MỤC LỤC


BẠN ĐÃ BIẾT
10 ĐIỀU CẦN BIẾT KHI LÀM VIỆC TỪ XA
MẬT KHẨU MẠNH
Là mật khẩu có 8 ký tự trở lên, trong đó phải bao gồm chữ cái, chữ số, chữ viết hoa, ký tự đặc biệt
KÍCH HOẠT TƯỜNG LỬA
Cần kích hoạt tường lửa khi thiết lập máy tính để làm việc từ xa
GỠ BỎ CHƯƠNG TRÌNH
Để bảo đảm an toàn, tăng hiệu năng cho máy tính, cần gỡ bỏ các chương trình không cần thiết khi thiết lập máy tính để làm việc từ xa
CẬP NHẬT CÁC PHẦN MỀM VÀ HỆ ĐIỀU HÀNH
Hệ điều hành, phần mềm trên máy tính có thể là phiên bản cũ, không bảo đảm an toàn. Cần thiết lập cập nhật tự động hoặc thủ công khi có thông báo cập nhật.
CÀI ĐẶT PHẦN MỀM PHÒNG CHỐNG MÃ ĐỘC
Người dùng có thể hạn chế các virus, mã độc bằng cách cài đặt và cập nhật thường xuyên phần mềm diệt virus
NCSC VN
National Cyber Security Center
MÃ HÓA & SAO LƯU DỮ LIỆU
Để bảo vệ thông tin, dữ liệu, cần sao lưu sang thiết bị lưu trữ hoặc nên tảng lưu trữ trực tuyến. Đối với dữ liệu quan trọng, nhạy cảm cần mã hóa trước khi sao lưu.
THẬN TRỌNG VỚI THƯ ĐIỆN TỬ
Khi đọc thư điện tử cần quan sát kĩ địa chỉ người gửi. Thận trọng và rà quét trước khi mở tập tin đính kèm hoặc đường dẫn trong thư điện tử.
USB, THIẾT BỊ LƯU TRỮ DI ĐỘNG
Cần trọng khi cắm USB và thiết bị lưu trữ di động không rõ nguồn gốc. Quét virus trước khi sử dụng.
TẤN CÔNG LỪA ĐẢO
Cảnh giác các tình huống lừa đảo, đề nghị chuyển tiền qua Mạng xã hội, thư điện tử, SMS. Không cung cấp thông tin cá nhân trên các website hoặc các tổ chức chưa được tin nhiệm.
MẠNG RIÊNG ẢO (VPN)
Cài đặt sẵn các ứng dụng VPN để truy cập vào hệ thống theo chính sách bảo mật của tổ chức. Không chia sẻ tài khoản VPN đã được cấp với người khác.

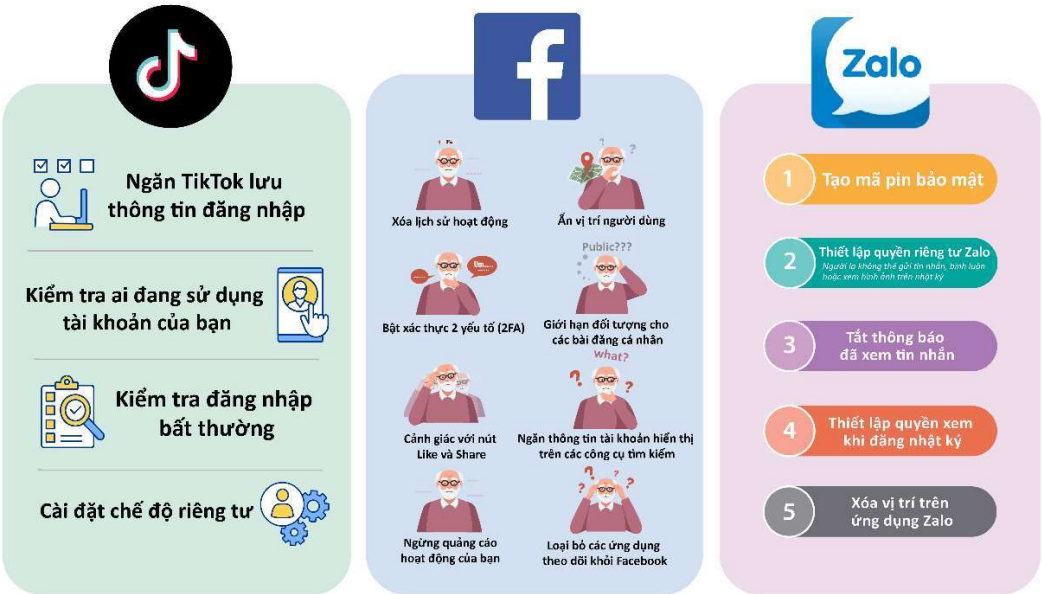

NCSC VN
National Cyber Security Center
7 ĐIỀU CẦN BIẾT
KHI HỌC - HỌP TRỰC TUYẾN
NGƯỜI THAM GIA
Kiểm soát người tham gia lớp học/cuộc họp, tránh việc các đối tượng lợi dụng để đánh cắp thông tin và phát tán mã độc qua các tập tin/đường link chia sẻ
CẨN THẬN KHI CHIA SẺ
Tắt chức năng chia sẻ màn hình của người tham gia, chia sẻ tập tin qua các dịch vụ đám mây như Box hoặc Google drive khi tham gia lớp học/cuộc họp.
ĐẶT MẬT KHẨU
Đặt mật khẩu để hạn chế các truy cập mạo danh hoặc sự tham gia của đối tượng không cần thiết
MẠNG KHÔNG DÂY AN TOÀN
Ví dụ như: Kích hoạt các phương thức mã hóa WEP/WPA/WPA2, thay đổi tên mạng không dây do các nhà sản xuất cài đặt sẵn, lọc địa chỉ MAC,v.v
CẬP NHẬT PHIÊN BẢN MỚI
Cập nhật các phiên bản mới nhất để đảm bảo phần mềm an toàn vì những phiên bản cũ thường sẽ có các lỗ hổng bảo mật chưa được vá.
CHÍNH SÁCH BẢO MẬT
Đọc kỹ các chính sách bảo mật của nhà cung cấp dịch vụ trước khi sử dụng. Lưu ý điều khoản có chia sẻ thông tin cho bên thứ ba hay không?!
CHỨC NĂNG BẢO MẬT
Trước khi sử dụng người dùng nên xem xét kỹ các chức năng bảo mật của ứng dụng, phần mềm để đảm bảo an toàn trong quá trình sử dụng.

NCSC VN
National Cyber Security Center

6 ĐIỀU CẦN BIẾT
KHI THANH TOÁN TRỰC TUYẾN

NCSC VN
National Cyber Security Center

NHỮNG ĐIỀU CẦN BIẾT
KHI SỬ DỤNG MẠNG XÃ HỘI



CHUYÊN ĐỀ 1: LÀM VIỆC TỪ XA AN TOÀN

1.1. Thiết lập máy tính, thiết bị an toàn để làm việc từ xa

Dưới đây là một số bước để thiết lập máy tính, thiết bị an toàn chống lại các nguy cơ bị tấn công.

1.1.1. Thiết lập xác thực tài khoản bằng mật khẩu

Khi sử dụng các thiết bị cá nhân, có nhiều tình huống bạn phải rời khỏi máy một khoảng thời gian. Những lúc như vậy, nếu không cẩn thận và có phương pháp bảo vệ thì thiết bị của bạn hoàn toàn có thể bị người khác sử dụng và có thể gặp phải tình trạng bị sao chép, đánh cắp dữ liệu…

Một trong các bước đầu tiên của việc thiết lập cấu hình máy tính là thiết lập mật khẩu cho các tài khoản với độ phức tạp nhất định. Do đó, người dùng cần có một mật khẩu an toàn, đủ mạnh để kẻ tấn công khó đoán và lợi dụng.

Mật khẩu đủ mạnh là mật khẩu: tối thiểu 8 ký tự, có chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt.

Ngoài ra, trong trường hợp người dùng quên khóa màn hình khi ra ngoài, cần thiết lập khóa màn hình thiết bị tự động trong khoảng thời gian nhất định. Buộc người dùng nếu muốn sử dụng thiết bị phải nhập đúng mật khẩu, nếu không sẽ không thể sử dụng được thiết bị và dữ liệu liên quan.

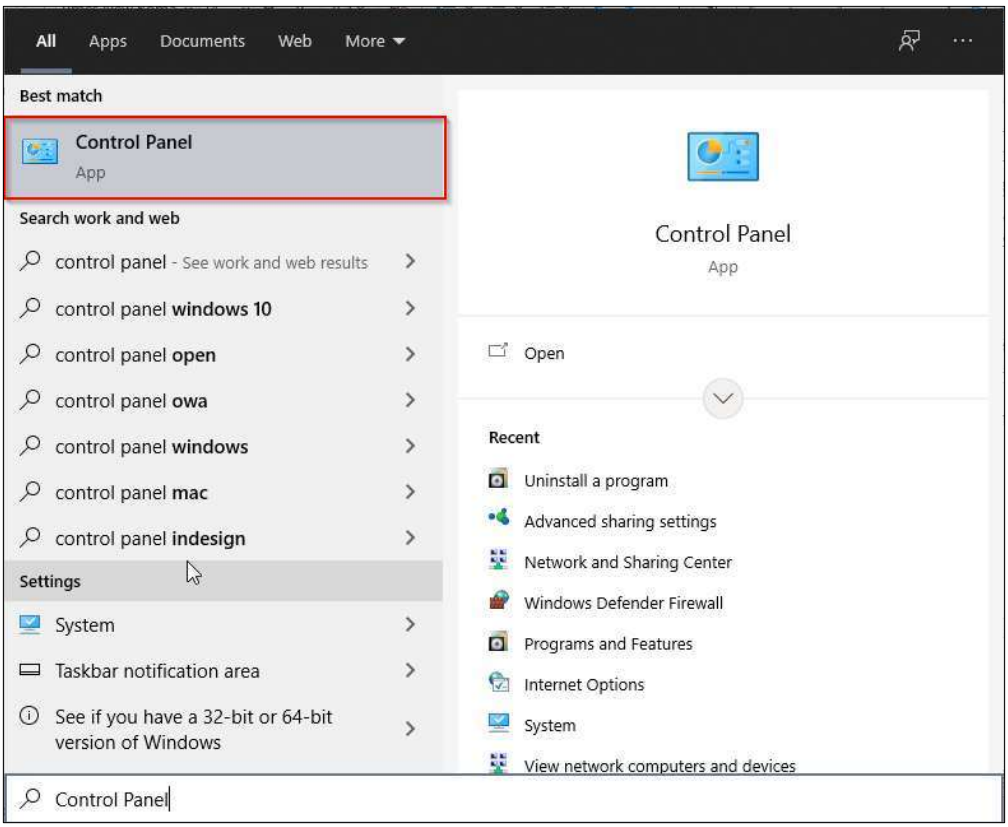
Việc khóa màn hình yêu cầu mỗi lần người dùng muốn mở khóa thiết bị hoặc bật thiết bị, họ sẽ được yêu cầu nhập mã PIN, mật khẩu hoặc dấu vân tay. Điều này có nghĩa là nếu ai đó giữ thiết bị của bạn, họ không thể truy cập dữ liệu trên thiết bị, khi người dùng không cung cấp mật khẩu, mẫu, mã PIN, dấu vân tay.

1.1.2. Kích hoạt chức năng tường lửa bảo vệ cá nhân trên thiết bị

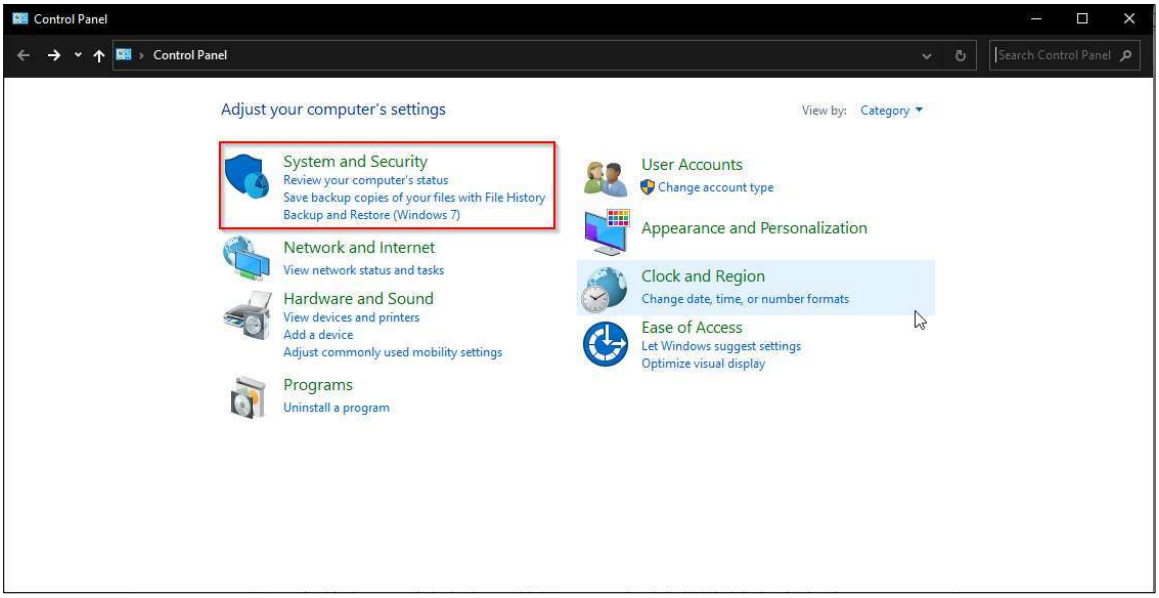
Một trong các tác vụ đầu tiên cần thực hiện sau khi cài đặt thiết bị cá nhân an toàn là thiết lập các cơ chế bảo vệ cơ bản cho thiết bị. Trong đó, tường lửa là biện pháp cơ bản để phòng tránh các nguy cơ mất an toàn thông tin. Hiện nay, hầu hết các hệ điều hành đã tích hợp tường lửa cá nhân nhằm bảo vệ người dùng khỏi các tấn công cơ bản. Do đó, cần kích hoạt phần mềm tường lửa này trước khi kết nối máy tính đến bất kỳ mạng máy tính nào như Internet, Wifi hay LAN.

Trên hệ điều hành Windows, có thể kích hoạt tường lửa bằng cách truy cập chức năng Windows Defender Firewall trong Control Panel. Sau đó, lựa chọn “Turn Win-dows Firewall on or off” để thực hiện việc kích hoạt. Tiếp tục chọn “Turn on…” và tuỳ chọn bên dưới để kích hoạt. Các bước thực hiện cụ thể như sau:

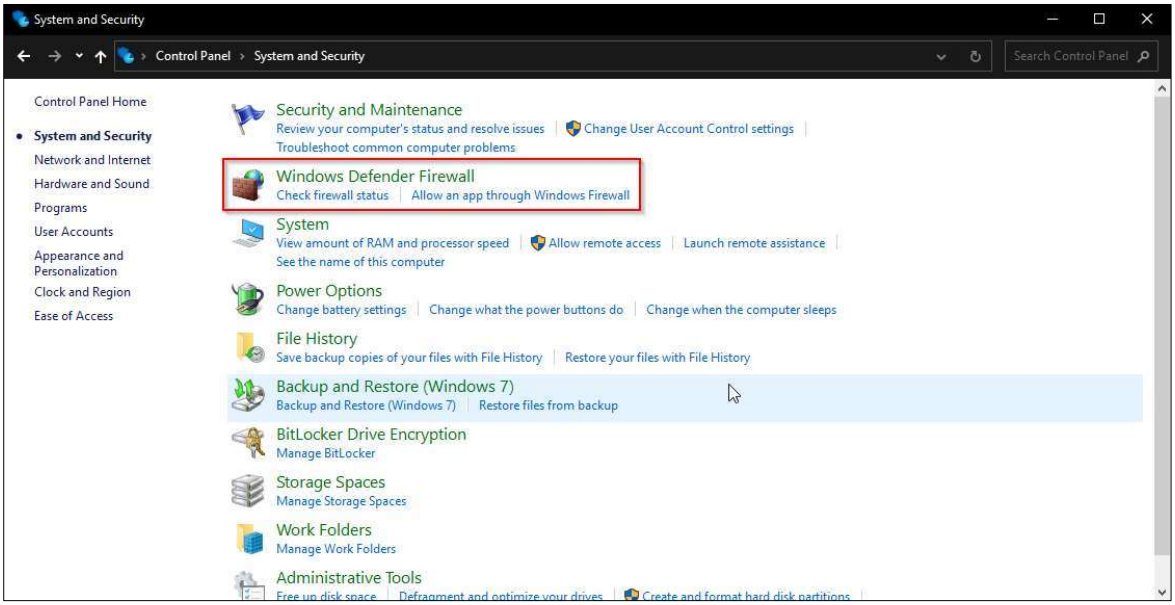
Bước 1: Tại thanh **Tìm kiếm,** nhập **Control Panel**, sau đó nhấn chọn vào



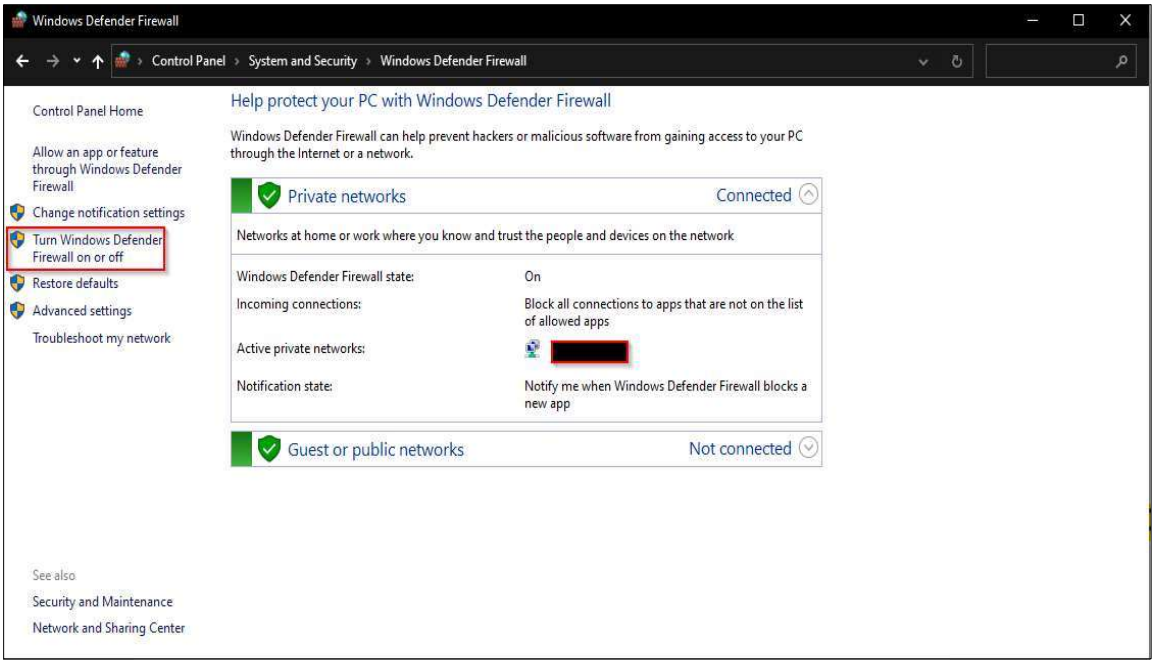
Bước 2: Sau đó, tại giao diện tiếp theo, nhấn chọn vào mục **System and Security**.



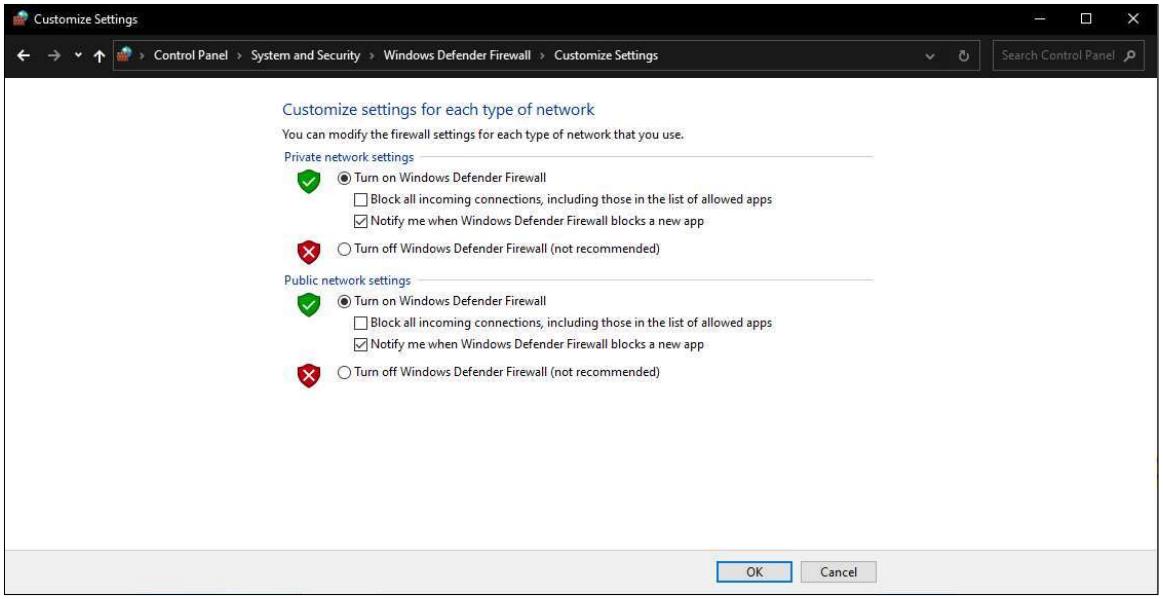
Bước 3: Chọn tiếp vào mục **Windowns Defender Firewall**.



Bước 4: Sau đó, giao diện mới sẽ hiển thị, bạn nhấn chọn tiếp vào mục **Turn Windowns Defender Firewall on or off** ở bên trái màn hình.



Bước 5: Lựa chọn bật tường lửa và nhấn vào mục OK để hoàn tất cài đặt.



1.1.3. Gỡ bỏ các chương trình không cần thiết

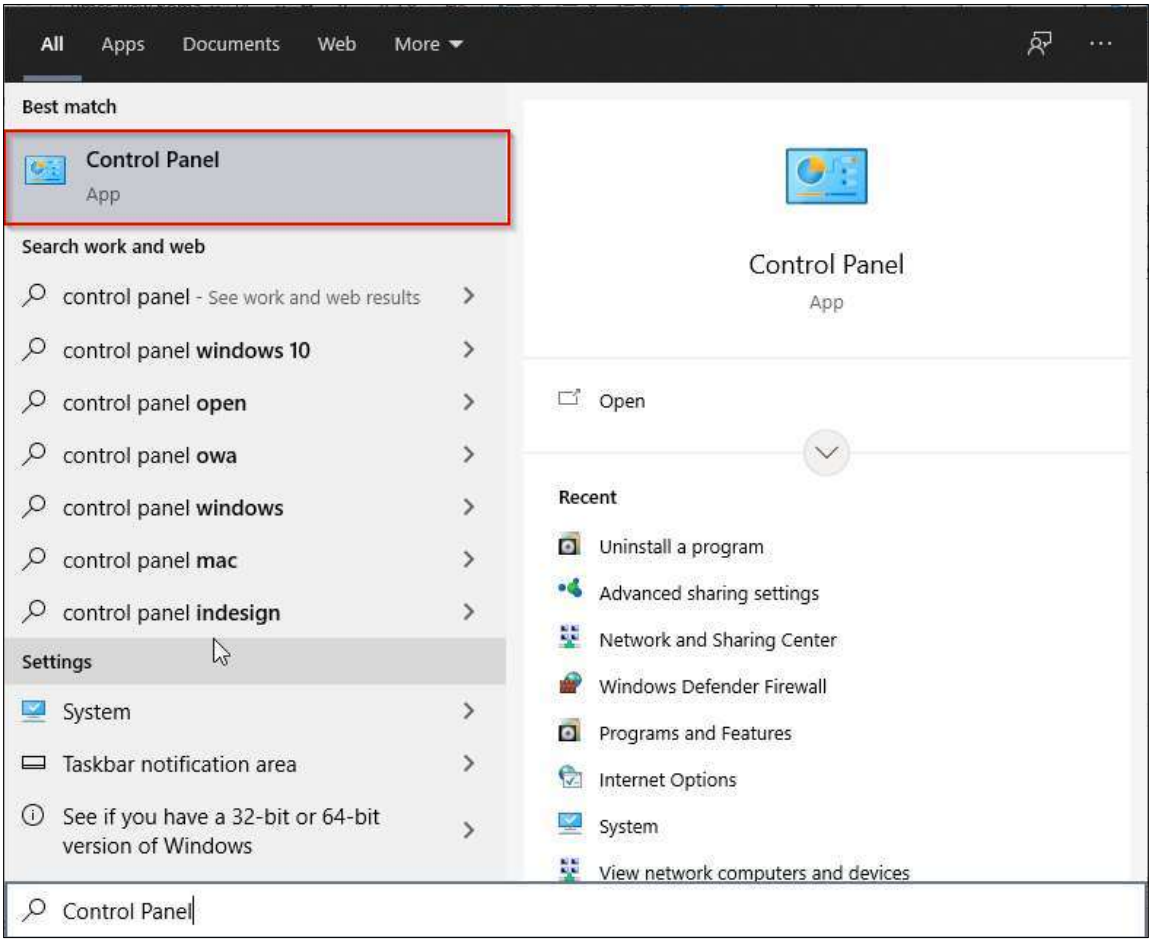
Các thiết bị cá nhân thường được nhà sản xuất cài đặt sẵn các chương trình quảng cáo, giới thiệu hoặc bản dùng thử của các phần mềm khác. Các chương trình này có thể ẩn chứa các nguy cơ gây mất an toàn thông tin mà kẻ tấn công có thể lợi dụng ngay trong quá trình sử dụng lần đầu tiên hoặc làm giảm hiểu năng của thiết bị. Vì vậy, người dùng cần tháo gỡ các chương trình không cần thiết trên máy tính của mình ngay trong quá trình thiết lập ban đầu để phòng tránh các nguy cơ mất an toàn thông tin cũng như làm tăng hiệu năng của thiết bị trong quá trình sử dụng.

