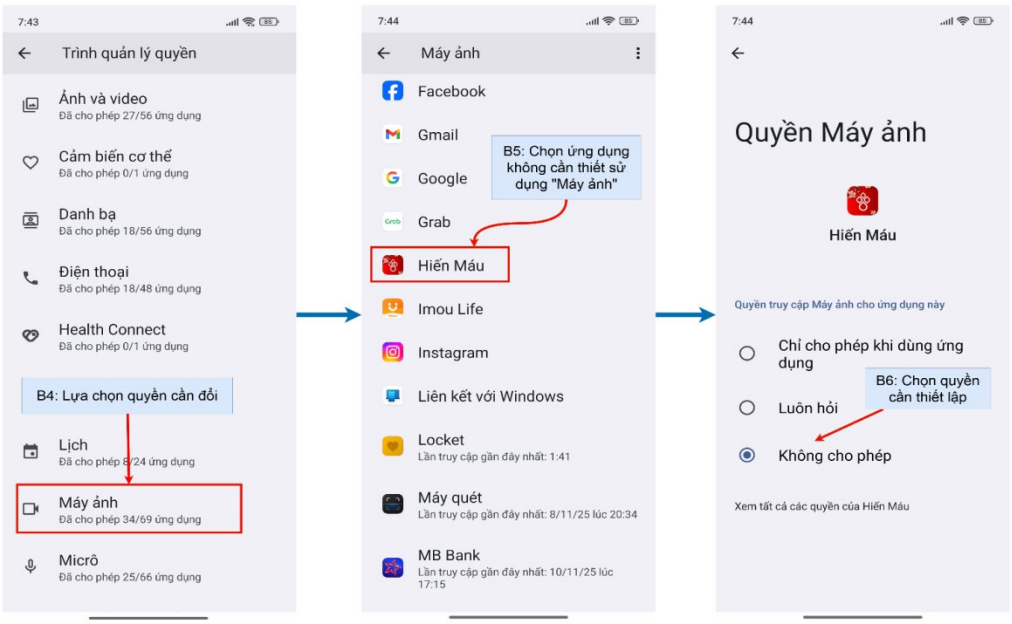
- Xem xét: Nếu thấy một ứng dụng không liên quan đến chụp ảnh (Ví dụ: Ứng dụng đọc tin tức) đang được phép truy cập Camera, hãy nhấp vào ứng dụng đó và chọn Từ chối (Deny) hoặc Chỉ cho phép khi ứng dụng đang được sử dụng.
- Lặp lại quy trình này với các quyền nhạy cảm khác như Micro và Vị trí.

Ví dụ các bước chỉnh sửa quyền **Máy ảnh** cho ứng dụng

Bước 1: Mở cài đặt. Từ màn hình chính, bấm vào biểu tượng "Cài đặt". Chọn vào ô "Cài đặt tìm kiếm". Tại ô tìm kiếm, nhập từ khóa "Quyền ứng dụng", chọn mục "Quyền ứng dụng" trong kết quả hiện ra.



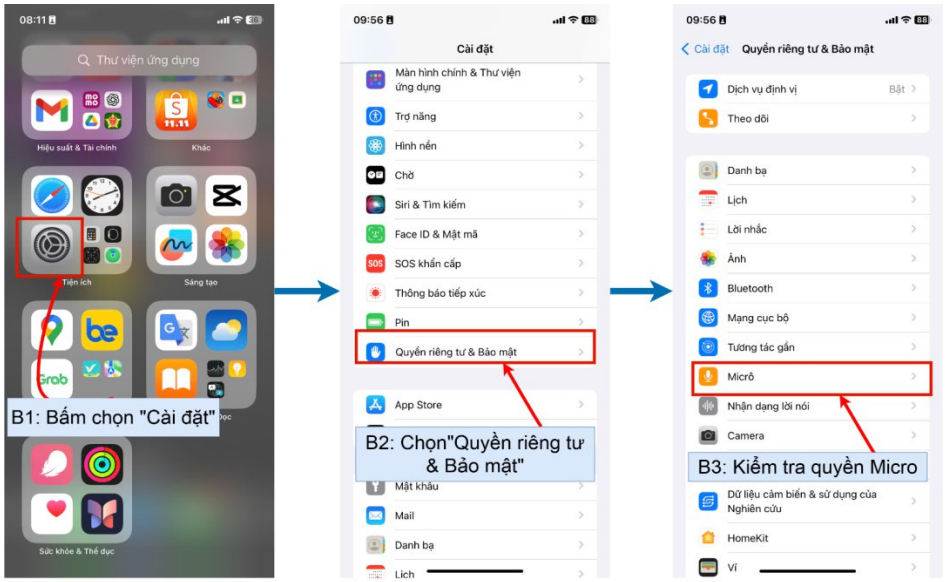
Bước 2: Chọn loại quyền cần thay đổi. Ở màn hình **Trình quản lý quyền**, kéo xuống và nhấn vào mục "**Máy ảnh**". Chọn ứng dụng cần chỉnh sửa quyền trong danh sách các ứng dụng đang dùng quyền "**Máy ảnh**" (Ví dụ, ứng dụng Hiến Máu). Ở màn hình **Quyền Máy ảnh của ứng dụng**, chọn tùy chọn mong muốn: **Không cho phép**; **Luôn hỏi**; **Chỉ cho phép khi dùng ứng dụng**.



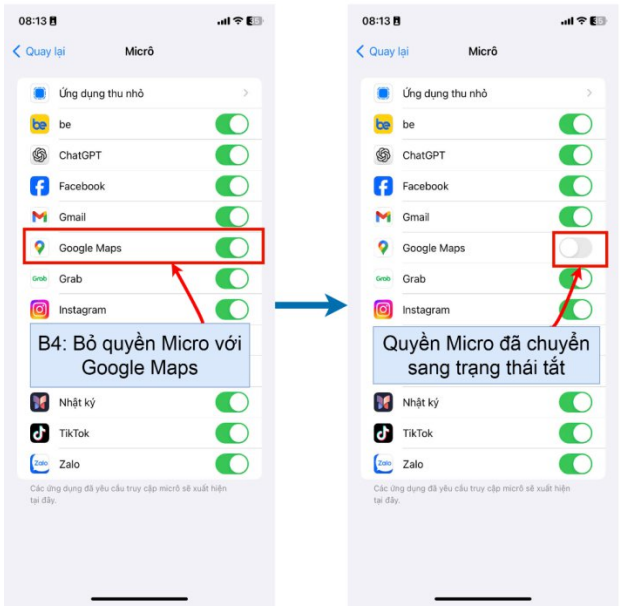
- ***Hướng dẫn quản lý quyền truy cập trên iOS (iPhone/iPad)***
  - ✔ *Vào cài đặt*: Mở ứng dụng Cài đặt (Settings) trên iPhone/iPad.
  - ✔ *Tìm quyền riêng tư*: Cuộn xuống và chọn Quyền riêng tư & Bảo mật (Privacy & Security).
  - ✔ *Kiểm tra từng loại quyền*: Bạn sẽ thấy danh sách chi tiết các loại quyền (Ví dụ: Camera, Micro, Danh bạ, Vị trí).
  - ✔ *Hành động cụ thể*
    - Cách 1: Kiểm tra theo quyền
      - Nhấp vào một loại quyền (Ví dụ: Micro).
      - Bạn sẽ thấy danh sách các ứng dụng được cấp quyền truy cập Micro.
      - Vô hiệu hóa: Gạt công tắc sang Tắt (Off) cho bất kỳ ứng dụng nào mà bạn thấy không cần thiết sử dụng Micro.
    - Cách 2: Kiểm tra theo ứng dụng
      - Cuộn xuống phía dưới cùng của Cài đặt để tìm tên ứng dụng (Ví dụ: Zalo, Shopee).
      - Nhấp vào ứng dụng đó và xem danh sách các quyền được cấp.
      - Chỉnh sửa: Tắt các quyền không cần thiết.

Ví dụ hướng dẫn quản lý quyền truy cập **Micro** trên điện thoại iPhone

Bước 1: Từ màn hình chính, bấm vào biểu tượng "**Cài đặt**". Trong danh sách, kéo xuống và chọn "**Quyền riêng tư & bảo mật**". Tại màn hình này, chọn mục "**Micro**".



Bước 2: Bật, tắt quyền Micro với Google Maps. Danh sách các ứng dụng cần sử dụng quyền Micro hiện ra. Tìm ứng dụng Google Maps và thực hiện gạt nút công tắc sang trạng thái Tắt hoặc Bật tùy theo nhu cầu sử dụng của người dùng.



Quy tắc kiểm soát quyền truy cập

Loại quyền	Mức độ nghiêm trọng	Lời khuyên
Micro/Máy ảnh (Camera)	Cao	Chỉ cấp cho các ứng dụng giao tiếp (Zalo, Messenger, Zoom) hoặc chụp ảnh/quay phim.
Vị trí (Location)	Cao	Chỉ cấp cho ứng dụng cần thiết như Bản đồ

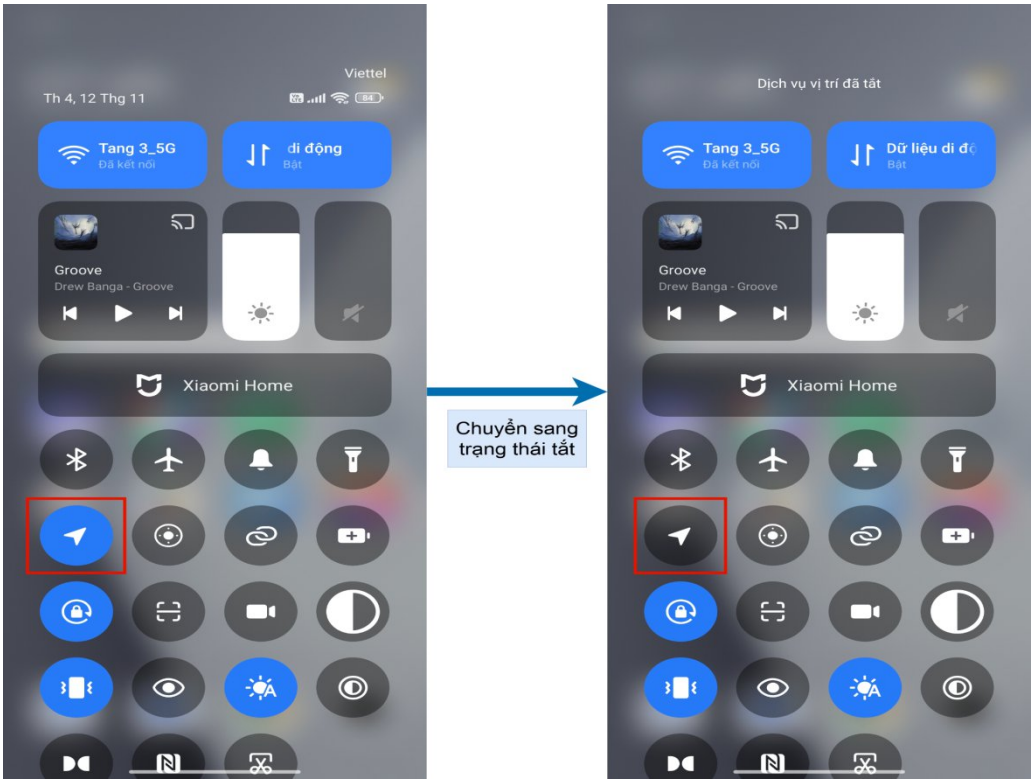
		(Maps), ứng dụng gọi xe. Hạn chế cấp quyền **"Luôn luôn"** (Always).
Danh bạ (Contacts)	Cao	Chỉ cấp cho các ứng dụng cần đồng bộ bạn bè (Messenger, Zalo, Viber).
Lịch (Calendar)	Trung bình	Chỉ cấp cho ứng dụng quản lý công việc/thời gian.
Tin nhắn/Điện thoại	Cao	Cấp cho các ứng dụng dùng để nhận mã xác thực (SMS) hoặc ứng dụng gọi điện mặc định.

❖ **Vô hiệu hóa tính năng định vị (GPS) khi không cần thiết**

Tính năng định vị cho phép các ứng dụng và dịch vụ biết chính xác vị trí địa lý thiết bị của bạn. Mặc dù, tiện lợi cho việc chỉ đường hoặc gọi xe, việc bật định vị liên tục sẽ tăng rủi ro bị theo dõi và bị ứng dụng thu thập dữ liệu di chuyển chi tiết của bạn.

