BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

TÀI LIỆU
HƯỚNG DẪN SỬ DỤNG AN TOÀN CÁC PHẦN MỀM, CÔNG CỤ DẠY, HỌC TRỰC TUYẾN

(Kèm theo Công văn số /CATTT-NCSC ngày tháng năm 2021 của Cục An toàn thông tin)

Loại tài liệu	Công khai
Phiên bản	Version 1.0
Đóng góp ý kiến: Mọi góp ý cho tài liệu xin gửi về Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) theo thư điện tử nscs@ais.gov.vn, số điện thoại 02432091616.	

LỜI MỞ ĐẦU

Covid-19 là một biến cố không mong muốn và ảnh hưởng tới mọi hoạt động của xã hội. Nhưng nhìn nhận ở góc độ tích cực, Covid-19 cũng góp phần xoá bỏ nhiều thói quen cũ và giúp những phương pháp giáo dục mới, hiện đại như học trực tuyến, dạy trực tuyến, ứng dụng phần mềm vào giáo dục được tiếp nhận nhanh chóng và dễ dàng hơn.

Covid-19 cũng tạo nên một bước ngoặt trong vai trò của người giáo viên. Cùng với hàm lượng ứng dụng công nghệ trong giáo dục ngày càng tăng cao, người giáo viên ngày nay không chỉ cần sử dụng thành thạo các phần mềm, công cụ để truyền tải kiến thức cho học sinh, mà còn có thêm vai trò hướng dẫn học sinh những kĩ năng lên mạng an toàn, bảo vệ học sinh khỏi những rủi ro có thể đến từ môi trường mạng. Bảo vệ các em khỏi những tác động tiêu cực từ công nghệ, cũng là nhu cầu chung của các bậc phụ huynh khi trang bị máy tính, điện thoại để con em mình tham gia vào quá trình học tập trực tuyến và các hình thức học tập số khác.

Nhận thấy những khó khăn của giáo viên và học sinh tại các cơ sở giáo dục trong việc làm quen với dạy và học trực tuyến an toàn, Cục An toàn thông tin đã xây dựng cuốn cẩm nang với tên gọi "HƯỚNG DẪN SỬ DỤNG AN TOÀN CÁC PHẦN MỀM, CÔNG CỤ DẠY, HỌC TRỰC TUYẾN" nhằm giúp giáo viên, các em học sinh và cha mẹ tự trang bị cho mình những kiến thức, kỹ năng cơ bản để nhận biết các nguy cơ mất an toàn thông tin trên không gian mạng nói chung, trong quá trình dạy, học trực tuyến nói riêng, để từ đó tự bảo vệ mình, bảo vệ lớp học của mình trên không gian mạng.

Cẩm nang gồm 03 chương:

Chương 1: Nguy cơ mất an toàn thông tin chung. Chương này đưa ra các nguy cơ, vấn đề mất an toàn thông tin mà bất kỳ ai tham gia, truy cập vào Internet cũng có thể gặp phải. Chương này cũng phân tích và đưa ra nguy cơ đặc thù đối với các em học sinh. Phần cuối của chương là hướng dẫn chung để giải quyết các nguy cơ.

Chương 2: Hướng dẫn bảo đảm an toàn thông tin cho thiết bị dạy, học trực tuyến. Chương này giúp giáo viên, cha mẹ, và các em học sinh tự thiết lập các tính năng có sẵn trên hệ điều hành hoặc sử dụng thêm các phần mềm tin cậy để bảo vệ máy tính, điện thoại di động khỏi các nguy cơ mất an toàn thông tin, bảo vệ khỏi các cuộc tấn công mạng từ đó hạn chế những hậu quả có thể xảy ra.

Chương 3: Hướng dẫn sử dụng an toàn các phần mềm. Chương này hướng dẫn riêng cho giáo viên, học sinh và cha mẹ khi sử dụng các phần mềm dạy, học trực tuyến phổ biến hiện nay (như Zoom, Microsoft Teams, Google Meeting, Trans, Zavi, Jitsi ...). Các phần mềm hướng dẫn trong chương này được Cục An toàn thông tin lựa chọn dựa trên kết quả khảo sát thực tế. Chúng tôi sẽ tiếp tục cập nhật hướng dẫn cho các phần mềm mới khi nhận được ý kiến đóng góp từ giáo viên, học sinh và các bậc cha mẹ trong quá trình sử dụng.