Để tháo gỡ các chương trình không cần thiết, người dùng có thể sử dụng chức năng quản lý chương trình đã được cài đặt trong máy tính để liệt kê tất cả các chương trình đã được cài đặt. Từ đó, lần lượt xem xét các chương trình đang có sẵn để tháo gỡ các chương trình không cần thiết khỏi hệ thống theo nhu cầu.

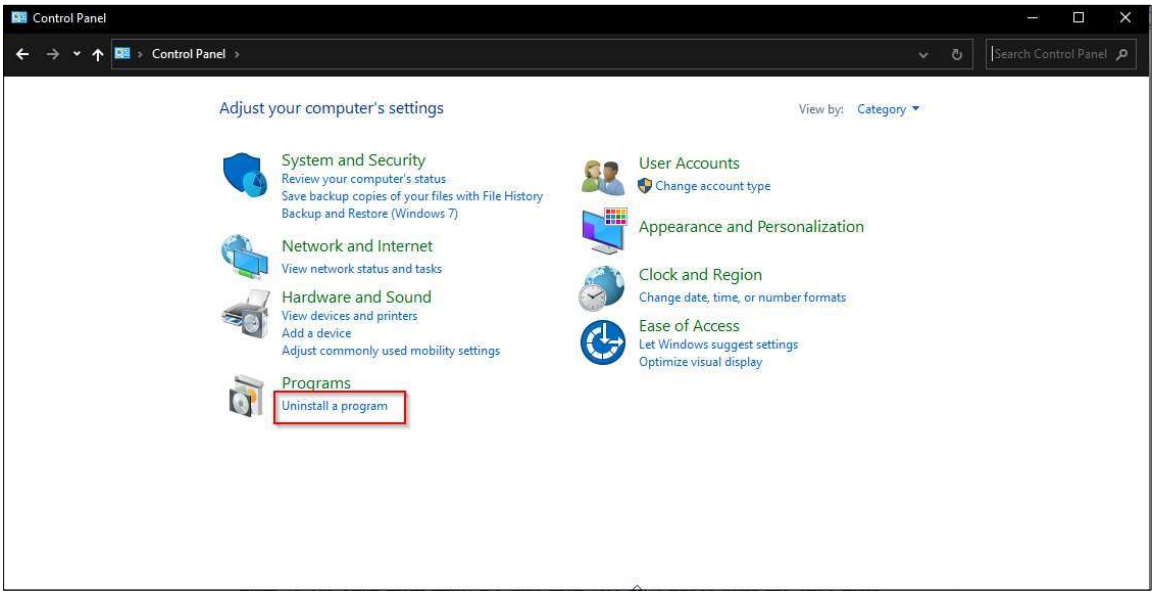
Để mở chức năng quản lý các chương trình đã cài đặt trong hệ điều hành Windows, người dùng có thể truy cập Control Panel, chọn Programs and Features để thực hiện việc gỡ bỏ hoặc tùy chọn khác.

Các bước cụ thể như sau:

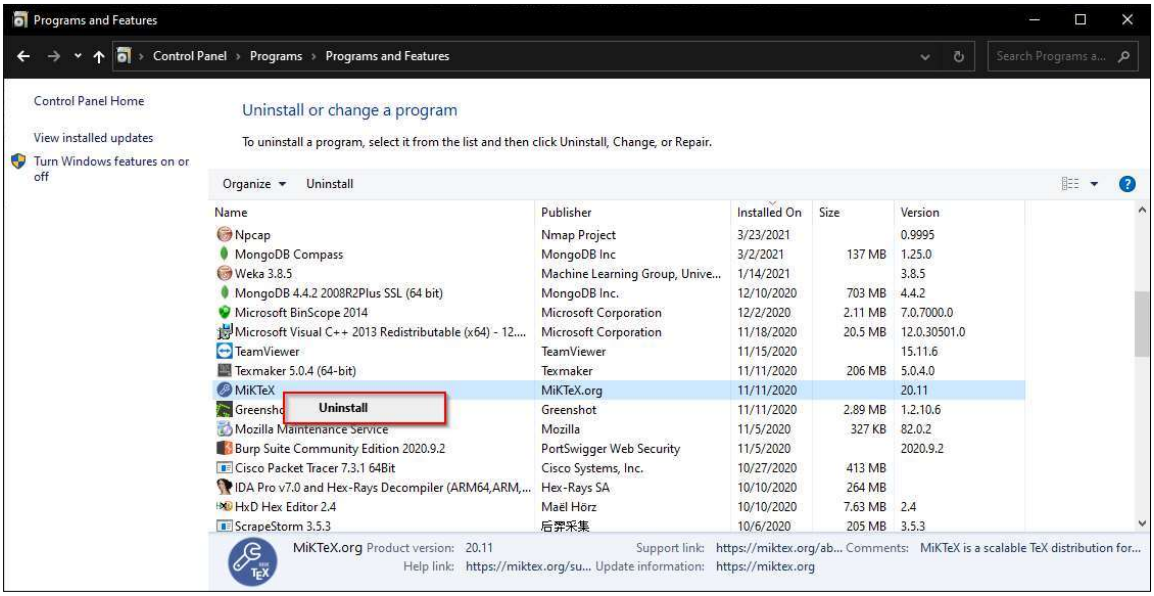
Bước 1: Tại thanh **Tìm kiếm,** nhập **Control Panel**, sau đó nhấn chọn vào



Bước 2: Sau đó, tại giao diện tiếp theo, nhấn chọn vào mục **Uninstall a program**.



Bước 3: Nhấn chuột phải vào chương trình cần gỡ bỏ và chọn **Uninstall**.



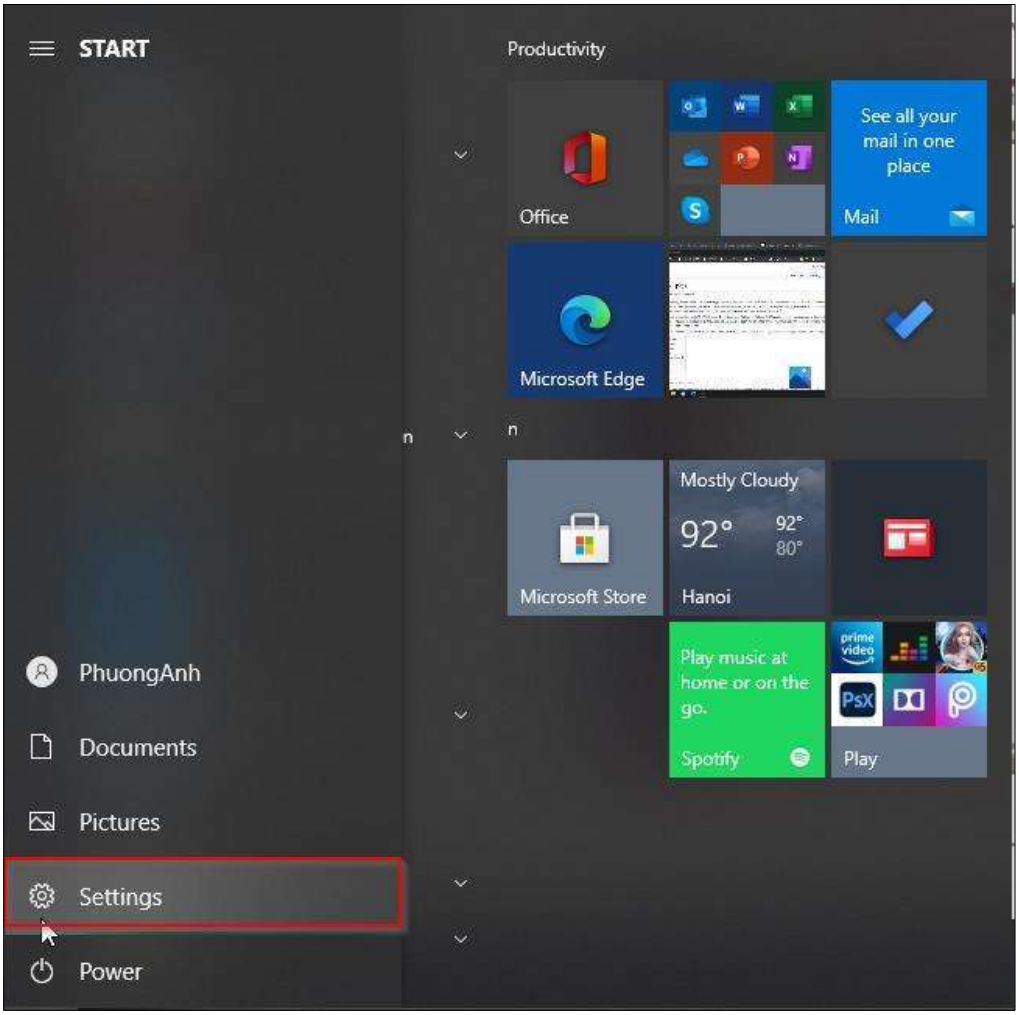
1.1.4. Cập nhật phần mềm và hệ điều hành

Sau khi cài đặt, hệ điều hành của máy tính có thể là phiên bản cũ chưa được vá lỗi bảo mật. Do đó, người sử dụng cần thiết lập chế độ tự động cập nhật hệ điều hành và các phần mềm khác. Để thực hiện việc này, người dùng mở chức năng Windows Update, sử dụng tuỳ chọn "Change Settings" để thiếp lập việc tự động cập nhật.

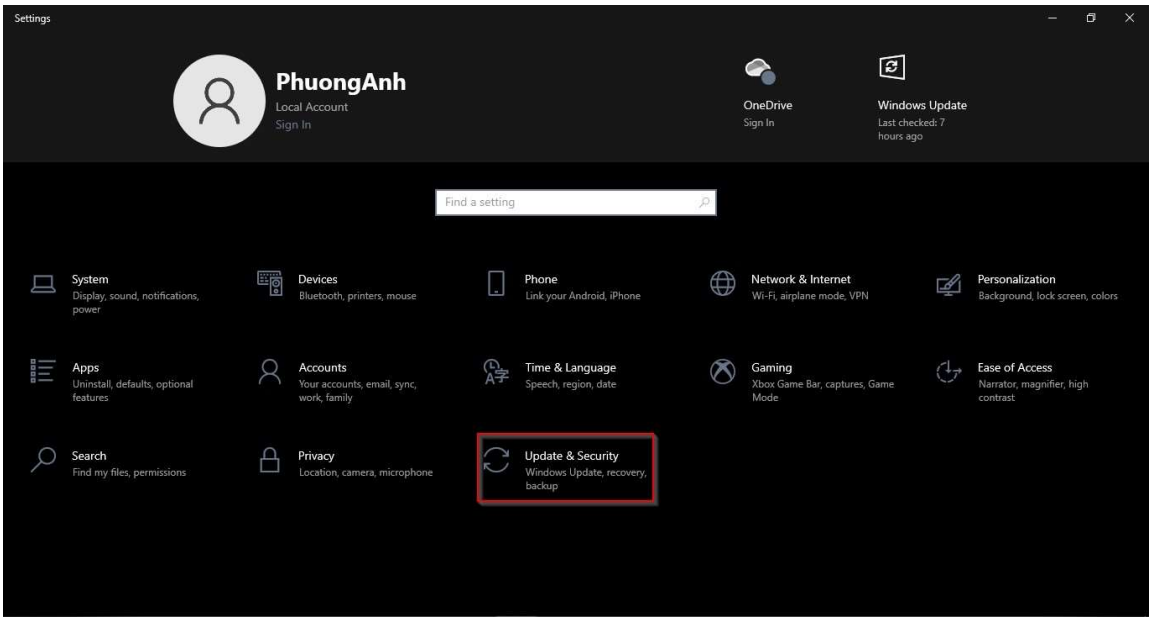
Người dùng có thể chọn chế độ tự động cập nhật theo nhu cầu để đảm bảo không bị gián đoạn công việc.

Các bước thực hiện cụ thể như sau:

Bước 1: Nhấn nút **Start** trên Windows (hoặc nhấn phím **Windows** trên bàn phím) -> chọn **Settings** hoặc nhấn tổ hợp phím **Windows + I**.

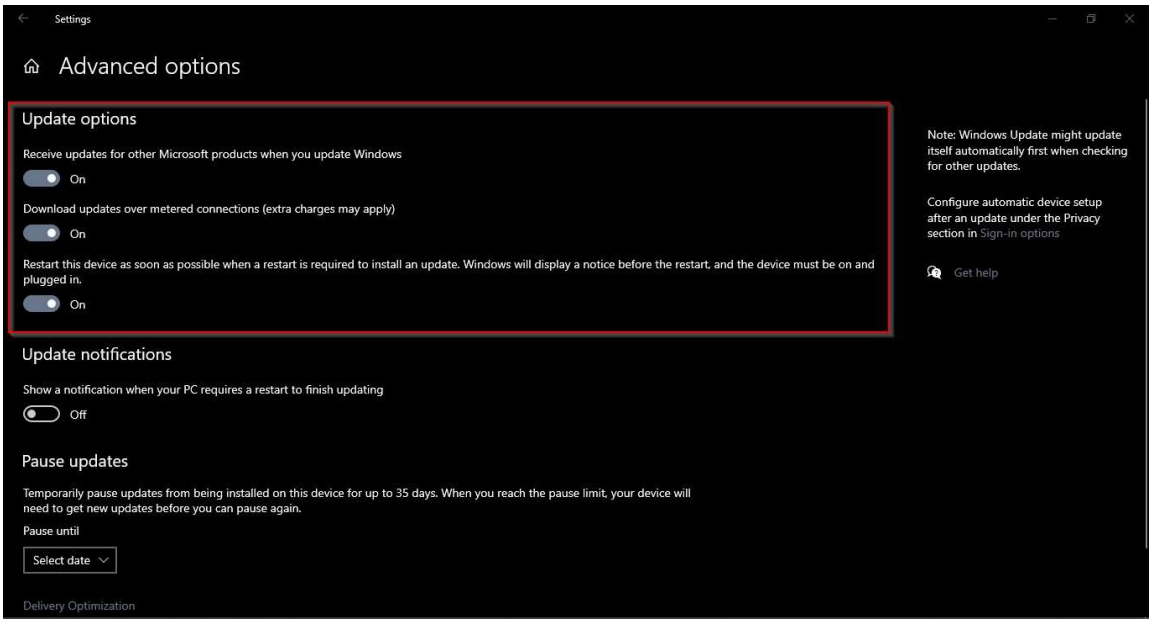


Bước 2: Chọn **Update & Security**



Bước 3: Chọn **Windows Update** -> Chọn **Advanced options**

Bước 4: Bật các option để tự động cập nhật hệ điều hành và các phần mềm



1.1.5. Cài đặt phần mềm phòng chống mã độc

Mỗi giây trên không gian mạng có khoảng 300 virus mới được tạo ra, cho nên máy tính của bạn hay của công ty, doanh nghiệp cần phải cài đặt phần mềm diệt virus mạnh, phát hiện nhanh các loại virus, phần mềm gián điệp,… để kịp thời tiêu diệt virus giảm thiểu tổn thất cho máy tính. Người sử dụng máy tính có thể hạn chế các virus, mã độc bằng cách cài đặt phần mềm diệt virus có bản quyền cho máy tính.

1.1.6. Mã hóa và sao lưu dữ liệu quan trọng định kỳ, thường xuyên

Mã hóa dữ liệu

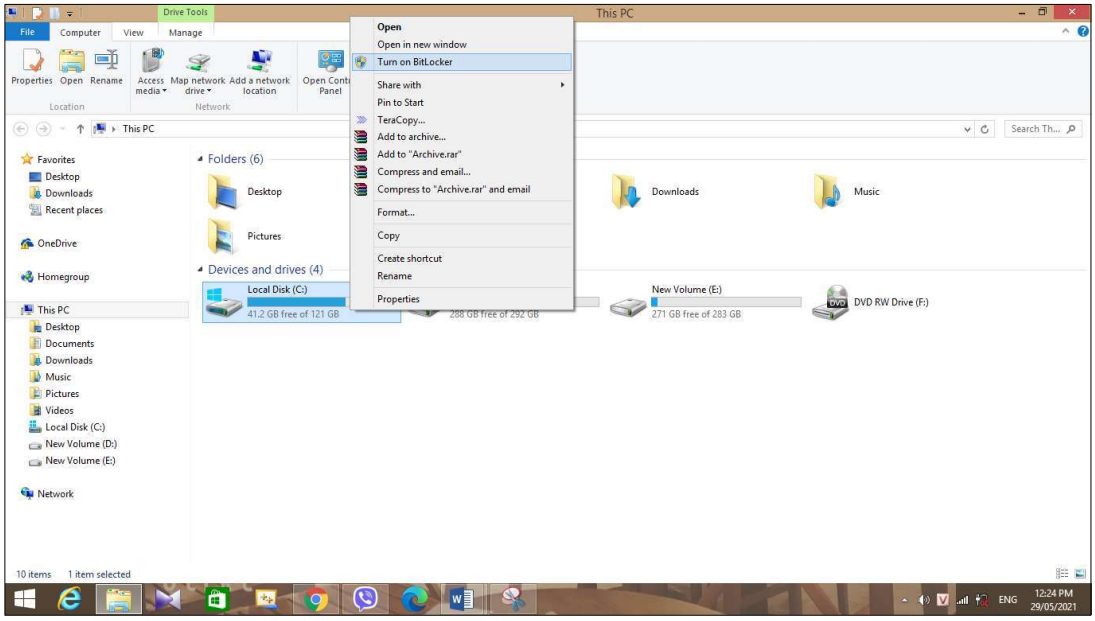
Mã hóa là một phương pháp bảo vệ thông tin, bằng cách chuyển đổi thông tin từ dạng có thể đọc và hiểu được thông thường trên các hệ điều hành sang dạng thông tin chỉ thể có thể đọc được qua giải pháp đã mã hóa. Việc làm này giúp ta có thể bảo vệ thông tin tốt hơn, an toàn trong việc lưu trữ dữ liệu. Dù kẻ xấu có được ổ cứng, thiết bị lưu trữ của người dùng cũng không thể có được thông tin và dữ liệu lưu trữ bên trong. Ngoài các giải pháp mã hóa dữ liệu thương mại trên thị trường, trên hệ điều hành Windows có tích hợp sẵn tính năng bảo vệ dữ liệu là BitLocker. Tính năng mã hóa toàn bộ ổ cứng hoặc phân vùng bất kỳ của BitLocker sẽ đảm bảo nếu thiết bị mất hoặc bị đánh cắp thì cũng sẽ không thể truy nhập vào tệp, dữ liệu trên ổ đĩa đã được bảo vệ. Tính năng này nên được người dùng hệ điều hành Windows tận dụng để đảm bảo các dữ liệu quan trọng của cơ quan, tổ chức không bị lộ lọt trong trường hợp xấu xảy ra.

Cách sử dụng BitLocker:

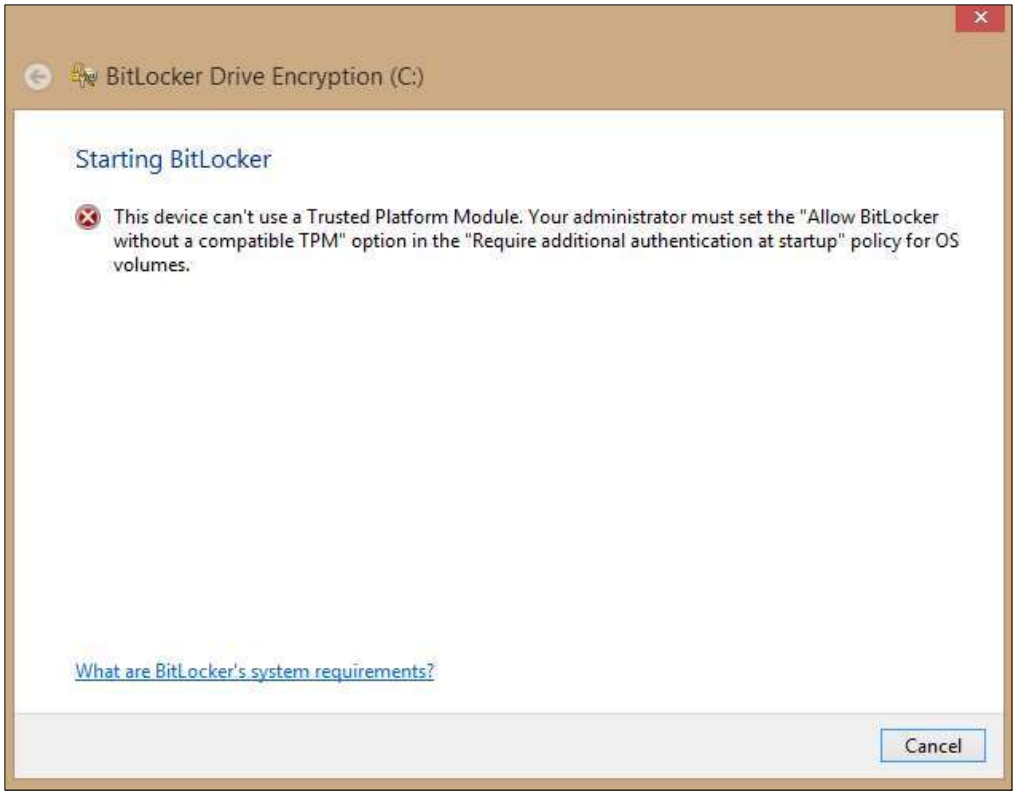
BitLocker là một tính năng bảo mật được tích hợp sẵn trong hệ điều hành Windows, với tính năng này chúng ta có thể mã hoá mọi dữ liệu trong ổ cứng hãy thiết bị nhớ như USB,…. Mọi dữ liệu của bạn sẽ được bảo vệ một cách an toàn bằng mật khẩu và mã hoá theo chuẩn riêng.

Mã hóa ổ đĩa hệ thống (ổ cài Win) bằng BitLocker:

Bước 1: Chuột phải lên ổ C (ổ cài Win) và chọn “Turn on Bitlocker”

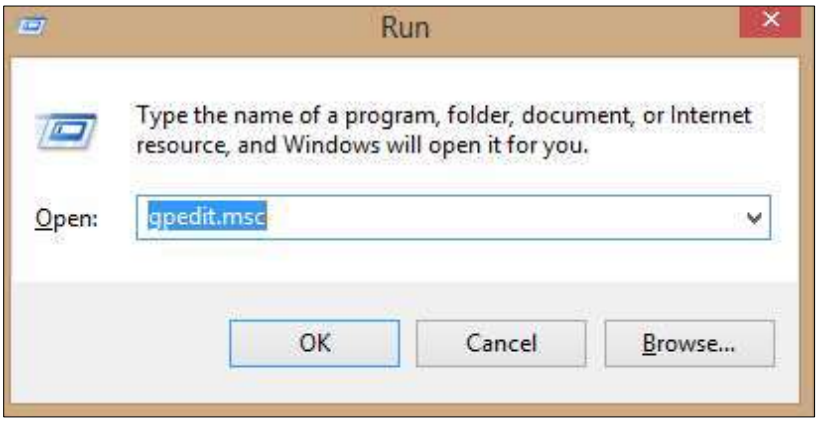


Nếu bạn gặp thông báo lỗi như hình dưới tức là máy tính của bạn không được tích hợp chip bảo mật TPM nên bạn không thể sử dụng BitLocker. Còn nếu không gặp thông báo này thì tiếp tục thực hiện Bước 2.