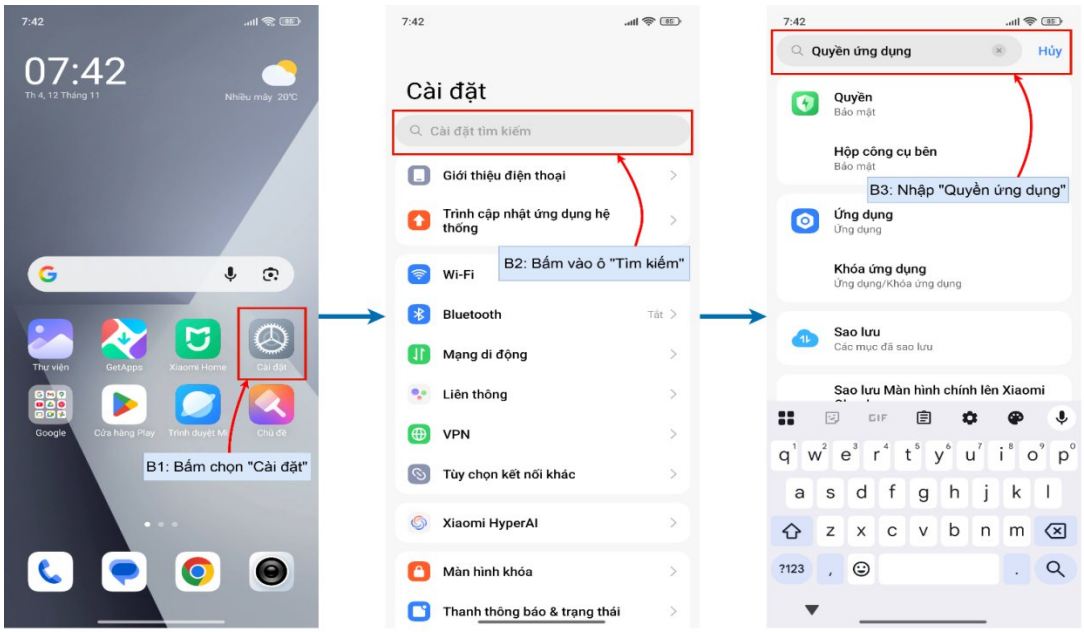
Hướng dẫn quản lý quyền vị trí trên Android

Tắt định vị tổng thể: Thanh thông báo: Vuốt màn hình từ trên xuống để mở thanh thông báo nhanh. Tìm biểu tượng Vị trí (Location) hoặc GPS và nhấn vào để tắt (biểu tượng chuyển sang màu xám/trắng).

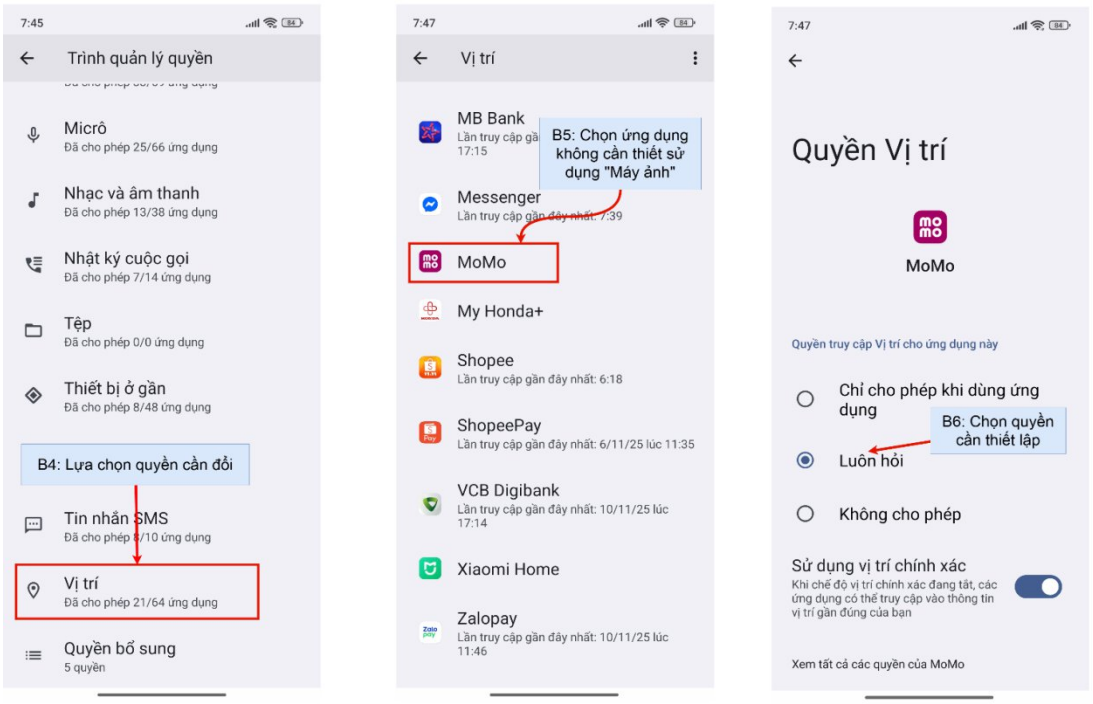


Cấp quyền tinh chỉnh

<u>Bước 1</u>: Từ màn hình chính, bấm vào biểu tượng "**Cài đặt**". Trong giao diện "**Cài đặt**", nhấn vào ô "**Cài đặt tìm kiếm**" ở phía trên. Gõ từ khóa "**Quyền ứng dụng**" và chọn mục "**Quyền ứng dụng**" trong kết quả hiện ra.



Bước 2: Chọn laoij quyền cần thay đổi tại **Trình quản lý quyền**, chọn mục "**Vị trí**" để mở danh sách các ứng dụng đang sử dụng quyền này. Chọn ứng dụng bạn muốn điều chỉnh, ví dụ MoMo. Thiết lập quyền vị trí cho ứng dụng tại màn hình đó.



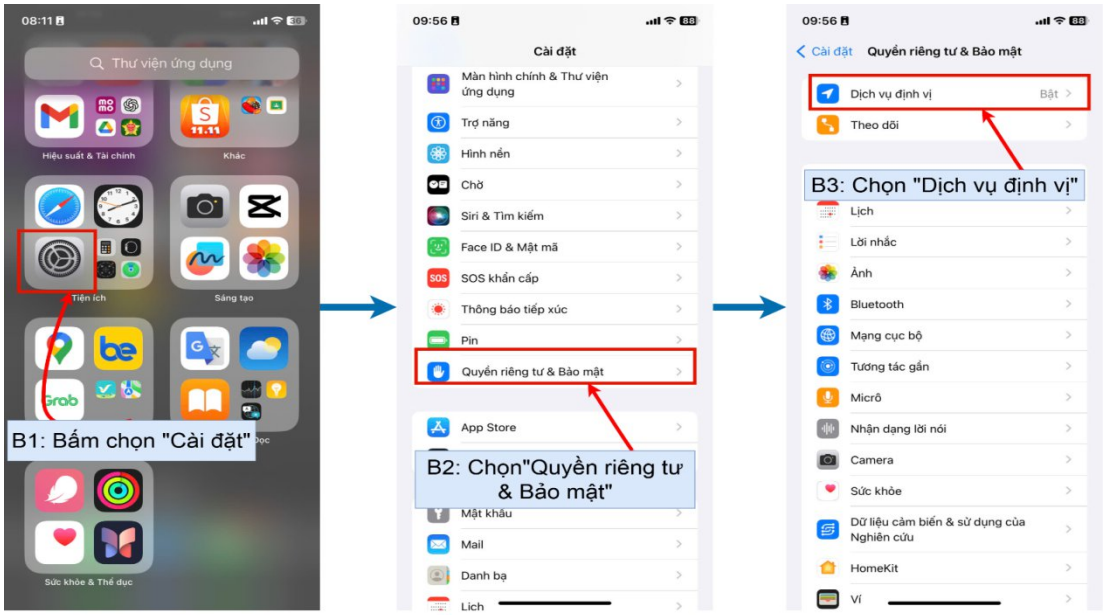
- ***Hướng dẫn quản lý quyền vị trí trên iOS (iPhone/iPad)***

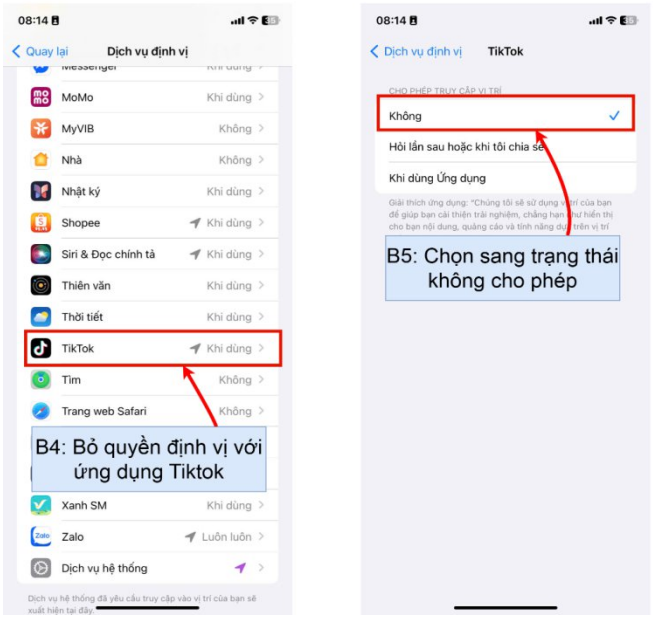
  ✔ *Tắt định vị tổng thể:* Vào Cài đặt àQuyền riêng tư & Bảo mật àDịch vụ Định vị àGạt nút tắt (nếu bạn muốn tắt hoàn toàn cho mọi thứ).

✔ *Cấp quyền tinh chỉnh theo ứng dụng*

Trong mục dịch vụ định vị (Location Services), bạn sẽ thấy danh sách các ứng dụng.Nhấp vào từng ứng dụng (Ví dụ: Google Maps, Facebook) và chọn một trong các tùy chọn:

- ***Không (Never)*:** Ứng dụng không bao giờ biết vị trí.
- ***Hỏi lần tới hoặc khi tôi chia sẻ:*** Ứng dụng sẽ hỏi lại mỗi lần cần truy cập.
- ***Khi dùng ứng dụng*:** Nên ưu tiên (Chỉ cấp quyền khi ứng dụng đang mở trên màn hình).
- ***Luôn luôn:*** Nên tránh (Ứng dụng biết vị trí của bạn ngay cả khi nó chạy nền).





6.2.1.2. Hạn chế chia sẻ thông tin cá nhân lên các trang mạng xã hội

Thông tin cá nhân như số chứng minh nhân dân (CMND/CCCD), số tài khoản ngân hàng, địa chỉ nhà, hoặc dữ liệu cá nhân như ảnh, tin nhắn, và tài liệu công việc là những tài sản quan trọng được lưu trữ trên các thiết bị số như điện thoại thông minh, máy tính bảng, hoặc laptop. Nếu không được quản lý cẩn thận, những thông tin này có thể bị đánh cắp, lạm dụng, hoặc mất mát, dẫn đến các rủi ro như lừa đảo trực tuyến, mất tiền, hoặc bị lợi dụng danh tính. Quản lý thông tin cá nhân hiệu quả giúp bảo vệ sự an toàn và quyền riêng tư của bạn khi sử dụng thiết bị số và các dịch vụ trực tuyến như mạng xã hội.