Đây là phiên bản đầu tiên của cẩm nang được ra mắt. Với thời gian yêu cầu cấp bách về dịch bệnh Covid-19 bùng phát mạnh, Cục An toàn thông tin đã nỗ lực trong thời gian ngắn nhất để xây dựng, đồng thời tiếp thu các ý kiến góp ý của đơn vị chức năng thuộc Bộ Giáo dục và Đào tạo để hoàn thiện tài liệu. Trong quá trình xây dựng, hoàn thiện tài liệu có tham khảo, tổng hợp (đã kiểm chứng, đánh giá về mặt nội dung) từ nhiều nguồn thông tin công khai trên Internet. Do điều kiện thời gian gấp rút, phiên bản đầu tiên có thể sẽ không tránh được thiếu sót, vì vậy Quý giáo viên, cha mẹ và các bạn học sinh phát hiện thấy bất kỳ nội dung cần được diễn giải tốt hơn, hoặc có những ý kiến đóng góp vào tài liệu này, đừng ngần ngại gửi ý kiến của mình tới Cục An toàn thông tin theo thông tin liên hệ sau: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thư điện tử nscs@ais.gov.vn, số điện thoại 02432091616.

MỤC LỤC

THUẬT NGỮ VÀ TỪ VIẾT TẮT

TT	Thuật ngữ	Giải thích
1	Học sinh	Học sinh, học viên
2	OTP	One Time Password Mật khẩu dùng một lần
3	PIN	Personal Identification Number Số định danh cá nhân
4	URL	Unifrom Resource Locator Đường dẫn truy cập các tài nguyên trên web
5	VPN	Virtual Private Network Mạng riêng ảo
6	ID	Identification Số định danh (duy nhất) thường dùng để tạo cuộc họp trong các ứng dụng
7	Visafe	Ứng dụng Internet An toàn
8	Hacker	Đối tượng thực hiện các cuộc tấn công trên Internet

DANH MỤC HÌNH ẢNH

CHƯƠNG 1: NGUY CƠ MẤT AN TOÀN THÔNG TIN

1. Nguy cơ mất an toàn thông tin chung đối với tất cả mọi người khi sử dụng Internet

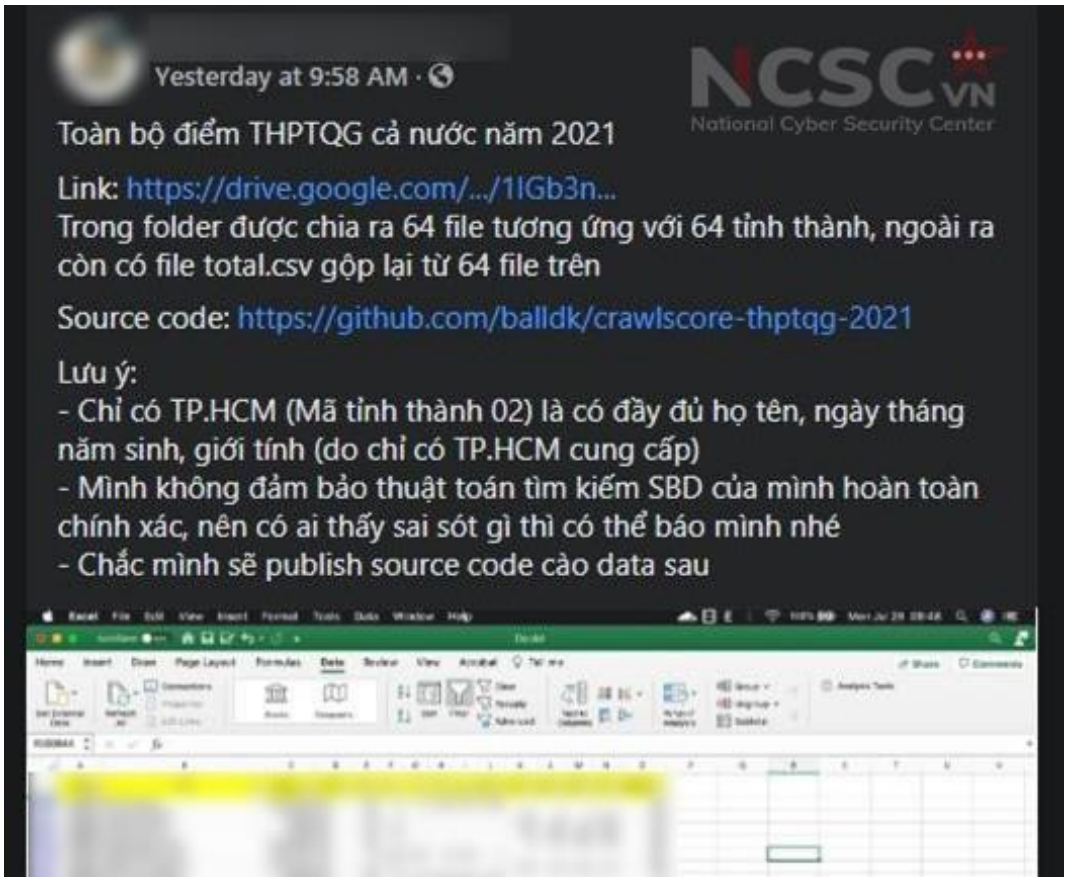
1.1. Nguy cơ bị thu thập, lộ lọt thông tin, dữ liệu cá nhân