Bạn cần kích hoạt BitLocker trên máy tính không hỗ trợ TPM như sau:

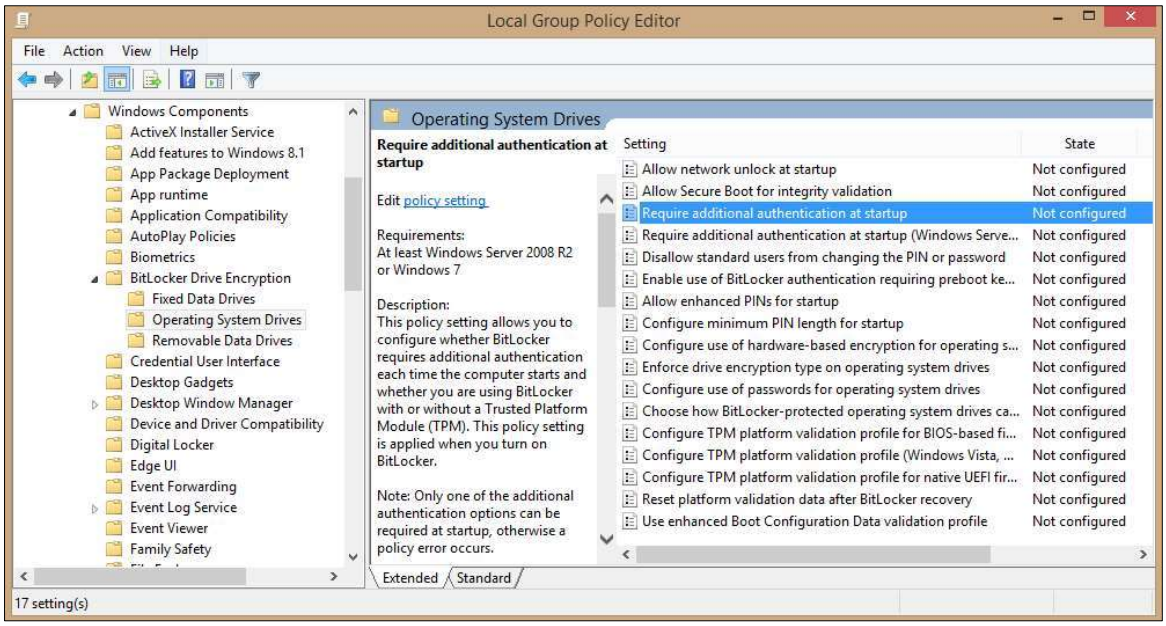
Nhấn tổ hợp phím Windows + R để mở hộp thoại Run sau đó nhập lệnh "gpedit.msc" và nhấn Enter.



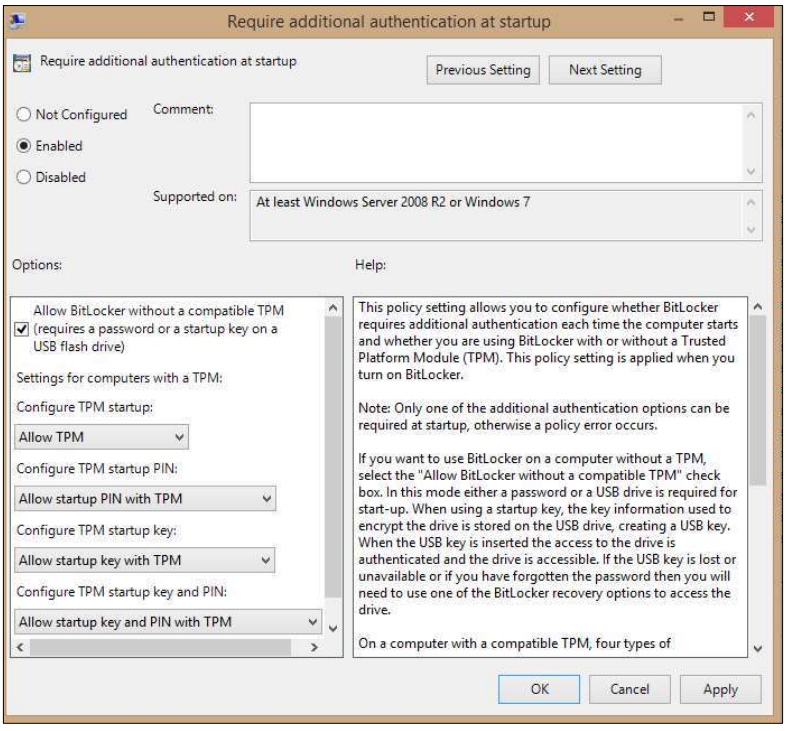
Cửa sổ Local Group Policy Editor hiện lên, các bạn thực hiện theo các bước chi tiết như sau:

Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives

Sau đó ở cửa sổ hiện tại các bạn kích đúp vào dòng "Require additional authentication at startup".

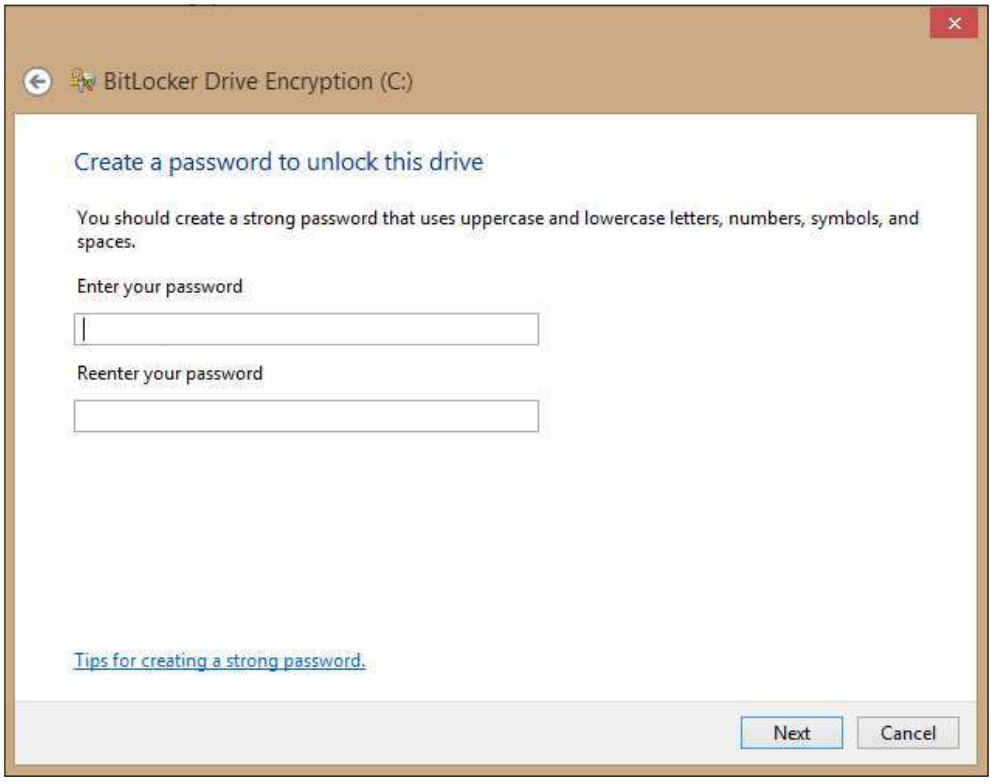


Trong cửa sổ mới bạn tích chọn Enabled sau đó xuống phía dưới tích chọn mục "Allow BitLocker without a compatible TPM". Cuối cùng nhấn Apply để lưu cài đặt và thoát cửa sổ.



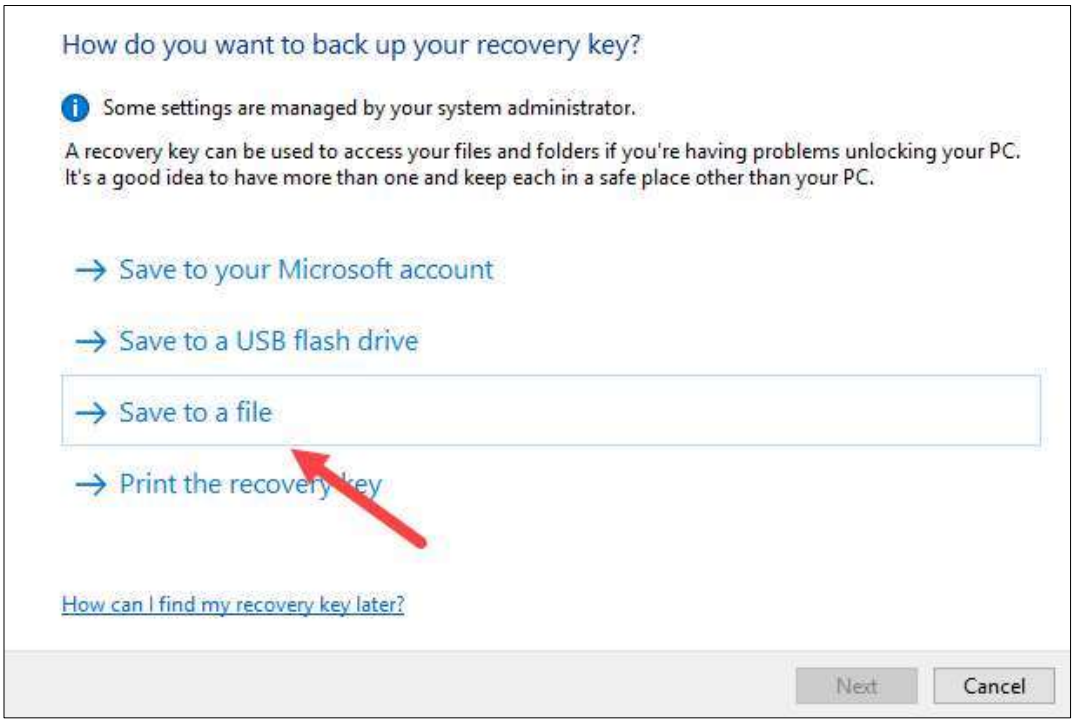
Bước 2: Nhấn chọn "Enter a password"

Bước 3: Nhập mật khẩu bảo vệ vào 1 ô trống và nhấn Next



Bước 4: tại đây chúng ta sẽ tiến hành tạo một file backup mật khẩu để có thể khôi phục mật khẩu BitLocker trong trường hợp bạn bị quên mật khẩu. Có nhiều phương pháp để lưu file Backup, bạn có thể lưu vào tài khoản Microsoft, lưu vào USB, lưu thành file txt,…

Ở đây, chọn lưu Save to a file.



Cửa sổ duyệt file hiện lên, bạn chọn nơi lưu trữ file backup và nhấn Save, lưu ý là bạn không thể lưu vào ổ mà bạn đang mã hóa. Ví dụ nếu bạn mã hóa ổ C thì phải lưu file backup vào ổ D hoặc USB.

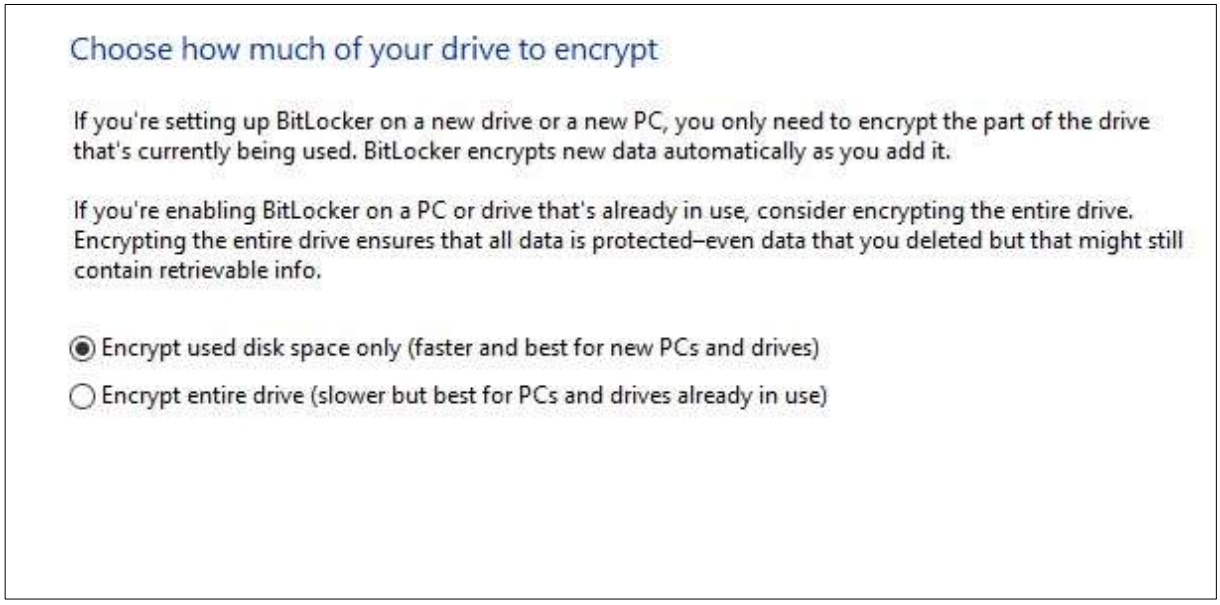
Trở về cửa sổ trước, bạn nhấn Next để tiếp tục.

Bước 5: Bạn có 2 lựa chọn mã hóa

Encrypt used disk space only (chỉ mã hóa dữ liệu đã sử dụng)

mã hóa toàn bộ ổ cứng.

Nếu máy tính bạn còn mới và chưa có dữ liệu gì thì có thể chọn Encrypt used disk space only để mã hóa nhanh nếu không thì có thể chọn mã hóa toàn bộ ổ cứng.



Bước 6: Nếu bạn dùng windows 10 từ version 1511 trở lên sẽ có thêm lựa chọn này, đây là một kiểu mã hoá mới tốt hơn nhưng chỉ có trên windows 10 version 1511 trở đi. Tuy nhiên nếu bạn chọn kiểu mã hoá này thì những máy tính sử dụng hệ điều hành cũ sẽ không giải mã được nếu bạn copy dữ liệu sang.

Vì vậy nếu bạn muốn chọn kiểu mã hoá mới thì chọn **New encryption mode**, nếu không thì chọn **Compatible mode** sau đó nhấn **Next**.

Bước 7: chọn Continue để tiếp tục.

Thông báo yêu cầu khởi động lại máy tính, bạn hãy nhận Restart now để khởi động lại ngay.

Trong quá trình khởi động máy tính, bạn phải nhập mật khẩu đã tạo ở Bước 3.

Khởi khởi động vào Windows bạn sẽ thấy trên ổ C có biểu tượng ổ khóa tức là đã được mã hóa bằng BitLocker.

Mã hóa dữ liệu trên ổ đĩa không phải là ổ hệ thống cũng tương tự nhưng chúng ta mã hóa ổ chứa hệ điều hành ở trên.

Sao lưu dự phòng dữ liệu

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

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

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

- Dịch vụ lưu trữ đám mây rất hữu ích để lưu trữ một bản sao dữ liệu của mình ở nơi khác qua internet.

1.1.7. Một số hướng dẫn thiết lập mật khẩu an toàn dành cho người dùng

Những quy tắc cơ bản để thiết lập mật khẩu an toàn sẽ giúp người dùng chủ động tạo ra các phương án bảo vệ cơ bản, có giá trị thiết thực trong việc sử dụng các ứng dụng, dịch vụ có xác thực qua mật khẩu. Các nguyên tắc này bao gồm:

Thay đổi tất cả mật khẩu mặc định

- ✓ Thay đổi tất cả mật khẩu mặc định trước khi sử dụng hay vận hành ứng dụng, thiết bị nào đó.
- ✓ Thực hiện kiểm tra thường xuyên các thiết bị và phần mềm hệ thống để tìm các mật khẩu mặc định chưa thay đổi.
- ✓ Ưu tiên các ứng dụng, thiết bị cơ sở hạ tầng quan trọng.

Đối phó với tình trạng quá tải mật khẩu

- ✓ Sử dụng một bộ công cụ để quản lý mật khẩu chuyên dụng (như Lastpass).
- ✓ Chỉ sử dụng mật khẩu khi thực sự cần thiết, như các mật khẩu quan trọng
- ✓ Không chia sẻ mật khẩu.

Tạo mật khẩu khó đoán, phức tạp

- ✓ Tránh việc chọn mật khẩu quá ngắn, đơn giản, dễ đoán và những mật khẩu phổ biến nhất đã được đưa vào các danh sách đen (blacklist). Mật khẩu khó đoán (Mật khẩu cần bao gồm: tối thiểu 8 ký tự, có chữ hoa, chữ thường trong bảng chữ cái, số và các ký tự đặc biệt).
- ✓ Không nên sử dụng cùng mật khẩu trong công việc và ứng dụng, thiết bị cá nhân.
- ✓ Có độ dài tối thiểu 8 ký tự và phù hợp với tính chất bí mật của từng loại tài khoản khác nhau

1.1.8. Sử dụng thư điện tử thận trọng

Mã độc có thể lây nhiễm vào máy tính người dùng thông qua các tệp tin đính kèm thư điện tử. Các tệp tin độc hại này thường được đính kèm trong thư điện tử từ địa chỉ lạ hoặc giả mạo hòm thư của một cơ quan tổ chức.

Do đó, người sử dụng không nên mở các tệp tin đính kèm thư điện tử nhận được từ một người lạ hoặc một người có địa chỉ thư điện tử giống với những người mà mình quen biết, mà không rõ lý do nhận được thư.

Ngoài ra, chúng ta có thể sử dụng chương trình phòng chống mã độc để dò quét tệp tin đính kèm trước mở.

1.1.9. Sử dụng USB, thiết bị lưu trữ di động cẩn trọng

Phần lớn, người dùng đều đã hoặc đang sở hữu thiết bị USB để lưu trữ dữ liệu phục vụ cho việc học tập, làm việc của bản thân. Các thiết bị lưu trữ hoàn toàn có thể bị nhiễm virus và ransomware (vô tình hoặc cố ý) và sử dụng với mục đích xấu, gây thiệt hại cho người sử dụng chúng. Thậm chí còn có những phần mềm độc hại được thiết kế dành riêng cho USB, biến chiếc USB thành công cụ lây nhiễm mã độc trung gian trên máy tính, qua đó đánh cắp thông tin đăng nhập và dữ liệu nhạy cảm.

Một số lưu ý để bảo vệ máy tính, dữ liệu của người dùng khỏi USB, thiết bị lưu trữ độc hại bao gồm:

- ✓ Không cắm USB chưa xác định nguồn gốc vào các máy tính quan trọng. Đánh vào tâm lý tò mò của con người cũng là một kỹ thuật tấn công phổ biến của tin tặc. Điều này đặc biệt hay xảy ra trong trường hợp bạn nhặt được USB rơi ở đâu đó.
- ✓ Không sử dụng chung một ổ USB cho máy tính cả gia đình và cơ quan. Điều này có thể làm giảm nguy cơ lây nhiễm chéo giữa các máy tính.
- ✓ Luôn bật các tính năng bảo mật như xác thực mật khẩu, vân tay (nếu có) đối với kết nối USB. Điều này sẽ giúp bảo vệ thiết bị khỏi hoạt động truy cập vật lý của hacker.
- ✓ Luôn cập nhật phần mềm trên máy tính của bạn lên phiên bản mới nhất để được bảo vệ tối đa trước các loại mã độc, lỗ hổng bảo mật đã biết.
- ✓ Luôn dùng giải pháp phòng chống phần mềm độc hại như Anti-Virus, Endpoint Security để rà quét, tìm và loại bỏ các mã độc trên các thiết bị lưu trữ di động trước khi sử dụng.

1.2. Phòng chống thư điện tử lừa đảo, giả mạo (Phishing)

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

Một số cách phát hiện thư điện tử lừa đảo đối với người dùng

Không nên tin tưởng tên hiển thị trong mail

Một chiến thuật lừa đảo yêu thích của các tin tặc là giả mạo tên hiển thị của một thư điện tử để đánh lừa người nhận. Các tên hiển thị hay được giả mạo như tên của các Công ty, tổ chức, hãng lớn; Người quen của bạn; Người nổi tiếng …

Cân nhắc kỹ lưỡng khi bấm vào liên kết trong thư điện tử

Cẩn trọng khi bấm vào bất cứ liên kết được gửi trong nội dung thư điện tử. Liên kết đó có thể dẫn bạn tới một website lừa đảo giả mạo, quảng cáo hay một website độc hại mà hacker dựng lên để tấn công.

Bỏ qua các thư điện tử yêu cầu cung cấp thông tin cá nhân

Một tổ chức, công ty, ngân hàng,…sẽ không yêu cầu người sử dụng cung cấp thông tin cá nhân vô lý qua Internet. Do vậy bạn hoàn toàn có thể bỏ qua chúng khi nhận được các thư điện tử với nội dung đó. Và thậm chí hạn chế tối đa, cân nhắc cẩn thận khi cung cấp thông tin cá nhân cho bất kỳ tổ chức nào.

Cẩn trọng với các thư điện tử có tiêu đề "Hấp dẫn – Nhạy cảm – Khẩn cấp"

Đánh vào tâm lý của người dùng, hacker thường xuyên sử dụng các tiêu đề email có tính Hấp dẫn – Nhạy cảm - Khẩn cấp trong thư điện tử để lừa người dùng. Một số tiêu đề thư điện tử mà chắc chắn là lừa đảo hoặc có mã độc như: "Cập nhật bảng lương công ty Quý 2/2019" ; "Cảnh bảo: Tài khoản của bạn bị đình chỉ" …

Cẩn thận, cân nhắc khi tải về các File đính kèm trong thư điện tử

Tấn công bằng việc cài mã độc, virus trong các file đính kèm trong thư điện tử là phương thức tấn công phổ biến và hiệu quả nhất hiện nay. Không nên tải và mở chạy file ngay khi nhận được thư điện tử có file đính kèm. Chú ý tới định dạng file và tạo thói quen quét virus với các file đính kèm trước khi mở chúng, đặc biệt là các tập tin đính kèm có đặt mật khẩu gửi kèm theo nhằm qua mặt các giải pháp bảo vệ ở lớp mạng.

Nhận diện các thư điện tử spam –thư điện tử quảng cáo

Người dùng cần cảnh giác khi nhận các thư điện tử spam, thư điện tử quảng cáo từ Internet. Trong các thư điện tử này thường đi kèm với nhiều rủi ro mất an toàn thông tin mà chúng ta không mong muốn như: lừa đảo, mã độc, gây ảnh hưởng tới công việc khi nhận quá nhiều…

Cẩn trọng với các tin nhắn rác

Cũng tương tự như thư điện tử spam thì các tin nhắn rác (sms spam) cũng gây cho người dùng rất nhiều phiền toái. Bên cạnh đó ngày nay các tin nhắn rác thường xuyên được sử dụng như một phương thức để lừa đảo người dùng như: Bạn trúng thưởng một xe SH….Nhắn tin, gọi tới 1800XXXX, 1900XXXX, 1900XXXXXX, 6XXX, 7XXX, 8XXX, 9XXX,… Truy cập vào đường link, trang web.

1.3. Sử dụng mạng riêng ảo (VPN)

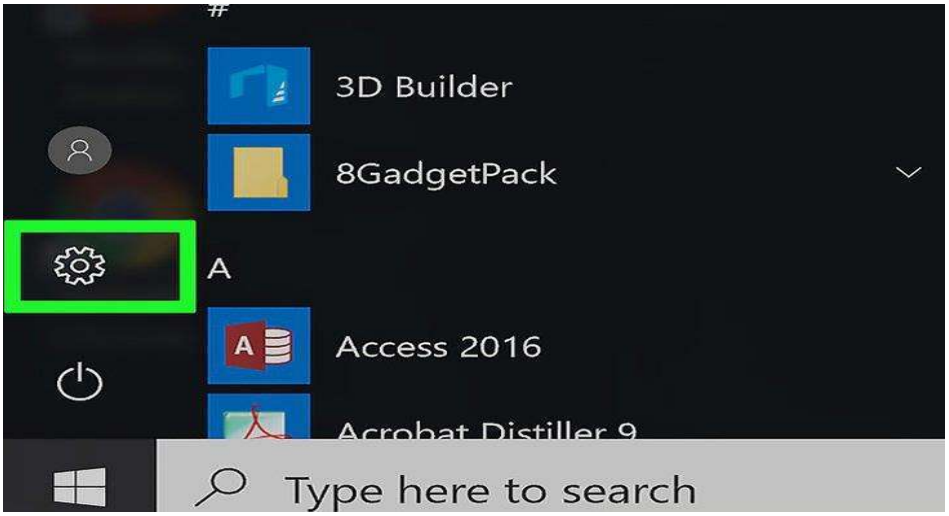
Để kiểm soát và bảo vệ các kết nối truy cập vào hệ thống, các cơ quan, tổ chức có thể lựa chọn phương án mã hóa tất cả lưu lượng truy cập mạng với một mạng riêng kết nối ảo (VPN - Virtual Private Network). Các kết nối VPN sử dụng một loạt các giao thức để thực hiện một kết nối an toàn giữa điểm kết nối vào hệ thống. VPN có thể sử dụng để kết nối từ một mạng không an toàn (như kết nối không dây trong một khách sạn, quán cafe hay tại nhà của nhân viên) đến các nguồn tài nguyên nội bộ trong hệ thống của cơ quan, tổ chức.

Tại sao nên sử dụng VPN?