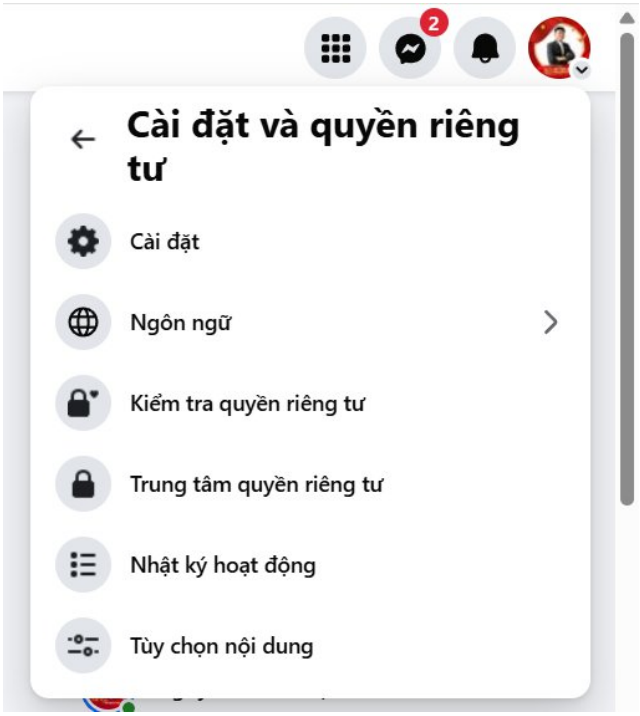
Để quản lý thông tin cá nhân hiệu quả, bạn cần thực hiện ba biện pháp chính: hạn chế chia sẻ thông tin nhạy cảm, thiết lập quyền riêng tư trên mạng xã hội, và sao lưu dữ liệu thường xuyên. Đầu tiên, hãy cẩn trọng khi chia sẻ thông tin như số CMND/CCCD, số tài khoản ngân hàng, hoặc địa chỉ nhà, chỉ cung cấp cho các tổ chức đáng tin cậy (như ngân hàng chính thức) và tránh chia sẻ qua tin nhắn, email, hoặc mạng xã hội. Ví dụ, nếu nhận được tin nhắn yêu cầu cung cấp số CMND để "nhận thưởng", hãy gọi đến hotline chính thức của tổ chức để xác minh. Thứ hai, trên các nền tảng mạng xã hội như Facebook và Zalo, bạn nên thiết lập quyền riêng tư để giới hạn người xem bài đăng, ảnh, hoặc thông tin cá nhân, đảm bảo chỉ bạn bè thân thiết hoặc người được phép mới thấy được.

Là một người dùng trên môi trường số, bạn cần nắm rõ những quy tắc sau để bảo vệ thông tin cá nhân của bản thân:

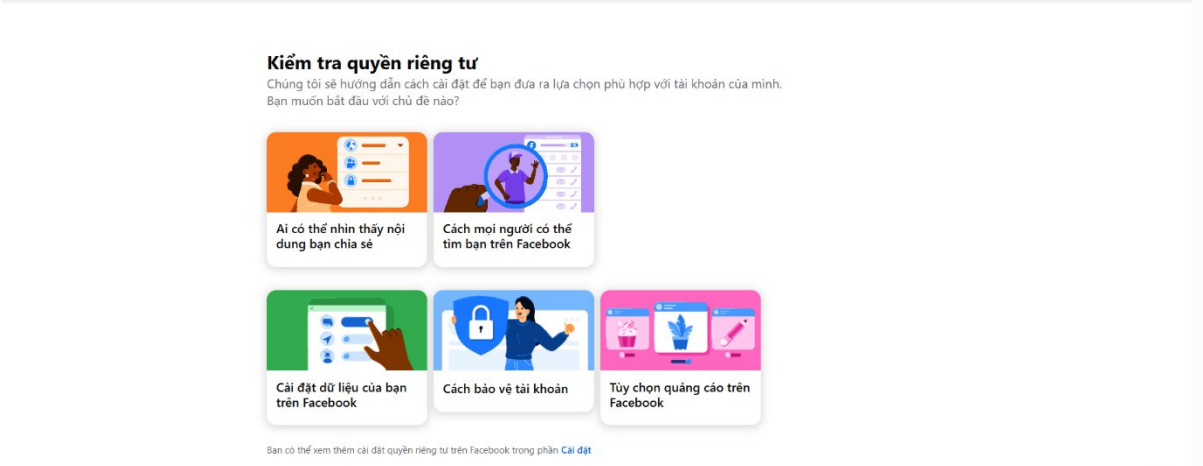
- Không cung cấp thông tin như số CMND/CCCD, số tài khoản ngân hàng, mật khẩu, hoặc địa chỉ nhà qua tin nhắn SMS, email, hoặc cuộc gọi từ số lạ.
- Xác minh nguồn yêu cầu thông tin bằng cách gọi đến hotline chính thức, ví dụ: Vietcombank (1900 54 54 13).
- Tránh đăng thông tin cá nhân (như ảnh CMND, vé máy bay có mã vạch) lên mạng xã hội vì có thể bị lạm dụng.
- Nếu lỡ chia sẻ thông tin, thay đổi mật khẩu ngay lập tức và thông báo cho ngân hàng hoặc cơ quan liên quan.

Đối với mạng xã hội Facebook bạn cần thiết lập quyền riêng tư, chỉ để cho bạn bè, người thân biết thông tin hoặc để chế độ "chỉ mình tôi":

Bước 1: Ấn vào avatar >**Cài đặt và quyền riêng tư**>**Kiểm tra quyền riêng tư**.



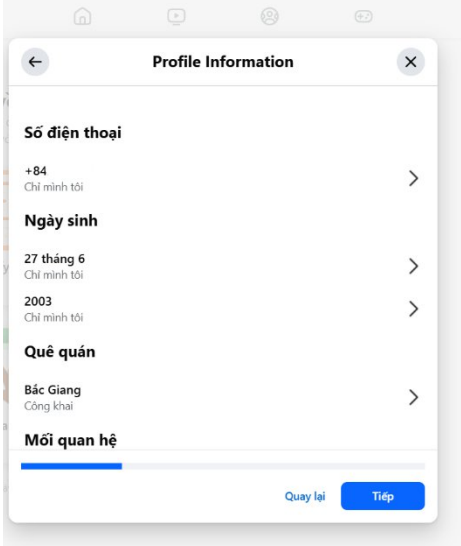
Bước 2: Tại giao diện quyền riêng tư, chọn **Ai có thể nhìn thấy nội dung bạn chia sẻ** để tiến hành cài đặt các quyền



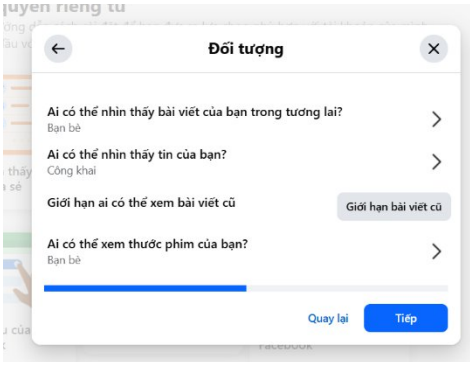
Bước 3: Ẩn thông tin cá nhân trong **Profile Information,** mục tiêu: số điện thoại, ngày sinh, quê quán… chỉ hiển thị ở phạm vi an toàn.

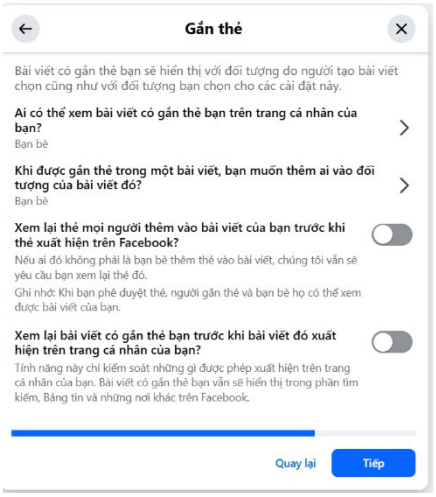
- **Số điện thoại** → bấm vào → đặt quyền riêng tư **Chỉ mình tôi***(khuyến nghị)* hoặc **Bạn bè** nếu bạn muốn bạn bè thấy.
- **Ngày sinh**
  - **Ngày & Tháng** → đặt **Chỉ mình tôi***(khuyên dùng)*.
  - **Năm sinh → Chỉ mình tôi***(tránh lộ tuổi cho người lạ)*.
- **Quê quán** → đặt **Bạn bè** hoặc **Chỉ mình tôi**.

- Bấm **Xong/Tiếp** để lưu.



Bước 4: Cài đặt quyền cho các **Đối tượng**





6.2.1.3. Cẩn trọng với các ứng dụng yêu cầu quyền truy cập

Các ứng dụng trên điện thoại thông minh hoặc máy tính thường yêu cầu quyền truy cập vào dữ liệu cá nhân như danh bạ, vị trí, máy ảnh, hoặc micro để hoạt động. Cẩn trọng với các ứng dụng yêu cầu quyền truy cập là một bước quan trọng để bảo vệ thông tin cá nhân và đảm bảo an toàn khi sử dụng thiết bị số.

Để bảo vệ thông tin cá nhân, bạn cần cẩn trọng khi cài đặt ứng dụng và quản lý các quyền truy cập mà chúng yêu cầu. Trước khi cài đặt, hãy kiểm tra kỹ danh sách quyền truy cập và chỉ cấp những quyền cần thiết cho chức năng của ứng dụng, ví dụ, một ứng dụng chỉnh sửa ảnh có thể cần quyền truy cập máy ảnh nhưng không cần danh bạ. Chỉ tải ứng dụng từ các nguồn đáng tin cậy như **Google Play** hoặc **App Store**, và kiểm tra đánh giá, số lượt tải để đảm bảo ứng dụng an toàn. Sau khi cài đặt, bạn có thể kiểm tra và tắt quyền truy cập không cần thiết trong cài đặt thiết bị.

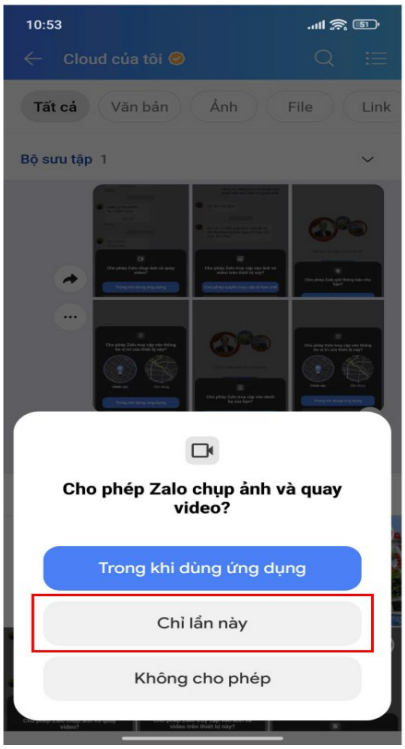
❖ ***Bạn cần kiểm tra quyền truy cập trước khi cài đặt ứng dụng:***

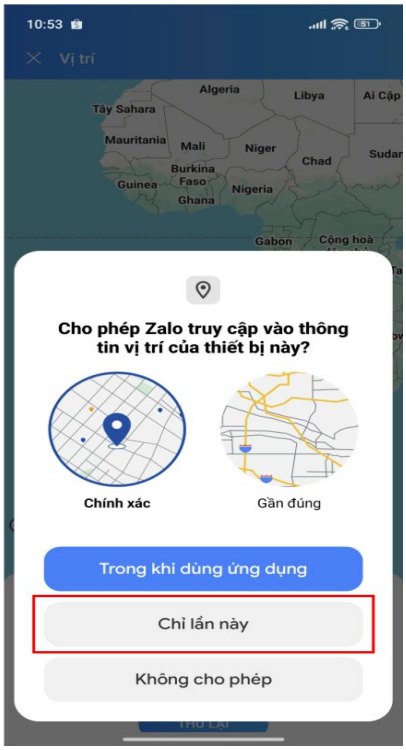
- Khi cài đặt ứng dụng từ Google Play hoặc App Store, đọc kỹ danh sách quyền truy cập hiển thị trước khi nhấn Cài đặt (Google - App Permissions).
- Đánh giá xem quyền yêu cầu có hợp lý không, ví dụ: ứng dụng đèn pin không cần truy cập danh bạ, vị trí, hoặc micro.
- Kiểm tra đánh giá ứng dụng (trên 4 sao) và số lượt tải (trên 100.000) để đảm bảo độ tin cậy (FPT - App Safety).

❖ ***Khi sử dụng phần mềm Zalo cần quản lý quyền truy cập trên thiết bị:***

Chụp ảnh & quay video: nếu chỉ để gửi ảnh, chọn **"Chỉ lần này"** hoặc chụp sẵn rồi **chọn từ thư viện**. Tránh cho phép vĩnh viễn vì app có thể kích hoạt camera mỗi khi mở.