1.1.1. Bạn có thể bị thu thập, lộ lọt thông tin, dữ liệu cá nhân gì?

Thông tin, dữ liệu cá nhân người dùng có thể gồm một trong những thông tin sau: họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu … Những thông tin thuộc bí mật cá nhân gồm có hồ sơ giáo dục, hồ sơ y tế, hồ sơ nộp thuế, số thẻ bảo hiểm xã hội, số thẻ tín dụng và những bí mật cá nhân khác.

Đây là loại dữ liệu bị đánh cắp nhiều nhất và dễ sử dụng nhất. Hacker thường dùng thông tin này để thực hiện các hành vi trục lợi như: Nộp đơn xin vay tiền hoặc thẻ tín dụng dưới tên người sử dụng; xin vay vốn dưới tên của nạn nhân ... thậm chí đe dọa, tống tiền

Đối với lĩnh vực Giáo dục, thông tin giáo dục đề cập đến dữ liệu của một cá nhân dựa trên hồ sơ giáo dục bao gồm bảng điểm học bạ và hồ sơ. Mặc dù thông tin giáo dục không mang lại hậu quả tức thì nhưng người dùng có thể bị tống tiền từ đây.



Hình 1: Lộ lọt thông tin, dữ liệu các nhân trên Internet

Hacker có thể sử dụng thông tin giáo dục để làm người dùng sợ hoặc lừa người dùng thực hiện theo những yêu cầu của chúng hoặc giả danh là sinh viên hoặc cán bộ của một cơ sở giáo dục để lừa đảo.

1.1.2. Nguyên nhân lộ thông tin, dữ liệu cá nhân: từ vô tình đến cố tình

Bạn thường đã gặp các trường hợp như: Nhận được tin nhắn, cuộc gọi, thư điện tử quảng cáo về khóa học tiếng Anh khi có con đang trong độ tuổi đi học; quảng cáo mua bán bất động sản; mời sử dụng các gói bảo hiểm, dịch vụ chăm sóc sắc đẹp miễn phí …

Một số ứng dụng mua hàng trực tuyến gợi ý liên tục những món đồ mà người dùng từng tìm kiếm. Thậm chí, chỉ cần dùng Internet tại một quán ăn … một lát sau trên điện thoại của bạn xuất hiện các câu hỏi đánh giá địa điểm đó thế nào … Những điều này làm bạn cảm thấy dường như thiết bị di động thông minh đang "theo dõi" các hoạt động của chúng ta. Đây là những trường hợp lọt lộ thông tin, dữ liệu cá nhân mà người dùng thường không để ý, không hiểu tại sao và không biết làm thế nào để tránh.

Phần lớn (tới 80%) nguyên nhân lộ lọt thông tin cá nhân là xuất phát từ chính sự bất cẩn của người dùng. Đây là những cơ hội thuận lợi để đối tượng xấu thu thập thông tin, dữ liệu cá nhân nhằm mục đích trục lợi.

