

CHỦ ĐỀ 3:
BẢO VỆ CÁC THIẾT BỊ SỐ

Bài 2: Sử dụng ứng dụng di động an toàn



MỤC TIÊU:



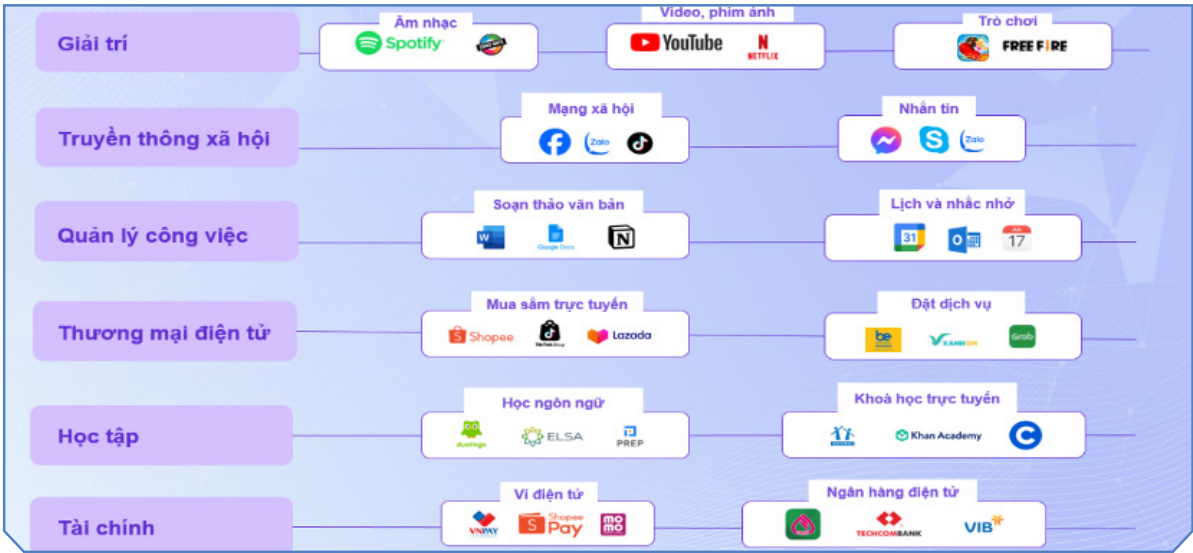
- Nắm được cách lựa chọn các ứng dụng di động an toàn
- Hiểu về các quyền truy cập dữ liệu của các ứng dụng
- Hiểu được các thực hành thiếu an toàn khi cài đặt và sử dụng ứng dụng (di động)

Trong thời đại công nghệ số, điện thoại thông minh và các ứng dụng di động đã và đang trở thành một phần không thể thiếu trong cuộc sống hàng ngày. Tuy nhiên, việc sử dụng ứng dụng không đúng cách có thể tiềm ẩn nhiều rủi ro về bảo mật và quyền riêng tư. Vì vậy, hiểu và áp dụng các nguyên tắc sử dụng ứng dụng di động an toàn là điều quan trọng để bảo vệ thông tin cá nhân và tránh những nguy cơ không mong muốn.

1. Ứng dụng di động là gì ?

Ứng dụng di động, hay còn gọi là ứng dụng điện thoại hay app (áp), là phần mềm được thiết kế để chạy trên các thiết bị di động như điện thoại thông minh và máy tính bảng và các thiết bị di động khác.

Hiện nay có rất nhiều loại ứng dụng di động đang có trên thị trường. Tuy nhiên, căn cứ theo mục đích sử dụng, chúng ta có thể phân loại một số ứng dụng phổ biến như sau:



Ngoài ra, theo sự phát triển của công nghệ và nhu cầu của người dùng mạng, các loại ứng dụng phục vụ đời sống con người sẽ ngày càng phong phú và đa dạng hơn. Cách phân loại này chỉ có ý nghĩa tương đối.

2. Lưu ý an toàn khi cài đặt sử dụng ứng dụng di động

2.1. Lưu ý khi lựa chọn

Hãy xem xét ví dụ: Anh Khoa muốn cài một ứng dụng đọc báo để theo dõi tin tức hàng ngày. Anh Khoa tìm kiếm và thấy có rất nhiều ứng dụng đọc báo khác nhau. Vậy làm thế nào để anh Khoa có thể lựa chọn một ứng dụng phù hợp với nhu cầu của mình mà lại đảm bảo an toàn trực tuyến?