Vị trí: ưu tiên **"Trong khi dùng ứng dụng"** và **vị trí gần đúng**. Chỉ dùng "chính xác" khi cần định tuyến/thanh toán theo vị trí. Không bật quyền nền trừ app dẫn đường.





6.2.2. Các rủi ro về mất an toàn thông tin cá nhân trên môi trường số

6.2.2.1. Bị lừa đảo trực tuyến.

Sự thành công của các chiến dịch lừa đảo hiện đại không chỉ dựa vào kỹ thuật mà còn phụ thuộc rất lớn vào khả năng khai thác các lỗ hổng tâm lý của con người. Các đối tượng lừa đảo thường nhắm vào ba yếu tố cốt lõi:

- **Lòng tin:** Chúng lợi dụng uy tín của các tổ chức lớn như ngân hàng, cơ quan nhà nước, hoặc khai thác sự tin tưởng trong các mối quan hệ cá nhân như bạn bè, người thân để khiến nạn nhân mất cảnh giác.
- **Nỗi sợ hãi:** Bằng cách giả danh cơ quan công an, viện kiểm sát, chúng tạo ra một áp lực tâm lý cực độ, đe dọa nạn nhân có liên quan đến các vụ án hình sự nghiêm trọng. Nỗi sợ bị pháp luật trừng phạt buộc nạn nhân phải hành động một cách phi lý trí theo yêu cầu của kẻ lừa đảo.
- **Lòng tham:** Các chiêu trò đánh vào mong muốn kiếm tiền nhanh, việc nhẹ lương cao, hoặc nhận các phần thưởng, ưu đãi hấp dẫn cũng là một phương thức phổ biến để dẫn dụ nạn nhân vào bẫy.

Các hình thức lừa đảo mạo danh ngày càng đa dạng và nhắm vào nhiều nhóm đối tượng khác nhau. Sau đây là các hình thức lừa đảo phổ biến:

❖ **Hình thức mạo danh cơ quan chức năng**

Tiếp cận và tạo áp lực: Các đối tượng sử dụng số điện thoại ảo, khó truy vết, hoặc các ứng dụng giả lập số điện thoại của cơ quan công an để gọi cho nạn nhân. Chúng tự xưng là cán bộ điều tra, viện kiểm sát viên hoặc thẩm phán, nói chuyện với giọng điệu nghiêm nghị và sử dụng các thuật ngữ pháp lý để tạo uy tín.

Dựng lên vụ án giả: Nạn nhân được thông báo rằng họ có liên quan đến một vụ án hình sự đặc biệt nghiêm trọng như buôn bán ma túy, rửa tiền, hoặc gây tai nạn chết người. Để tăng tính thuyết phục, chúng có thể đọc chính xác các thông tin cá nhân của nạn nhân (họ tên, ngày sinh, số CCCD), những thông tin này thường bị rò rỉ từ các nguồn khác.

Yêu cầu giữ bí mật và chuyển tiền: Kẻ lừa đảo yêu cầu nạn nhân phải giữ bí mật tuyệt đối, không được tiết lộ cho bất kỳ ai, kể cả người thân, với lý do "để không ảnh hưởng đến quá trình điều tra". Sau đó, chúng yêu cầu nạn nhân chuyển toàn bộ tiền trong tài khoản vào một "tài khoản tạm giữ của cơ quan điều tra" để xác minh, hứa hẹn sẽ hoàn trả sau khi chứng minh được sự trong sạch.

Thủ đoạn "bắt cóc online": Một biến thể tinh vi hơn là yêu cầu nạn nhân (thường là học sinh, sinh viên) tự thuê phòng ở một khách sạn, tự cách ly và duy trì cuộc gọi video liên tục để "giám sát". Sau đó, chúng sử dụng chính những hình ảnh này để gửi cho gia đình, dàn dựng một vụ bắt cóc và yêu cầu tiền chuộc.

Cần phải khẳng định rằng, cơ quan Công an, Viện Kiểm sát, và Tòa án **tuyệt đối không bao giờ** làm việc, triệu tập, hay yêu cầu người dân chuyển tiền qua điện thoại hoặc bất kỳ nền tảng mạng xã hội nào. Mọi hoạt động tố tụng đều được thực hiện thông qua giấy triệu tập, giấy mời chính thức và làm việc trực tiếp tại trụ sở cơ quan có thẩm quyền.

❖ **Chiếm đoạt tài khoản mạng xã hội và mạo danh người thân**

Cách thức chiếm đoạt: Kẻ lừa đảo thường gửi các đường link lừa đảo (phishing) qua tin nhắn với các nội dung hấp dẫn như "bình chọn cho bé", "nhận quà miễn phí". Khi nạn nhân nhấp vào và đăng nhập, thông tin tài khoản Facebook, Zalo sẽ bị đánh cắp.

Kỹ thuật "nghiên cứu" nạn nhân: Sau khi chiếm quyền kiểm soát tài khoản, kẻ lừa đảo không hành động ngay. Thay vào đó, chúng dành thời gian âm thầm đọc lại các đoạn hội thoại cũ để nắm bắt cách xưng hô, mối quan hệ thân thiết, và các vấn đề tài chính gần đây của chủ tài khoản. Quá trình "nằm vùng" này giúp chúng tạo ra các kịch bản vay tiền hết sức tự nhiên và thuyết phục.

Vượt qua bước xác minh: Khi người nhận tin nhắn tỏ ra nghi ngờ và yêu cầu gọi điện xác nhận, kẻ lừa đảo sẽ sử dụng hình ảnh và video cũ của nạn nhân (lấy từ chính tài khoản mạng xã hội) để thực hiện một cuộc gọi video rất ngắn, chỉ vài giây. Chất lượng hình ảnh thường mờ, rung lắc, và không có âm thanh hoặc âm thanh rất kém. Ngay sau đó, chúng sẽ ngắt kết nối và nhắn tin lại với lý do "sóng yếu", "đang ở ngoài đường, không tiện nói chuyện", đủ để nạn nhân tin rằng mình vừa nói chuyện với người thật và tiến hành chuyển tiền.

❖ **Mạo danh doanh nghiệp (Ngân hàng, Nhà mạng, Công ty tài chính)**

Hỗ trợ vay vốn và tuyển dụng: Các đối tượng tạo ra các trang Facebook, website giả mạo các công ty tài chính, ngân hàng uy tín, sau đó chạy quảng cáo các gói vay với thủ tục đơn giản, lãi suất thấp. Khi có người liên hệ, chúng sẽ yêu cầu nạn nhân cài đặt một ứng dụng lạ (thực chất là phần mềm gián điệp) hoặc nộp các khoản phí vô lý như "phí duyệt hồ sơ", "phí bảo hiểm khoản vay" rồi chiếm đoạt.

Thông báo sự cố tài khoản/thẻ: Kẻ lừa đảo gửi SMS Brandname giả mạo ngân hàng hoặc gọi điện thông báo tài khoản của nạn nhân có giao dịch bất thường, sắp bị khóa. Chúng yêu cầu nạn nhân truy cập vào một trang web phishing có giao diện giống hệt trang web của ngân hàng để cung cấp tên đăng nhập, mật khẩu và mã OTP. Ngay khi có được thông tin này, chúng sẽ rút hết tiền trong tài khoản của nạn nhân.

Yêu cầu chuẩn hóa thuê bao di động: Giả danh nhân viên nhà mạng, các đối tượng gọi điện hoặc nhắn tin đe dọa sẽ khóa SIM hai chiều nếu người dùng không "chuẩn hóa thông tin thuê bao". Sau đó, chúng hướng dẫn nạn nhân thực hiện các cú pháp trên điện thoại, thực chất là cú pháp chuyển hướng cuộc gọi. Khi đã chiếm quyền nhận cuộc gọi, chúng sẽ sử dụng số điện thoại của nạn nhân để đăng nhập và chiếm đoạt các tài khoản mạng xã hội, ví điện tử, tài khoản ngân hàng liên kết với số điện thoại đó.

❖ **Lừa đảo sử dụng công nghệ Deepfake**

Cuộc gọi video khẩn cấp: Đây là kịch bản phổ biến và nguy hiểm nhất. Kẻ lừa đảo thu thập hình ảnh, video và giọng nói của một người từ tài khoản mạng xã hội của họ. Sau đó, chúng sử dụng Deepfake để tạo một cuộc gọi video giả mạo người đó, dựng lên một tình huống khẩn cấp như bị tai nạn, bị bắt cóc, hoặc cần tiền gấp để giải quyết công việc. Cuộc gọi thường ngắn, chất lượng không hoàn hảo, nhưng đủ để khiến người thân, bạn bè tin tưởng và lập tức chuyển tiền.

Gian lận tài chính quy mô lớn: Công nghệ này cũng được sử dụng trong các vụ lừa đảo doanh nghiệp. Một ví dụ điển hình là vụ việc tại Hồng Kông, nơi một nhân

viên tài chính đã bị lừa chuyển 25 triệu USD sau khi tham gia một cuộc họp trực tuyến. Kẻ lừa đảo đã sử dụng Deepfake để giả mạo hình ảnh và giọng nói của Giám đốc tài chính và nhiều đồng nghiệp khác trong cuộc họp, tạo ra một môi trường hoàn toàn đáng tin cậy để ra lệnh chuyển tiền.

Tống tiền và phá hoại danh tiếng: Một mối đe dọa khác là việc tạo ra các video hoặc hình ảnh nhạy cảm giả mạo. Kẻ xấu có thể ghép khuôn mặt của nạn nhân vào các nội dung khiêu dâm hoặc các hành vi phạm pháp, sau đó sử dụng chúng để tống tiền hoặc phát tán lên mạng xã hội nhằm hủy hoại danh dự, uy tín cá nhân và nghề nghiệp của nạn nhân.

Dấu hiệu nhận biết cuộc gọi video Deepfake bao gồm các dấu hiệu sau:

Về hình ảnh: Biểu cảm và chuyển động: Khuôn mặt của đối tượng thường khá "trơ", thiếu cảm xúc tự nhiên, hoặc biểu cảm không phù hợp với lời nói. Chuyển động của đầu, mắt và cơ thể có thể không đồng nhất với nhau. Chi tiết khuôn mặt: Tần suất chớp mắt bất thường (quá nhiều hoặc quá ít). Đường viền khuôn mặt, tóc, hoặc tai có thể bị mờ, nhòe hoặc biến dạng khi đối tượng quay đầu. Màu sắc và ánh sáng: Màu da của nhân vật có thể trông không tự nhiên, hoặc thay đổi nhẹ giữa các khung hình. Ánh sáng và bóng đổ trên khuôn mặt có thể không nhất quán với môi trường xung quanh.

Về âm thanh:Đồng bộ hóa: Chuyển động của môi thường không khớp hoàn toàn với lời nói. Chất lượng: Âm thanh có thể bị méo, không đều, có nhiều tiếng ồn lạ hoặc giọng nói thiếu ngữ điệu, cảm xúc tự nhiên.

Về hành vi và bối cảnh: Thời lượng cuộc gọi: Các cuộc gọi video lừa đảo thường rất ngắn (chỉ vài giây), sau đó đối tượng sẽ đột ngột ngắt kết nối với lý do như "sóng yếu", "mạng chập chờn". Tương tác: Khi nạn nhân gọi lại, đối tượng thường không nghe máy hoặc nếu có, chúng có thể lặp lại những câu nói đã được lập trình sẵn.

❖ **Quy trình xử lý khi có dấu hiệu lừa đảo với "3 bước"**

Dừng lại: Giữ bình tĩnh, không hành động vội vàng theo yêu cầu của đối tượng. Kẻ lừa đảo luôn cố gắng tạo ra cảm giác cấp bách để nạn nhân không có thời gian suy nghĩ.

Xác minh: Cúp máy và chủ động liên lạc lại với người thân, bạn bè qua một kênh khác mà bạn tin tưởng (ví dụ: gọi vào số điện thoại đã lưu trong danh bạ từ trước). Đặt ra những câu hỏi mang tính cá nhân, những kỷ niệm riêng mà chỉ người thật mới biết để xác thực danh tính.

Hành động: Chỉ thực hiện việc chuyển tiền sau khi đã xác minh chắc chắn thông tin là thật. Nếu xác định đây là một vụ lừa đảo, hãy ngay lập tức thông báo cho người thân có liên quan và báo cáo cho cơ quan chức năng.