Người dùng cung cấp thông tin cá nhân khi đăng ký tài khoản, dịch vụ

Hình 2: Cung cấp thông tin cá nhân khi đăng ký tài khoản, dịch vụ

Người dùng thiết lập chế độ công khai thông tin cá nhân khi sử dụng dịch vụ

Trên các trang, hội nhóm mua bán hàng hóa người bán/người mua thường công

khai thông tin mình như số điện thoại, thông tin tài khoản để tiện cho việc liên hệ

Hình 3: Ý thức bảo vệ thông tin cá nhân trên Internet

Lựa chọn sử dụng dịch vụ của những bên trung gian không uy tín, không có chính sách an toàn thông tin hoặc chính sách an toàn thông tin không tốt.

Phần nhỏ (20%) còn lại là do từ phía các nhà cung cấp dịch vụ chia sẻ, làm lộ thông tin cá nhân của chúng ta:

Hình 4: Lộ lọt thông tin do lỗ hổng từ các hệ thống có lưu trữ thông tin cá nhân

Lỗ hổng trên các hệ thống, ứng dụng của đơn vị cung cấp dịch vụ (bao gồm cả hệ thống của các cơ sở giáo dục).

Lỗ hổng trong chính sách bảo mật thông tin khách hàng của đơn vị cung cấp dịch vụ:

Có những doanh nghiệp chủ ý đưa thông tin khách hàng cho bên thứ ba.

1.1.3. Hậu quả của việc lộ lọt thông tin

Lộ thông tin cá nhân, nhất là số điện thoại di động, tên tài khoản trên các mạng xã hội Facebook, Instagram … khiến người sử dụng gặp rắc rối vì tin nhắn rác, tin nhắn quảng cáo ...

Sử dụng ảnh thật của người dùng để tạo nên những tài khoản giả mạo để đi lừa chính bạn bè, người thân của họ. Những thông tin trên ảnh như tên của con, tên cơ sở giáo dục, khu nội trú, thẻ xe đưa đón con… cũng có thể trở thành thông tin hữu ích đối với tội phạm mạng khi bạn đăng tải công khai trên mạng xã hội.

Tội phạm mạng có thể sử dụng những thông tin do chính chủ tự nguyện cung cấp hoặc bằng cách nào đó thu thập được để đe dọa tống tiền, bắt cóc, hoặc lừa người sử dụng chuyển tiền vào tài khoản của tội phạm.

1.2. Nguy cơ lừa đảo trực tuyến

1.2.1. Vì sao bạn bị lừa đảo?

90% các cuộc tấn công lừa đảo thường đánh vào lòng tin của người dùng, đặc biệt là người dùng không có kiến thức, kỹ năng để tự bảo vệ mình trên không gian mạng. Những người dùng có kỹ năng thì đôi khi cũng bị "mất cảnh giác"

1.2.2. Bạn có thể bắt đầu bị lừa đảo qua đâu?

- Lừa đảo qua mạng xã hội: lừa đảo qua mạng xã hội hiện nay được sử dụng khá nhiều và không đòi hỏi kiến thức, trình độ cũng có thể thực hiện các cuộc tấn công lừa đảo người dùng

+ Đánh cắp tài khoản Facebook, sau đó giả vờ là người thân để nhắn tin nhờ chuyển tiền, mua thẻ điện thoại.

+ Gửi đường dẫn trang web lừa đảo lừa người dùng điền các thông tin cá nhân quan trọng. Các trang web lừa đảo trúng thưởng hay được tận dụng trong những trường hợp này.

+ Phát tán mã độc qua Messenger, gửi các tin nhắn trúng thưởng, nội dung hấp dẫn qua Messenger.

- Lừa đảo qua thư điện tử: lừa đảo qua thư điện tử chủ yếu được sử dụng để phát tán mã độc, hoặc thu thập thông tin, dữ liệu cá nhân.

Đối tượng xấu gửi hàng loạt thư điện tử với nội dung và có tệp tin đính kèm mang tính chất như: "hấp dẫn"; "khơi dậy tính tò mò"; "Mang tính chất khẩn cấp" đến một danh sách địa chỉ thư điện tử mà Hacker đã thu thập và chuẩn bị sẵn. Sau đó chỉ chờ nạn nhân mắc bẫy và tin tặc sẽ thực hiện mục đích của mình.

