



CHỦ ĐỀ 2:

BẢO VỆ THÔNG TIN VÀ CÁC TÀI KHOẢN TRỰC TUYẾN

Bài 2: Quyền riêng tư trong thế giới số



MỤC TIÊU:



- Hiểu về quyền riêng tư và tầm quan trọng của quyền riêng tư
- Biết cách thực hiện kiểm tra và cài đặt quyền riêng tư trên các tài khoản trực tuyến
- Nắm được một số lưu ý về chính sách bảo vệ dữ liệu cá nhân ở cấp độ doanh nghiệp

Trong thời đại công nghệ số, quyền riêng tư cần được ưu tiên từ cấp độ chính phủ, tổ chức cho đến cấp độ cá nhân. Khi thông tin cá nhân ngày càng được chia sẻ và lưu trữ trực tuyến, việc bảo vệ dữ liệu trở thành nhiệm vụ quan trọng. Nâng cao nhận thức và áp dụng các biện pháp bảo vệ quyền riêng tư không chỉ giúp giảm thiểu rủi ro mà còn đảm bảo an toàn cho cả cá nhân và tổ chức trong môi trường kỹ thuật số.

1. Quyền riêng tư là gì?

Hãy cùng xem xét tình huống sau: Anh Khoa vừa chụp một bức ảnh gia đình trong chuyến du lịch. Bức ảnh ghi lại khoảnh khắc ấm áp của cả nhà và anh rất muốn lưu giữ nó như một kỷ niệm đẹp. Khi chuẩn bị đăng lên mạng xã hội, anh Khoa suy nghĩ:



- Nếu để chế độ **công khai**, bất kỳ ai, kể cả người anh không quen biết, cũng có thể xem và tải về bức ảnh này. Anh lo lắng rằng có thể sẽ có người dùng bức ảnh vào mục đích không mong muốn.

- Vì vậy, anh quyết định chọn chế độ **chỉ chia sẻ với các thành viên gia đình**. Điều này giúp đảm bảo rằng chỉ những người thân thiết, trong danh sách mà anh đã chọn, mới có thể nhìn thấy bức ảnh. Và đây là lựa chọn của anh Khoa về mức độ riêng tư khi chia sẻ bức ảnh về gia đình.

Quyền riêng tư, có thể hiểu một cách đơn giản, là *cách chúng ta lựa chọn xử lý thông tin cá nhân*. Thông tin này có thể bao gồm danh tính, hoạt động, sở thích, thói quen và nhiều khía cạnh khác trong cuộc sống. Trong thế giới số ngày nay, cơ hội chia sẻ thông tin ngày càng nhiều và thuận tiện. Mỗi người có thể đưa ra quyết định khác nhau về quyền riêng tư, và các quyết định này có thể thay đổi theo thời gian hoặc hoàn cảnh. Không có quyết định nào là tuyệt đối đúng hay sai, nhưng chúng ta cần hiểu rõ điều gì là riêng tư với mình, điều gì khiến mình cảm thấy thoải mái, và nhận thức được tác động của việc chia sẻ các thông tin trực tuyến để lựa chọn mức độ bảo vệ quyền riêng tư phù hợp nhất.

SUY NGẪM

Bạn có chia sẻ địa chỉ nhà của mình với các đối tượng sau đây không và tại sao?:

- Người thân
- Đồng nghiệp hoặc sếp
- Bạn bè trên mạng xã hội
- Một người mới quen trên mạng

(Gợi ý: Mỗi người có thể có quyết định khác nhau về quyền riêng tư với từng loại thông tin. Không có câu trả lời tuyệt đối đúng hay sai - bạn có thể chọn chia sẻ hoặc không tùy theo đối tượng. Điều quan trọng là cân nhắc xem bạn có cảm thấy

thoải mái khi chia sẻ không và liệu việc chia sẻ có thể mang lại rủi ro gì. Ví dụ: Bạn có thể sẵn sàng chia sẻ địa chỉ nhà với người thân nhưng không chia sẻ với người mới quen trên mạng vì có nguy cơ bị lợi dụng, lừa đảo hoặc quấy rối. Trong khi đó, một người khác có thể cảm thấy thoải mái khi chia sẻ địa chỉ với người mới quen vì họ tin rằng mình có thể xử lý hoặc ứng phó tốt với các tình huống rủi ro.)