Khi lựa chọn cài đặt ứng dụng di động, chúng ta thường xuất phát từ nhu cầu thực tế và đôi lúc là không thể thiếu. Tuy nhiên, bạn nên cân nhắc một vài điều quan trọng sau để đảm bảo an toàn và bảo mật cho chính bản thân mình và dữ liệu của bạn:



- **Sự cần thiết của ứng dụng:** Trước khi cài đặt bất kỳ ứng dụng nào, bạn hãy cân nhắc có *cần thiết* phải cài ứng dụng đó không. Hãy nhớ rằng việc cài đặt các ứng dụng sẽ vừa tốn bộ nhớ của điện thoại và vừa có thể đi kèm các rủi ro về bảo mật. Ở phần sau, chúng ta sẽ đề cập đến những rủi ro khi bạn cấp quyền cho ứng dụng. Hãy tưởng tượng điện thoại của chúng ta là một ngôi nhà có nhiều tầng, các ứng dụng di động sẽ giống như những khách thuê ở mỗi tầng. Và việc càng có nhiều khách thuê trong

ngôi nhà sẽ đồng nghĩa với việc chúng ta sẽ càng có nhiều rủi ro với mình khi sinh sống trong căn nhà đó (VD: rủi ro trộm cắp, đe dọa, nghe lén, quay lén...).

- **Uy tín của ứng dụng:** Khi lựa chọn cài đặt ứng dụng trên điện thoại, bạn hãy nhớ *lựa chọn các ứng dụng uy tín*. Để lựa chọn các ứng dụng uy tín, hãy lưu ý thực hành và xem xét các yếu tố sau:
 - **Cửa hàng ứng dụng chính thức:** Hãy luôn tải ứng dụng từ các cửa hàng chính thức như **CH Play** đối với điện thoại Android và **App Store** đối với điện thoại iOS. Các ứng dụng được đặt trên các cửa hàng này cơ bản đều phải đáp ứng những tiêu chuẩn tối thiểu của các nhà cung cấp nền tảng mới có thể được đưa ra thị trường. Không nên tải từ các đường dẫn khác không phải từ các cửa hàng này.
 - **Đơn vị phát triển phần mềm ứng dụng:** Hãy chọn những ứng dụng từ *các nhà phát triển có uy tín và được nhiều người tin dùng*. Việc lựa chọn nhà phát triển cũng giống như việc lựa chọn khách thuê trong ngôi nhà mình sở hữu. Do vậy, hãy tìm hiểu về người khách đó trước khi quyết định cho họ vào thuê.
 - **Đánh giá và xếp hạng ứng dụng:** Hãy kiểm tra các đánh giá và xếp hạng từ người dùng khác trên cửa hàng cho ứng dụng mà bạn định chọn. Bạn nên *lưu ý tới những đánh giá không tốt* nhiều hơn là những đánh giá tốt vì những đánh giá tốt có thể mua được hoặc làm giả được nhưng những đánh giá không tốt thường là từ những người dùng thực và chúng sẽ giúp bạn đánh giá rủi ro tốt hơn.
 - **Thời gian có mặt trên thị trường:** Những ứng dụng có mặt trên thị trường càng lâu thì càng đảm bảo độ tin nhiệm tốt hơn trên thị trường. *3 năm* là khoảng thời gian đủ để bạn an tâm hơn những ứng dụng mới ra mắt trên thị trường.

- **Miễn phí hay trả phí:** Bạn hãy xem xét liệu ứng dụng là *miễn phí hay yêu cầu phải trả phí*. Có rất nhiều ứng dụng chỉ cho bạn dùng thử trong một thời gian ngắn (VD: 7 ngày), và bạn có thể không nhận ra rằng ứng dụng sẽ tự động chuyển sang chế độ tính phí ngay sau thời gian dùng thử. Ngoài ra, một số ứng dụng có thể có các chi phí ẩn cho các tính năng bổ sung hoặc dịch vụ hỗ trợ...

2.2. Lưu ý khi cài đặt và sử dụng – Quản lý quyền truy cập của ứng dụng

Để thực hiện đầy đủ các chức năng cung cấp, các ứng dụng di động sẽ yêu cầu người dùng các quyền truy cập vào điện thoại. Khi bạn cài đặt và mở một ứng dụng lần đầu, ứng dụng đó sẽ yêu cầu quyền truy cập vào các chức năng trên điện thoại của bạn như máy ảnh, danh bạ, vị trí, micrô, và nhiều tính năng khác. **Mỗi quyền truy cập** sẽ cho phép ứng dụng sử dụng một phần cứng hoặc dữ liệu cụ thể trên thiết bị, giúp nó hoạt động đúng với mục đích của mình. Ví dụ, ứng dụng bản đồ cần quyền truy cập vị trí để chỉ đường chính xác, ứng dụng gọi điện hoặc nhắn tin cần quyền truy cập danh bạ để giúp người dùng liên lạc dễ dàng, còn ứng dụng mạng xã hội cần quyền truy cập máy ảnh và bộ nhớ để người dùng có thể chụp và đăng ảnh.