Khi nhận ra mình đã trở thành nạn nhân của một vụ lừa đảo, hành động nhanh chóng và quyết đoán là yếu tố then chốt để giảm thiểu thiệt hại.

Ngừng mọi liên lạc: Chặn ngay lập tức số điện thoại, tài khoản mạng xã hội và mọi kênh liên lạc khác của kẻ lừa đảo để tránh bị thao túng thêm.

Liên hệ ngân hàng: Đây là bước quan trọng nhất. Gọi ngay đến số hotline chính thức của ngân hàng để thông báo về vụ lừa đảo. Yêu cầu họ phong tỏa khẩn cấp tài khoản của bạn và nếu có thể, truy vết và tạm khóa tài khoản của kẻ lừa đảo đã nhận tiền. Cung cấp đầy đủ thông tin về giao dịch để ngân hàng có cơ sở xử lý. Một số hotline ngân hàng lớn tại Việt Nam bao gồm: Vietcombank (1900545413), Agribank (1900558818), Techcombank (1800588822), MBBank (1900545426).

Thu thập và lưu trữ bằng chứng: Tập hợp tất cả các bằng chứng liên quan đến vụ lừa đảo, bao gồm: ảnh chụp màn hình các đoạn tin nhắn, thông tin số tài khoản và tên chủ tài khoản của kẻ lừa đảo, các file ghi âm cuộc gọi, video (nếu có), và các biên lai chuyển tiền thành công.

Bảng 1: Bảng tổng hợp các hình thức lừa đảo trực tuyến

Hình thức mạo danh	Mục tiêu chính	Thủ đoạn đặc trưng	Dấu hiệu nhận biết nhanh
Cơ quan chức năng	Gây hoang mang, đe dọa tâm lý để ép buộc nạn nhân.	Gọi điện thoại thông báo nạn nhân có liên quan đến vụ án nghiêm trọng, yêu cầu chuyển tiền vào tài khoản chỉ định để "phục vụ điều tra".	Cơ quan chức năng không bao giờ làm việc, điều tra hoặc yêu cầu chuyển tiền qua điện thoại hay mạng xã hội.
Người thân/ Bạn bè	Lợi dụng tình cảm, sự tin tưởng và tính cấp bách.	Chiếm đoạt tài khoản mạng xã hội, nhắn tin vay tiền gấp, thực hiện cuộc gọi video ngắn, chất lượng mờ ảo để tạo lòng tin.	Yêu cầu chuyển tiền bất thường, giọng điệu hoặc cách xưng hô lạ, chất lượng cuộc gọi video kém và thời gian ngắn.
Doanh	Lợi dụng uy tín	Gửi SMS/email giả mạo,	Địa chỉ URL lạ, yêu cầu

nghiệp/ Tổ chức	thương hiệu và sự thiếu cảnh giác của khách hàng.	tạo website lừa đảo (phishing), mời chào vay vốn, thông báo khóa SIM, thông báo trúng thưởng.	cung cấp thông tin nhạy cảm (mật khẩu, mã OTP), hứa hẹn lợi ích bất thường, có lỗi chính tả.
Deepfake	Lừa đảo tài chính, mạo danh người thân hoặc lãnh đạo để chiếm đoạt tiền	Dùng video/giọng nói giả mạo bằng AI để đóng giả người quen, cấp trên, hoặc cơ quan chính thống	Nói chuyện không tự nhiên, giọng đều đều, không tương tác linh hoạt; video mờ, cứng, âm thanh không khớp khẩu hình

6.2.2.2. Bị tấn công cài mã độc để lấy cắp dữ liệu.

Virus: Là loại mã độc tự nhân bản bằng cách chèn mã của nó vào các chương trình hoặc tệp tin khác. Virus cần một hành động từ người dùng, chẳng hạn như mở một tệp bị nhiễm, để kích hoạt và bắt đầu quá trình lây lan. Ví dụ:

- Khi có email được gửi đến, kế toán mở "Hóa_đơn_9-2025.xlsm" từ email lạ → macro chạy, chèn mã vào các file Office khác, tự gửi email lây lan tiếp cho đồng nghiệp.
- Tác hại gây ra: phá hỏng/làm hư file tài liệu, làm chậm máy, vô hiệu hoá antivirus; lây sang file chia sẻ nội bộ, tạo "ổ dịch" trong phòng ban.
- Dấu hiệu nhận biết: File tự tăng kích thước, xuất hiện shortcut lạ, Office hỏi bật macro bất thường.

Sâu máy tính: Tương tự như virus ở khả năng tự nhân bản, nhưng sâu máy tính nguy hiểm hơn ở chỗ chúng có thể tự lây lan qua các mạng máy tính mà không cần bất kỳ sự tương tác nào từ người dùng. Chúng thường khai thác các lỗ hổng bảo mật trong hệ điều hành để di chuyển từ máy tính này sang máy tính khác, có khả năng gây tê liệt toàn bộ hệ thống mạng. Ví dụ:

- Một máy Windows chưa vá lỗi kết nối Wi-Fi công ty → Worm xâm nhập, dùng máy đó làm bàn đạp quét toàn mạng; vài phút sau hàng chục máy CPU 100%, mạng nội bộ tê liệt.
- Tác hại: tốc độ lây nhiễm cực kỳ nhanh, có thể bị cài thêm các loại mã độc khác, lợi dụng máy để thực hiện việc khai thác tiền ảo, làm chậm tốc độ Internet, dừng hoạt động các dịch vụ trong mạng nội bộ.

- Dấu hiệu: thiết bị mặc dù chưa chạm gì đã nóng/rít quạt; quản trị viên hệ thống mạng xem bản ghi kết nối phát hiện nhiều kết nối lạ ra/vào, log tường lửa rất nhiều dấu vết được ghi lại.

Ngựa Troja: Đây là một trong những loại mã độc nguy hiểm nhất, hoạt động bằng cách ngụy trang thành một phần mềm hợp pháp hoặc hữu ích để lừa người dùng cài đặt. Một khi đã xâm nhập thành công, Trojan sẽ tạo ra một "cửa hậu" (backdoor), cho phép kẻ tấn công truy cập và kiểm soát hệ thống từ xa. Từ đó, chúng có thể đánh cắp dữ liệu, theo dõi hoạt động của người dùng hoặc cài đặt thêm các loại mã độc khác như ransomware. Ví dụ:

- Người dùng tải "Zoom_Portable_Full_Crack.exe" → cài xong tưởng bình thường nhưng Trojan âm thầm mở backdoor (cửa hậu) chờ kẻ tấn công truy cập.
- Tác hại: bị điều khiển từ xa, cài thêm keylogger(ghi lại những nội dung người dùng gõ phím), ransomware; đánh cắp mật khẩu trình duyệt, dữ liệu công việc.
- Dấu hiệu: rất khó để phát hiện đối với người dùng phổ thông; với người có chuyên môn về an ninh mạng có thể theo dõi cổng mạng lạ mở (netstat thấy kết nối đến IP bất thường), bật/tắt chuột, cửa sổ hiện rồi tắt, antivirus bị tắt.

Mã độc tống tiền: Loại mã độc này thực hiện mã hóa các tệp tin trên thiết bị của nạn nhân, khiến họ không thể truy cập được dữ liệu của mình. Sau đó, kẻ tấn công sẽ yêu cầu một khoản tiền chuộc, thường là bằng tiền điện tử, để đổi lấy khóa giải mã. Đây là một trong những mối đe dọa gây thiệt hại tài chính trực tiếp và nặng nề nhất hiện nay. Ví dụ:

- Nhân viên mở tệp "Đơn_đặt_hàng_2025.pdf.exe" nhìn qua sẽ nghĩ là file "pdf" thông thường nhưng thực chất là file cài đặt "exe" → vài phút sau file máy chủ và thư mục chung bị đổi sang đuôi .lock/.encrypted, xuất hiện thư "readme_restore.txt" đòi tiền mã hoá.
- Tác hại: không truy cập được vào tài liệu, ảnh hưởng công việc công ty, dừng vận hành, thất thoát doanh thu, dữ liệu bị rò rỉ ra ngoài.
- Dấu hiệu: File có dấu hiệu bị đổi đuôi lạ ("pdf.exe")

Phần mềm gián điệp & Phần mềm quảng cáo: Phần mềm gián điệp được thiết kế để bí mật thu thập thông tin về người dùng, bao gồm lịch sử duyệt web, thông tin đăng nhập và dữ liệu cá nhân. Phần mềm quảng cáo thì tự động hiển thị các quảng cáo

không mong muốn. Cả hai đều xâm phạm nghiêm trọng đến quyền riêng tư và có thể làm giảm đáng kể hiệu suất củathiết bị.

6.2.2.3. Giao dịch trực tuyến an toàn

Thanh toán trực tuyến, từ mua sắm trên các sàn thương mại điện tử đến chuyển khoản qua ứng dụng ngân hàng, đã trở thành một phần không thể thiếu trong đời sống hiện đại. Tội phạm mạng không ngừng phát triển các thủ đoạn mới để đánh cắp thông tin và chiếm đoạt tài sản, biến không gian mạng thành một môi trường tiềm ẩn nhiều cạm bẫy.

Ngân hàng Nhà nước Việt Nam đã ban hành Quyết định 2345/QĐ-NHNN(Ngân hàng Nhà nước, 2023), Quy định này bắt buộc các giao dịch trực tuyến phải được xác thực bằng sinh trắc học (cụ thể là nhận dạng khuôn mặt, đối chiếu với dữ liệu sinh trắc học được lưu trong chip của thẻ Căn cước công dân) đối với các giao dịch có giá trị cao. Các ngưỡng áp dụng bao gồm:

- Giao dịch chuyển tiền có giá trị trên 10 triệu đồng mỗi lần.
- Tổng giá trị giao dịch chuyển tiền trong ngày vượt quá 20 triệu đồng.

Một số hình thức lừa đảo phổ biến hiện này liên quan đến giao dịch trực tuyến bao gồm:

❖ **Giả danh nhân viên giao hàng (shipper) để yêu cầu thanh toán hoặc cung cấp thông tin**

Đối tượng mạo danh nhân viên giao hàng, gọi điện thông báo có bưu phẩm đang được gửi đến, nhưng "thiếu phí xử lý, phí hoàn tất hồ sơ" hoặc "thiếu thông tin nhận hàng". Kẻ lừa đảo tạo cảm giác gấp gáp và yêu cầu người dùng chuyển khoản ngay một khoản phí nhỏ, thường chỉ vài chục đến vài trăm nghìn đồng để "hoàn tất thủ tục".

Một số trường hợp còn gửi đường link giả dạng website của công ty chuyển phát (như Giao hàng nhanh, Viettel Post, EMS…), yêu cầu điền thông tin cá nhân hoặc tài khoản ngân hàng. Sau đó, lợi dụng thông tin người dùng để chiếm đoạt tiền trong tài khoản. Dấu hiệu nhận biết bao gồm:

- Không có đơn hàng nào trước đó nhưng vẫn báo có hàng gửi.
- Nói năng gấp gáp, dùng số điện thoại lạ (không phải tổng đài).
- Gửi link lạ, yêu cầu chuyển khoản hoặc cung cấp thông tin riêng tư.

❖ **Giả mạo hóa đơn điện, nước, internet để chiếm đoạt tiền**

Tội phạm mạng gọi điện hoặc nhắn tin tự xưng là nhân viên công ty điện lực, cấp nước, viễn thông, thông báo người dùng đang "nợ tiền hóa đơn", nếu không thanh toán ngay sẽ bị cắt dịch vụ. Kèm theo đó là đường link để thanh toán nhanh hoặc mã QR giả.

Khi người dùng bấm vào link hoặc quét mã QR, sẽ bị điều hướng đến trang giả mạo có giao diện giống hệ thống thanh toán điện tử, nơi kẻ gian thu thập thông tin thẻ ngân hàng, OTP, hoặc cài mã độc. Dấu hiệu nhận biết:

- Tin nhắn/cuộc gọi đến ngoài giờ hành chính, xưng danh nhân viên nhưng không nói rõ thuộc chi nhánh nào.
- Số điện thoại không phải đầu số tổng đài chính thức.
- Link thanh toán nhìn giống thật nhưng sai tên miền, ví dụ: *evn-thanh-toan.net (thay vì evn.com.vn).*

❖ **Lừa đảo qua mã QR giả**

Mã QR là công cụ tiện lợi nhưng cũng dễ bị lợi dụng để lừa đảo. Đối tượng có thể:

- Gửi mã QR qua tin nhắn/Zalo/Facebook bảo là để "xác nhận thông tin", "nhận hoàn tiền" hoặc "nhận quà khuyến mãi".
- Đặt mã QR giả tại nơi công cộng (như thay mã chuyển khoản tại quán cà phê, bãi giữ xe, tờ rơi khuyến mãi).