2. Tầm quan trọng của quyền riêng tư

Hãy cùng quay lại với tình huống của anh Khoa. Trong trường hợp anh chia sẻ bức ảnh gia đình trong chuyến du lịch lên mạng xã hội và để ở chế độ công khai. Nếu người khác tiếp cận bức ảnh này thì sẽ có những rủi ro số nào có thể xảy ra?



Một kẻ xấu có thể tải về ảnh gia đình của anh Khoa và tạo tài khoản giả mạo trên Facebook, giả vờ là người thân trong gia đình để lừa đảo bạn bè, người quen mượn tiền.



Một hãng du lịch hoặc nhà trọ/khách sạn có thể lấy ảnh gia đình anh Khoa để quảng cáo dịch vụ du lịch mà không xin phép. Điều này có thể khiến anh bị hiểu lầm rằng đang quảng bá cho họ.



Ai đó có thể chỉnh sửa ảnh để ghép vào các nội dung xấu, tin giả, tin bịa đặt, làm ảnh hưởng đến danh tiếng của gia đình anh Khoa.



Nếu bức ảnh có chi tiết về vị trí địa lý, nơi ở, hoặc biển số xe, người khác có thể lần ra thông tin cá nhân của gia đình anh, gây nguy cơ bị theo dõi hoặc quấy rối. Những kẻ trộm có thể dùng ảnh để tìm hiểu gia đình anh có đi vắng hay không, từ đó lên kế hoạch trộm cắp.



Nếu trong ảnh có con cái anh Khoa, kẻ xấu có thể dùng ảnh trẻ em vào mục đích xấu, chẳng hạn như đăng tải trên các trang web không phù hợp.

Như vậy, việc anh Khoa quyết định chỉ chia sẻ bức ảnh này cho những người trong gia đình đã giúp anh hạn chế rất nhiều việc xảy ra các rủi ro số nêu trên. Từ ví dụ này, chúng ta thấy rằng việc xem xét và cài đặt quyền riêng tư có vai trò rất quan trọng để đảm bảo sự an toàn trực tuyến của người dùng mạng. Cụ thể như sau:



Bảo vệ thông tin và tránh các rủi ro an ninh mạng: Quyền riêng tư giúp ngăn chặn việc rò rỉ hoặc sử dụng sai mục đích các thông tin nhạy cảm như tên, địa chỉ, số điện thoại và thông tin tài chính. Điều này giúp hạn chế các nguy cơ

như lừa đảo trực tuyến, quảng cáo không mong muốn, đánh cắp danh tính, và các hành vi phân biệt đối xử. Ví dụ: việc tiết lộ giới tính, tình trạng hôn nhân, hoặc thông tin sức khỏe sinh sản có thể khiến phụ nữ và các nhóm cần trợ giúp (như người khuyết tật, người cao tuổi, trẻ em, người thuộc nhóm thiểu số...) đối mặt với định kiến, bắt nạt trực tuyến hoặc ngôn ngữ thù ghét. Ngoài ra, nếu hình ảnh hoặc địa chỉ liên hệ bị lộ, họ có nguy cơ cao bị quấy rối, đe dọa hoặc lợi dụng thông tin cá nhân cho các mục đích xấu như giả mạo danh tính có thể có kết hợp thêm yếu tố công nghệ deepfake (video siêu thật được tạo bởi trí tuệ nhân tạo).



Duy trì kiểm soát thông tin: Quyền riêng tư giúp bạn kiểm soát ai có thể truy cập và sử dụng thông tin cá nhân của bạn. Điều này rất quan trọng để bảo vệ quyền lợi, sự tự do cá nhân, cảm giác thoải mái và an toàn khi được thể hiện chính mình trên các nền tảng trực tuyến.