Hãy quay trở lại ví dụ anh Khoa cài đặt *ứng dụng đọc báo* ở trên. Sau khi lựa chọn một ứng dụng phù hợp, anh Khoa cài đặt ứng dụng đó vào điện thoại. Lúc đó, ứng dụng hỏi anh cho truy cập vào các quyền trên máy điện thoại như micrô, camera, danh bạ điện thoại. Vậy anh Khoa có cần cân nhắc việc chấp nhận cấp quyền cho ứng dụng này không?



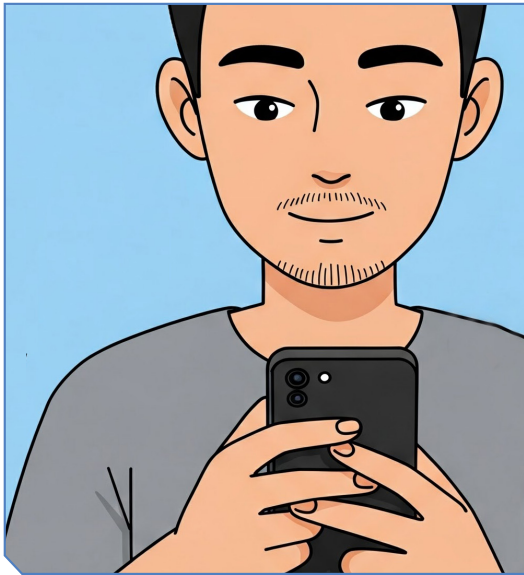
Trước tiên hãy tìm hiểu *một số quyền thường gặp* trên ứng dụng di động tương ứng với các tính năng và cách ứng dụng điện thoại dùng quyền đó trong điện thoại của bạn.¹

	Nhật ký cuộc gọi	Tính năng: Xem và thay đổi nhật ký cuộc gọi. Ứng dụng dùng quyền: Theo dõi các cuộc gọi trong nhật ký cuộc gọi của điện thoại.
	Máy ảnh	Tính năng: Dùng máy ảnh để chụp ảnh hoặc quay video. Ứng dụng dùng quyền: Gọi điện video qua nhà mạng.
	Danh bạ	Tính năng: Xem danh bạ. Ứng dụng dùng quyền: Hiển thị tên khi có cuộc gọi đến đối với số điện thoại được lưu trong danh bạ.
	Tệp và nội dung nghe nhìn	Tính năng: Sử dụng ảnh, nội dung nghe nhìn và các tệp khác trên điện thoại. Ứng dụng dùng quyền: Cho phép đính kèm ảnh qua cuộc gọi đối với một số nhà mạng.
	Vị trí	Tính năng: Truy cập thông tin vị trí của thiết bị. Ứng dụng dùng quyền: Nhận thông tin liên hệ cho các địa điểm ở gần bạn.
	Micrô	Tính năng: Phát hiện và ghi âm. Ứng dụng dùng quyền: Bật micro trong các cuộc gọi điện thoại.
	Điện thoại	Tính năng: Thực hiện và quản lý cuộc gọi điện thoại. Ứng dụng dùng quyền: Gọi điện.
	Tin nhắn SMS	Tính năng: Gửi và xem tin nhắn SMS. Ứng dụng dùng quyền: Gửi tin nhắn khi bạn từ chối cuộc gọi.

1 Nguồn tham khảo: <https://support.google.com/phoneapp/answer/11291807?hl=vi>

Tuy nhiên, không phải lúc nào các quyền này cũng được sử dụng hợp lý. Bởi vậy, khi cài đặt và sử dụng ứng dụng di động, việc **cấp quyền cho ứng dụng** là một yếu tố quan trọng cần được xem xét kỹ lưỡng vì nó ảnh hưởng trực tiếp đến quyền riêng tư, bảo mật và trải nghiệm sử dụng của người dùng. Nếu một ứng dụng có quyền truy cập quá nhiều thông tin không cần thiết, nó có thể thu thập dữ liệu cá nhân, theo dõi hoạt động hoặc thậm chí gây nguy cơ rò rỉ dữ liệu. Ngoài ra, một số ứng dụng độc hại có thể lợi dụng quyền truy cập để thực hiện các hành vi như đánh cắp thông tin, gửi tin nhắn lừa đảo hoặc hiển thị quảng cáo không mong muốn. Do đó, người dùng *chỉ nên cấp những quyền thực sự cần thiết và kiểm tra lại trong cài đặt nếu cảm thấy có dấu hiệu bất thường*.

Đối với trường hợp anh Khoa ở trên, với ứng dụng đọc báo, quyền truy cập vị trí có thể hợp lý vì ứng dụng có thể sẽ có chức năng hiển thị tin tức theo khu vực người dùng đang sinh sống. Tuy nhiên, cũng cần xem xét ứng dụng đó có thực tế có cần dùng tới quyền truy cập đó đó không. Còn việc *truy cập danh bạ điện thoại, camera hay micro có vẻ không hợp lý* vì có thể chúng ta chưa xác định rõ việc ứng dụng sẽ cần dùng các quyền này vào tính năng gì.