Đối tượng xấu xác định được mục tiêu, sau đó tìm kiếm các thông tin liên quan đến mục tiêu, cuối cùng sẽ giả mạo một địa chỉ thư điện tử mà mục tiêu "tin cậy" sau đó sẽ gửi thư điện tử có gắn kèm tệp tin chứa mã độc hoặc đường dẫn độc hại, lừa đảo dựa trên các thói quen, sở thích của mục tiêu.

- Lừa đảo qua SMS

Giả mạo tin nhắn thương hiệu (SMS Brandname) của Ngân hàng để chiếm đoạt tài sản: tin nhắn giả mạo được gửi nhìn như từ các ngân hàng, gửi tiếp nối sau các SMS của ngân hàng mà khách hàng vẫn nhận. Tin nhắn giả mạo đính kèm đường dẫn (link) và yêu cầu khách hàng nhập Tên đăng nhập cùng Mật khẩu vào một trang web bắt chước giao diện của ngân hàng để lừa đảo khách hàng nhận thưởng, cảnh báo đổi mật khẩu, cảnh báo cập nhật dịch vụ… Khi khách hàng truy cập vào đường dẫn trong tin nhắn và thực hiện nhập Tên đăng nhập, Mật khẩu, OTP để thực hiện giao dịch sẽ bị kẻ gian chiếm thông tin và mất tiền.

- Lừa đảo qua Cuộc gọi.

Giả mạo số điện thoại tổng đài gọi đến cho bạn, khi bạn nghe máy sẽ bị tính tiền. Số điện thoại gọi đến cho bạn có thể là đầu số từ nước ngoài như: Modova (+373), Tunisia (+216), Equatorial Guinea (+240), Burkina Faso (+226) …

Giả mạo nhân viên ngân hàng hoặc các cơ quan, tổ chức cung cấp dịch vụ gọi để

yêu cầu cung cấp thông tin cá nhân hoặc thu tiền các loại hình dịch vụ.

Giả mạo cuộc gọi từ cơ quan chức năng như "Cán bộ Bộ Công an" gọi điện dọa nạt, uy hiếp tinh thần và buộc phải chuyển tiền cho tin tặc.

- Lừa đảo qua Website giả mạo

Đối tượng xấu thường giả mạo các Website chính thống, sau đó lừa người dùng truy cập và đăng nhập vào các website đó. Thông thường hình thức này sẽ được kết hợp với lừa đảo qua Email, SMS hay mạng xã hội.

- Lừa đảo chiếm đoạt sim số điện thoại để lấy mã OTP từ ngân hàng:

Một trong những chiêu thức lừa đảo mới xuất hiện gần đây của tội phạm công nghệ đó là chiếm đoạt quyền kiểm soát sim của chủ thuê bao di động để lấy mã OTP từ ngân hàng. Sau đó thực hiện hành vi chuyển, rút tiền hoặc vay tiền online. Thủ đoạn chung là mạo danh nhân viên nhà mạng, gọi điện thoại giới thiệu đang có chương trình "hỗ trợ chuyển đổi sim từ 3G lên 4G", hoặc đổi sim để nhận ưu đãi và hối thúc nạn nhân nâng cấp lên sim 4G nếu không sẽ không thể sử dụng. Đối tượng sẽ hướng dẫn chủ sim số điện thoại soạn tin theo cú pháp. Sau khi thực hiện thao tác soạn và gửi tin nhắn, ngay lập tức sim số điện thoại đã bị đánh cắp. Sau khi chiếm quyền kiểm soát sim của người dùng, kẻ gian dùng chính sim đó lấy mã OTP từ ngân hàng gửi về sử dụng các dịch vụ tín dụng, vay tiền online… dưới danh nghĩa nạn nhân.

1.2.3. Dấu hiệu của một cuộc tấn công lừa đảo

Những dấu hiệu sau đây có thể là dấu hiệu bắt đầu cuộc tấn công lừa đảo.

- "Một ngày đẹp trời/xấu trời", bạn nhận được Email/tin nhắn Facebook/Tin nhắn SMS/Cuộc gọi…từ một người lạ đề nghị "cung cấp" các loại hình thông tin, dữ liệu cá nhân.

- Nhận được tin nhắn chào hỏi và vay tiền từ một người quen qua Facebook.

- Nhận được tin nhắn SMS "Đề nghị kiểm tra thông tin", "Đề nghị truy cập một trang web lạ lạ hoặc quen quen" từ một số điện thoại/Tên định danh bất kỳ.