Khi người dùng quét mã, có thể bị điều hướng đến trang thanh toán giả hoặc cài đặt phần mềm độc hại âm thầm trên thiết bị. Dấu hiệu nhận biết:

- Mã QR xuất hiện bất ngờ, không rõ nguồn gốc.
- Trang web mở ra yêu cầu cung cấp thông tin thẻ hoặc đăng nhập tài khoản ngân hàng.
- Giao diện quen nhưng có lỗi chính tả nhỏ hoặc thiếu yếu tố xác thực (biểu tượng khóa, tên miền an toàn)

6.2.2.4. Nhận diện lừa đảo, mã độc và bảo vệ tài chính trực tuyến

❖ **Tấn công lừa đảo– Mối đe dọa Số 1**

Lừa đảo là hành vi kẻ xấu giả mạo là tổ chức uy tín (Ngân hàng, Cơ quan thuế, Facebook, v.v.) để lừa bạn cung cấp thông tin cá nhân, mật khẩu hoặc mã OTP.

Bảng 2. Hướng dẫn nhận biết tấn công lừa đảo

Loại hình	Mô tả kẻ xấu	Dấu hiệu nhận biết quan trọng
Giả mạo Email (Email/Web)	Email giả mạo thông báo tài khoản bị khóa, yêu cầu nhấp vào liên kết (link) để đăng nhập lại ngay lập tức.	1. Địa chỉ Email lạ: Người gửi có địa chỉ email không phải của tổ chức chính thức (ví dụ: `nganhangA@gmail.com` thay vì `hotro@nganhangA.vn`). 2. Lỗi chính tả/Thiết kế: Email có lỗi chính tả, hoặc thiết kế (logo, font chữ) trông không chuyên nghiệp. 3. Liên kết (Link) Lạ: Khi di chuột qua link, thấy địa chỉ không phải của trang chính thức (ví dụ: `facebook.com.vn-security.biz`).
Giả mạo tin nhắn (SMS/Zalo)	Tin nhắn SMS/Zalo thông báo trúng thưởng, nhận quà, hoặc cảnh báo bạn đang nợ tiền, yêu cầu gọi lại hoặc nhấp vào link.	1. Yêu cầu khẩn cấp/Đe dọa: Thúc giục hành động *ngay lập tức* (ví dụ: "Tài khoản sẽ bị khóa sau 2 giờ"). 2. Yêu cầu lợi ích: Hứa hẹn phần thưởng quá lớn (ví dụ: "Trúng Iphone 15").
Kỹ thuật xã hội	Kẻ xấu giả danh người thân/bạn bè (qua Facebook/Zalo bị hack) nhắn tin vay tiền, nhờ mua thẻ cào hoặc lừa cung cấp Mã OTP.	1. Ngôn ngữ khác thường: Cách nói chuyện khác biệt so với người thân của bạn. 2. Yêu cầu chuyển tiền gấp: Đòi hỏi chuyển khoản ngay mà không có lý do rõ ràng.

- ***Quy tắc VÀNG phòng tránh***

Luôn luôn nghi ngờ! Đừng bao giờ hành động dựa trên cảm xúc (sợ hãi hoặc tham lam) khi nhận được các thông báo lạ.

Tuyệt đối không nhấp: Không nhấp vào liên kết (link) hay tải về tệp đính kèm từ người lạ, ngay cả khi người gửi trông có vẻ quen.

Kiểm tra kỹ Lưỡng: Nếu nhận được cảnh báo từ Ngân hàng/Facebook, hãy tự mở trình duyệt và gõ địa chỉ trang web chính thức để kiểm tra (ví dụ: tự gõ `facebook.com`), không dùng link trong email/tin nhắn.

Không cung cấp OTP/Mật khẩu: Không bao giờ cung cấp mã OTP, mật khẩu, hay số PIN cho bất kỳ ai, kể cả nhân viên ngân hàng (họ sẽ không bao giờ hỏi).

❖ **Phần mềm độc hại và mã độc tống tiền**

Nhận diện mã độc

- ✔ **Phần mềm độc hại:** Là thuật ngữ chung cho các phần mềm được tạo ra để phá hoại, đánh cắp dữ liệu, hoặc kiểm soát thiết bị của bạn.
- ✔ **Mã độc tống tiền:** Là loại mã độc nguy hiểm, khi xâm nhập sẽ mã hóa (khóa) tất cả dữ liệu trên thiết bị và yêu cầu bạn trả tiền chuộc để mở khóa.
- ✔ **Tác hại:** Mất vĩnh viễn dữ liệu quý giá (ảnh gia đình, tài liệu công việc) nếu bạn không có bản sao lưu (backup).

Hành động phòng tránh

- ✔ **Tuyệt đối không tải lậu:** Không tải các phần mềm "bẻ khóa", trò chơi game lậu, hay ứng dụng từ các nguồn không chính thức (ví dụ: các trang web không phải App Store hoặc Google Play Store).
- ✔ **Sao lưu dữ liệu thường xuyên:** Đây là biện pháp phòng thủ cuối cùng và hiệu quả nhất.
- ✔ **Thực hiện:** Thường xuyên sao lưu dữ liệu quan trọng lên đám mây (như Google Drive, iCloud, Dropbox) hoặc ổ cứng ngoài.
- ✔ **Lợi ích:** Nếu bị mã độc tấn công, bạn có thể xóa sạch thiết bị và khôi phục dữ liệu từ bản sao lưu mà không cần trả tiền chuộc.
- ✔ **Không chạy tệp lạ:** Không mở hoặc chạy các tệp lạ có đuôi .exe hoặc các tệp đính kèm lạ trong email.

❖ **Bảo mật giao dịch và thanh toán trực tuyến**

- ***Kiểm tra bảo mật trang web***
  - ✔ **Kiểm tra HTTPS:** Trước khi nhập bất kỳ thông tin thẻ ngân hàng hoặc mật khẩu nào, luôn kiểm tra trên thanh địa chỉ trình duyệt:
    - Có biểu tượng ổ khóa màu xanh lá cây hoặc màu xám.
    - Địa chỉ bắt đầu bằng `https://` (chứ không phải `http://`).
    - Ý nghĩa: Điều này đảm bảo kết nối của bạn đã được mã hóa an toàn, khó bị kẻ xấu nghe lén.
- ***Sử dụng phương thức thanh toán an toàn***

- ✔ **Ưu tiên cổng thanh toán uy tín:** Ưu tiên thanh toán qua các cổng thanh toán trung gian lớn, đã được bảo mật (ví dụ: VNPay, Momo, ZaloPay, PayPal).
- ✔ **Hạn chế nhập thẻ trực tiếp:** Hạn chế nhập trực tiếp số thẻ tín dụng/ATM vật lý vào các trang web nhỏ hoặc lần đầu giao dịch.
- ✔ **Sử dụng thẻ ảo/thẻ phụ:**
  - Nếu ngân hàng của bạn cung cấp Thẻ ảo (Virtual Card) hoặc Thẻ phụ (Secondary Card), hãy sử dụng chúng cho các giao dịch online.
  - Bạn có thể giới hạn số tiền trong thẻ phụ/thẻ ảo, hoặc hủy thẻ ngay sau khi giao dịch, giảm thiểu rủi ro nếu thông tin thẻ bị lộ.

❖ **Quy tắc an toàn khi dùng wifi công cộng**

- ***Nhận diện và kết nối mạng an toàn***
  - ✔ *Xác minh nguồn*: Luôn hỏi nhân viên hoặc quản lý địa điểm (quán cà phê, sân bay, ga tàu …) về tên chính xác của mạng wi-fi công cộng. Kẻ xấu thường tạo ra các mạng giả mạo có tên tương tự. Ví dụ như "Free-café-wifi".
  - ✔ *Ưu tiên mạng có mật khẩu*: Chỉ kết nối vào các mạng có yêu cầu mật khẩu. Mạng mở (không có mật khẩu) có độ bảo mật thấp nhất.
  - ✔ *Tránh tự động kết nối*: Tắt tính năng Tự động kết nối (Auto-connect) trên điện thoại và máy tính. Điều này ngăn thiết bị của bạn tự động tham gia vào các mạng wi-fi đã lưu mà không có sự cho phép của bạn.
- ***Quy tắc vàng bảo mật dữ liệu***

Hành động BẮT BUỘC TRÁNH	Hành động NÊN LÀM thay thế
Tuyệt đối không thực hiện các giao dịch tài chính (chuyển khoản, thanh toán thẻ).	Sử dụng **mạng 3G/4G/5G** của bạn cho các giao dịch nhạy cảm.
Tuyệt đối không đăng nhập vào tài khoản ngân hàng, email (có chứa mật khẩu), hoặc các ứng dụng lưu trữ tài liệu bí mật.	**Đợi đến khi** về nhà hoặc nơi làm việc có kết nối an toàn để đăng nhập các tài khoản này.
Tuyệt đối không tắt Tường lửa (Firewall) trên máy tính.	Đảm bảo **Tường lửa** của bạn luôn được bật để chặn các kết nối độc hại

	không mong muốn.

- ***Các biện pháp tăng cường bảo vệ***

  ✔ Kiểm tra HTTPS: Khi duyệt web công cộng, luôn kiểm tra xem trang web bạn đang truy cập có biểu tượng ổ khóa và bắt đầu bằng https:// hay không. Điều này xác nhận kết nối của bạn được mã hóa.

  ✔ Sử dụng mạng riêng ảo (VPN):

  - VPN là gì? VPN tạo ra một đường hầm mã hóa giữa các thiết bị của bạn và Internet.
  - Lợi ích: Ngay cả khi tin tặc chặn được dữ liệu của bạn trên wi-fi công cộng, chúng cũng không thể đọc được nội dung vì dữ liệu đã được mã hóa.
  - Hành động: Cân nhắc cài đặt và sử dụng dịch vụ VPN uy tín (có trả phí hoặc miễn phí phiên bản giới hạn) khi bắt buộc phải dùng wi-fi công cộng.

  ✔ Tắt chia sẻ tệp: khi kết nối wi-fi công cộng, hãy tắt ngay tính năng chia sẻ tệp và máy in trên máy tính để ngăn người lạ trong cùng mạng truy cập vào tệp cá nhân của bạn.

6.3. Bảo vệ sức khỏe khi làm việc trong môi trường số

6.3.1. Những yếu tố ảnh hưởng đến sức khỏe và tinh thần khi sử dụng công nghệ số

6.3.1.1. Ảnh hưởng về sức khỏe và tinh thần khi sử dụng công nghệ số

Môi trường làm việc hiện đại, với đặc trưng là thời gian dài tương tác với các thiết bị kỹ thuật số, đã tạo ra những thách thức chưa từng có đối với sức khỏe thể chất. Phần này sẽ đi sâu phân tích các vấn đề phổ biến nhất, từ cơ chế sinh lý bệnh học đến các giải pháp phòng ngừa và điều trị, nhằm cung cấp một cái nhìn toàn diện về gánh nặng thể chất mà người lao động trí thức phải đối mặt.

Sự xuất hiện của CVS bắt nguồn từ những yêu cầu phi tự nhiên mà màn hình kỹ thuật số đặt ra cho hệ thống thị giác của con người.

Giảm tần suất chớp mắt: Khi tập trung cao độ vào màn hình, tần suất chớp mắt của một người có thể giảm xuống chỉ còn khoảng 7 lần mỗi phút, so với mức bình thường là khoảng 20 lần. Việc chớp mắt ít hơn làm gián đoạn quá trình dàn đều lớp

phim nước mắt trên bề mặt nhãn cầu, dẫn đến tình trạng khô mắt, kích ứng, cảm giác cộm rát và đỏ mắt.