SUY NGẪM

Hãy cùng nhau phân tích các tình huống sau đây, xem bạn nên hay không nên cấp quyền cho các ứng dụng này:

1.

Một ứng dụng đọc truyện online yêu cầu truy cập **danh bạ điện thoại, máy ảnh và micro**

2.

Một ứng dụng **nhắn tin, gọi điện** yêu cầu truy cập **micro và máy ảnh**

3.

Một ứng dụng **chỉnh sửa ảnh và video** yêu cầu truy cập **micro và máy ảnh**

Gợi ý:



Tình huống 1: Đối với *ứng dụng đọc truyện online*, ứng dụng chỉ cần cung cấp nội dung truyện không cần phải chụp ảnh, hay ghi âm lại, lại càng không cần thiết phải dùng danh bạ điện thoại của người dùng nên việc yêu cầu cấp quyền truy cập vào danh bạ điện thoại, máy ảnh và micrô là không hợp lý.



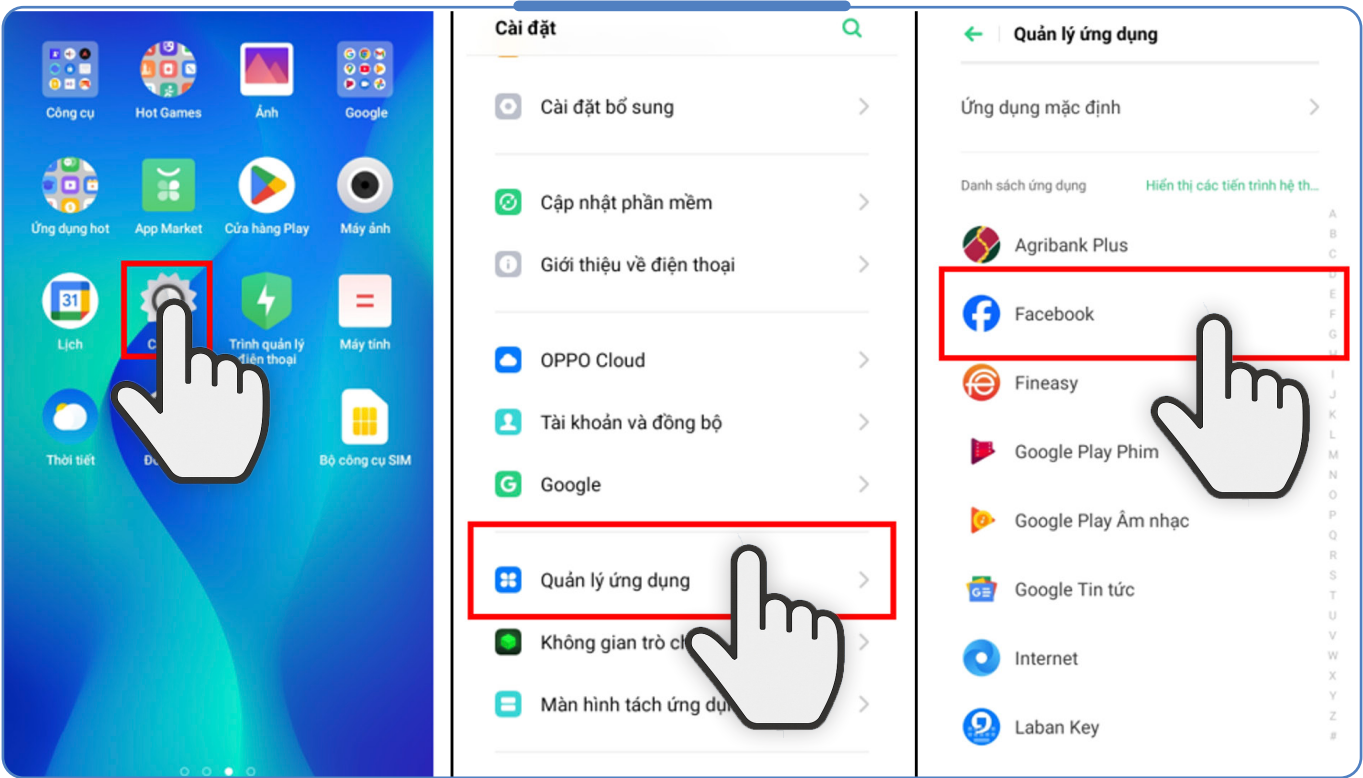
Tình huống 2: Đối với *ứng dụng nhắn tin, gọi điện* thì việc truy cập micro và máy ảnh có thể là cần thiết vì ứng dụng đó cần phải truyền tải âm thanh và hình ảnh trực tiếp của người nói đến người nghe. Tuy nhiên, khi cấp quyền truy cập micro và máy ảnh, đặc biệt nếu cấp quyền ở dạng “luôn luôn” thì ứng dụng sẽ có khả năng chụp ảnh, quay video hoặc ghi âm bất cứ lúc nào mà bạn không hề phát hiện ra. Hãy thử tưởng tượng, nếu bạn nói chuyện gì đó mà không muốn ai biết nhưng có chiếc điện thoại bên cạnh và bị ghi âm cuộc nói chuyện đó thì sẽ có rủi ro gì có thể xảy ra. Bởi vậy khi đã cấp những quyền này cho ứng dụng, bạn cần đảm bảo ứng dụng đó uy tín và an toàn (xem lại *mục 2.1 - lưu ý về lựa chọn ứng dụng*).