Ngăn ngừa sự lợi dụng và theo dõi trái phép: Quyền riêng tư giúp bạn hạn chế việc các tổ chức hoặc cá nhân thu thập, theo dõi và phân tích dữ liệu trực tuyến của bạn mà không được phép. Khi bạn duyệt web, các công ty và tổ chức có thể theo dõi hoạt động của bạn để xây dựng hồ sơ cá nhân. Việc cài đặt quyền riêng tư có thể giúp bạn hạn chế việc các thông tin của mình được sử dụng cho các mục đích không mong muốn như thương mại, chính trị,...

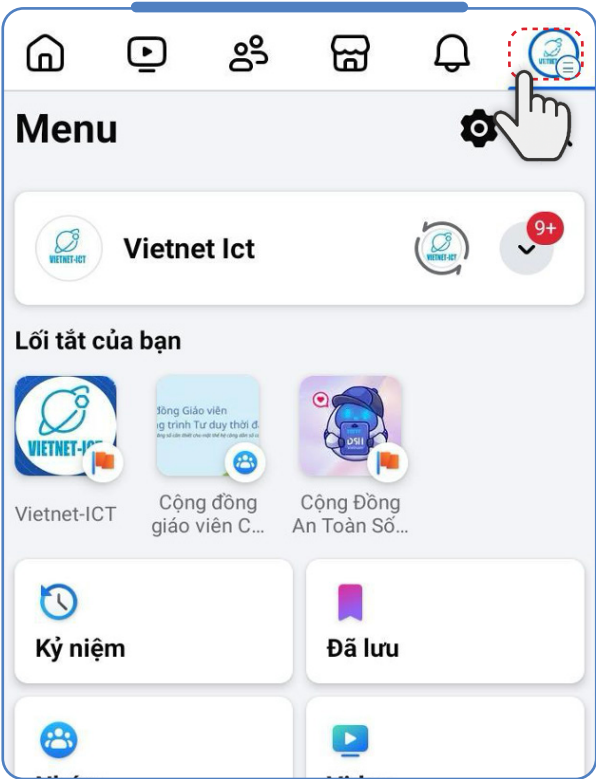
3. Kiểm tra và cài đặt quyền riêng tư

Để bảo vệ quyền riêng tư của bạn trên mạng, việc thường xuyên kiểm tra và cài đặt quyền riêng tư trên các nền tảng và ứng dụng là rất quan trọng. Hầu hết các nền tảng và ứng dụng mạng xã hội đều cho phép chúng ta thiết lập cài đặt quyền riêng tư.