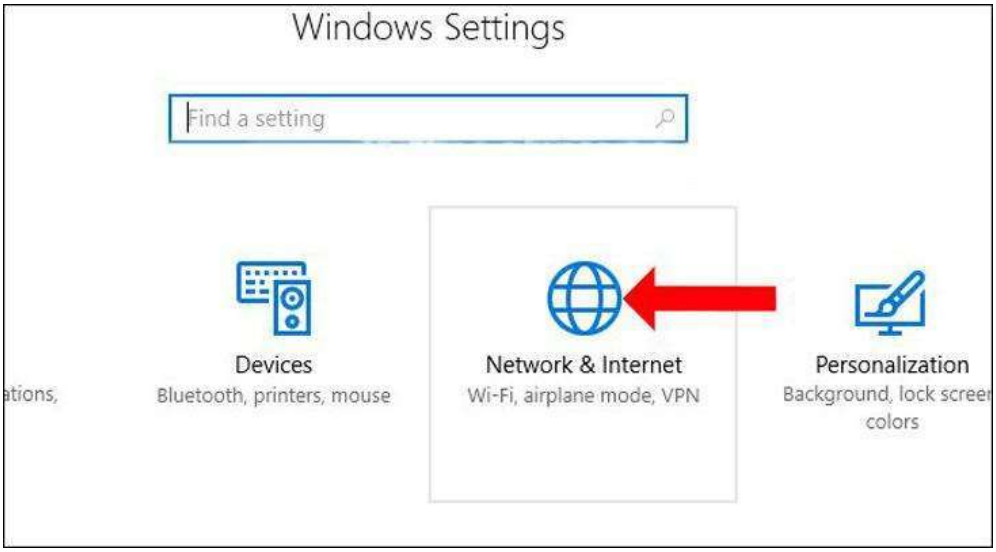
VPN là các kết nối mạng được mã hóa. Điều này cho phép người dùng từ xa truy cập an toàn từ xa vào các dịch vụ của tổ chức. VPN là một cách để đảm bảo tính bảo mật cho "dữ liệu truyền qua" trên một mạng không tin cậy, nhưng chúng cũng cung cấp một số lợi ích khác. Ví dụ: Một tổ chức có văn phòng ở nhiều địa điểm có thể sử dụng VPN để cung cấp cho người dùng từ xa quyền truy cập vào các dịch vụ tệp và thư điện tử của công ty.

Hướng dẫn tạo cấu hình VPN trên Windows 10:

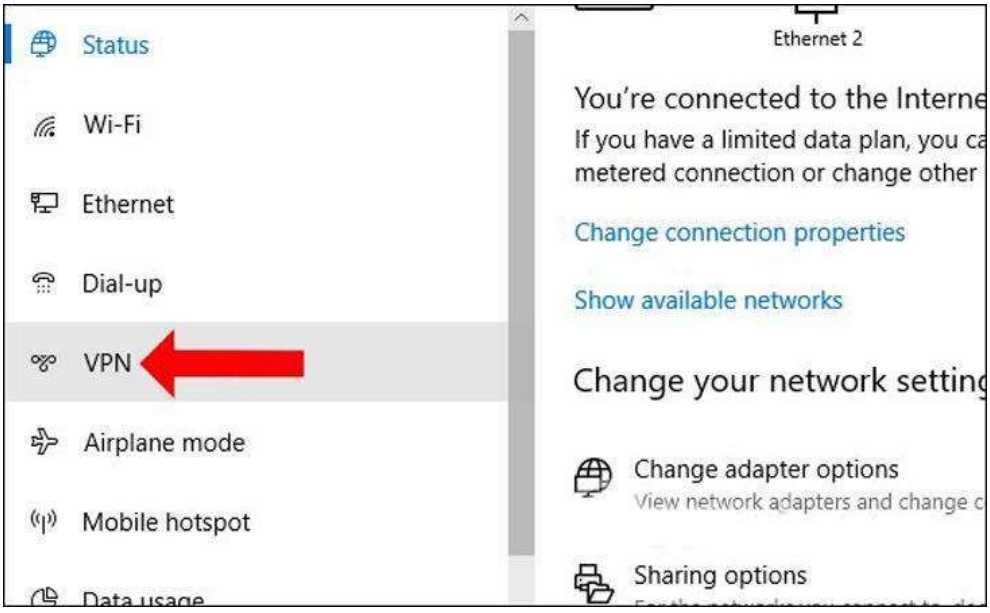
Bước 1: Nhấn nút Start trên giao diện rồi chọn tiếp vào mục Setting



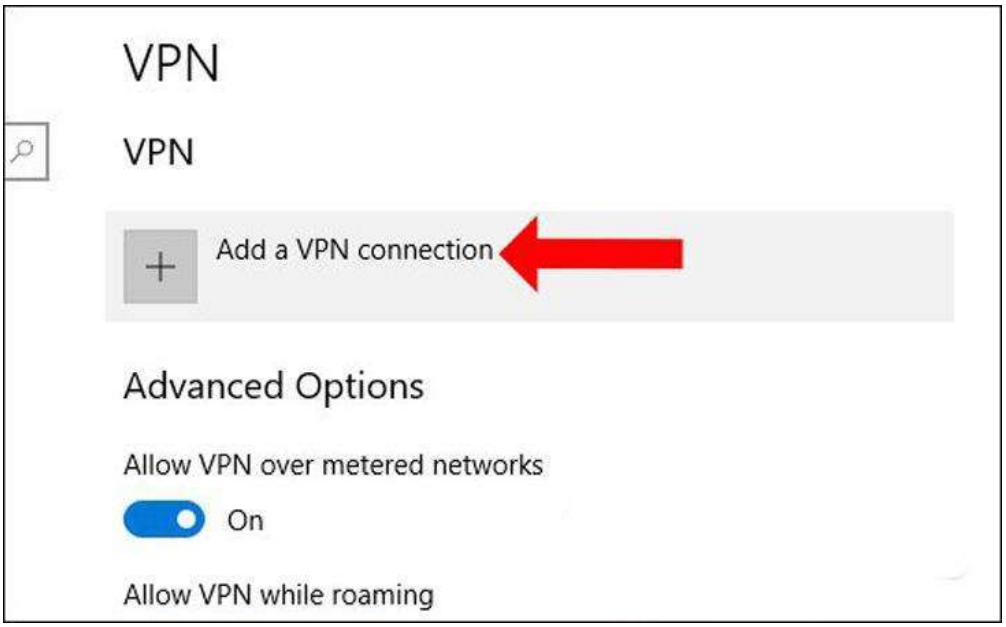
Bước 2: Trong giao diện Windows Setting nhấn chọn vào mục Netwwork&Internet.



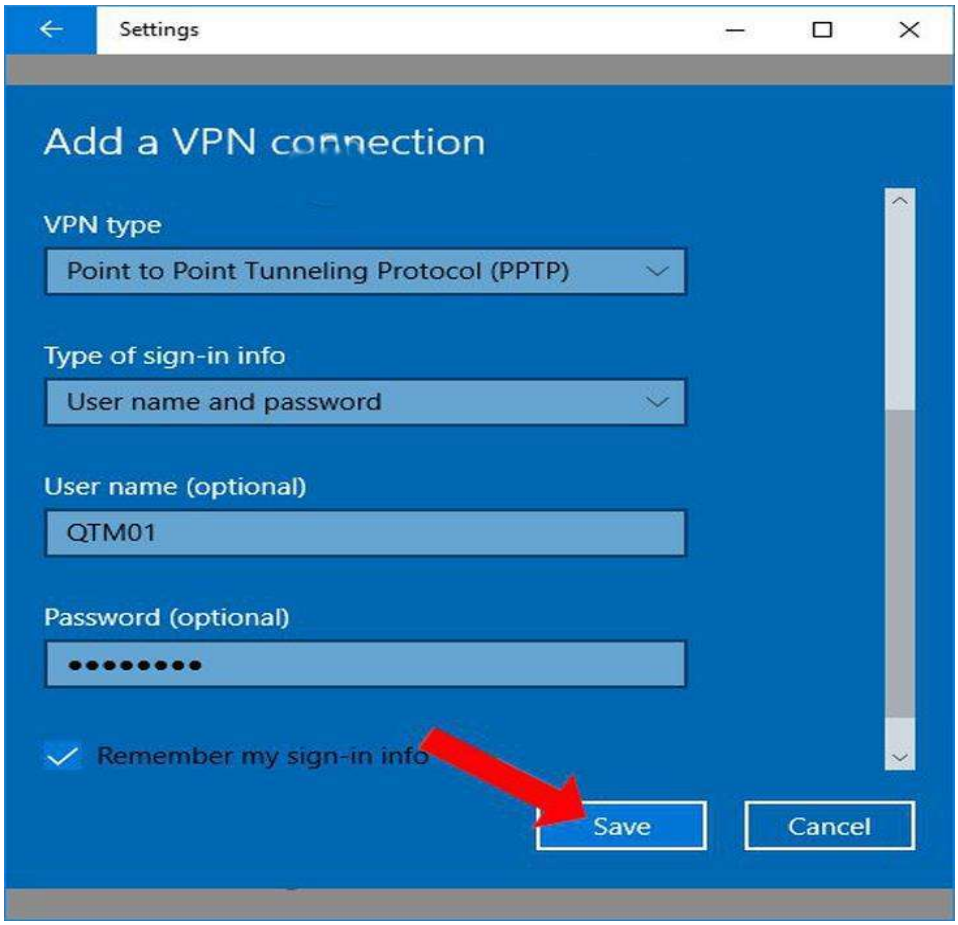
Bước 3: Chuyển sang giao diện mới. Tại danh sách bên trái giao diện nhấn vào mục VPN.



Bước 4: Sau đó nhìn sang nội dung bên phải sẽ thấy một số mục thiết lập để tạo VPN, chọn Add a VPN connection.



Bước 5: Xuất hiện giao diện **Add a VPN connection,** điền một số thông tin gồm:



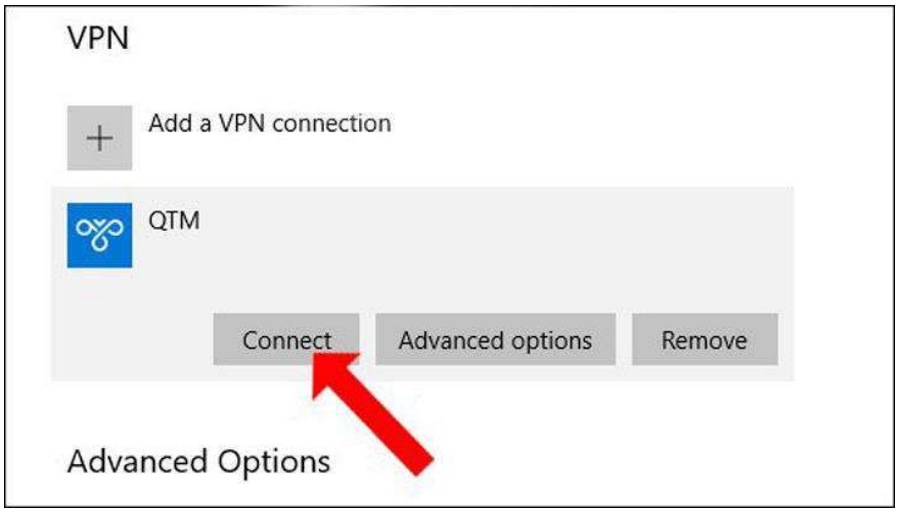
- VPN provider: nhấn chọn Windows (built-in).

- Connection name: chọn tên kết nối bạn muốn.
- Server name or address: nhập tên máy chủ hoặc địa chỉ IP của máy chủ đó.
- VPN Type: chọn Point to Point Tunneling Protocol (PPTP) hoặc L2TP/IPsec with pre-shared key.
- Type of sign-in info: chọn Username and password.
- User name: tên người dùng.
- Password: mật khẩu.

Bước 6: Nhấn Save để lưu lại.

Hướng dẫn kết nối với VPN trên Windows 10

- Quay trở lại giao diện VPN trên **Setting** bạn sẽ nhìn thấy mạng VPN được tạo mới. Để kết nối với mạng này chỉ cần click chọn rồi nhấn tiếp vào **Connect**.



CHUYÊN ĐỀ 2: HỌC TRỰC TUYẾN AN TOÀN

Trong mùa dịch Covid, việc học từ xa bằng các thiết bị điện tử tại nhà sẽ là giải pháp thay thế tối ưu cho việc học tập trung ở trường đối với học sinh, sinh viên và giáo viên. Hiện nay, sự phát triển của công nghệ đã cho ra đời nhiều phần mềm, hình thức học trực tuyến như Zoom, Microsoft Teams, Skype, Google Meeting, Google Class,... Việc nhà trường, các cơ sở giáo dục đào tạo phổ biến hướng dẫn sử dụng các phần mềm học trực tuyến trong mùa dịch là điều cần thiết, vì tại thời điểm khủng hoảng như thế này, hacker dễ lợi dụng xâm nhập vào không gian mạng, các phần mềm học trực tuyến để đánh cắp thông tin cá nhân, phát tán mã độc gây ảnh hưởng đến người dùng và quá trình học tập. Nhà trường, giáo viên cần hướng dẫn học sinh, sinh viên các chức năng, cách truy cập cụ thể trên các phần mềm học trực tuyến để tránh xảy ra sai sót liên quan đến vấn đề bảo mật thông tin và an toàn thông tin trong quá trình giảng dạy.

Ngoài những hướng dẫn của nhà trường, tổ chức, dưới đây là một số hướng dẫn của NCSC để thiết lập tính năng bảo mật trong ứng dụng học trực tuyến phổ biến hiện nay:

2.1. Phần mềm Zoom

2.1.1. Đặt mật khẩu cho lớp học

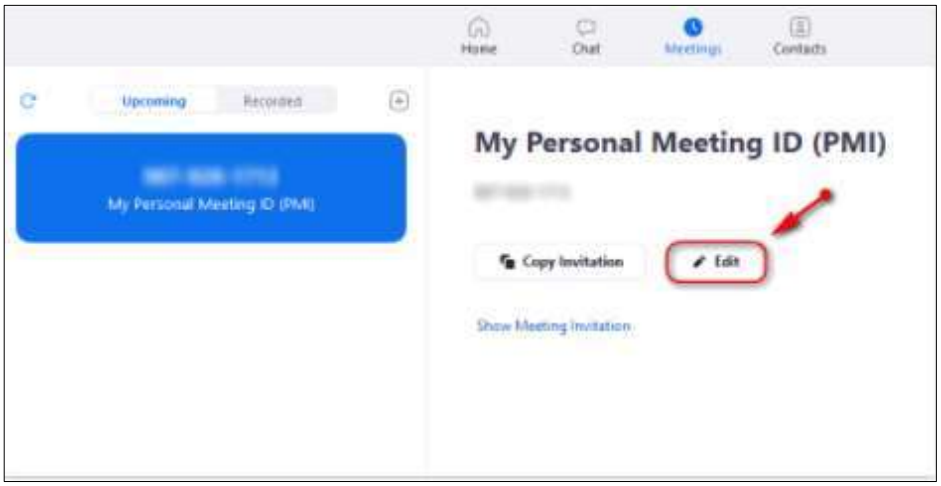
Tính năng mật khẩu cho lớp học giúp bảo mật thông tin. Hạn chế việc truy cập mạo danh hoặc truy cập từ các đối tượng không cần thiết.

Mật khẩu Zoom giúp đơn giản và thuận tiện hơn trong công việc quản lý các lợp học và buổi họp trực tuyến mà bạn là người chủ trì.

Các bước thực hiện:

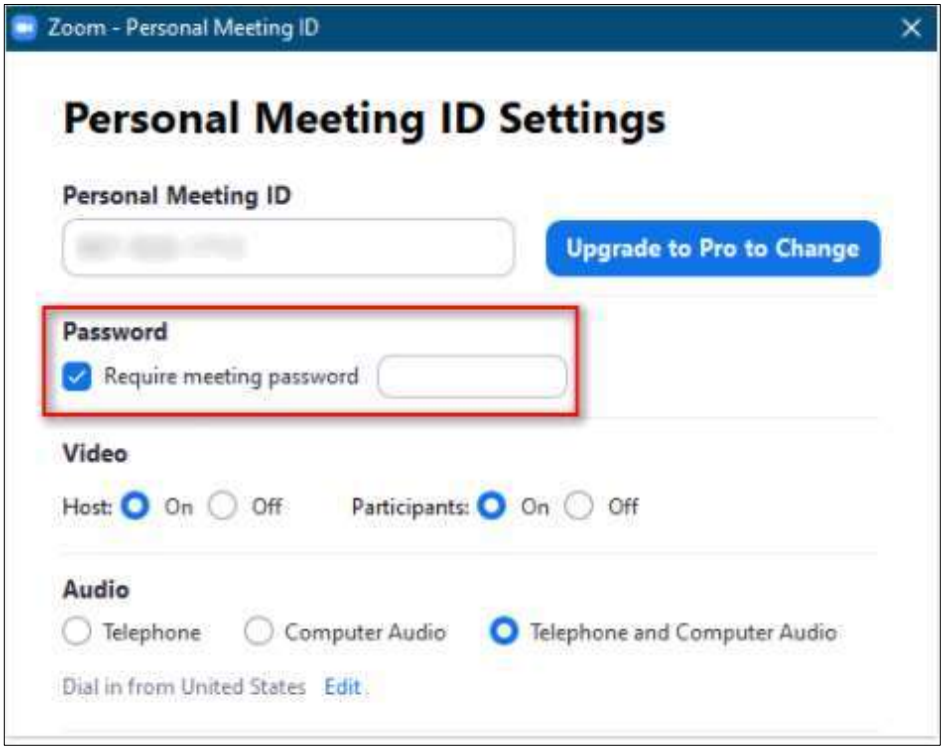
Bước 1: Tại giao diện chính của phần mềm, bấm chọn vào thẻ "Meetings".

Bước 2: Tại giao diện cấu hình ID cho tài khoản, bấm "**Edit**" để chỉnh sửa thông tin.



Bước 3: Mặc định, Zoom sẽ tự động đặt mật khẩu cho ID của bạn. Nếu muốn thay đổi mật khẩu, hãy tích chọn và nhập mật khẩu muốn cài đặt.

Bước 4: Nhấn lưu lại và cung cấp ID và mật khẩu lớp học cho người tham gia để truy cập lớp học.



2.1.2. Xác thực người tham gia

Bước 1: Đăng nhập vào cổng web Zoom.

Bước 2: Trong bảng điều hướng, nhấp vào Settings.

Bước 3: Trong phần Security, xác minh "Only authenticated users can join meetings"

Nếu cài đặt bị tắt, hãy nhấp vào nút chuyển đổi để bật. Nếu hộp thoại xác minh hiển thị, chọn Turn on để xác minh sự thay đổi.

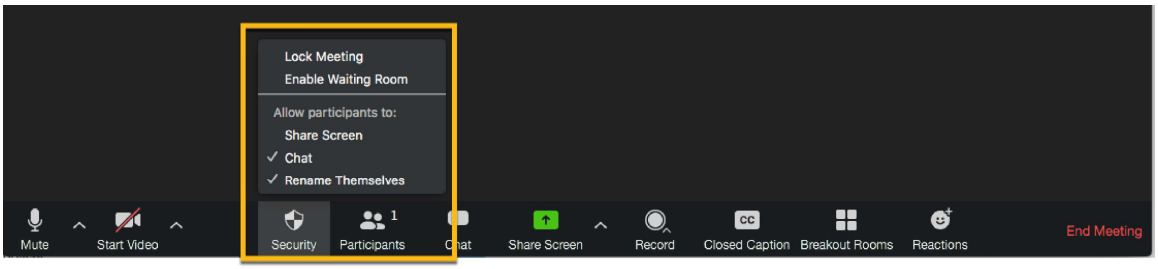
Lưu ý: Nếu các tùy chọn chuyển sang màu xám, nó đã bị khóa ở cấp nhóm hoặc cấp tài khoản. Bạn cần liên hệ với quản trị viên Zoom.

Nếu chưa đăng nhập vào Zoom, sẽ hiện thị:

Nếu đăng nhập email không hợp lệ:

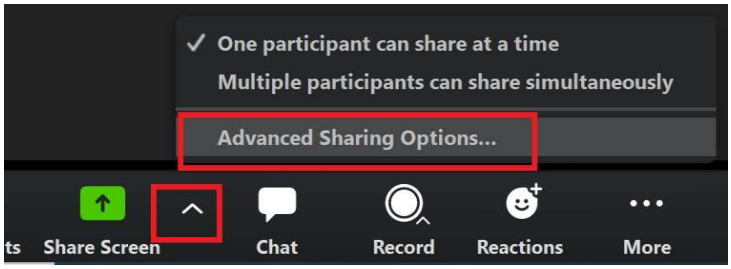
2.1.3. Khóa cuộc họp

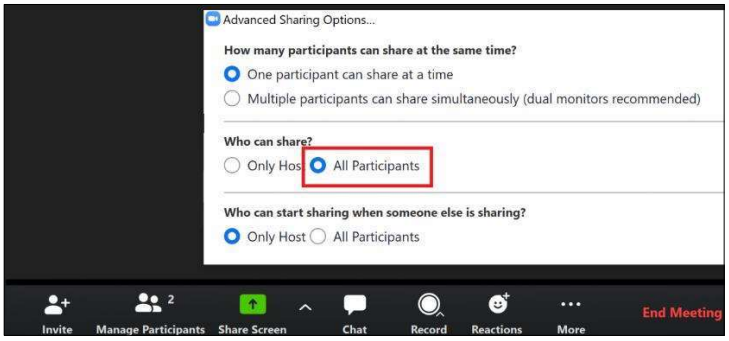
Khi phiên đã bắt đầu, hãy chuyển đến tab "Manage Participants", chọn "More" và chọn "Lock" cuộc họp của bạn ngay sau khi tất cả mọi người tham gia đã vào. Điều này sẽ ngăn những người khác tham gia kể cả khi thông tin ID cuộc họp hoặc thông tin truy cập bị rò rỉ.



2.1.4. Tắt chia sẻ màn hình của người tham gia

Để ngăn người tham gia chia sẻ màn hình trong khi gọi, bằng cách sử dụng các điều khiển máy chủ lưu trữ ở dưới cùng, nhấp vào mũi tên bên cạnh "Share Screen" rồi chuyển đến "Advanced Sharing Options". Trong phần "Who can share?" chọn "Only Host " và đóng cửa sổ.



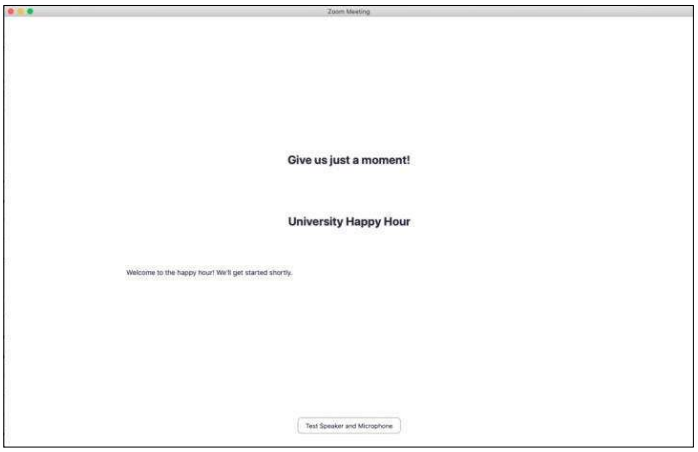


2.1.5. Sử dụng ID ngẫu nhiên

Người dùng không nên sử dụng ID cuộc họp cá nhân của mình, vì điều này có thể tạo điều kiện cho những kẻ tấn công làm gián đoạn các phiên họp trực tuyến. Thay vào đó, hãy chọn một ID được tạo ngẫu nhiên cho các cuộc họp. Ngoài ra, không nên chia sẻ công khai ID cá nhân của mình.

2.1.6. Sử dụng phòng chờ

Tính năng Phòng chờ (Waiting Room) là một cách để lọc những người tham gia trước khi họ được phép tham gia cuộc họp. Điều này cũng cho phép chủ cuộc họp kiểm soát tốt hơn bảo mật trong phiên họp.