Tình huống 3: Đối với trường hợp *chỉnh sửa ảnh và video* thì việc truy cập micro và máy ảnh là cần thiết hay không tùy nhu cầu thực tế của người sử dụng. Nếu bạn chỉ sử dụng chỉnh sửa với những ảnh và video đã có sẵn trong máy thì ứng dụng không cần thiết phải được cấp quyền truy cập micro và máy ảnh. Tuy nhiên, nếu ứng dụng có thêm tính năng thu âm bài hát mình hát hoặc lồng tiếng của mình thuyết minh qua micrô, hoặc kèm tính năng chụp ảnh trực tiếp từ ứng dụng với các hiệu ứng thì bạn mới cần cân nhắc cho ứng dụng truy cập micrô hoặc máy ảnh. Hãy nhớ rằng việc cấp quyền sẽ luôn đi cùng với các rủi ro có thể xảy ra.)

Để kiểm tra việc cấp quyền cho các ứng dụng, bạn có thể tham khảo các thực hành sau:

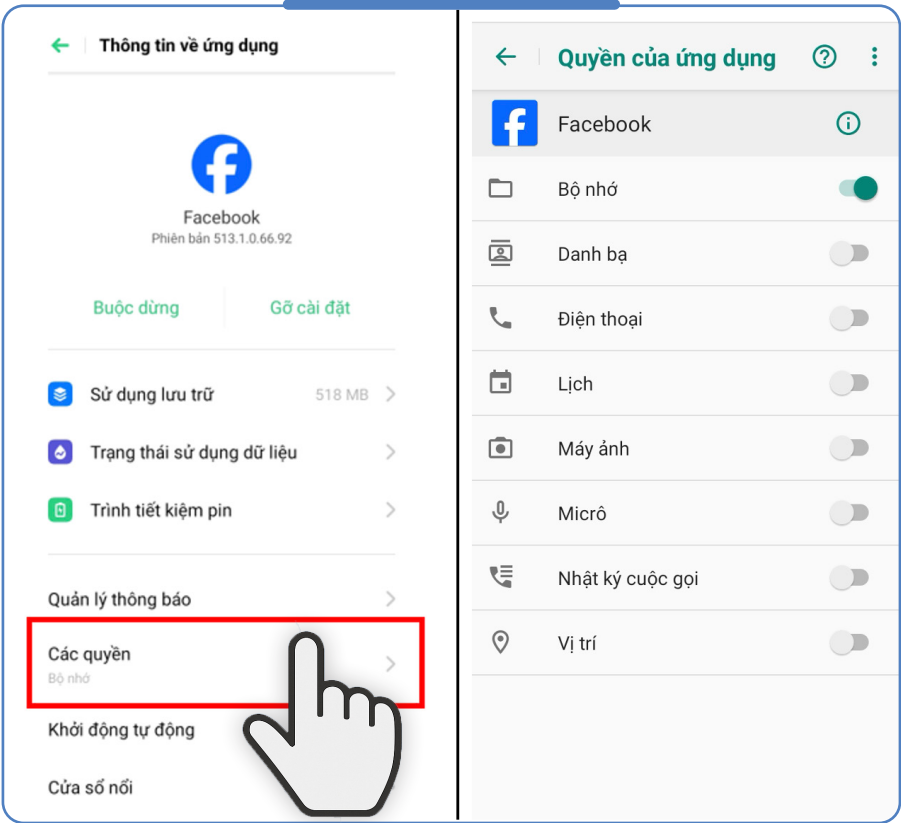
Đối với điện thoại Android:



BƯỚC 1: Trên thiết bị, hãy mở **Cài đặt**

BƯỚC 2: Nhấn vào **Quản lý ứng dụng**.