Hình 5: Dấu hiệu một cuộc tấn công lừa đảo

- Nhận được cuộc gọi từ số điện thoại lạ tự xưng là Nhân viên ngân hàng, cơ quan chức năng (công an, viện kiểm soát, hải quan) với yêu cầu dạng "đề nghị cung cấp thông tin, chuyển tiền ..."

Cập nhật dấu hiệu mới thường xuyên tại https://tinnhiemmang.vn.

1.3. Nguy cơ bị mã độc tấn công, nghe lén

1.3.1. Mã độc có thể gây nguy hại như thế nào

Mã độc (còn gọi là virus) là chương trình hoặc đoạn mã đưa vào máy tính, điện thoại, các thiết bị mạng hoặc bất kỳ thiết bị điện tử, phần mềm, ứng dụng trong hệ thống thông tin (có kết nối mạng hoặc không có kết nối mạng) nhằm thực hiện các hành vi trái phép (như ăn trộm dữ liệu, thông tin trên máy tính, điện thoại bị lây nhiễm, gửi thư rác, hay tham gia các cuộc tấn công mạng dưới điều khiển của Hacker hoặc tiếp tục phát tán mã độc khác).

Như vậy đối với người dùng Internet mã độc giống như kẻ xấu, khi đã lây nhiễm thành công vào máy tính, điện thoại di động, mã độc có thể làm bất cứ việc gì như:

- Theo dõi hoạt động của bạn trên các thiết bị này;
- Phá hủy dữ liệu (xóa dữ liệu, mã hóa dữ liệu …);
- Đánh cắp dữ liệu, thông tin, tài khoản bạn đăng nhập, sử dụng lưu trữ trên máy tính, điện thoại di động, để đe dọa, tống tiền.
- Ghi âm cuộc gọi, đọc trộm tin nhắn … thậm chí còn có thể theo dõi, chụp hình xung quanh nếu thiết bị có chức năng chụp hình.

1.3.2. Khi nào bạn có thể bị mã độc tấn công

Bạn có thể bị mã độc tấn công bất cứ lúc nào nếu như:

- Không cảnh giác trong lúc sử dụng Intertnet để làm việc, học tập, giải trí, trò chuyện với bạn bè từ đó vô tình truy cập vào những đường dẫn độc hại, mở những tập tin có đính kèm mã độc, hay cài đặt phần mềm không tin cậy.
- Máy tính, điện thoại hoặc những phần mềm bạn đang sử dụng trên các thiết bị này có những điểm yếu, lỗ hổng mà mã độc có thể khai thác và xâm nhập vào máy tính của bạn
- Ngay cả khi bạn đã cảnh giác, đã biết cách bảo vệ máy tính, vẫn có những trường hợp bạn bị tấn công có chủ đích và bị cài cắm mã độc, tuy nhiên những trường hợp này rất ít xảy ra với người dùng bình thường.

Dưới đây là một số nguồn lây nhiễm mã độc chính bạn cần biết để ngăn chặn mã độc lây nhiễm vào máy tính, điện thoại của mình:

- Các trang web lưu trữ tập tin độc hại/mã khai thác trên toàn thế giới, các trang web này có thể do Hacker chiếm quyền điều khiển hoặc cố tình dựng lên sau đó sử dụng để phát tán mã độc.
- Thư điện tử có đính kèm tập tin hoặc nội dung thư có đường dẫn độc hại
- Lỗ hổng phần mềm: Lỗ hổng, lỗi phần mềm cho phép Hacker truy cập từ xa vào máy tính người dùng, từ đó cài cắm mã độc, lấy trộm dữ liệu.
- Phương tiện lưu trữ di động, các ổ đĩa USB cũng là hình thức phổ biến để cài cắm mã độc vào máy tính người dùng.
- Phần mềm, ứng dụng miễn phí có đính kèm sẵn mã độc. Khi người dùng cài đặt

phần mềm, ứng dụng này thì đồng thời cũng cài đặt mã độc vào máy tính, điện thoại của mình.

1.3.3. Dấu hiệu khi bị lây nhiễm mã độc

Đối với những mã độc tinh vi, chỉ hoạt động âm thầm thì người dùng thông thường (người không có kiến thức chuyên sâu về an toàn thông tin) rất khó có thể phát hiện ra, thậm chí những phần mềm phòng chống mã độc cũng không phát hiện. Tuy nhiên những trường hợp này rất ít xảy ra với người dùng bình thường.