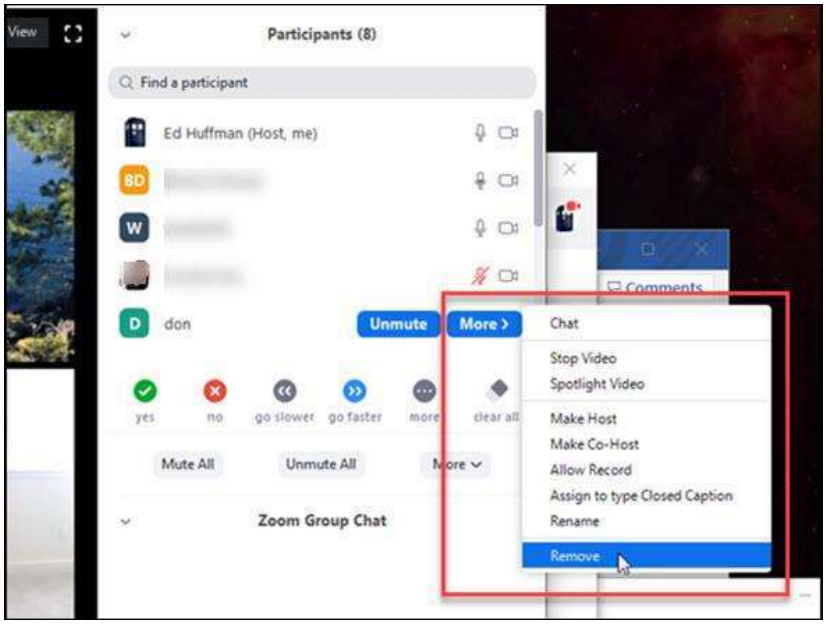


2.1.7. Tránh chia sẻ tệp tin

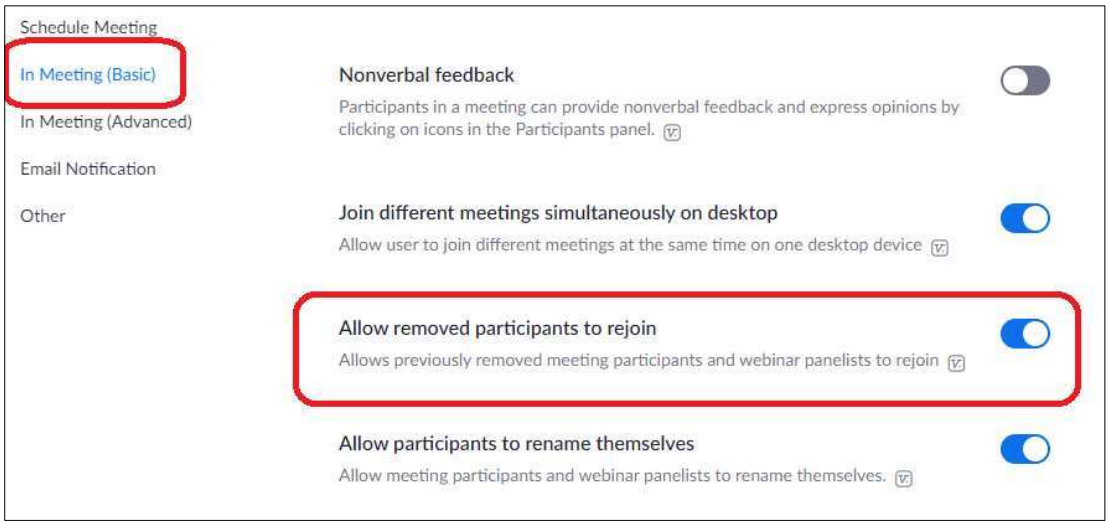
Cẩn thận với tính năng chia sẻ tệp của các cuộc họp, đặc biệt nếu người dùng không xác định đang gửi một tệp tin hoặc liên kết qua đó, những thứ này có thể chứa virus. Thay đó, hãy chia sẻ tài liệu thông qua các dịch vụ đáng tin cậy như Box hoặc Google Drive.

2.1.8. Loại bỏ những người tham gia không cần thiết

Nếu nhận thấy ai đó đang làm gián đoạn cuộc họp, người dùng có thể kick họ trong tab "Participants". Di chuột qua tên, chọn "More" và xóa chúng.

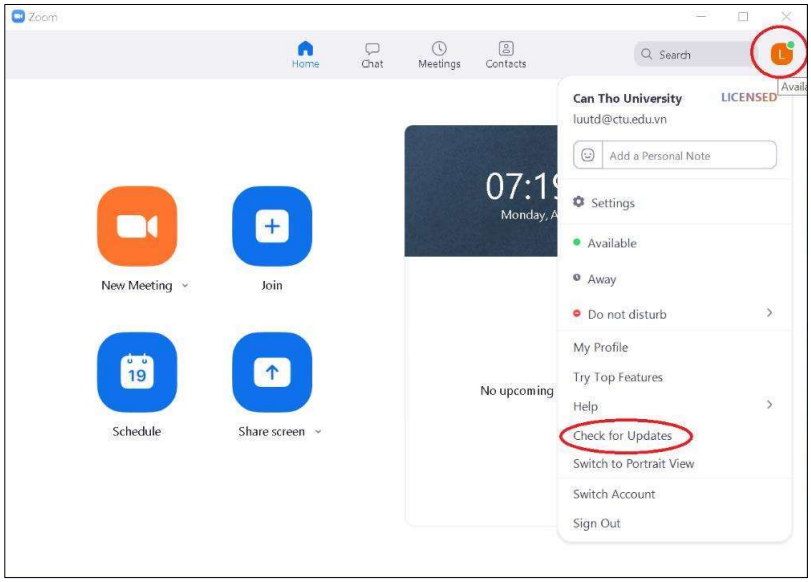


Người dùng cũng có thể đảm bảo họ không thể tham gia lại bằng cách tắt "Allow Removed Participants to Rejoin" trong tab "Settings: Meetings – Basic".



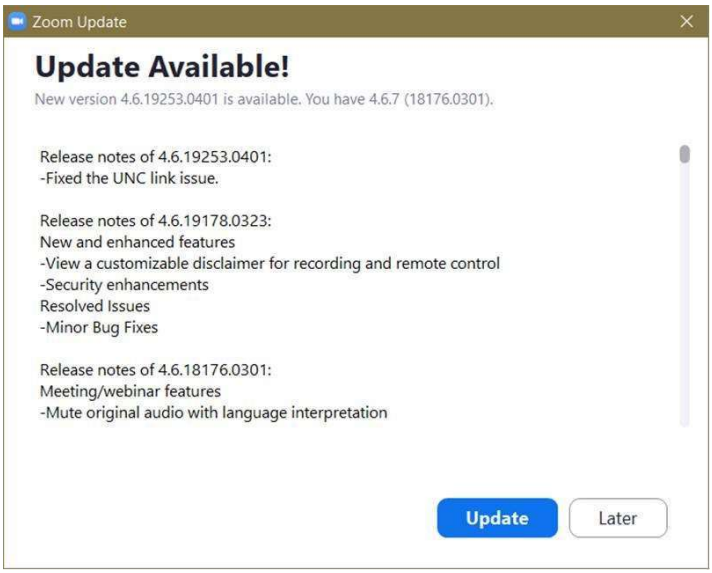
2.1.9. Kiểm tra các bản cập nhật

Khi các vấn đề bảo mật xuất hiện và các bản vá phần mềm được triển khai hoặc các chức năng không an toàn sẽ được xử lý. Người dùng nên đảm bảo rằng mình đang dùng bản phần mềm mới nhất. Để kiểm tra, hãy mở ứng dụng dành cho máy tính để bàn, chọn profile ở trên cùng bên phải và chọn "Check for updates".



Nếu phiên bản là mới nhất chúng ta sẽ nhận được thông tin **"You are up to date"**

Nếu phiên bản chưa phải là mới nhất, người dùng sẽ nhận được thông tin **"Update Available!"**, nhấn vào **"Update"** để cập nhật bản mới nhất.

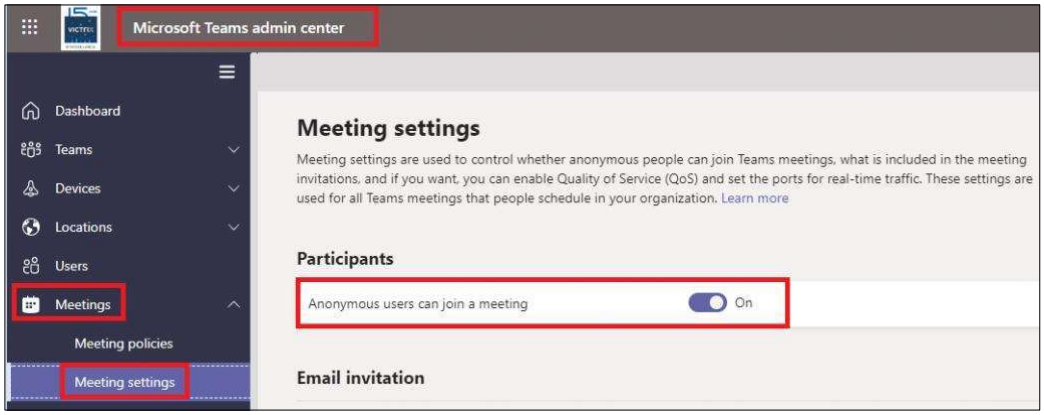


2.2. Phần mềm Microsoft Teams

2.2.1. Kiểm soát khách mời và người dùng ẩn danh trong nhóm

Khách mời (Guest User) là người ngoài tổ chức mà được gửi lời mời thông qua email. Sau khi trở thành thành viên trong cuộc họp, khách mời sẽ có quyền được gọi, nhắn tin, họp và chia sẻ các tập tin.

Mặt khác, người dùng ẩn danh (Anonymous users) sẽ không có thông tin chi tiết về bản thân và không có thông tin đăng nhập nào được lưu trữ trong Azure AD. Vậy nên nếu muốn hạn chế người dùng ẩn danh tham gia cuộc họp, có thể tắt chức năng "Anonymous users can join a meeting" từ Trung tâm quản trị của Teams.



2.2.2. Sử dụng các ID và link khách nhau cho từng phần

Để bảo vệ cuộc họp trên Teams, người dùng nên đảm bảo rằng mỗi phần trong cuộc họp sẽ được tạo một meeting riêng với ID riêng.

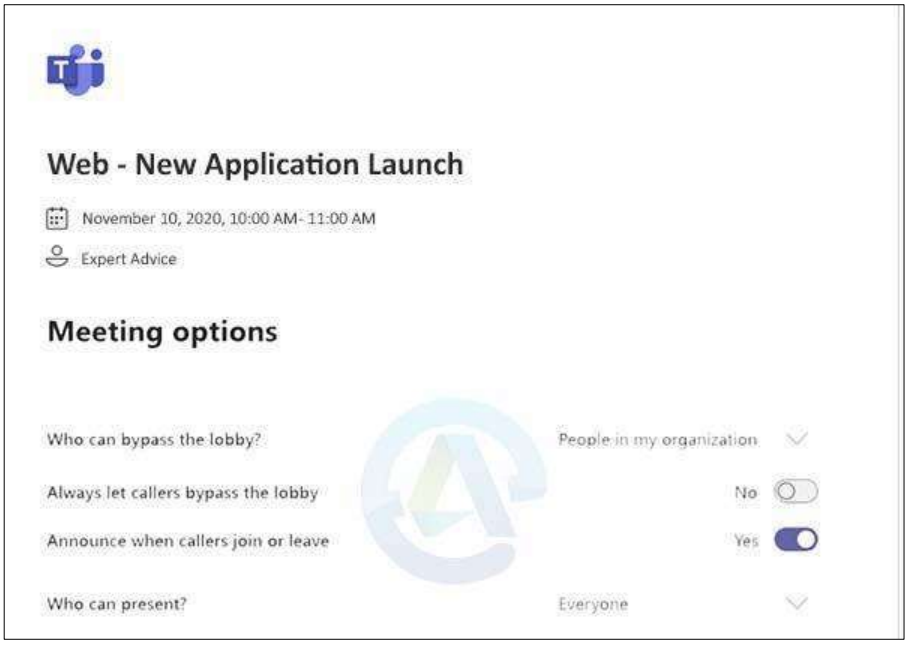
2.2.3. Thiết lập cài đặt đối với người dùng trong cuộc họp

Có một vài chức năng cuộc họp trên Microsoft Teams. Điều này phụ thuộc vào người tổ chức cuộc họp, có thể chọn hoặc để họ thoát khỏi sảnh chờ (mục Lobby

trong Ms Teams) và để họ chờ cho đến khi có người cho phép họ tham gia vào cuộc họp.

Trên MS Teams còn có chức năng cho Caller, người dùng có thể để họ tự động rời khỏi sảnh Lobby và nhận thông báo khi mà họ tham gia hoặc rời cuộc họp.

Đối với chức năng Present, người dùng có thể cho phép tất cả mọi người hoặc lựa chọn từng đối tượng tham gia vào cuộc họp.



CHUYÊN ĐỀ 3: LIÊN LẠC, KẾT NỐI AN TOÀN

Trong khi tất cả chúng ta phải ở nhà do các đợt dịch bùng phát, nhiều người vẫn cần giữ liên lạc với bạn bè và gia đình bằng các ứng dụng trò chuyện nhóm, video call. Đây là một sự kết nối vui vẻ, nhưng đôi khi điều đó cũng mang lại nhiều rủi ro trong việc đảm bảo an toàn thông tin mà chúng ta không để ý hoặc có cảnh giác cao độ. Vì vậy, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) khuyến nghị một số hướng dẫn để giữ an toàn sau đây.

3.1. An toàn khi sử dụng các phần mềm video conference (Zoom, Microsoft Team,…)

Dịch Covid đem lại thách thức lớn cho toàn bộ xã hội. Một trong những thử thách đó là làm sao giúp mọi người làm việc từ xa và kết nối với nhau một cách hiệu quả. Các công cụ giúp liên lạc và họp video call đang nổi lên trở thành phương thức quan trọng trong việc giúp vận hành giữa người dùng, các tổ chức và doanh nghiệp. Tuy nhiên, cùng với đó, dấy lên một số nghi ngại về tính bảo mật và đảm bảo tính riêng tư trong thông tin liên lạc dựa trên nền tảng video call. Dưới đây là một số phương pháp để đảm bảo an toàn và bảo mật khi sử dụng các phần mềm video conference:

Cẩn thận khi chia sẻ ID cuộc họp: Mặc dù bạn có thể muốn càng nhiều người tham gia càng tốt cho cuộc họp hoặc sự kiện trực tiếp của mình, việc hiển thị ID cuộc họp trên phương tiện truyền thông xã hội, trang web hoặc các diễn đàng công khai khác có thể thu hút những người tham gia có mục đích xấu.

Nắm rõ thông tin chính sách bảo mật dữ liệu của nhà cung cấp ứng dụng mà bạn sử dụng: vì có những nhà cung cấp chia sẻ một số mức độ dữ liệu với các bên thứ ba.

Theo dõi và kiểm tra những người tham gia cuộc họp: Người tổ chức cuộc họp có khả năng theo dõi những ai tham gia cuộc họp theo nhiều cách khác nhau, tùy thuộc vào hệ thống đang sử dụng. Hầu hết cho phép người tổ chức đặt cảnh báo âm thanh để thông báo khi những người tham gia mới tham gia. Người chủ trì cũng nên xem danh sách thành viên để xác minh những ai tham gia. Nếu những cái tên không được công nhận hoặc ẩn danh có trong danh sách, người chủ trì nên yêu cầu họ xác nhận danh tính của mình bằng giọng nói hoặc trò chuyện.

Làm chủ các tính năng điều khiển cuộc họp: Để ngăn chặn những người tham gia không mong muốn, hãy đảm bảo hệ thống bạn đang sử dụng cho phép máy chủ loại một người tham gia và ngăn họ tham gia lại. Một số hệ thống cũng cho phép bạn khóa cuộc họp khi tất cả các cá nhân được yêu cầu đều có mặt.

Hầu hết các hệ thống cho phép máy chủ tắt âm thanh và video call của một số hoặc tất cả người tham gia và đặt cuộc họp ở chế độ chỉ dành cho máy chủ. Điều này giúp giữ cho nhóm tập trung và ngăn chặn sự gián đoạn, kể cả từ những vị khách không mong muốn.

Hãy lưu ý rằng một số nền tảng cho phép truyền tệp có thể là đường dẫn cho việc chia sẻ phần mềm độc hại. Ít nhất, hãy đảm bảo rằng người tổ chức cuộc họp có thể tắt tính năng truyền tệp để ngăn phần mềm độc hại được chia sẻ.

Sử dụng các tính năng nâng cao trong cuộc họp trực tiếp cho các cuộc họp và sự kiện lớn: Khi công ty cần tổ chức các cuộc họp hoặc sự kiện lớn với hơn 25 người, nên đầu tư vào hệ thống có khả năng và tính năng bảo mật phù hợp.

Nâng cao nhận thức bảo đảm an toàn thông tin cơ bản: Nếu bạn nhận được một liên kết qua email hoặc các kênh xã hội để tham gia video conference, hãy liên hệ với người gửi để xác nhận tính hợp pháp của nó. Không mở các liên kết và tệp đính kèm trong email từ những người gửi không xác định. Một số cách nhận biết ban đầu là đường dẫn có lỗi chính tả.

Một số hướng dẫn thiết lập bảo mật nâng cao trong các phần mềm video conference phổ biến Zoom và Microsoft Team **có tại chuyên đề 2** trong tài liệu này.

3.2. An toàn khi kết nối video call, chat qua các ứng dụng trực tuyến (Zalo, Facebook, Viber, Skype,…)

- Chỉ chấp nhận các yêu cầu trò chuyện từ những người bạn biết
- Giữ thông tin cá nhân của bạn ở chế độ riêng tư. Chọn cài đặt riêng tư trên tất cả các ứng dụng trò chuyện và chỉ chia sẻ nội dung cá nhân với những người bạn biết.
- Hãy cẩn thận với những gì bạn trò chuyện. Không chia sẻ nội dung cá nhân như số điện thoại, nơi bạn đi học/làm hoặc nơi bạn sống.
- Hãy thực sự cẩn thận với bất kỳ ảnh hoặc video nào bạn chia sẻ, đặc biệt nếu chúng khiến bạn xấu hổ. Nếu bạn không muốn người quen của mình nhìn thấy nó thì đừng chia sẻ
- Nếu ai đó gây áp lực buộc bạn phải làm bất cứ điều gì bạn không muốn làm hoặc cảm thấy không thoải mái, bạn có thể nói không. Hãy dừng cuộc trò chuyện lại và nói chuyện với người quen của bạn. Bạn sẽ không gặp rắc rối và họ sẽ có thể giúp đỡ.

- Nếu bạn thấy video hoặc hình ảnh trong cuộc trò chuyện của mình gây nhầm lẫn hoặc đáng sợ, hãy dừng cuộc trò chuyện lại và nói chuyện với người quen của bạn.

Một số hướng dẫn thiết lập bảo mật nâng cao trong các ứng dụng trực tuyến (Zalo, Facebook) tham khảo **tại chuyên đề 4** trong tài liệu này.

Ngoài ra, người dùng nên chú ý nâng cao bảo mật bằng cách sử dụng mật khẩu mạnh **(tham khảo các hướng dẫn tại chuyên đề 1)**.

3.3. Sử dụng an toàn mạng không dây

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

Nếu mạng không dây không được bảo vệ đúng mức thì bất cứ một máy tính nào có hỗ trợ truy cập không dây đều có thể kết nối để truy cập Internet.

3.3.1. Các nguy cơ

Bị xâm phạm dịch vụ: dung lượng, số lượng kết nối…có thể vượt quá giới hạn mà nhà cung cấp dịch vụ cho phép, tốc độ có thể rất chậm do bị chiếm dụng băng thông.

Bị lợi dụng: một số người có thể lợi dụng hệ thống để thực hiện những hành động bất hợp pháp.

Bị theo dõi: các hoạt động trên Internet có thể bị theo dõi, những thông tin nhạy cảm (mật khẩu, số thẻ tín dụng có thể bị đánh cắp).

Bị tấn công: các tệp tin trên máy tính có thể bị truy cập trái phép, máy tính có thể bị cài đặt virus và các chương trình độc hại khác.

3.3.2. Các phương pháp thiết lập mạng không dây an toàn

Do chi phí triển khai các mạng không dây nhỏ tại gia đình, khu vực nhỏ, nên các biện pháp bảo đảm an toàn thông tin là một vấn đề không được lưu tâm đầu tư. Người dùng có thể áp dụng một số biện pháp để giảm thiểu rủi ro mất an toàn thông tin bao gồm:

- Cập nhật phần mềm, firmware cho các thiết bị truy cập và các điểm truy nhập với phiên bản mới nhất do nhà sản xuất cung cấp.

- Kích hoạt các phương thức mã hóa WEP/WPA/WPA2 theo thứ tự ưu tiên sử dụng WPA2, WPA nếu thiết bị hỗ trơ.

- Thay đổi tên mạng không dây (Service Set Identifier – SSID) mặc định do các nhà sản xuất cài đặt sẵn. Không sử dụng các tên gọi có gợi ý như tên đường phố hay địa chỉ, công ty, nhà riêng hay họ tên các thành viên trong gia đình, cơ quan, văn phòng. Có thể lựa chọn thêm tính năng "ẩn" tên mạng không dây để các thiết bị thu nhận không nhìn thấy các tên mạng.

- Không kích hoạt chức năng quảng bá SSID. Để thực hiện tính năng này, cần đảm bảo người dùng hợp pháp đã lưu trữ thông tin SSID trên thiết bị.

- Lọc địa chỉ MAC (Media Access Control): Một vài điểm truy cập có khả năng chấp nhận các kết nối chỉ đối với các địa chỉ MAC đáng tin cậy là các địa chỉ duy nhất trên mạng (không trùng khớp nhau). Thực hiện điều này là rất khó khăn trong một môi trường với hơn 20 người dùng do việc thiết lập điểm truy cập bằng tay rất mất thời gian. Tuy nhiên, nó có thể được thiết lập một cách đơn giản trong môi trường nhà ở và văn phòng nhỏ.

CHUYÊN ĐỀ 4: GIẢI TRÍ AN TOÀN

Trong thời đại 4.0, Mạng xã hội là một trong các tiện ích đem lại các trải nghiệm dành cho người dùng. Mạng xã hội (Facebook, Zalo,…), các trang mạng mua bán, giải trí, thanh toán hoặc các trang tin tức xuất hiện ở mọi lúc mọi nơi và trở thành thói quen hàng ngày. Cùng với những lợi ích to lớn, các đe dọa từ không gian mạng cũng hiện hữu song song, do vậy người dùng cần hiểu và có các giải pháp nhằm đảm bảo an toàn khi tham gia không gian mạng.

Phần này đưa ra các hướng dẫn cơ bản nhằm đảm bảo an toàn thông tin đối với người dùng trong các hoạt động giải trí trực tuyến.

4.1. Sử dụng mạng xã hội an toàn

Các trang Mạng xã hội đang ngày càng phổ biến như là công cụ gián tiếp để khai thác thông tin vì lượng người dùng lớn, lượng thông tin cá nhân được đăng tải. Bản chất của các trang mạng xã hội là khuyến khích người dùng đăng thông tin cá nhân.

Bảo mật và quyền riêng tư liên quan đến các trang Mạng xã hội về cơ bản là vấn đề hành vi, không phải vấn đề công nghệ. Một người càng đăng nhiều thông tin, thì càng có nhiều thông tin tiềm ẩn nguy cơ bị xâm phạm bởi những kẻ có ý đồ xấu. Những người cung cấp thông tin riêng tư, nhạy cảm hoặc bí mật về bản thân hoặc người khác, dù vô tình hay cố ý, đều có nguy cơ cao bị tấn công. Thông tin như số an sinh xã hội, địa chỉ đường phố, số điện thoại, thông tin tài chính hoặc thông tin kinh doanh bí mật của một người không nên cung cấp trực tuyến. Tương tự, việc đăng ảnh, video hoặc tệp âm thanh có thể dẫn đến vi phạm bí mật của tổ chức hoặc vi phạm quyền riêng tư của một cá nhân. Điều quan trọng là người dùng cần nhận ra và xác định được việc đăng bất kì thông tin gì lên Mạng xã hồi đồng nghĩa với việc có nhiều người biết đến, và có thể có những tác động lâu dài.

Chia sẻ thông tin quá mức:

Khi tạo một tài khoản mới, hầu hết các Mạng xã hội sẽ yêu cầu thông tin cá nhân như địa chỉ nhà, ngày sinh và số điện thoại. Việc cung cấp thông tin này có thể nguy hiểm và sẽ được công khai cho bất kỳ ai truy cập trang hồ sơ của người dùng, đặc biệt nếu thiết lập các tuỳ chọn bảo mật liên quan đến quyền riêng tư.

Xác minh cài đặt tài khoản:

Ngay cả khi các thông tin, bài viết của tài khoản được đặt ở chế độ riêng tư; tài khoản người dùng vẫn có nguy cơ bị tấn công nếu ai đó xâm nhập vào tài khoản, người đó sẽ có thể xem và sử dụng thông tin. Chia sẻ những thứ đơn giản như màu sắc yêu thích của chủ tài khoản có thể khiến đối tượng tấn công thử xem người ấy có sử dụng nó làm mật khẩu trên tài khoản của mình hay không. Mối đe dọa lớn nhất của việc chia sẻ thông tin quá mức là đánh cắp danh tính. Đánh cắp danh tính không phải là hiếm trong thế giới của mạng xã hội trực tuyến. Đặc biệt khi tính năng ẩn danh được cung cấp trực tuyến giúp hacker dễ dàng không bị phát hiện.

Che dấu danh tính:

Các trang mạng xã hội khiến người dùng rất dễ giả mạo là người khác. Ngay cả khi một cá nhân có thể kết bạn với ai đó trên trang web, bất kỳ ai cũng có thể kiểm soát tài khoản của người dùng nếu người đó có thể lấy được mật khẩu của người dùng. Do đó, ai đó là "Bạn bè" có thể yêu cầu tiền hoặc lấy thông tin cá nhân có thể được sử dụng để xâm nhập vào các tài khoản khác. Ví dụ: bạn có thể nhận được tin nhắn từ một người bạn, yêu cầu bạn cung cấp thông tin ngân hàng của bạn vì họ muốn chuyển cho bạn một số tiền nhân ngày sinh nhật của bạn. Bạn có thể nghĩ rằng mình đang nói chuyện với người thân của mình, nhưng thực tế là do hacker đã xâm nhập vào tài khoản của người thân của bạn.