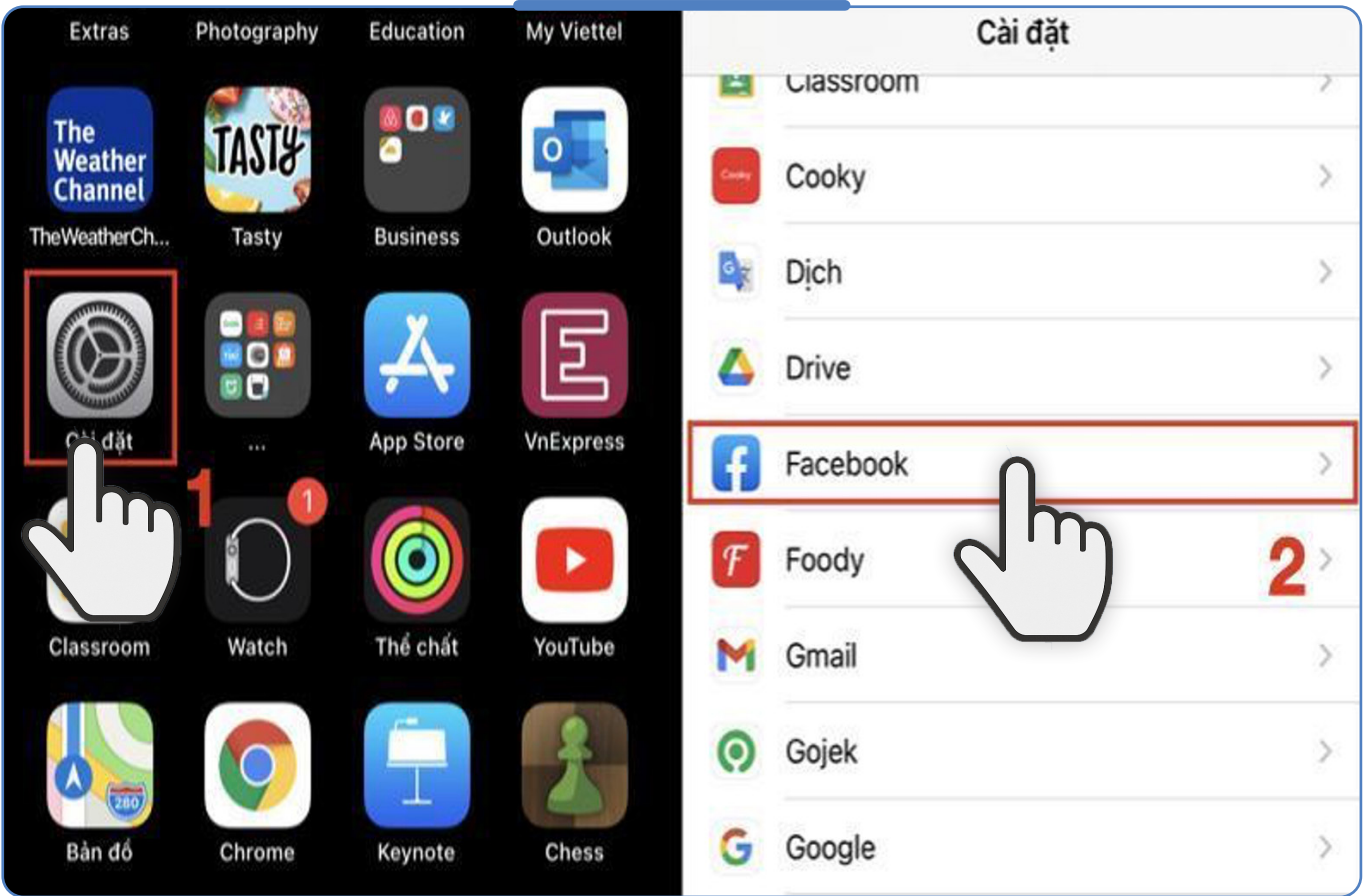
BƯỚC 3: Nhấn vào ứng dụng mà bạn muốn thay đổi



BƯỚC 4: Nhấn vào **Các quyền**

BƯỚC 5: Để thay đổi một chế độ cài đặt quyền, hãy chọn bật để **Cho phép** hoặc tắt để **Không cho phép**.

Đối với điện thoại iOS:



BƯỚC 1: Truy cập vào **Cài đặt**, tìm chọn **Ứng dụng** cần kiểm tra quyền truy cập.