Căng thẳng điều tiết: Không giống như chữ in có độ sắc nét cao, các ký tự trên màn hình được tạo thành từ các điểm ảnh, có tâm sáng hơn và mờ dần về phía các cạnh. Điều này buộc hệ thống cơ thể mi của mắt phải liên tục điều tiết để duy trì sự tập trung, gây ra tình trạng quá tải và mỏi cơ, dẫn đến các triệu chứng như mỏi mắt, nhìn mờ và khó tái tập trung từ gần ra xa.

Tác động của ánh sáng xanh: Màn hình LED của các thiết bị điện tử phát ra ánh sáng xanh, một dạng ánh sáng năng lượng cao có thể gây kích thích và góp phần gây mỏi mắt khi tiếp xúc kéo dài.

Các triệu chứng của CVS không chỉ giới hạn ở mắt mà còn có thể ảnh hưởng đến toàn thân:

Tại mắt: Mỏi mắt, căng thẳng thị giác, nhìn mờ, khô mắt, nhức mắt, mắt đỏ, co giật mí mắt và hiện tượng nhìn đôi.

Toàn thân: Nhức đầu, đau cổ, và đau mỏi vai gáy. Các triệu chứng này thường xuất phát từ việc người dùng phải duy trì các tư thế sai lệch (như cúi đầu, rướn người về phía trước) để điều chỉnh tầm nhìn cho phù hợp với màn hình, đặc biệt khi thị lực bắt đầu suy giảm do mỏi mắt.

Cột sống và đĩa đệm: Khi ngồi gù lưng hoặc trượt dài trên ghế, áp lực lên các đĩa đệm cột sống thắt lưng có thể tăng lên đáng kể. Tình trạng này kéo dài sẽ làm mòn các cấu trúc hỗ trợ, đẩy nhanh quá trình thoái hóa cột sống và làm tăng nguy cơ mắc các bệnh lý nghiêm trọng như thoát vị đĩa đệm. Tư thế vắt chéo chân cũng góp phần làm cong vẹo cột sống và mất cân bằng vùng chậu.

Hệ cơ và vai gáy: Tư thế đầu hướng về phía trước khi nhìn vào màn hình gây căng thẳng liên tục cho các cơ ở vùng cổ và vai. Điều này không chỉ gây đau mỏi cục bộ mà còn có thể dẫn đến đau đầu do căng cơ, một trong những loại đau đầu phổ biến nhất.

Tuần hoàn máu và chuyển hóa: Ngồi không đúng tư thế có thể chèn ép các mạch máu, làm cản trở quá trình lưu thông máu đến các cơ quan và chi dưới. Hơn nữa, việc ngồi lâu làm giảm hoạt động của các nhóm cơ lớn, dẫn đến quá trình trao đổi chất chậm lại. Tư thế gập bụng cũng làm dồn trọng tâm vào vùng bụng, khiến cơ bụng và cơ lưng không được hoạt động, góp phần vào việc tích tụ mỡ thừa.

6.3.1.2. Ảnh hưởng tới tinh thần

Cơ chế gây mất ngủ của các thiết bị điện tử có nền tảng khoa học vững chắc, xoay quanh sự tương tác giữa ánh sáng và hệ thống nội tiết của cơ thể.

Vai trò của Melatonin: Cơ thể con người vận hành theo một đồng hồ sinh học nội tại, hay còn gọi là nhịp sinh học, được điều hòa chủ yếu bởi hormone Melatonin. Melatonin được ví như "hormone của bóng tối", được tuyến tùng trong não bộ sản xuất khi môi trường xung quanh tối đi, báo hiệu cho cơ thể rằng đã đến giờ nghỉ ngơi và chuẩn bị cho giấc ngủ.

Sự ức chế của ánh sáng xanh: Màn hình của điện thoại, máy tính bảng và máy tính phát ra ánh sáng trong dải quang phổ màu xanh lam, đặc biệt là ở bước sóng khoảng 450-480nm. Các tế bào cảm quang chuyên biệt trong võng mạc mắt rất nhạy cảm với dải ánh sáng này. Khi tiếp xúc với ánh sáng xanh vào buổi tối, các tế bào này gửi tín hiệu đến não, làm não bộ lầm tưởng rằng vẫn còn là ban ngày. Kết quả là quá trình sản xuất Melatonin bị ức chế mạnh mẽ, khiến cơ thể khó đi vào giấc ngủ và làm giảm chất lượng giấc ngủ.

Sự gián đoạn chu kỳ ngủ-thức tự nhiên gây ra những hậu quả nghiêm trọng cả trong ngắn hạn và dài hạn như sau:

Ngắn hạn: Người bị ảnh hưởng sẽ cảm thấy khó ngủ, giấc ngủ chập chờn, không sâu. Sáng hôm sau, họ thức dậy trong trạng thái mệt mỏi, uể oải, dẫn đến suy giảm khả năng tập trung, giảm trí nhớ và hiệu suất làm việc kém.

Dài hạn: Thiếu ngủ kinh niên là một yếu tố nguy cơ đáng kể đối với nhiều bệnh lý nghiêm trọng, bao gồm các bệnh về chuyển hóa như tăng huyết áp, tiểu đường loại 2, các vấn đề tim mạch, và đặc biệt là các rối loạn sức khỏe tâm thần như trầm cảm và rối loạn lo âu.

Môi trường số không chỉ là nơi kết nối mà còn là một không gian tràn ngập thông tin, trong đó có cả những luồng thông tin tiêu cực và độc hại. Việc tiếp xúc với chúng, dù chủ động hay bị động, đều để lại những vết sẹo sâu sắc lên sức khỏe tâm thần. "Doomscrolling" (hay "doomsurfing") là thuật ngữ mô tả hành vi tiêu thụ một lượng lớn tin tức tiêu cực trên internet một cách liên tục và ám ảnh, mặc dù việc này gây ra cảm giác buồn bã, lo lắng và chán nản.

Thiên kiến tiêu cực: Về mặt tiến hóa, não bộ con người được lập trình để chú ý nhiều hơn đến các mối đe dọa và thông tin tiêu cực như một cơ chế sinh tồn. Trong thế giới hiện đại, thiên kiến này khiến chúng ta dễ bị cuốn hút vào các tin tức xấu.

Nhu cầu kiểm soát: Đối mặt với các sự kiện lớn và bất ổn như đại dịch hay khủng hoảng kinh tế, con người có xu hướng tìm kiếm càng nhiều thông tin càng tốt với hy vọng hiểu rõ và kiểm soát được tình hình, giảm bớt cảm giác bất an. Tuy nhiên, hành vi này thường phản tác dụng, dẫn đến việc bị nhấn chìm trong luồng thông tin tiêu cực.

Tác động tâm lý: được chứng minh là có mối liên hệ trực tiếp với việc gia tăng các triệu chứng lo âu, căng thẳng, trầm cảm, rối loạn giấc ngủ và cảm giác bất lực, vô vọng. Nó tạo ra một vòng luẩn quẩn: lo lắng thúc đẩy việc tìm kiếm thông tin, và thông tin tiêu cực lại càng làm tăng thêm sự lo lắng.

Với tác động của bạo lực mạng như vậy, hậu quả gây ra đối với nạn nhân như sau:

Tâm lý - Tình cảm: Nạn nhân của bạo lực mạng thường trải qua cảm giác xấu hổ, tức giận, lo lắng, bất an và bị cô lập. Tình trạng này kéo dài có thể dẫn đến các vấn đề sức khỏe tâm thần nghiêm trọng như trầm cảm, rối loạn lo âu, và trong những trường hợp bi thảm, có thể dẫn đến ý định tự tử.

Thể chất: Căng thẳng tâm lý mãn tính do bị bắt nạt có thể biểu hiện ra các triệu chứng thể chất như mất ngủ, mệt mỏi, đau đầu và đau bụng.

6.3.2. Bảo vệ bản thân khi làm việc trong môi trường số

❖ **Giải quyết vấn đề thể chất**

- Tối ưu công thái học cho mắt: đặt màn hình cách ~50–70 cm, mép trên thấp hơn tầm mắt ~10–15°; tránh chói bằng chỉnh độ sáng/độ tương phản và bố trí nguồn sáng bên hông, không chiếu thẳng vào màn hình.
- Quy tắc 20–20–20: cứ 20 phút, nhìn vật cách ≥20 feet (≈6 m) trong 20 giây; đây là khuyến cáo tiêu chuẩn của giới nhãn khoa để giảm gánh nặng điều tiết và khô mắt.
- Gia tăng chớp mắt/chớp mắt chủ động; cân nhắc nước mắt nhân tạo khi có khô mắt (theo hướng dẫn lâm sàng về DES).
- Trước giờ ngủ 1–2 giờ, hạn chế màn hình hoặc bật chế độ giảm ánh sáng xanh; bằng chứng thực nghiệm cho thấy dùng thiết bị phát sáng buổi tối trì hoãn tiết melatonin và làm giảm buồn ngủ.

Đối với các triệu chứng đau lưng, cổ, vai gáy:

- Thiết kế công thái học: vai thả lỏng, cẳng tay gần song song sàn, cổ tay trung tính; màn hình đối diện người dùng, mắt cách ~50–70 cm; ghế hỗ trợ thắt lưng và cho phép bàn chân đặt phẳng.
- Nghỉ vi mô và thay đổi tư thế định kỳ (đứng dậy/đi vài bước/giãn cơ mỗi 30–60 phút); bằng chứng quan sát và khuyến cáo công thái học cho thấy gián đoạn tĩnh lực giảm khó chịu cơ xương khớp.
- Rời "thiết bị thấp" (điện thoại/máy tính bảng) khi gõ dài: dùng chân đế/nâng màn hình, bàn phím rời để giảm cúi gập cổ.

❖ **Hành vi và sinh lý**

Để phòng tránh chúng ta cần thực hiện các bước sau:

- "Vùng không màn hình" 1–2 giờ trước ngủ; nếu bắt buộc dùng, bật bộ lọc ấm màu/giảm độ sáng và ưu tiên nội dung ít kích thích.
- Giữ lịch ngủ–thức nhất quán, tận dụng ánh sáng tự nhiên ban ngày để củng cố nhịp sinh học.

Khuyến nghị WHO 2020 nêu rõ: người trưởng thành nên đạt 150–300 phút/tuần hoạt động thể lực mức vừa (hoặc 75–150 phút mức mạnh) và giảm thời gian ngồi tĩnh; trẻ vị thành niên trung bình 60 phút/ngày hoạt động mức vừa–mạnh. Các bài tập bạn có thể tập tại nhà bao gồm:

- Chu kỳ "ngồi–đứng–đi bộ ngắn" 30–60 phút/lần trong ngày làm việc; tận dụng bàn đứng hoặc họp đứng để cắt chuỗi bất động kéo dài.
- Lập "mục tiêu tuần": tối thiểu 150–300 phút mức vừa + 2 buổi tăng cơ; dùng nhắc việc/thiết bị đếm bước để theo dõi

❖ **Sức khỏe tinh thần**

Đối với sức khỏe tinh thần, chúng ta có những cách phòng chống sau:

- "Vệ sinh số" cho nguồn tin: giới hạn thời lượng đọc tin tiêu cực, đặt giờ "ngắt" và ưu tiên nguồn đáng tin (giảm doomscrolling)
- Dùng chủ động có chọn lọc (chia sẻ–tương tác có mục đích) thay vì lướt thụ động; nhiều nghiên cứu ghi nhận dùng thụ động liên hệ nhiều hơn với so sánh xã hội và tâm trạng tiêu cực.
- Thiết lập công cụ chống quấy rối: chặn/báo cáo tài khoản, lưu bằng chứng, và tìm hỗ trợ chuyên môn/kênh pháp lý khi cần.

- Gộp lượt kiểm thông báo theo "khung giờ" (ví dụ: 3–4 lần/ngày) và tắt đẩy thời gian thực cho kênh không khẩn.
- Thiết kế "vùng làm sâu" (deep-work): lịch chặn thông báo 45–90 phút, thông báo cho đồng nghiệp kênh khẩn cấp nếu cần.

Để hệ thống hóa lại toàn bộ các vấn đề và giải pháp đã thảo luận, giúp bạn có một cái nhìn tổng quan và một công cụ tra cứu nhanh chóng trong cuộc sống hàng ngày, bảng tổng hợp dưới đây sẽ tóm lược những thông tin cốt lõi nhất.