Dịch vụ dựa trên vị trí:

Dịch vụ dựa trên vị trí có thể là một trong những tính năng nguy hiểm nhất do các trang Mạng xã hội cung cấp. Nó tiết lộ vị trí và nơi ở của người dùng. Dịch vụ này cũng có một tính năng cho phép người dùng gắn thẻ họ với ai vào bất kỳ thời điểm nào. Những đối tượng tấn công có thể sử dụng công cụ này để theo dõi hoạt động vị trí của người dùng.

Đăng ảnh:

Một trong những tính năng của Mạng xã hội mà nhiều người sử dụng là tính năng chia sẻ ảnh. Internet giúp dễ dàng lấy ảnh và sử dụng ảnh theo bất kỳ cách nào. Giả mạo ảnh là một mối đe dọa lớn đối với người dùng khi đăng ảnh trực tuyến. Việc sử dụng các công cụ chỉnh sửa ảnh cho phép mọi người thao tác trên hình ảnh trực tuyến theo bất kỳ cách nào họ chọn, cho dù nó được sử dụng cho mục đích tốt hay xấu.

Dưới đây là một số hướng dẫn để thiết lập các tính năng bảo mật cho tài khoản Mạng xã hội.

4.2. Thiết lập các tính năng bảo mật cho tài khoản Mạng xã hội

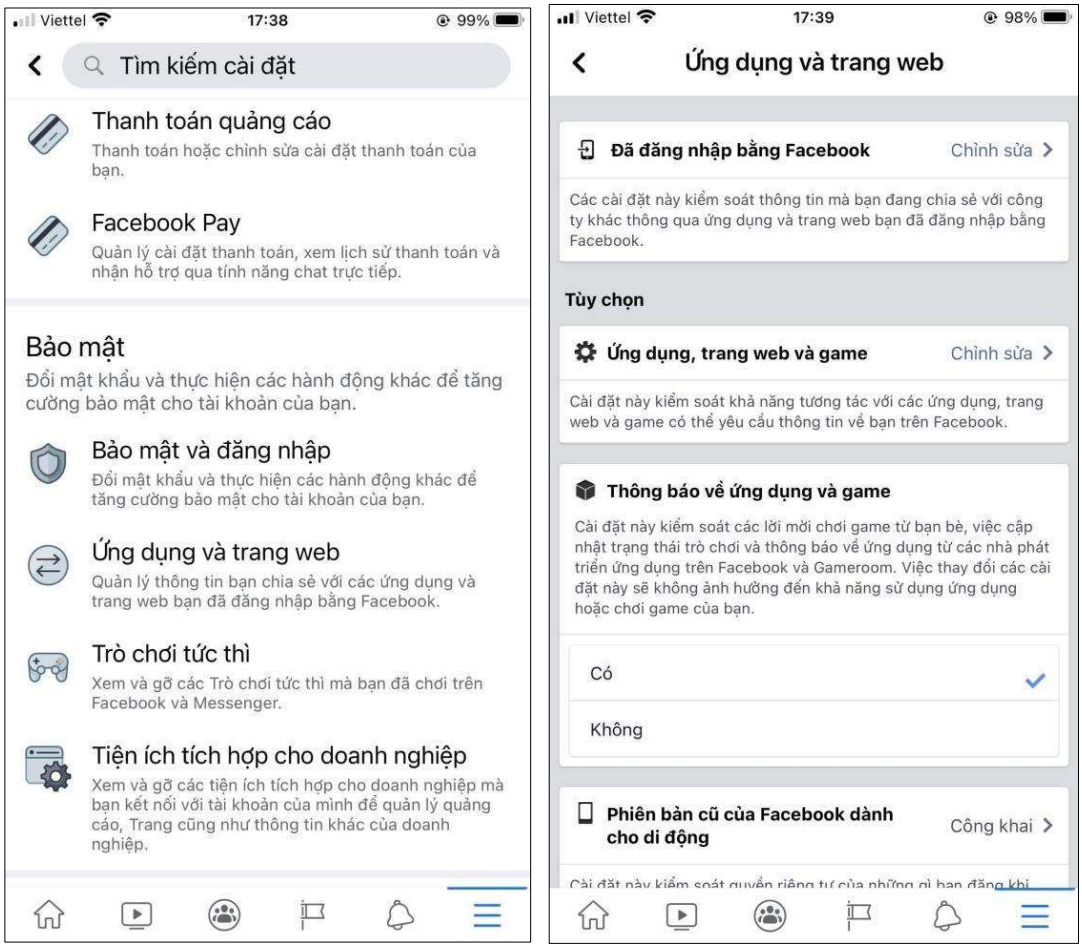
4.2.1. Tài khoản Facebook

4.2.1.1. Cài đặt quyền riêng tư

Đăng nhập vào Facebook, nhấp vào menu "Cài đặt".

•Chọn "Quyền riêng tư" để xem và chỉnh sửa những ai có thể xem ảnh, hoạt động và thông tin của bạn.

•Chọn "Ứng dụng và Trang web" để kiểm soát quyền truy cập vào tài khoản Facebook của bạn bằng các ứng dụng và trang web.



•Chọn "Có" để chặn người dùng cụ thể hoặc lời mời ứng dụng.

4.2.1.1.2. Xóa lịch sử hoạt động Facebook

Facebook liên tục theo dõi hoạt động của người dùng. Các ứng dụng và trang web tự động kiểm tra người dùng có đăng nhập hay không và thu thập thông tin những hoạt động của người dùng đang làm trực tuyến về cho Facebook (dữ liệu này từng là một phần được che giấu kỹ càng trong chiến lược quảng cáo của Facebook).

Chú ý: Việc xóa lịch sử sẽ ngắt kết nối dữ liệu thông tin của người dùng khỏi tài khoản; điều này sẽ ngăn Facebook phát tán quảng cáo đến người dùng. Tuy nhiên nó sẽ không hoàn toàn ngăn nó thu thập các báo cáo phân tích từ các trang web khác.

Công cụ Quản lý hoạt động trong tương lai "**The Manage Future Activity**" hoạt động như 1 phiên bản lâu dài hơn của Clear History. Khi người dùng tắt nó đi, nó sẽ ngăn các doanh nghiệp gửi dữ liệu nhằm mục tiêu quảng cáo của Facebook về người dùng.

Việc tắt "Hoạt động trong tương lai" sẽ ngăn người dùng đăng nhập vào các ứng dụng và trang web khác bằng Facebook.

Nhấp vào mũi tên ở trên cùng bên phải của Facebook và nhấp vào "**Cài đặt & Quyền riêng tư" .**

Chọn "**Cài đặt**". Kéo xuống đến mục "**Thông tin Facebook của bạn**".

Nhấp vào "**Hoạt động bên ngoài Facebook**" để xem lại. Nhấp vào "**Quản lý hoạt động ngoài Facebook".**

Người dùng sẽ được yêu cầu nhập lại mật khẩu của mình. Sau khi được xác minh, màn hình sẽ hiển thị cho người dùng các ứng dụng và trang web đã chia sẻ quảng cáo với tài khoản Facebook.

4.2.1.1.3. Ẩn vị trí của người dùng

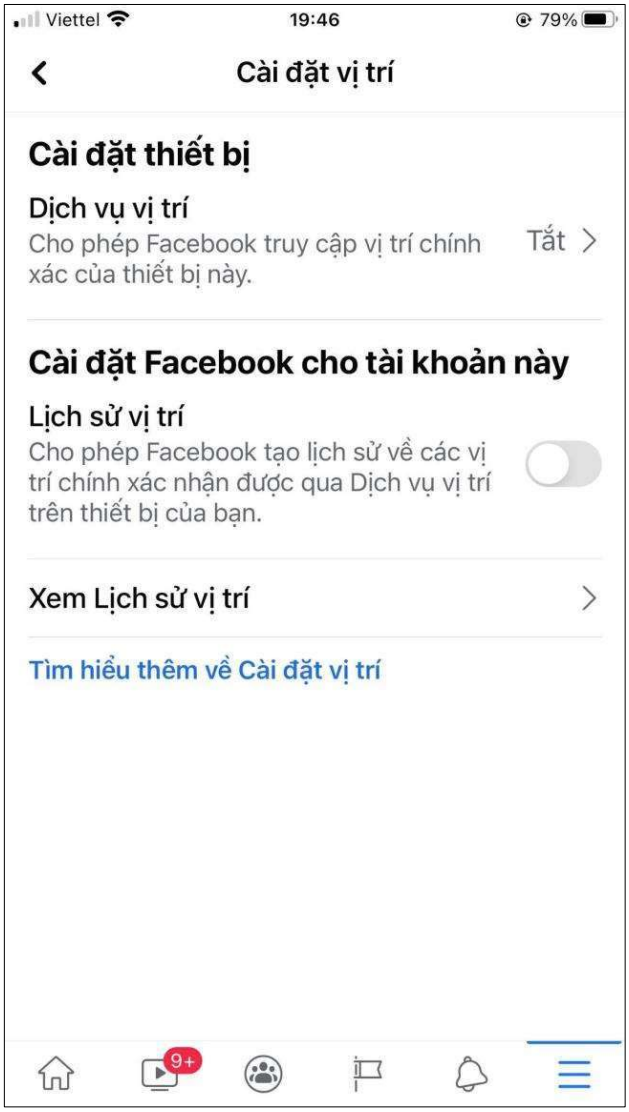
Facebook sử dụng dữ liệu vị trí để cung cấp tin tức cho người dùng hoặc bán những thứ người dùng quan tâm. Nếu tắt dịch vụ vị trí, nó sẽ không thể sử dụng vị trí chính xác của người dùng để nhằm mục tiêu bạn bằng quảng cáo. Thật không may, Facebook vẫn có quyền truy cập vào vị trí mạng của bạn, vì vậy bạn sẽ cần phải tắt tính năng này trên cả điện thoại và ứng dụng của mình.

Để tắt dịch vụ định vị của ứng dụng Facebook trên điện thoại:

Đi tới "Cài đặt" của điện thoại và nhấn vào "Quyền riêng tư".

Nhấn vào "Vị trí". Sẽ xuất hiện màn hình cài đặt vị trí:

Ở đây bạn có thể tắt tính năng "Cho phép Facebook truy cập vị trí chính xác của thiết bị này" và tính năng "Cho phép Facebook tạo lịch sử về các vị trí chính xác nhận được qua Dịch vụ vị trí trên thiết bị của bạn".



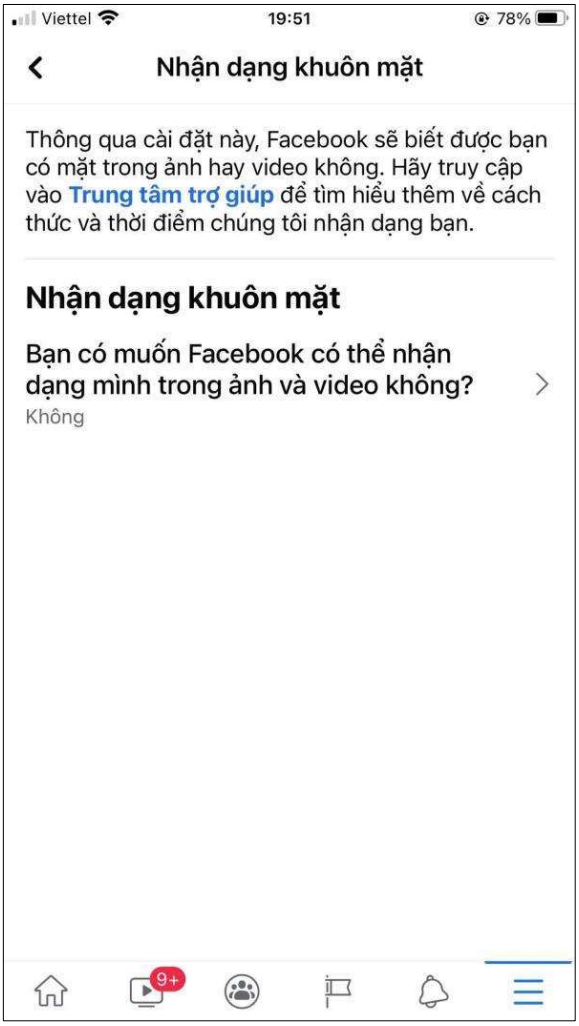
Tắt nhận dạng khuôn mặt:

Nhận dạng khuôn mặt là trung tâm trong thuật toán ảnh của Facebook. Đó là lý do bạn tự động được gắn thẻ trong ảnh mà người khác đăng.

Người dùng có thể tắt tính năng nhận dạng khuôn mặt trên phiên bản Facebook dành cho máy tính để bàn. Làm theo các bước sau:

Nhấp vào mũi tên chỉ xuống ở trên cùng bên phải của màn hình.

Chọn "Cài đặt & Quyền riêng tư", sau đó chọn "Cài đặt" nhấp vào "Nhận dạng khuôn mặt".



Nhấn vào "Bạn có muốn Facebook có thể nhận ra bạn trong ảnh và video không? " Chọn "Không" trong phần "Chỉnh sửa" và đóng để hoàn tất các bước.

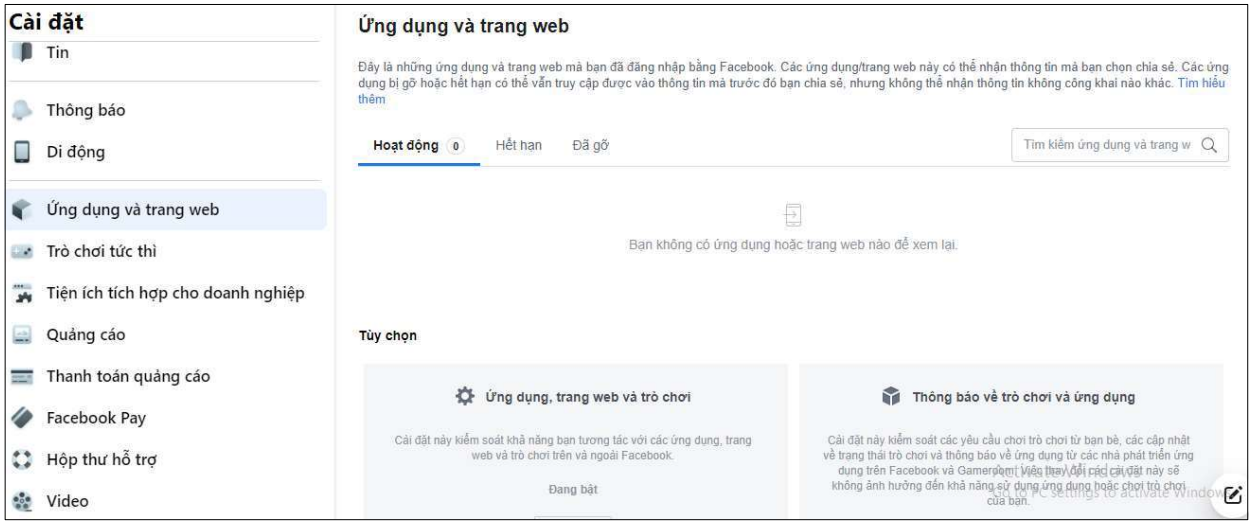
4.2.1.1.4. Loại bỏ các ứng dụng theo dõi khỏi Facebook

Đăng nhập vào các nền tảng hoặc trang web khác bằng tên người dùng Facebook của bạn cung cấp cho các công ty đó quyền truy cập vào dữ liệu cá nhân của bạn và có thể cho phép họ chia sẻ hoạt động của bạn với Facebook.

Tắt theo dõi ứng dụng của bên thứ ba khỏi máy tính:

Nhấp vào mũi tên chỉ xuống ở trên cùng bên phải của màn hình.

Chọn "Cài đặt & Quyền riêng tư", sau đó chọn "Cài đặt". Ở mục Bảo mật nhấn vào "Ứng dụng và Trang web".



Chọn "Hoạt động".

Nhấp vào hộp bên cạnh tên ứng dụng để ngừng theo dõi bạn và nhấp vào "Xóa". Điều này sẽ vô hiệu hóa nó theo dõi bạn.

4.2.1.1.5. Bật xác thực 2 yếu tố (2FA)

Xác thực hai yếu tố là một trong những cách mạnh nhất để bảo mật hồ sơ của bạn khỏi những lần đăng nhập không mong muốn. Khi ai đó cố gắng đột nhập vào tài khoản đã bật 2FA, họ không thể vào mà không có mã xác thực OTP. Vì mã được chuyển đến điện thoại của bạn nên chỉ bạn mới có thể đăng nhập.

Bước 1: Truy cập Facebook.com/settings
Bước 2: Chọn *Security and Login* (Bảo mật và đăng nhập)

Bước 3: Chọn *Two-factor authentication* (Xác thực 2 yếu tố) → Chọn *Edit* (Chỉnh sửa) → Nhập lại mật khẩu

Bước 4: Chọn *Use authentication app* (Dùng ứng dụng xác thực)

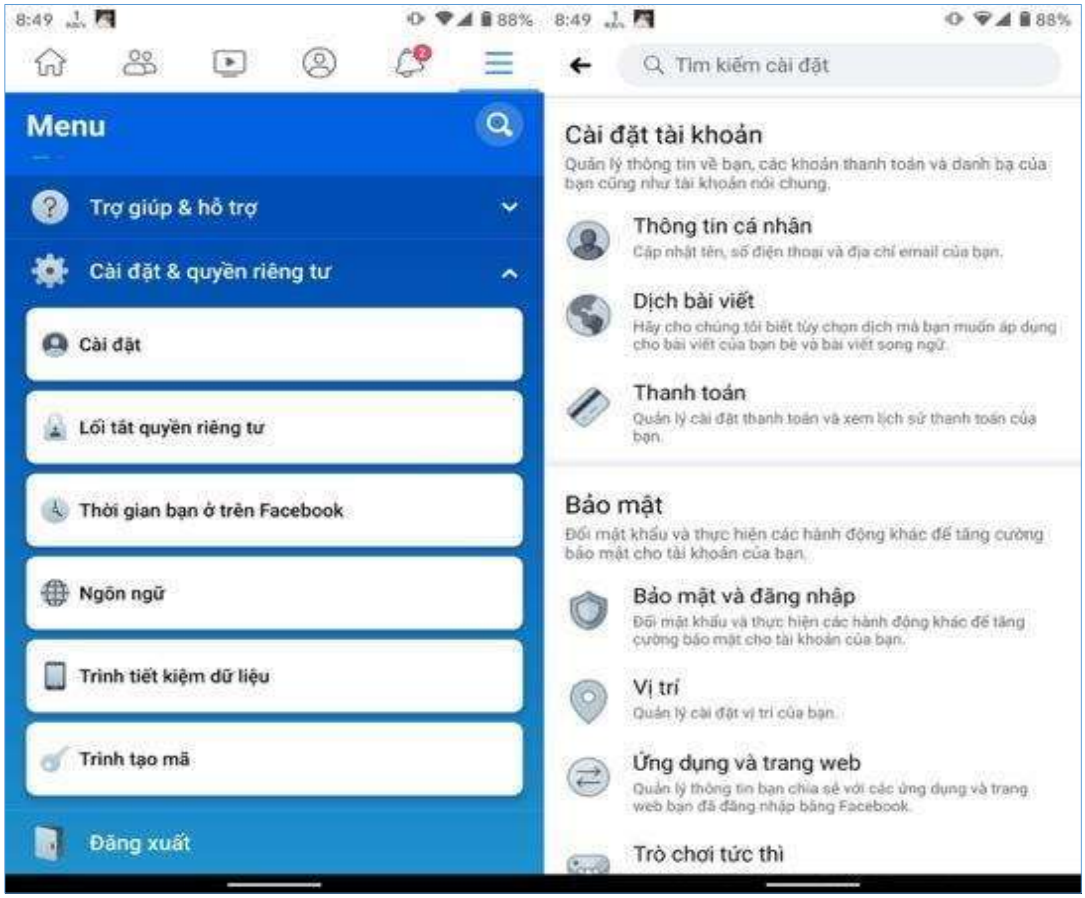
Bước 5: Tải ứng dụng xác thực của bên Thứ 3 (Google Authenticator, Microsoft Authenticator, LastPass Authenticator,…) trên điện thoại.

Bước 6: Hoàn tất cài đặt ứng dụng xác thực, mở và quét mã QR hoặc nhập mã hiển thị trên màn hình, bấm *Continue* (Tiếp tục).

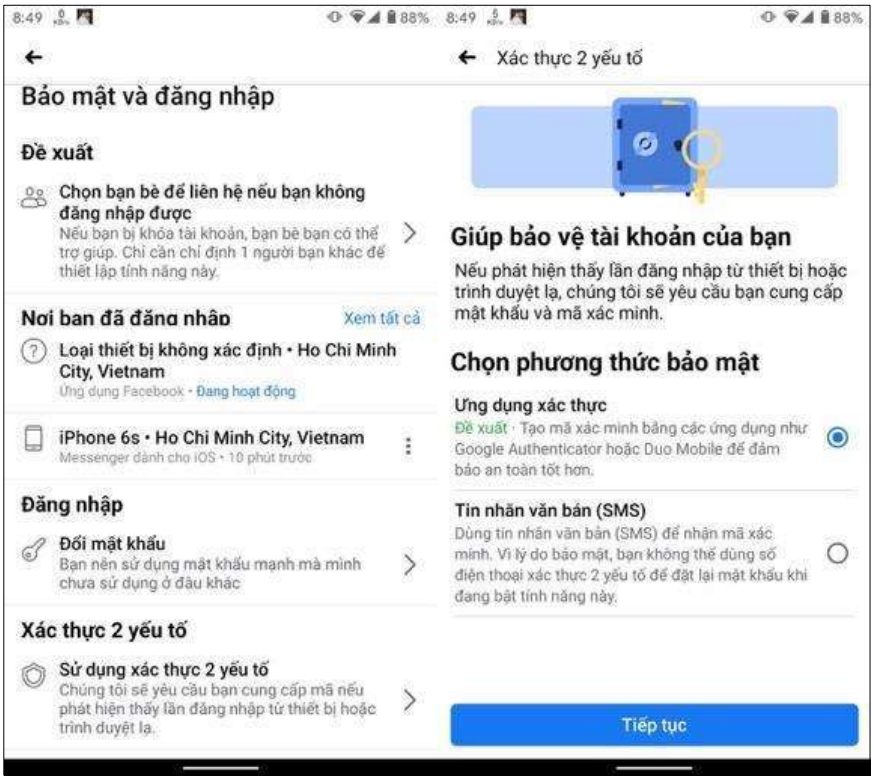
Bước 7: Nhập mã xác minh từ ứng dụng xác thực trên điện thoại vào hộp *Two-factor authentication* (Xác thực 2 yếu tố) → Bấm nút *Continue* (Tiếp tục).

Đối với ứng dụng Facebook trên điện thoại:

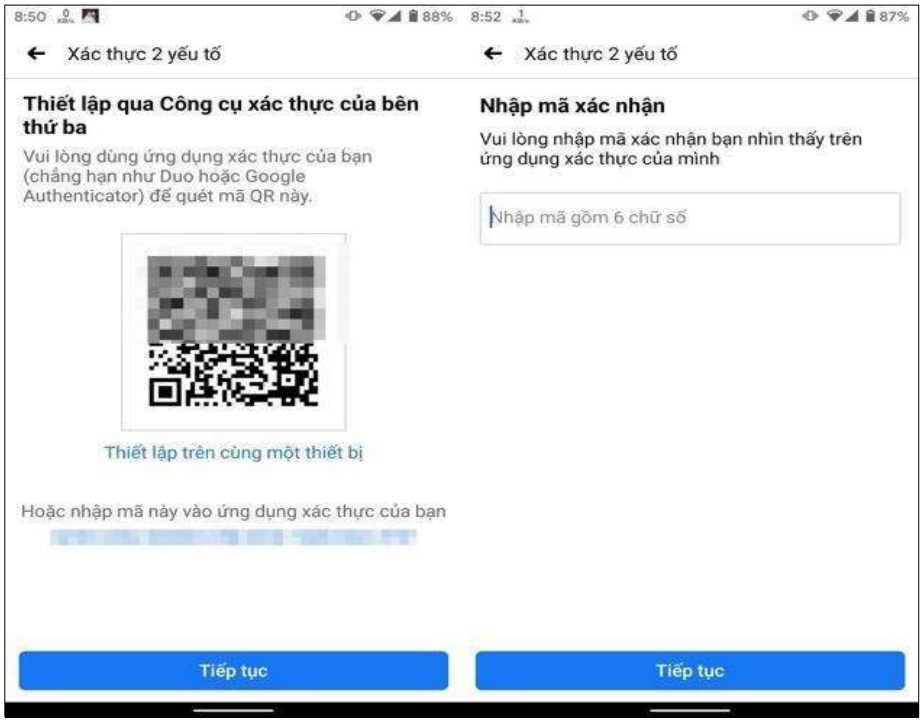
Bước 1: Bấm hình ba thanh ngang phía trên góc phải của ứng dụng
Bước 2: Chọn *Setting and Privacy* (Cài đặt & quyền riêng tư)
Bước 3: Chọn *Setting* (Cài đặt)
Bước 4: Chọn *Security and Login* (Bảo mật và đăng nhập).