BƯỚC 2: Chọn Quyền truy cập mà bạn muốn tương tác, nhấn **bật/tắt** quyền truy cập thông tin cho ứng dụng đó

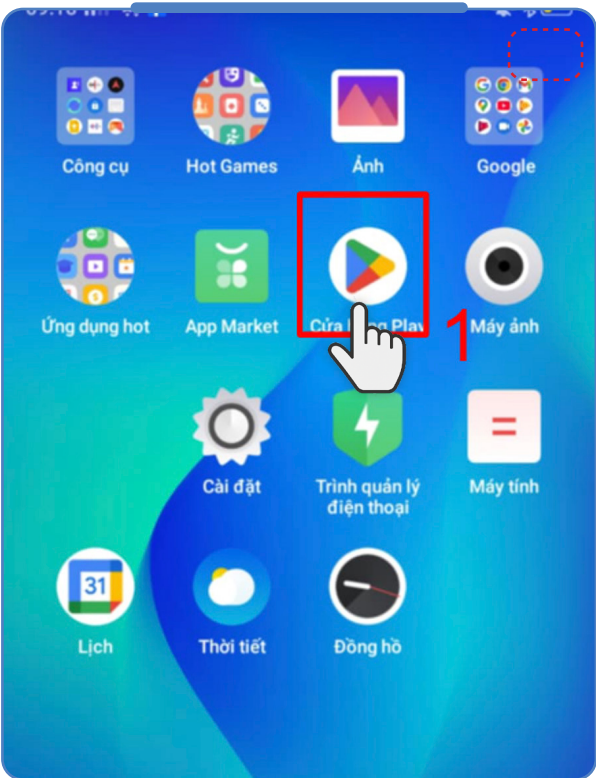
2.3. Lưu ý khác về an toàn và bảo mật

Ngoài ra, để an toàn và bảo mật, chúng ta vẫn cần phải duy trì thêm một số thực hành sau:

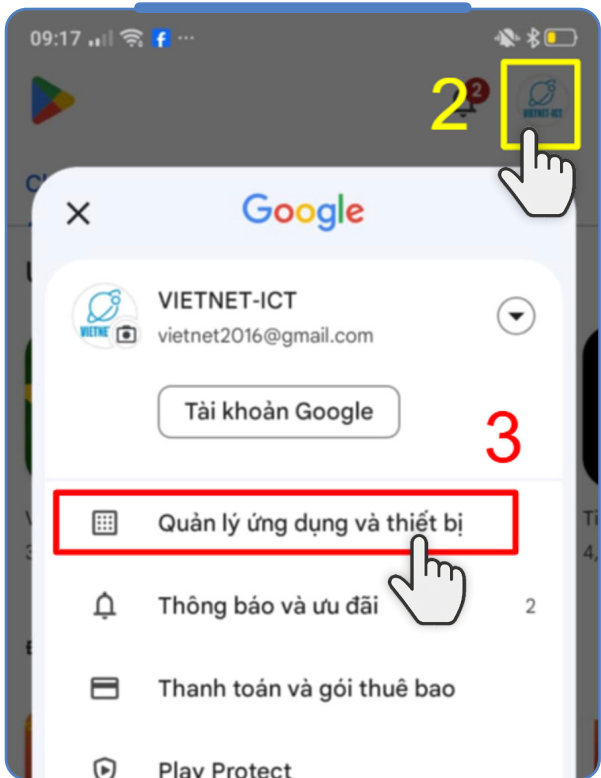


Cập nhật ứng dụng thường xuyên:
Việc này giúp vá các lỗ hổng bảo mật, ngăn chặn hacker khai thác để đánh cắp dữ liệu. Các bản cập nhật thường chứa các bản vá lỗi giúp bảo vệ thông tin cá nhân, tài khoản và giao dịch trực tuyến. Nếu không cập nhật, ứng dụng có thể dễ bị tấn công bởi mã độc, phần mềm gián điệp hoặc lừa đảo trực tuyến. Ngoài ra, cập nhật còn giúp ứng dụng tương thích với các tiêu chuẩn bảo mật mới nhất, nâng cao khả năng chống lại các mối đe dọa an ninh mạng.