Bảng 3. Triệu chứng và biện pháp bảo vệ sức khỏe khi làm việc trong môi trường số

Lĩnh vực ảnh hưởng	**Vấn đề cụ thể**	**Triệu chứng/Biểu hiện chính**	**Nguyên nhân cốt lõi**	**Biện pháp bảo vệ (Cá nhân & Môi trường)**
Thể chất	Hội chứng Thị giác máy tính (CVS)	Mỏi mắt, khô mắt, nhìn mờ, đau đầu	Giảm chớp mắt, căng thẳng điều tiết, ánh sáng xanh	Áp dụng quy tắc 20-20-20, tối ưu vị trí màn hình và ánh sáng, sử dụng nước mắt nhân tạo
	Đau lưng, cổ, vai gáy	Đau mỏi các vùng cơ xương, cong vẹo cột sống, gù lưng	Ngồi lâu, sai tư thế, thiếu vận động	Thiết lập không gian làm việc công thái học (ghế, bàn, màn hình), thường xuyên đứng dậy vận động, kéo giãn
Hành vi & Sinh lý	Mất ngủ	Khó đi vào giấc ngủ, giấc ngủ không sâu, mệt mỏi	Ánh sáng xanh ức chế sản xuất melatonin, rối loạn nhịp sinh học	Ngừng sử dụng thiết bị điện tử 1-2 giờ trước khi ngủ, bật chế độ lọc ánh sáng xanh, tạo môi trường ngủ tối và yên tĩnh
	Nghiện mạng xã hội & Game	Sử dụng quá mức, lo lắng khi không được dùng, sao lãng công việc và cuộc sống	Vòng lặp Dopamine, hội chứng FOMO, thiết kế nền tảng gây nghiện	Tắt thông báo, đặt giới hạn thời gian sử dụng, thực hành "digital detox", tăng cường hoạt động thực tế

		thực		
Tinh thần	Tác động tâm lý	Liên tục xem tin tức tiêu cực, cảm giác lo âu, bất lực, trầm cảm	Thiên kiến tiêu cực, nhu cầu kiểm soát thông tin trong bối cảnh bất ổn	Giới hạn thời gian đọc tin tức, chọn lọc nguồn tin uy tín, thực hành chánh niệm, tham gia hoạt động sáng tạo để giải tỏa
	Bạo lực mạng	Bị công kích, lăng mạ, đe dọa trên mạng; cảm thấy xấu hổ, cô lập, trầm cảm	Hành vi bắt nạt có chủ đích của người khác trên không gian số	Không phản ứng, lưu bằng chứng, chặn và báo cáo kẻ bắt nạt, tìm kiếm sự hỗ trợ từ người thân và chuyên gia

6.4. Bảo vệ môi trường số

6.4.1. Tác động của công nghệ số đối với môi trường

Thế kỷ 21 được định hình bởi sự trỗi dậy mạnh mẽ của công nghệ số. Từ cách chúng ta giao tiếp, vận hành nền kinh tế, đến quản trị xã hội, cuộc cách mạng kỹ thuật số đã len lỏi vào mọi khía cạnh của đời sống hiện đại, tạo ra một thế giới kết nối với tốc độ tăng trưởng dữ liệu và thiết bị theo cấp số nhân. Về lý thuyết, công nghệ số hứa hẹn một tương lai "phi vật chất", nơi các quy trình được tối ưu hóa, tài nguyên được sử dụng hiệu quả hơn và nhiều hoạt động vật lý được thay thế bằng các tương tác ảo.

Sự gia tăng chóng mặt của rác thải điện tử không phải là một hiện tượng ngẫu nhiên mà được thúc đẩy bởi các yếu tố kinh tế và xã hội sâu sắc.

Vòng đời sản phẩm ngắn: Động lực cốt lõi của ngành công nghệ là sự đổi mới không ngừng, tạo ra các sản phẩm nhanh hơn, mạnh hơn và nhiều tính năng hơn. Chu kỳ đổi mới này trực tiếp rút ngắn tuổi thọ của các sản phẩm hiện có, khiến các thiết bị chỉ mới vài năm tuổi đã trở nên lỗi thời. Điều này tạo ra một vòng lặp luẩn quẩn: sự thành công về mặt công nghệ và kinh tế lại trực tiếp thúc đẩy cuộc khủng hoảng rác thải điện tử, biến nó thành một đặc tính cố hữu của mô hình kinh doanh công nghệ hiện tại thay vì là một tác dụng phụ không mong muốn.

Chủ nghĩa tiêu dùng và nhu cầu không bền vững: Cùng với sự phát triển của công nghệ là sự thay đổi trong hành vi người tiêu dùng. Nhu cầu liên tục cập nhật các thiết bị mới nhất và các đòi hỏi ngày càng cao về tiện ích và tính năng đã thúc đẩy một

nền văn hóa "thay thế thay vì sửa chữa". Việc tiêu dùng thiếu bền vững này là một trong những nguyên nhân chính khiến các bãi rác điện tử không ngừng bành trướng.

Sự thiếu hiệu quả của hệ thống thu gom và xử lý: Tại nhiều quốc gia đang phát triển, bao gồm cả Việt Nam, hệ thống thu gom và xử lý rác thải điện tử chuyên nghiệp còn rất yếu kém hoặc chưa tồn tại. Hầu hết các thiết bị thải bỏ bị vứt chung với rác thải sinh hoạt hoặc rơi vào tay các cơ sở tái chế phi chính thức, dẫn đến việc xả thải các chất độc hại ra môi trường một cách không kiểm soát.

Sự phát triển bùng nổ của Trí tuệ nhân tạo (AI), đặc biệt là các mô hình AI tạo sinh, đang đẩy nhu cầu năng lượng của các trung tâm dữ liệu lên một tầm cao mới. Các tác vụ huấn luyện và vận hành AI đòi hỏi năng lực tính toán cực lớn, dẫn đến việc tiêu thụ điện năng cao hơn đáng kể. Một máy chủ AI trang bị 8 GPU có thể tiêu thụ tới 10,2 kW điện, cao hơn nhiều so với các máy chủ truyền thống. Các dự báo từ IEA và Morgan Stanley cho thấy mức tiêu thụ điện của các trung tâm dữ liệu chuyên dụng cho AI có thể tăng gấp bốn lần, và lượng khí thải carbon liên quan có thể tăng gấp ba vào năm 2030.

6.4.2. Các biện pháp bảo vệ môi trường khi sử dụng thiết bị số

6.4.2.1. "Cơn khát" năng lượng vô hình

❖ **Giải pháp từ các "Gã khổng lồ" Công nghệ**

Dùng năng lượng sạch: Họ đang đầu tư hàng tỷ đô la vào năng lượng mặt trời và gió. Mục tiêu của Google là đến năm 2030, mỗi giờ hoạt động của họ sẽ dùng năng lượng sạch được tạo ra ngay tại thời điểm đó [13]. Điều này giống như việc bạn chỉ dùng điện khi nhà bạn có nắng hoặc gió, thay vì dùng điện lưới rồi cuối tháng trồng một cái cây để "bù đắp".

Làm mát thông minh hơn: Thay vì chỉ dùng điều hòa, họ tìm đến những giải pháp sáng tạo. Microsoft đã thử nghiệm đặt trung tâm dữ liệu dưới đáy biển để tận dụng nước lạnh tự nhiên làm mát. Các công nghệ làm mát bằng chất lỏng cũng hiệu quả hơn rất nhiều, giống như hệ thống tản nhiệt nước trong các máy tính cao cấp.

Chọn phần cứng tiết kiệm điện: Việc chuyển từ ổ cứng HDD (loại đĩa từ quay) sang ổ cứng SSD (loại chip nhớ) có thể tạo ra khác biệt lớn. Hãy hình dung ổ HDD giống như một người thủ thư phải chạy đi tìm sách trên các kệ đĩa quay, còn ổ SSD giống như một thư viện số, tìm thông tin ngay lập tức. SSD không chỉ nhanh hơn mà còn tiết kiệm tới 80% năng lượng so với HDD.

❖ **Giải pháp từ chính chúng ta**

Dọn dẹp "đám mây": "Đám mây" không phải là một đám mây thật. Nó là những máy chủ trong trung tâm dữ liệu. Mỗi email rác, mỗi tấm ảnh trùng lặp, mỗi tệp tin không bao giờ dùng đến mà bạn lưu trên Google Drive hay iCloud giống như một bóng đèn nhỏ bị bỏ quên, vẫn âm thầm tiêu thụ điện 24/7. Hãy dành thời gian dọn dẹp định kỳ.

Xem video một cách thông minh: Xem video chất lượng 4K Ultra HD giống như dùng một chiếc xe tải lớn để chở một món hàng nhỏ, rất tốn "xăng" (dữ liệu và năng lượng). Nếu bạn chỉ nghe nhạc hoặc xem những nội dung không đòi hỏi độ sắc nét cao, hãy chuyển chất lượng video xuống 480p. Sự khác biệt về năng lượng là rất đáng kể.

Mua sắm có ý thức: Khi mua đồ điện tử mới, hãy tìm nhãn Energy Star. Nó giống như một "giấy chứng nhận bé ngoan", đảm bảo rằng thiết bị đó được thiết kế để tiêu thụ ít điện năng hơn.

6.4.2.2. "Quả bom nổ chậm" rác thải điện tử

Chiếc điện thoại, laptop, hay TV cũ của bạn khi bị vứt đi sẽ trở thành rác thải điện tử (e-waste). Đây không phải là rác thông thường. Bên trong vẻ ngoài vô hại đó là một "bãi mìn" hóa học, chứa đầy chì, thủy ngân, cadmium và nhiều chất độc khác. Khi bị chôn lấp không đúng cách, những chất độc này sẽ ngấm vào đất, vào nước, và cuối cùng đi vào chuỗi thức ăn, ảnh hưởng trực tiếp đến sức khỏe của chúng ta.

❖ **Giải pháp tốt nhất: Kéo dài sự sống cho thiết bị**

Trước khi vứt một món đồ đi, hãy tự hỏi ba câu hỏi vàng: Giảm thiểu? Tái sử dụng? Sửa chữa?

Giảm thiểu: Các nhà sản xuất thường muốn chúng ta nâng cấp điện thoại mỗi năm. Hãy chống lại sự cám dỗ đó. Hãy tự hỏi: "Chiếc điện thoại hiện tại có thực sự không đáp ứng được nhu cầu của mình nữa không?". Mua ít hơn chính là cách bảo vệ môi trường hiệu quả nhất.

Tái sử dụng: Đừng vứt đi! Một chiếc điện thoại cũ vẫn có thể trở thành camera an ninh, máy nghe nhạc, đồng hồ báo thức thông minh, hoặc một món quà ý nghĩa cho người cần nó hơn. Bạn có thể bán lại trên các nền tảng như Chợ Tốt hoặc quyên góp cho các tổ chức từ thiện.

Sửa chữa: Sửa chữa là một "siêu năng lực" mà ai cũng nên có! Vỡ màn hình hay hỏng pin không có nghĩa là thiết bị đã "chết". Các nền tảng như iFixit là một kho báu với hàng ngàn hướng dẫn sửa chữa miễn phí. Việc tự mình sửa chữa không chỉ tiết kiệm tiền mà còn mang lại cảm giác làm chủ công nghệ tuyệt vời.

❖ **Giải pháp cuối cùng: Tái chế đúng cách**

Khi một thiết bị thực sự không thể cứu vãn, đây là con đường cuối cùng. Vứt nó vào thùng rác thông thường là một tội ác với môi trường. Hãy tìm đến những điểm tái chế có trách nhiệm.

Bảo vệ hành tinh không phải là việc gì đó quá to tát. Nó bắt đầu từ những lựa chọn nhỏ của bạn mỗi ngày. Mỗi lần bạn sửa một món đồ, dọn dẹp email rác, hay mang một cục pin cũ đến đúng điểm thu gom, bạn đang là một người hùng của môi trường.

Tài liệu tham khảo

Bộ Công An. (2025). Cảnh báo. *https://bocongan.gov.vn/tag/816*.

Kaspersky Team. (2025). Creating an unforgettable password. *https://www.kaspersky.com/blog/international-password-day-2025/53355/*.

Ngân hàng Nhà nước. (2023). Quyết định 2345/QĐ-NHNN. *https://thuvienphapluat.vn/van-ban/Tien-te-Ngan-hang/Quyet-dinh-2345-QD-NHNN-2023-giai-phap-bao-mat-thanh-toan-truc-tuyen-va-the-ngan-hang-591895.aspx*.