Bước 5: Chọn *Use two-factor authentication* (Sử dụng xác thực hai yếu tố)

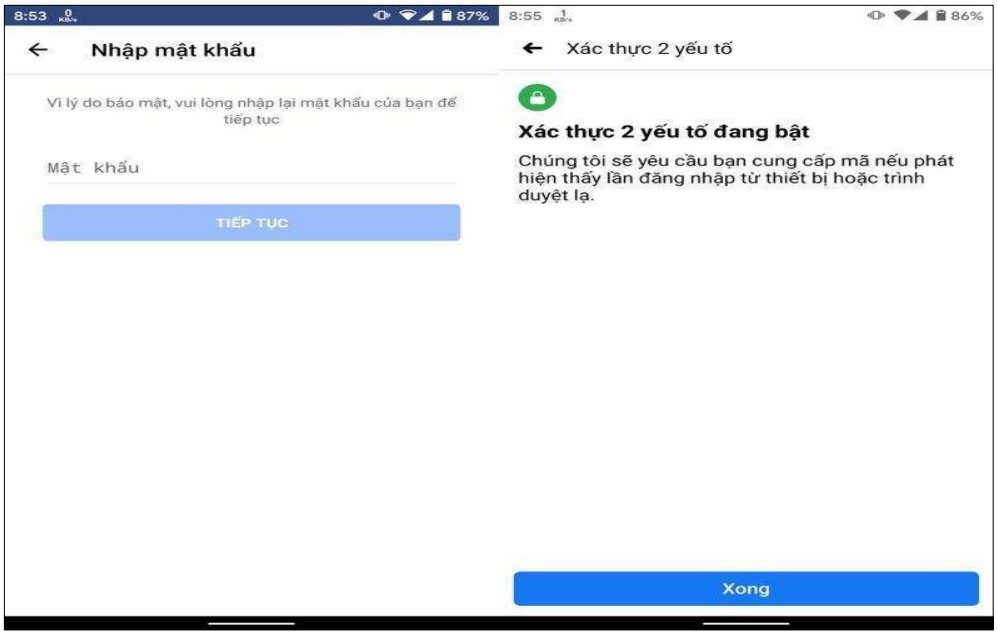


Bước 6: Chọn *Authentication App* (Ứng dụng xác thực) trong phần *Security methods* (Phương thức xác thực) → Bấm *Next* (Tiếp tục)



Bước 7: Tải ứng dụng xác thực của bên Thứ 3 (Google Authenticator, Microsoft Authenticator, LastPass Authenticator,…) trên điện thoại.

Bước 8: Nhập mã xác minh từ ứng dụng xác thực trên điện thoại vào hộp thoại *Two-factor authentication* (Xác thực 2 yếu tố) → Bấm nút *Continue* (Tiếp tục).



Bước 9: Nhập lại mật khẩu Facebook để xác minh

Bước 10: Nhập lại mật khẩu Facebook để xác minh

Bước 11: Hiện thông báo *Two-factor authentication is ON* (Xác thực 2 yếu tố đang bật) → Bấm nút *Done* (Xong).

4.2.1.1.6. Ngăn thông tin tài khoản Facebook hiển thị trên các công cụ tìm kiếm

Bạn có biết hồ sơ Facebook được lập chỉ mục trên Google? Điều đó có nghĩa là bất kỳ ai đang tìm kiếm tên của bạn sẽ có thể tìm thấy tài khoản mạng xã hội của bạn, cùng với tất cả dữ liệu hiển thị công khai.

Google và các công cụ tìm kiếm mọi người có một cách khó chịu để công khai cuộc sống riêng tư của người dùng.

Với Facebook, ít nhất, người dùng có thể giữ cho hồ sơ của mình không bị tìm kiếm. Làm theo các bước sau:

Trên máy tính, hãy mở Facebook và nhấp vào mũi tên chỉ xuống ở trên cùng bên phải màn hình.

Nhấn vào "Cài đặt & Quyền riêng tư", sau đó nhấn "Cài đặt", sau đó là "Quyền riêng tư".

Trong phần "Bạn có muốn các công cụ tìm kiếm bên ngoài Facebook liên kết đến hồ sơ của bạn không? " Nhấp vào Chỉnh sửa.

Nhấp vào hộp kiểm ở dưới cùng để tắt cài đặt.

4.2.1.1.7. Giới hạn đối tượng cho các bài đăng cá nhân

Không phải mọi người bạn trong danh sách của bạn đều cần biết những thông tin chi tiết về cuộc sống của bạn. Điều này thậm chí còn rủi ro hơn khi bạn tính đến số lượng hồ sơ giả đang trôi nổi.

Từ máy tính, hãy làm theo các bước sau:

Mở lại "Cài đặt & Quyền riêng tư", sau đó chọn "Cài đặt" và nhấp vào "Quyền riêng tư".

Chọn "Ai có thể xem các bài đăng trong tương lai của bạn?" và nhấp vào "Chỉnh sửa". Bạn có thể điều chỉnh cài đặt cho các đối tượng cụ thể trong đó.

Chọn "Giới hạn bài đăng trước đây" để thay đổi người có thể truy cập nội dung trước đó của bạn.

Mọi người vô tình chia sẻ tất cả các loại sự kiện và thông tin cá nhân mà không nhận ra nó. Thay đổi cài đặt này có thể bảo vệ bạn khỏi bị lừa đảo hoặc ngăn tin tặc đoán chính xác một trong các câu hỏi bảo mật của bạn.

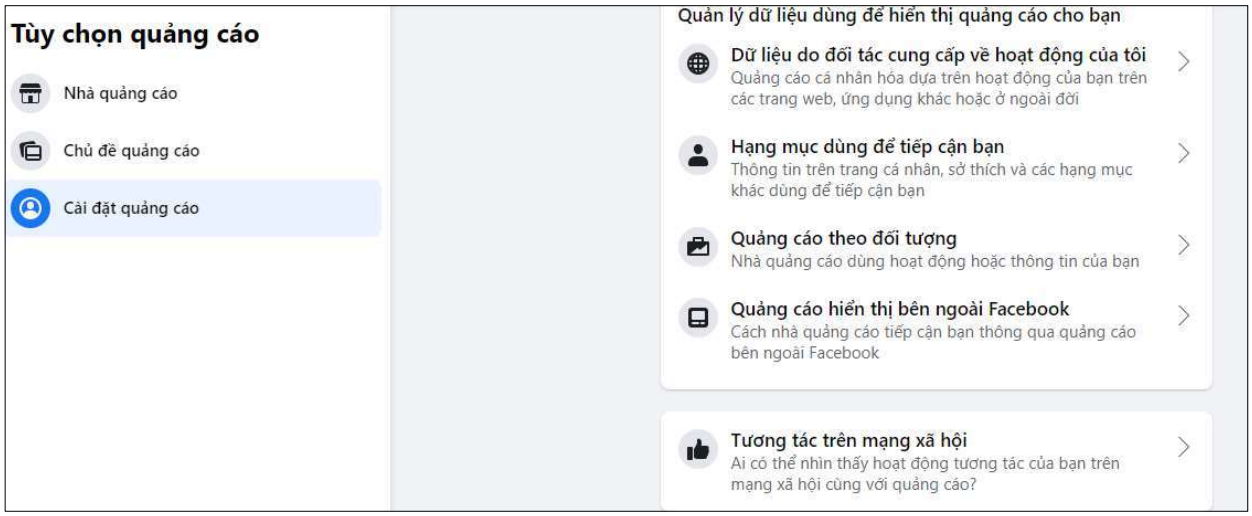
4.2.1.1.8. Ngừng hoạt động của bạn không được quảng cáo

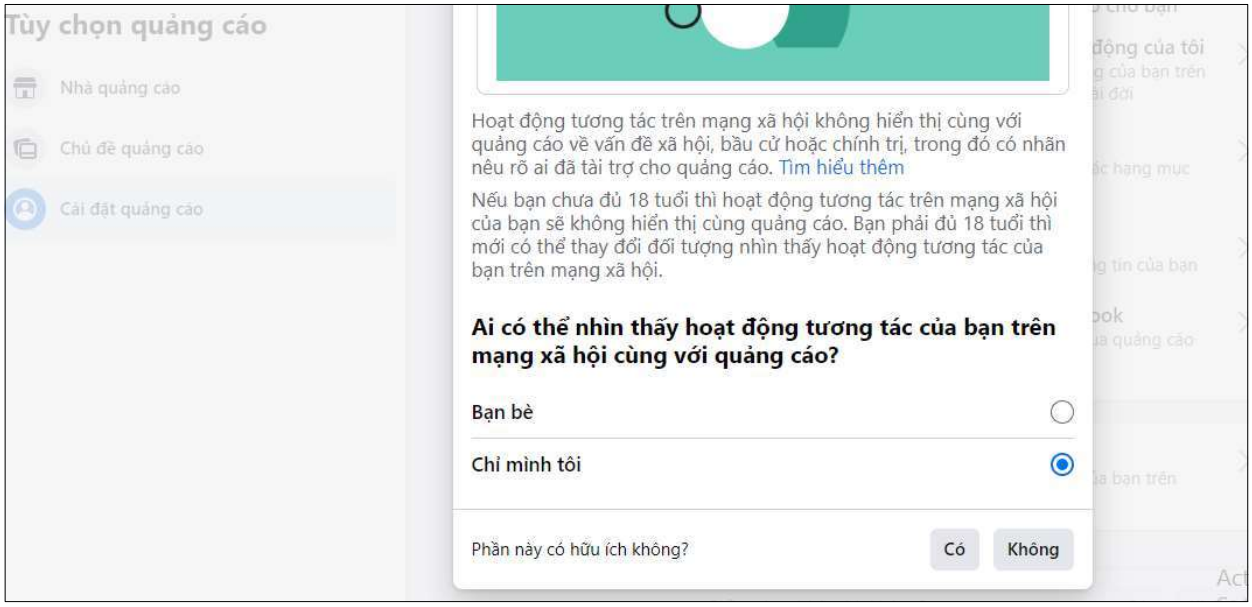
Bạn đã bao giờ nhìn thấy một quảng cáo cho bạn biết ai trong số bạn bè của bạn Thích nó chưa? Đó là bởi vì Facebook tự động sử dụng những xác nhận này để nhắm mục tiêu quảng cáo đến bạn và bạn bè của bạn. Và nếu bạn Thích thứ gì đó, bạn bè của bạn sẽ thấy những loại quảng cáo tương tự.

Tất nhiên, họ không xin phép bạn. Tuy nhiên, bạn có thể tắt cài đặt này để giữ các sở thích và Lượt thích của mình riêng tư hơn. Làm theo các bước sau trên màn hình của bạn:

Trong "Cài đặt & Bảo mật", hãy chọn "Cài đặt", sau đó nhấp vào "Quảng cáo", tiếp theo là "Cài đặt Quảng cáo".

Nhấp vào "Tương tác xã hội" và chọn "Chỉ mình tôi".





4.2.1.1.9. Tránh các nút Like và Share

Bất cứ khi nào bạn sử dụng nút Facebook trên một trang web khác, bạn đang nuôi con quái vật là cỗ máy quảng cáo của Facebook. Mọi Chia sẻ, Thích và đề xuất, đều trở thành một phần của nguồn cấp dữ liệu mà Facebook sử dụng để điều chỉnh thuật toán của mình.

Ngay cả khi bạn đã tắt theo dõi bên ngoài Facebook, việc sử dụng các nút này giống như cho phép nó biết bạn đang làm gì. Bạn không cần phải thay đổi bất kỳ cài đặt nào để tránh những cạm bẫy của các nút này. Chỉ cần không sử dụng chúng.

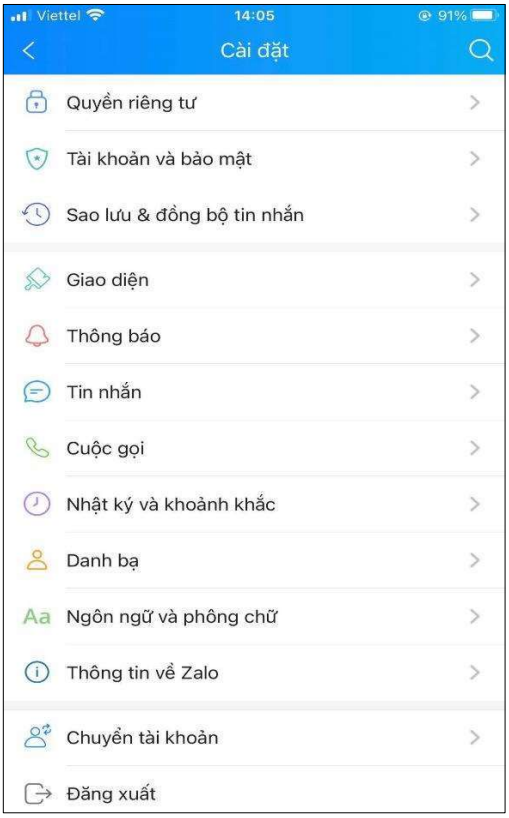
Nếu bạn phải chia sẻ điều gì đó, hãy làm theo cách cũ bằng cách sao chép và dán nó vào một bài đăng.

4.2.2. Tài khoản Zalo

4.2.2.1. Tạo mã pin bảo mật

Khi người dùng thiết lập mã khóa này, không ai có thể truy cập vào tài khoản của bạn để xem danh sách bạn bè, tin nhắn trừ khi biết mã khóa đã đặt.

Trong giao diện nhận chọn vào biểu tượng 4 ô vuông nhỏ ở góc bên dưới màn hình, rồi nhấn tiếp vào biểu tượng bánh răng cưa. Sau đó nhấn tiếp vào mục thiết lập "Tài khoản và bảo mật".



Chọn "Đặt mã khóa Zalo" để tiến hành đặt mật khẩu. Tại giao diện khóa Zalo trước hết cần kích hoạt tính năng tạo mã pin bằng cách gạt thanh ngang sang phải tại "Đặt mã khóa".

Xuất hiện màn hình tạo mã khóa Zalo. Mã khóa sẽ có 4 ký tự, nhận các ký tự để thiết lập sau đó nhập lại chính xác 4 ký tự của mã khóa đã nhận để xác nhận lại.

Lưu ý: Hãy chọn dãy mã khóa mà bạn có thể nhớ vì nếu quên mã khóa buộc phải gỡ ứng dụng và cài đặt lại. Như vậy toàn bộ dữ liệu, tin nhắn Zalo sẽ đều bị xóa sách.

Để thiết lập thời gian hoạt động tự động khóa ứng dụng Zalo, truy cập vào mục "Tự động khóa". Xuất hiện các mốc thời gian để bạn lựa chọn. Tối thiểu sẽ tự động khóa trong 5 giây hoặc tối đa là 30 giây.

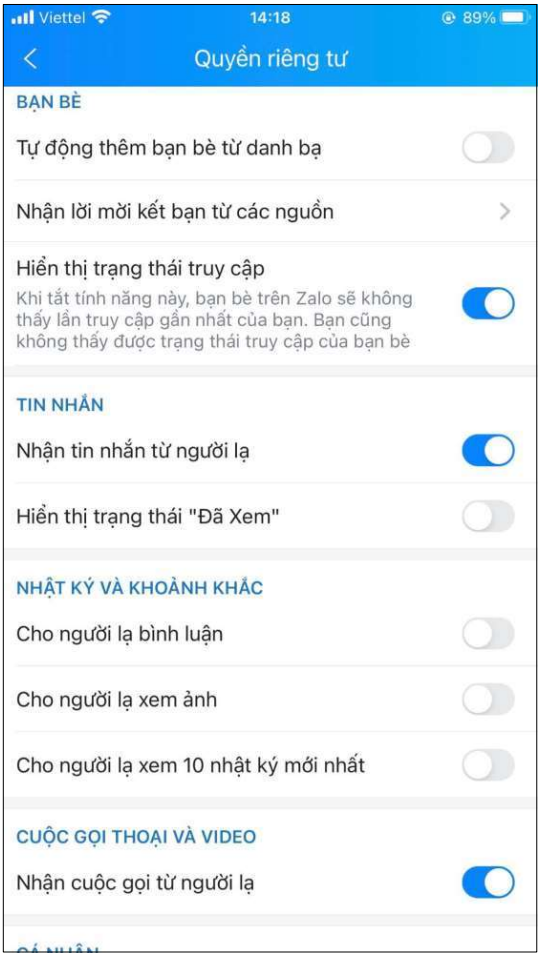
4.2.2.2. Thiết lập quyền riêng tư Zalo

Trên Zalo cũng có chế độ chặn người lạ bình luận, xem thông tin cá nhân, hình ảnh của chúng ta. Tại giao diện cá nhân trên Zalo, chọn vào hình bánh răng cưa, nhấn vào biểu tượng ổ khóa (Quyền riêng tư). Tại giao diện "Thiếp lập quyền riêng tư", kéo xuống dưới và chuyển sang chế độ Tắt của những tùy chọn sau:

Nhận tin nhắn từ người lạ: Tắt chế độ này để người lạ không thể gửi tin nhắn tới bạn

Cho người lạ bình luận: Tắt để chặn người lạ bình luận trên nhật ký của bạn.

Cho người lạ xem ảnh: Người lạ không thể xem hình ảnh của bạn.



Ngoài ra, chúng ta cũng có thể ẩn ngày sinh trên Zalo, hoặc hiện ngày sinh, tháng sinh hay năm sinh tùy chọn. Bạn kéo xuống dưới và nhấn vào mục "Hiển thị ngày sinh", sau đó lựa chọn "Không hiển thị với người khác", kể cả với bạn bè và người lạ đều không thể biết ngày sinh.

4.2.2.3. Tắt thông báo đã xem tin nhắn

Có thể vì lý do nào đó mà sau khi đã xem tin nhắn nhưng bạn không thể trả lời ngay được, hoặc không muốn trả lời. Tuy nhiên, mặc định Zalo sẽ có thông báo Đã xem tới người gửi khi người nhận đã đọc được tin nhắn.

Trước hết tại giao diện của Zalo, nhấn chọn vào biểu tượng bánh răng cưa. Sau đó, trong giao diện "Cài đặt" nhấn chọn mục "Quyền riêng tư". Tiếp theo, bạn chỉ cần tắt tùy chỉnh "Hiển thị trạng thái Đã xem".

4.2.2.4. Chặn bạn bè xem nhật ký

Khi bạn chia sẻ thông tin nào đó trên Zalo, tất cả bạn bè của chúng ta đều có thể đọc được nội dung đó. Nhưng đôi khi bạn lại không muốn một người bạn nào đó

của mình có thể đọc được nội dung đó, thì có thể sử dụng tính năng Chặn xem nhật ký trên Zalo.

Để thực hiện, tìm tới trang cá nhân bạn bè trên Zalo muốn chặn, nhấn vào biểu tượng 3 dấu gạch ngang ở bên phải và Bật chế độ "Chặn xem nhật ký". Bên cạnh đó, cũng có thể bật chế độ "Ẩn nhật ký người này" nếu muốn.

4.2.2.5. Thiết lập quyền xem khi đăng nhật ký

Cũng giống như việc thiết lập quyền riêng tư cho status trên Facebook, người dùng Zalo hoàn toàn có thể điều chỉnh quyền xem trước khi chia sẻ lên nhật ký Zalo.

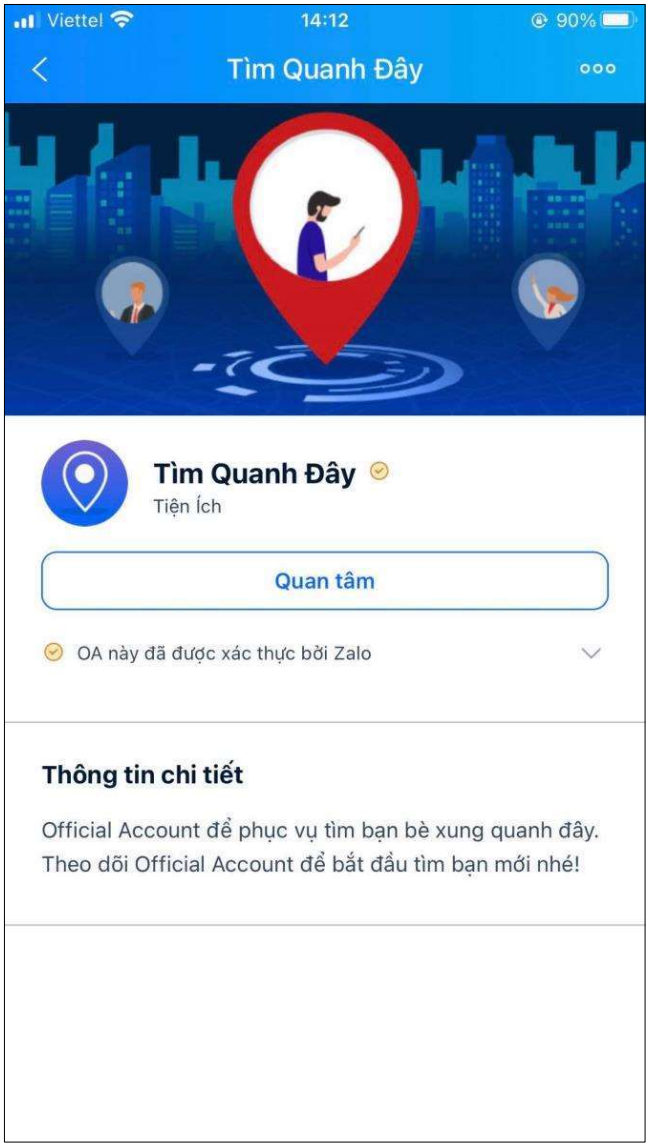
Trước hết, tại giao diện nhật ký cá nhân Zalo, nhấn vào mục "Bạn đang nghĩ gì". Tiếp đến tại mục "Quyền xem", nhấn chọn vào hình tam giác màu đen. Mặc định Zalo sẽ để chế độ Công khai cho mọi bài viết. Chúng ta có thể điều chỉnh sang Mình tôi, Bạn bè tôi hoặc chọn Bạn bè trong nhóm để xem được nhật ký mới đăng.

Còn với những nhật ký đã đăng lên Zalo, cũng có thể điều chỉnh lại quyền xem. Tại bài viết đã đăng, nhấn vào biểu tượng 3 dấu chấm. Tiếp tục nhấn chọn "Thiếp lập quyền xem" và điều chỉnh lại quyền xem cho bài viết này.

4.2.2.6. Xóa vị trí trên Zalo

Khi người dùng Zalo sử dụng tính năng "Tìm quanh đây", bạn bè của bạn hoặc người lạ có thể tìm kiếm chúng ta thông qua vị trí đó. Tuy nhiên, tính năng này đôi khi cũng gây phiền phức, nên nếu không thật sự cần thiết hãy tắt vị trí.

Nhấn tìm "tìm quanh đây" trên thanh tìm kiếm, chọn "Quan tâm" và nhấn vào bắt đầu ngay (đối với người mới bắt đầu sử dụng tính năng này)

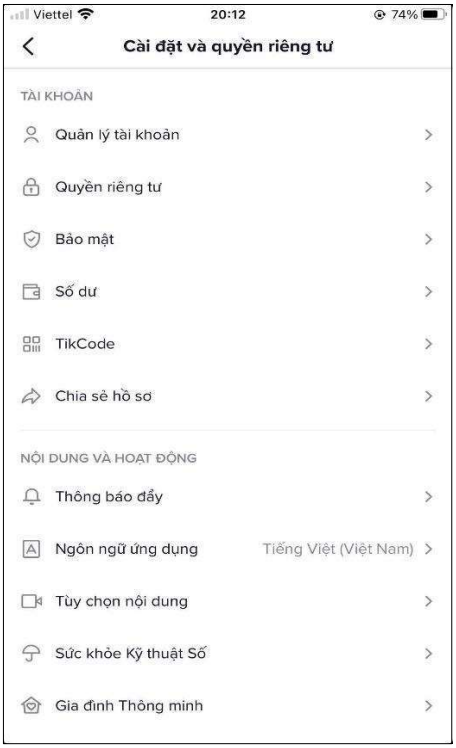


Tại vị trí màn hình, chọn vào mục "Tìm bạn", bấm vào mũi tên, chọn "xóa vị trí để tránh làm phiền".