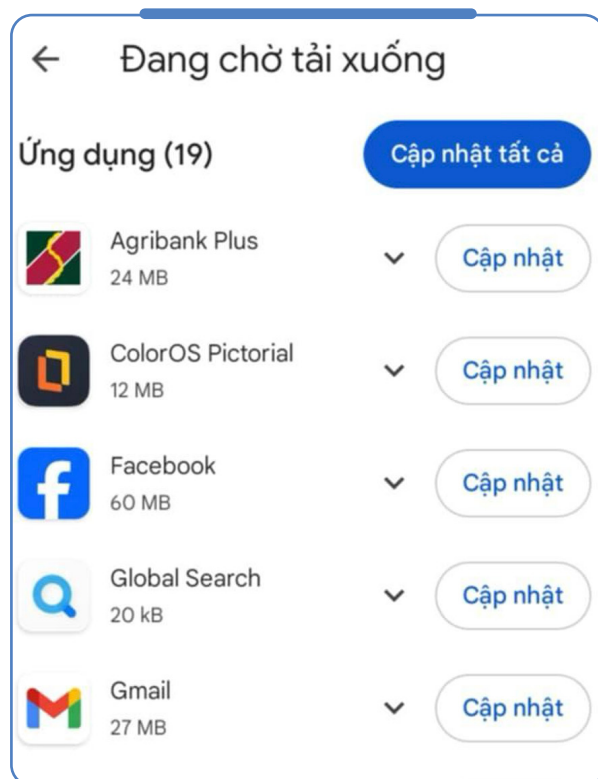
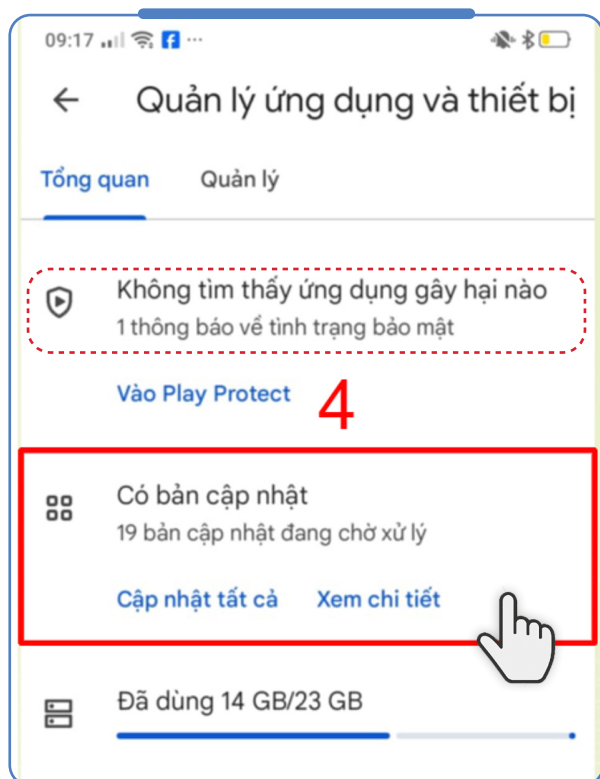
Tham khảo các cập nhật ứng dụng điện thoại Android (minh họa trên điện thoại Oppo A1k, các dòng điện thoại khác và hệ điều hành khác có thể có sự khác biệt):



BƯỚC 1: Vào cửa hàng ứng dụng CH Play



BƯỚC 2: Bấm vào Tài khoản > Quản lý ứng dụng và thiết bị



BƯỚC 3: Bấm vào **Cập nhật tất cả** để cập nhật tất cả ứng dụng hoặc bấm vào **Xem chi tiết** để cập nhật từng ứng dụng



Gỡ bỏ ứng dụng ngay khi thấy có rủi ro hoặc khi không cần sử dụng: Việc gỡ bỏ các ứng dụng không chỉ khiến cho *máy vận hành tốt hơn* mà còn giúp chúng ta giảm bớt các rủi ro mà đôi khi chúng ta chưa lường trước.

Đặt mật khẩu mạnh cho các ứng dụng có tài khoản đăng nhập: Đôi lúc các ứng dụng của chúng ta cũng lưu trữ các dữ liệu nào đó mà chúng ta không muốn chia sẻ nên việc đặt mật khẩu mạnh sẽ giúp cho chúng ta *loại bỏ những kẻ xấu đánh cắp điện thoại* đọc được các dữ liệu quan trọng (*tham khảo Chủ đề 2 - Bài 1 - Mật khẩu để biết cách đặt mật khẩu mạnh*).



Nội dung chính cần ghi nhớ

- 1. Ứng dụng di động**, hay còn gọi là ứng dụng điện thoại hay app (áp), là phần mềm được thiết kế để chạy trên các thiết bị di động như điện thoại thông minh và máy tính bảng và các thiết bị di động khác.
- 2. Khi lựa chọn cài đặt ứng dụng**, hãy cân nhắc:
 - Sự cần thiết của ứng dụng
 - Lựa chọn các ứng dụng uy tín: chỉ tải trên CH Play hoặc App Store, chú ý tới các yếu tố như đơn vị phát triển phần mềm ứng dụng; đánh giá và xếp hạng ứng dụng; thời gian có mặt trên thị trường
 - Ứng dụng miễn phí hay yêu cầu phải trả phí
- 3. Khi cài đặt và sử dụng ứng dụng**, cần lưu ý việc cấp quyền và quản lý quyền truy cập của ứng dụng bởi không phải lúc nào các quyền này cũng được sử dụng hợp lý, và nó sẽ trực tiếp ảnh hưởng tới quyền riêng tư, bảo mật và trải nghiệm sử dụng của người dùng.
- 4. Ngoài ra**, cần duy trì thêm một số thực hành sau:
 - Cập nhật ứng dụng thường xuyên
 - Gỡ bỏ ứng dụng ngay khi thấy có rủi ro hoặc khi không cần sử dụng nữa
 - Đặt mật khẩu mạnh cho các ứng dụng có tài khoản đăng nhập