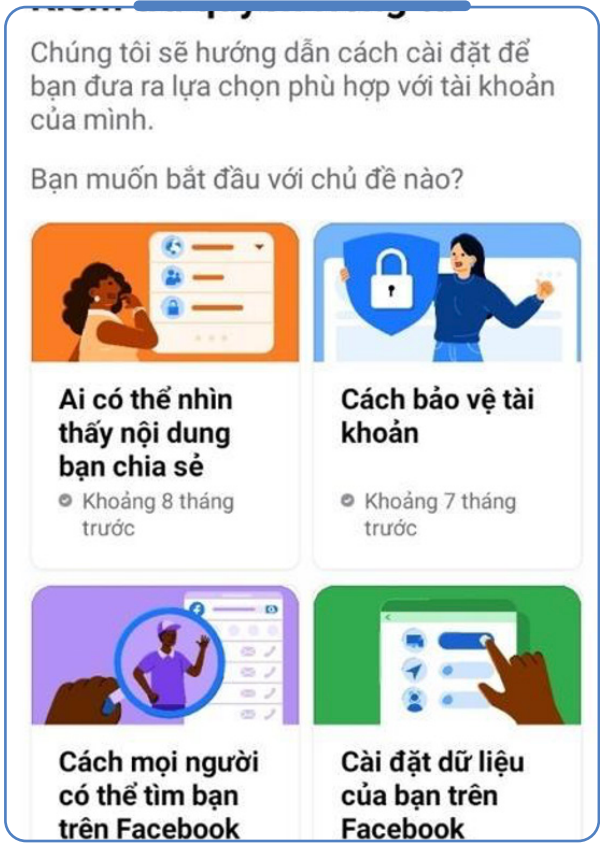
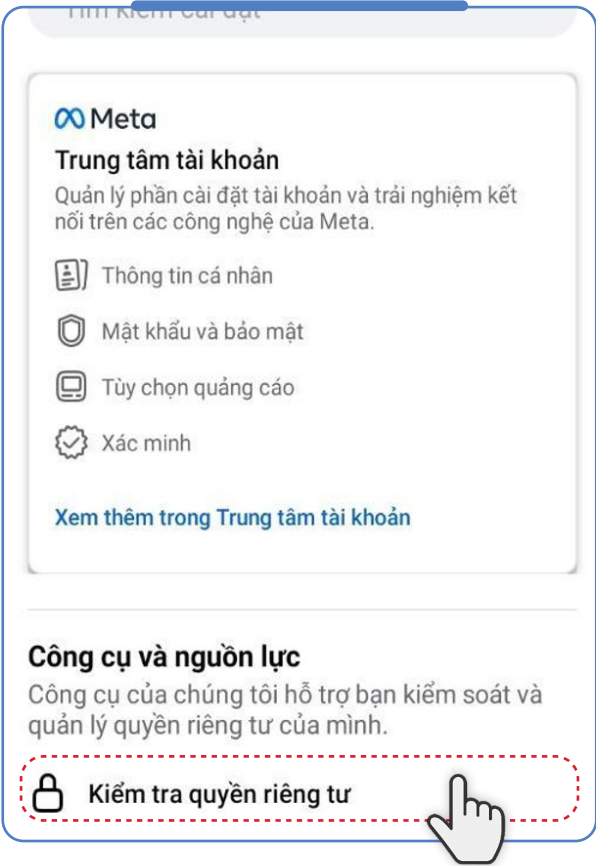
Dưới đây, bạn có thể tham khảo cách kiểm tra cài đặt Quyền riêng tư trên nền tảng mạng xã hội Facebook (minh họa trên điện thoại với hệ điều hành Android). Các dòng

máy khác và hệ điều hành khác như iOS có thể sẽ có sự thay đổi). Đối với các nền tảng, ứng dụng khác, bạn có thể tìm ở các mục tương tự hoặc tìm kiếm trên Google để có các hướng dẫn chi tiết.



BƯỚC 1: Vào mục Menu chỗ góc bên trên ngoài cùng bên phải ứng dụng

BƯỚC 2: Vào Cài đặt & quyền riêng tư, rồi vào mục Cài đặt



BƯỚC 3: Vào mục Trung tâm quyền riêng tư

BƯỚC 4: Vào Kiểm tra quyền riêng tư, rồi kiểm tra các mục

Cần lưu ý rằng, việc cài đặt và kiểm soát quyền riêng tư trên một nền tảng chỉ giúp giới hạn đối tượng có thể xem thông tin bạn chia sẻ, ***nhưng không thể ngăn chặn hoàn toàn tính lan truyền của thông tin***. Ví dụ, người khác có thể chụp màn hình và chia sẻ qua các kênh khác (tin nhắn, nền tảng khác), khiến thông tin lan rộng tới cả những người bạn không biết. Nói cách khác, quyền riêng tư hỗ trợ giới hạn phạm vi người xem nhưng không đảm bảo tuyệt đối. Vì vậy, bạn hãy luôn ***cân nhắc kỹ trước khi chia sẻ bất cứ điều gì trên mạng*** để đảm bảo an toàn trực tuyến, đặc biệt trong việc chia sẻ các thông tin cá nhân.