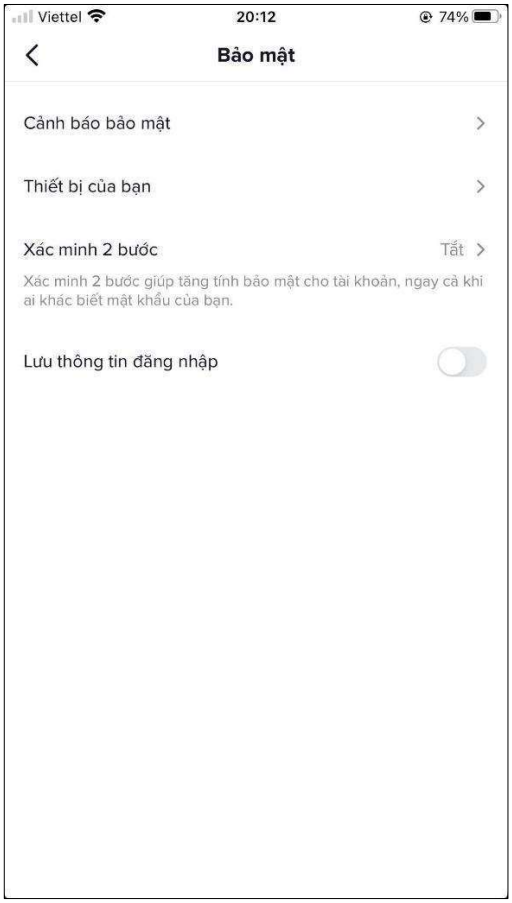
4.2.3. Ứng dụng TikTok

Ngăn TikTok lưu thông tin đăng nhập

Bước 1: Truy cập *biểu tượng người dùng* → Chọn *dấu 3 chấm*

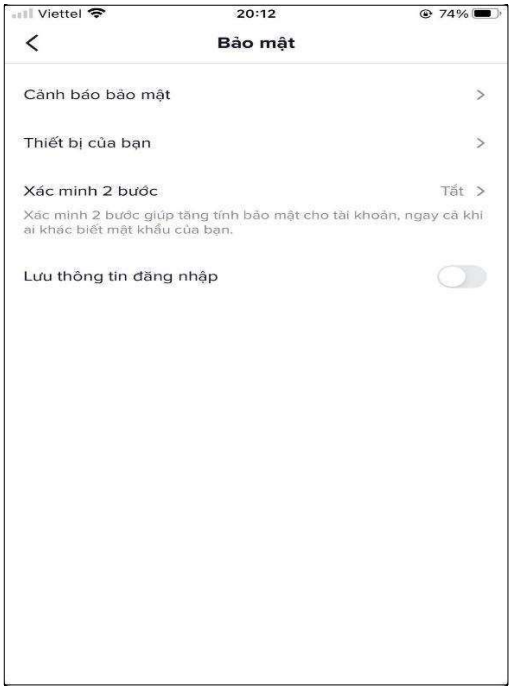


Bước 2: Chọn *Bảo mật* → Hủy kích hoạt cài đặt "*Lưu thông tin đăng nhập*"

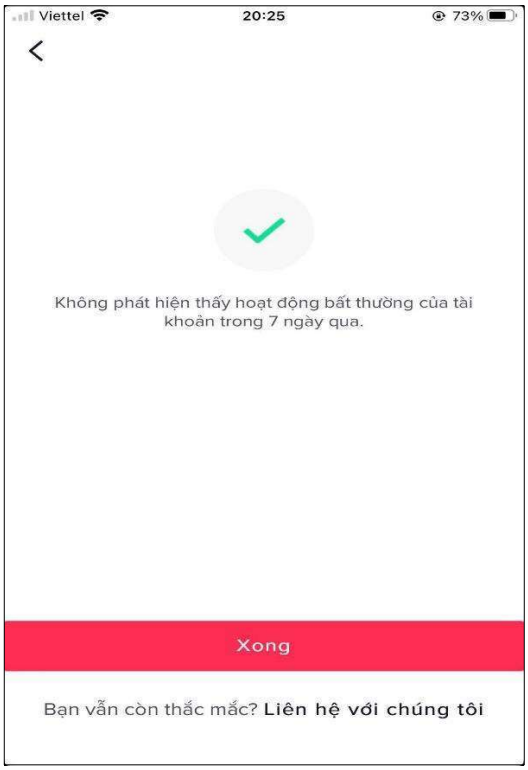


Kiểm tra ai đang sử dụng tài khoản của bạn

Bước 1: Truy cập *biểu tượng người dùng* → Chọn *dấu 3 chấm* → Chọn *Bảo mật*



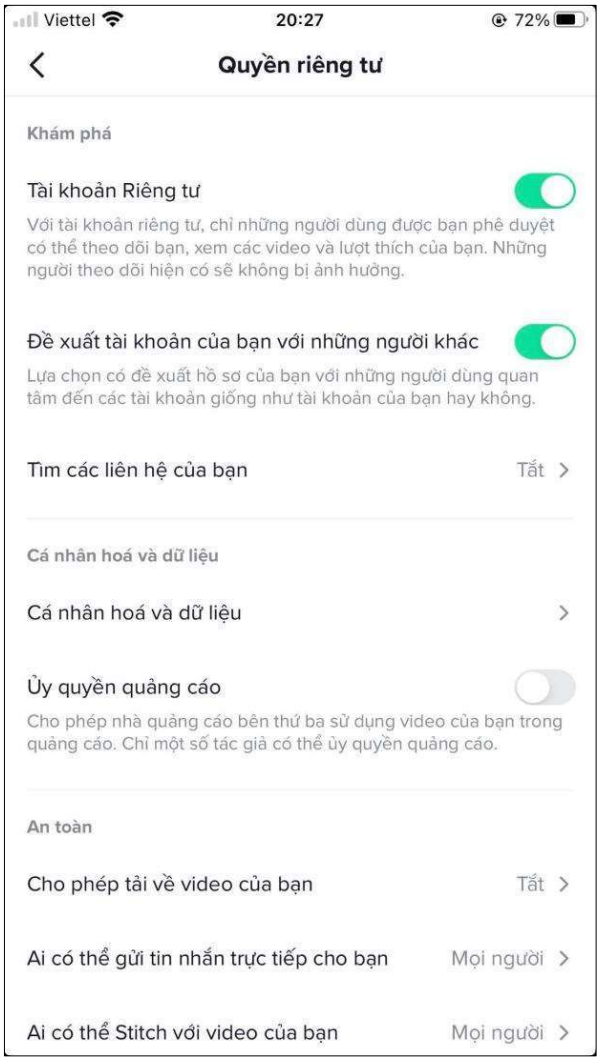
Bước 2: Chọn *Cảnh báo bảo mật* → Các cảnh báo/ cảnh báo bảo mật bổ sung sẽ được hiển thị trên màn hình này → chọn *Xong*



Cài đặt chế độ riêng tư: Cài đặt riêng tư giúp tài khoản người dùng không hiển thị trên TikTok

Bước 1: Truy cập *Biểu tượng người dùng* → Chọn *dấu 3 chấm*

Bước 2: Chọn *Quyền riêng tư* → Bật *Tài khoản riêng tư*



Kiểm tra đăng nhập bất thường

Bước 1: Truy cập *biểu tượng người dùng* → Chọn *dấu 3 chấm* → Chọn *Bảo mật*

Bước 2: Chọn *Thiết bị của bạn* → Chọn thiết bị muốn xóa → Chọn biểu tượng *Thùng rác*

4.3. Sử dụng ứng dụng thanh toán trực tuyến an toàn

Để thanh toán trực tuyến an toàn, cụ thể là thanh toán trực tuyến qua dịch vụ e-banking, Internet banking của các tài khoản ngân hàng, thẻ ATM, thẻ VISA,… cũng như tránh bị đánh cắp thông tin thanh toán, chúng ta cần phải tuân thủ một số nguyên tắc cơ bản.

Sử dụng cổng giao dịch "chính hãng"

Khi sử dụng dịch vụ ngân hàng trực tuyến của các nhà băng, tuyệt đối không thực hiện gián tiếp thông qua các đường link nhận được từ email/tin nhắn hoặc trên trang Web nào đó tạo ra mà phải truy cập trực tiếp vào trang chủ của nhà băng để thực hiện giao dịch.

Trong trường hợp thanh toán qua kênh thứ 3, cần kiểm tra cẩn thận trên thanh địa chỉ xem nơi mình đang dự định nhập tên đăng nhập và mật khẩu có đúng là website chính thức của nhà băng không, có kí hiệu mã hóa kết nối an toàn không. Nếu không, tuyệt đối đừng nhập tên đăng nhập hoặc mật khẩu.

Một số hình thức lừa đảo:

Giả mạo email từ ngân hàng, thông báo tài khản bị trừ tiền (hoặc được cộng tiền trúng thưởng chẳng hạn) và đưa đường link đăng nhập, nhưng thực chất là đường link giả có giao diện giống với trang web của ngân hàng thật. Khi bạn sơ ý nhập thông tin tài khoản, mật khẩu vào, chúng sẽ bị đánh cắp.

Tài khoản Yahoo/Facebook người thân bị đánh cắp, gửi link đăng nhập dịch vụ ngân hàng, nhưng **thực chất là đường link giả** và sẽ bị đánh cắp thông tin nếu mình nhập vào.

Nạn nhân do sử dụng các kết nối wifi nơi công cộng không an toàn dẫn đến bị giả mạo và đánh cắp thông tin cũng như cài phần mềm theo dõi.

Giữ bí mật thông tin cá nhân

Tuyệt đối giữ bảo mật thông tin tài khoản ngân hàng như: số thẻ, số tài khoản và tên truy cập dịch vụ ngân hàng điện tử qua Internet, Mobile,… Tuyệt đối giữ bảo mật các thông tin cá nhân như: họ và tên, địa chỉ, ngày sinh, số CMND.

Các thông tin này thường được khai thác qua nhiều hình thức như:

- được trúng thưởng,

- được tặng quà,
- dò hỏi người thân,
- hù dọa (Hù dọa thiếu cước viễn thông, nợ ngân hàng, hù bị ai rút tiền,…).

Cách đối phó là đừng cung cấp thông tin thật hoặc kiểm tra lại thông tin với ngân hàng bằng cách liên lạc qua số điện thoại hỗ trợ chính thức mà mình biết.

Đặt mật khẩu an toàn

Hãy đặt mật khẩu thật an toàn cho tài khoản Internet Banking. Nếu được, hãy đổi mật khẩu này định kỳ.

Sử dụng dịch vụ tin nhắn chủ động

Nên đăng ký sử dụng dịch vụ nhắn tin, truy vấn số dư chủ động (SMS Banking) để có thể chủ động theo dõi được những biến động số dư trên tài khoản tiền gửi hoặc thẻ thanh toán nhằm phát hiện và xử lý kịp thời khi có các thanh toán bất thường.

Đăng ký sử dụng OTP

OTP là mật khẩu sử dụng một lần, nó tạo ra rào an ninh vô cùng mạnh bằng cách nhắn tin đến số điện thoại của bạn một mậu khẩu xác thực trước khi phê duyệt và thực hiện giao dịch.

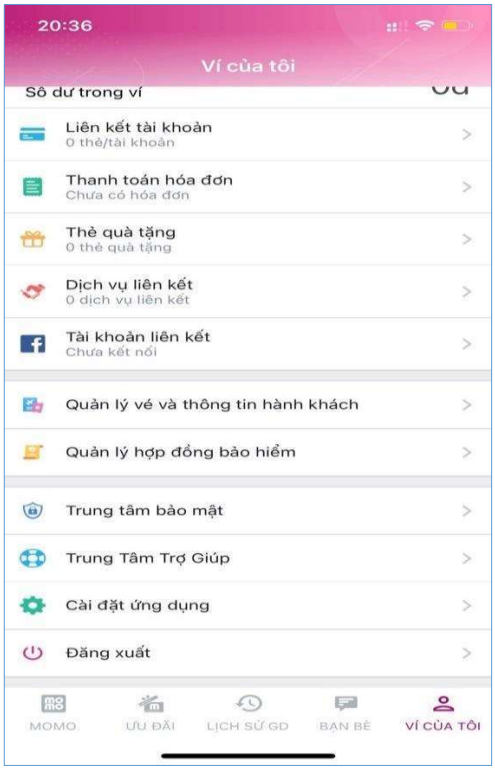
Vì vậy, khi kẻ xấu có hầu hết thông tin ngân hàng của bạn và tiến hành thanh toán bằng tài khoản này, một mật khẩu OTP sẽ được gửi qua điện thoại bạn đang cầm để xác thực.

Giao dịch sẽ thành công chỉ khi nào kẻ xấu cũng có được OTP này. Do đó, kẻ xấu sẽ không thể thực hiện giao dịch với tài khoản của bạn trừ khi bạn mất điện thoại và để lọt vào tay kẻ xấu đó hoặc cao hơn là bị hack/virus đọc được tin nhắn OTP

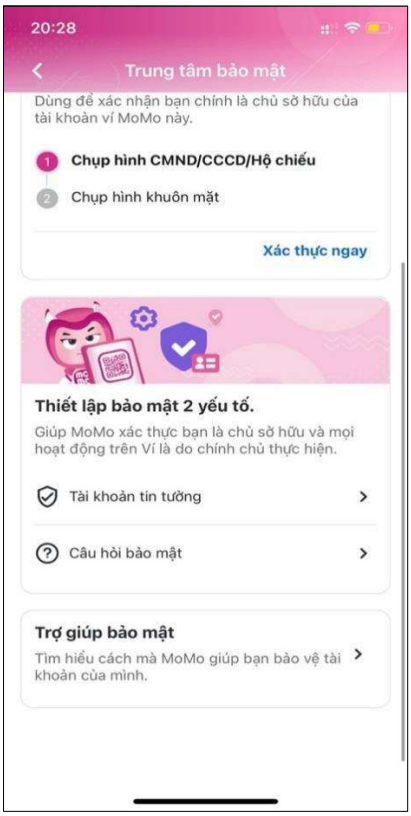
4.4. Một số hướng dẫn thiết lập bảo mật cho ứng dụng thanh toán trực tuyến Momo

Thiết lập bảo mật 2 yếu tố nhằm xác thực chủ sở hữu và các hoạt động trên ví là do chính chủ thực hiện:

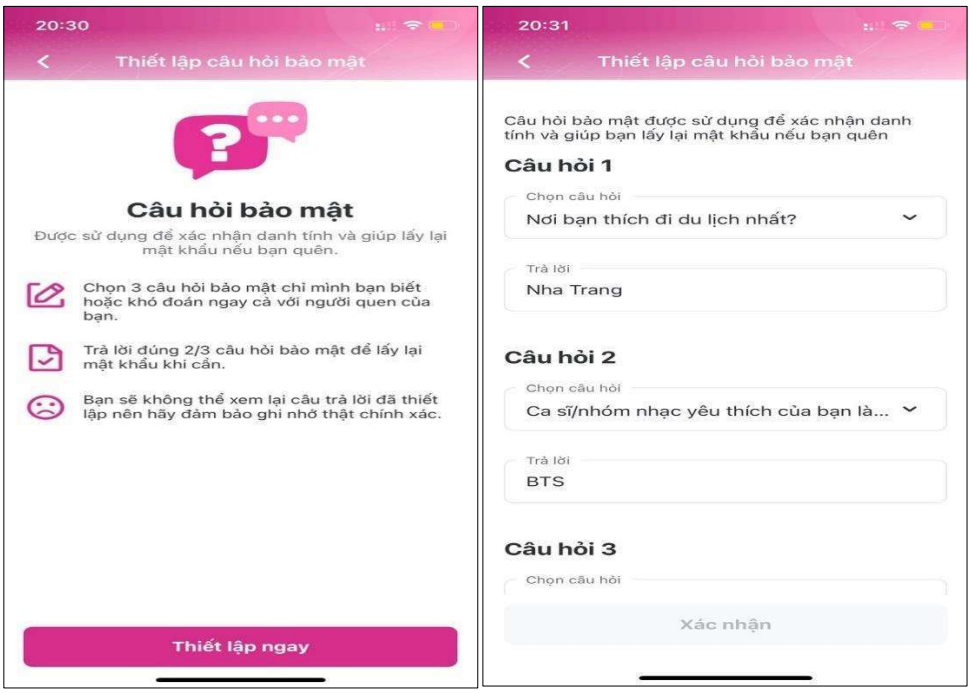
Bước 1: Chọn *Ví của tôi* → Chọn *Trung tâm bảo mật*



Bước 2: Chọn *Tài khoản tin tưởng* → Chọn 3 người từ danh bạ để nhận được sự trợ giúp an toàn trong trường hợp cần khôi phục lại mật khẩu

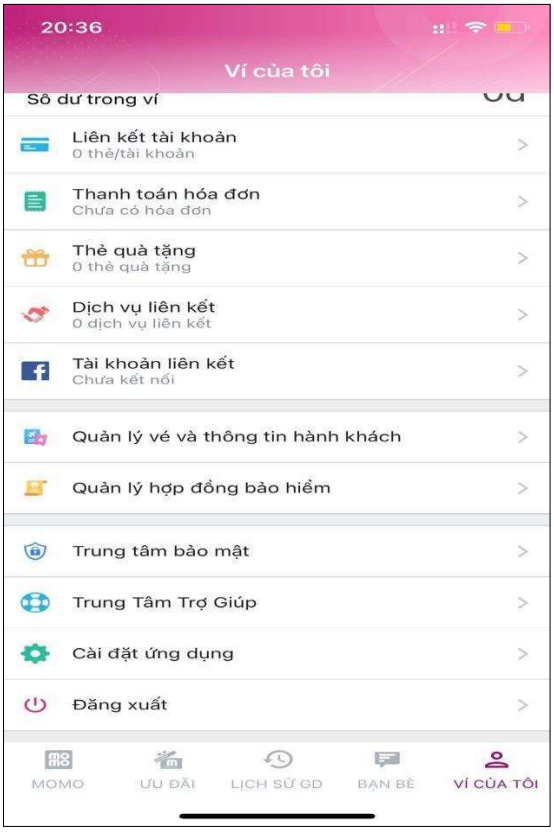


Bước 3: Chọn *Câu hỏi bảo mật* →Lựa chọn và trả lời 3 câu hỏi và ấn *Xác nhận*



Tắt xác nhận thanh toán nhanh:

Bước 1: Chọn *Ví của tôi* → Chọn *Cài đặt ứng dụng*



Bước 2: Tắt chức năng *Xác nhận thanh toán nhanh*

Bước 3: Chọn *Tự động khóa ứng dụng* sau khoảng thời gian (lựa chọn thời gian phù hợp với nhu cầu người dùng, khuyến nghị nên lựa chọn dưới 1 phút)

Phụ lục : Danh sách tài liệu tham khảo

(1) https://www.zdnet.com/article/make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things/

(2) https://expert-advice.org/office365/microsoft-teams-security-policy-best-practices/

(3) https://expert-advice.org/office365/microsoft-teams-security-policy-best-practices/

(4) https://expert-advice.org/office365/microsoft-teams-security-policy-best-practices/

(5) https://docs.microsoft.com/en-us/microsoftteams/manage-the-audio-conferencing-settings-for-a-user-in-teams

(6) https://www.ytria.com/blog/teams-tip-18-control-if-anonymous-users-can-join-meeting/

(7) https://helpdesk.ctu.edu.vn/day-hoc-truc-tuyen/85-zoomsecurity

(8) https://www.eduhk.hk/ocio/content/faq-i-have-removed-participants-during-zoom-meeting-they-wont-be-able-rejoin-meeting

(9) https://www.unr.edu/tlt/instructional-design/instructional-technology-resources/web-conferencing/zoom/securing-sessions/remove-participant

(10) https://blog.zoom.us/keep-uninvited-guests-out-of-your-zoom-event/#:~:text=Just%20click%20the%20Security%20icon,button%20that%20says%20Lock%20Meeting.

(11) https://www.technology.pitt.edu/help-desk/how-to-documents/zoom-enabling-screen-sharing-participants

(12) https://www.bluejeans.com/blog/eight-best-practices-safe-video-conferencing

(13) https://www.tugboatlogic.com/blog/top-3-most-secure-video-conferencing-solutions/

(14) US-Cert: Security Tip – Staying Safe on Social Network Sites

(15) https://us-cert.cisa.gov/ncas/tips/ST06-003

(16) SEC's Office of Investor Education and Advocacy, Investor.gov: Social Networking Safety Tips

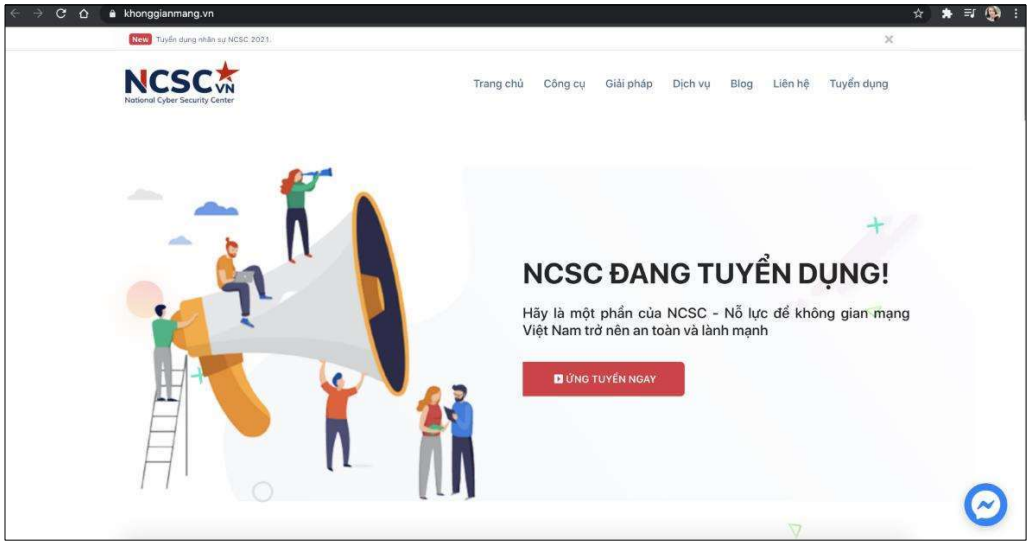
(17)https://www.investor.gov/protect-your-investments/fraud/how-avoid-fraud/protect-your-social-media-accounts

(18) https://www.technology.pitt.edu/security/best-practices-safe-social-networking

U.S. Attorneys » District of Minnesota: Online Safety Tips

MỘT SỐ CÔNG CỤ HỮU ÍCH, MIỄN PHÍ CỦA CHÚNG TÔI

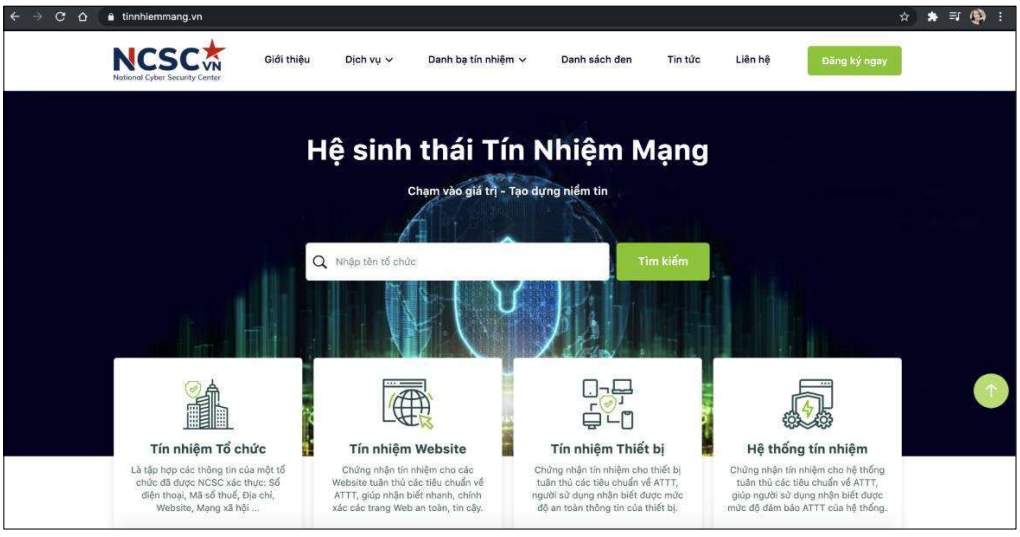
1. Công cụ, tài liệu miễn phí tại khonggianmang.vn



khonggianmang.vn được Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) xây dựng nhằm hỗ trợ người dùng Internet có thể tự kiểm tra mức độ an toàn thông tin khi sử dụng mạng với các công cụ hữu ích như: Kiểm tra mạng máy tính ma, kiểm tra lộ lọt thông tin tài khoản cá nhân, kiểm tra website phishing, kiểm tra tập tin độc hại, công cụ giải mã, nhận diện ransomware,…cùng với các tài liệu hướng dẫn (tài liệu hướng dẫn bảo đảm ATTT khi làm việc từ xa).

2. Kiểm tra mức độ tín nhiệm tại tinnhiemmang.vn

https://tinnhiemmang.vn



Tín nhiệm mạng cung cấp nhãn tin cậy về an toàn thông tin, giúp người dùng nhận biết và xác định các trang web tin cậy, ngăn ngừa các cuộc tấn công lừa đảo, hướng tới xây dựng một hệ sinh thái uy tín, an toàn nhằm tạo niềm tin khi sử dụng dịch vụ trên môi trường mạng.

Hệ sinh thái Tín nhiệm mạng bao gồm: Tín nhiệm Tổ chức, Tín nhiệm Website, Tín nhiệm Thiết bị, Hệ thống tín nhiệm.

Thông tin liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)

Email: ncsc@ais.gov.vn

Số điện thoại: 024.3209.1616

Địa chỉ: 115 Trần Duy Hưng, Cầu Giấy, Hà Nội