4. Một số lưu ý về tuân thủ chính sách bảo vệ dữ liệu cá nhân ở cấp độ tổ chức, doanh nghiệp

Tại sao bảo vệ dữ liệu cá nhân quan trọng đối với doanh nghiệp?

Hiện nay, tùy thuộc vào mục đích và nhu cầu cụ thể, các tổ chức và doanh nghiệp vẫn đang thu thập và lưu trữ nhiều

dữ liệu cá nhân như thông tin khách hàng thông qua nhiều hình thức khác nhau như biểu mẫu đăng ký, giao dịch trực tuyến, khảo sát nghiên cứu thị trường... Ngoài ra, mỗi tổ chức/ doanh nghiệp cũng lưu trữ rất nhiều thông tin của các cán bộ, thành viên đã hoặc đang công tác, làm việc hay hợp tác với tổ chức. **Dữ liệu cá nhân** (theo Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân¹) bao gồm:

Dữ liệu cá nhân cơ bản



HỌ VÀ TÊN



NGÀY SINH



SỐ ĐỊNH DANH
CÁ NHÂN



THÔNG TIN
LIÊN LẠC



TÌNH TRẠNG
HÔN NHÂN



QUỐC TỊCH



HÌNH ẢNH
CÁ NHÂN





TÀI KHOẢN
NGÂN HÀNG

Dữ liệu cá nhân nhạy cảm



QUAN ĐIỂM
CHÍNH TRỊ



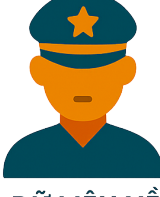
TÌNH TRẠNG
SỨC KHỎE



DỮ LIỆU
SINH TRẮC
HỌC



KHUYNH HƯỚNG
TÌNH DỤC



DỮ LIỆU VỀ
TỘI PHẠM



VỊ TRÍ CÁ NHÂN
ĐƯỢC XÁC ĐỊNH
QUA DỊCH VỤ
ĐỊNH VỊ



Việc thu thập, lưu trữ và xử lý các dữ liệu cá nhân này mang đến nhiều cơ hội nhưng cũng tiềm ẩn rủi ro nếu không được quản lý chặt chẽ.

1 <https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx>

Trường hợp điển hình: Vụ rò rỉ dữ liệu khách hàng của Marriott International (2018)²



Vào năm 2018, tập đoàn khách sạn Marriott International thông báo rằng thông tin cá nhân của khoảng 500 triệu khách hàng đã bị xâm phạm trong một cuộc tấn công mạng. Dữ liệu bị rò rỉ bao gồm tên, số hộ chiếu, địa chỉ email, số điện thoại và thậm chí cả thông tin thẻ tín dụng của khách hàng. Điều này đã gây ra những hậu quả nghiêm trọng với cả doanh nghiệp và các khách hàng của họ.

Sự cố này gây hậu quả nghiêm trọng

Về phía Marriott	Về phía khách hàng
 Bị phạt hàng trăm triệu USD	 Thông tin cá nhân bị rò rỉ có thể bị lợi dụng để lừa đảo, đánh cắp danh tính hoặc sử dụng trái phép trong các giao dịch tài chính
 Đối mặt với nhiều vụ kiện và chịu áp lực lớn từ công chúng	 Việc mất quyền riêng tư cũng có thể khiến họ gặp rủi ro an toàn cá nhân và gây ra nhiều bất tiện trong cuộc sống.
 Thương hiệu bị ảnh hưởng nặng nề, khiến khách hàng mất niềm tin	

2 <https://phienbanmoi.antoanthongtin.gov.vn/tin/marriott-phat-hien-su-co-bao-mat-nghiem-trong-500-trieu-khach-hang-bi-danh-cap-du-lieu>

Vậy doanh nghiệp cần làm gì để bảo vệ dữ liệu cá nhân?

Dưới đây là các thực hành về bảo vệ dữ liệu cá nhân mà các doanh nghiệp cần tuân thủ theo nghị định Chính phủ số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân:



Đảm bảo sự đồng ý của chủ thể dữ liệu: Doanh nghiệp phải thu thập sự đồng ý rõ ràng từ người dùng trước khi thu thập và xử lý dữ liệu.



Bảo mật dữ liệu: Tăng cường áp dụng các biện pháp kỹ thuật và tổ chức để bảo vệ dữ liệu cá nhân khỏi truy cập trái phép, mất mát, hoặc lạm dụng.



Tôn trọng quyền của chủ thể dữ liệu: Người dùng có quyền yêu cầu doanh nghiệp chỉnh sửa hoặc xóa dữ liệu cá nhân của họ.



Đánh giá tác động bảo vệ dữ liệu: Thực hiện đánh giá tác động bảo vệ dữ liệu để xác định các rủi ro tiềm ẩn và biện pháp giảm thiểu. Báo cáo này cần được cập nhật khi có sự thay đổi về loại hình hoặc phương thức xử lý dữ liệu.



Thông báo vi phạm dữ liệu: Trong trường hợp xảy ra vi phạm dữ liệu, doanh nghiệp phải thông báo cho cơ quan chức năng và chủ thể dữ liệu bị ảnh hưởng trong thời gian quy định (trong vòng 72 tiếng sau khi xảy ra hành vi vi phạm).



Trường hợp chuyển dữ liệu ra nước ngoài: Khi chuyển dữ liệu cá nhân ra nước ngoài, doanh nghiệp phải lập hồ sơ đánh giá tác động và tuân thủ các quy định về bảo vệ dữ liệu của quốc gia nhận dữ liệu.



Đào tạo và nâng cao nhận thức: Tổ chức cần đào tạo nhân viên về các quy định và chính sách bảo vệ dữ liệu cá nhân, đồng thời nâng cao nhận thức của họ về tầm quan trọng của việc bảo vệ dữ liệu trong toàn bộ tổ chức.

Ngoài các quy định nêu trên, các doanh nghiệp cần phổ biến cho nhân viên về các thực hành an toàn số nói chung. Một nhân viên an toàn là một tổ chức an toàn, bởi tài sản số có tính liên kết chặt chẽ. Mỗi tài khoản cá nhân hay thiết bị làm việc đều có liên kết với hệ thống chung, nên bất kỳ lỗi hỏng nào cũng có thể gây rủi ro cho toàn bộ tổ chức. Các thực hành về an toàn số có thể được tìm hiểu chi tiết ở các bài học trong khoá học này.

Nội dung chính cần ghi nhớ

1. Quyền riêng tư là khả năng kiểm soát những gì người khác biết về mình, hay nói một cách đơn giản là cách bạn lựa chọn xử lý thông tin về bản thân. Quyết định về quyền riêng tư của mỗi người có thể sẽ không giống nhau.
2. Quyền riêng tư giúp:
 - Bảo vệ thông tin cá nhân và tránh các rủi ro an ninh mạng
 - Duy trì quyền kiểm soát thông tin
 - Ngăn ngừa sự lợi dụng và theo dõi trái phép
3. Quyền riêng tư giúp bạn giới hạn đối tượng người xem, nhưng không chắc chắn là chỉ họ mới đọc được hay họ sẽ không chia sẻ về điều đó ở một nơi khác, tốt hơn hết, bạn hãy suy nghĩ trước khi chia sẻ điều gì trên mạng, đặc biệt là khi chia sẻ thông tin cá nhân.
4. Các doanh nghiệp, tổ chức khi hoạt động và có lưu trữ các dữ liệu cá nhân thì cần tuân thủ các chính sách, quy định về bảo vệ dữ liệu cá nhân như:
 - Bảo mật dữ liệu
 - Tôn trọng quyền của chủ thể dữ liệu
 - Đánh giá tác động bảo vệ dữ liệu
 - Thông báo vi phạm dữ liệu
 - Tuân thủ quy định khi chuyển dữ liệu ra nước ngoài
 - Đào tạo và nâng cao nhận thức