Đối với những mã độc thông thường, thì hầu hết các phần mềm phòng chống mã độc (còn gọi là anti-virus) sẽ cảnh báo cho người dùng và xử lý

Tuy nhiên nếu không dùng bất kỳ phần mềm phòng chống mã độc nào, hoặc có cài nhưng không sử dụng bạn có thể lưu ý những dấu hiệu sau:

- Máy tính, điện thoại chạy chậm, hoạt động không ổn định: mã độc lây nhiễm vào máy có thể gây ảnh hưởng đến hoạt động máy.
- Liên tục gặp lỗi khi mở tập tin trong ổ đĩa, đây có thể là một dấu hiệu đáng ngờ, cảnh báo nguy cơ mã độc đã bị cài cắm vào máy tính.
- Xuất hiện tập tin, ứng dụng, phần mềm lạ trên máy tính mặc dù không hề cài đặt.
- Dữ liệu trên máy tính, điện thoại đột nhiên bị mã hóa không mở được.
- Liên tục nhận được các cảnh báo giả
- Ổ cứng nhanh hết dung lượng trống
- Trình duyệt bị thay đổi bất thường, thanh công cụ mới xuất hiện dù không cài, những website tự động truy cập dù không gõ địa chỉ.
- Nhận được cảnh báo từ nhà cung cấp dịch vụ Internet hoặc các cơ quan chức năng.

2. Nguy cơ đặc trưng đối với các em học sinh

Bên cạnh những nguy cơ chung đã đề cập ở trên, riêng đối với các em học sinh trong quá trình tương tác trên không gian mạng còn gặp phải những nguy cơ đặc thù của riêng lứa tuổi gồm:

Nội dung không phù hợp: các em học sinh có thể sẽ tiếp xúc với các tài liệu có nội dung không phù hợp (hình ảnh khiêu dâm, bạo lực, phân biệt chủng tộc, thù địch, cực đoan và các tài liệu kích động các hành vi nguy hiểm như tự kỷ, tự hủy hoại, tự tử).

Tương tác với những đối tượng, tình huống nguy hiểm mà các em học sinh không phân biệt được: các em học sinh bên cạnh việc tham gia vào các lớp học trực tuyến, có thể sử dụng thiết bị học để trao đổi, tương tác với các đối tượng lạ… từ đó có thể đối mặt với nguy cơ bị bắt nạt, quấy rối, dụ dỗ, khiêu khích thực hiện các hành vi không phù hợp với lứa tuổi.

Bên cạnh đó, các em học sinh có thể sử dụng điện thoại, máy tính của bố mẹ để học, trong đó có sẵn các ứng dụng ngân hàng, tài khoản thư điện tử mà các bậc cha mẹ không quản lý chặt có thể dẫn đến việc bị mất tiền trong tài khoản hoặc mất tài khoản

thư điện tử….

3. Hướng dẫn bảo đảm ATTT chung

Đối với bất kỳ người dùng dù là đối tượng (giáo viên, học sinh, bác sĩ, kỹ sư… hay cả những chuyên gia an toàn thông tin), khi đã sử dụng Internet sẽ phải đối mặt với các nguy cơ mất an toàn thông tin, tuy nhiên nếu bạn có kiến thức và kỹ năng thì cũng đã hạn chế được 80% các nguy cơ này.

Do vậy để đảm bảo an toàn thông tin cho mình và người thân, người dùng cần thực hiện:

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

Bảo đảm an toàn cho máy tính, thiết bị di động sử dụng để truy cập Internet: cài đặt, thiết lập tính năng bảo mật có sẵn của thiết bị, và sử dụng thêm một số phần mềm ứng dụng bảo đảm an toàn thông tin (như phần mềm anti virus);

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

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

Tham khảo thêm tại Cẩm nang Bảo đảm an toàn thông tin trong đại dịch Covid-19 (https://tinnhiemmang.vn/cam-nang-bao-dam-an-toan-thong-tin-trong-dai-dich-covid-19)

CHƯƠNG 2: BẢO ĐẢM AN TOÀN CHO THIẾT BỊ DẠY/HỌC

1. Máy tính sử dụng hệ điều hành Windows

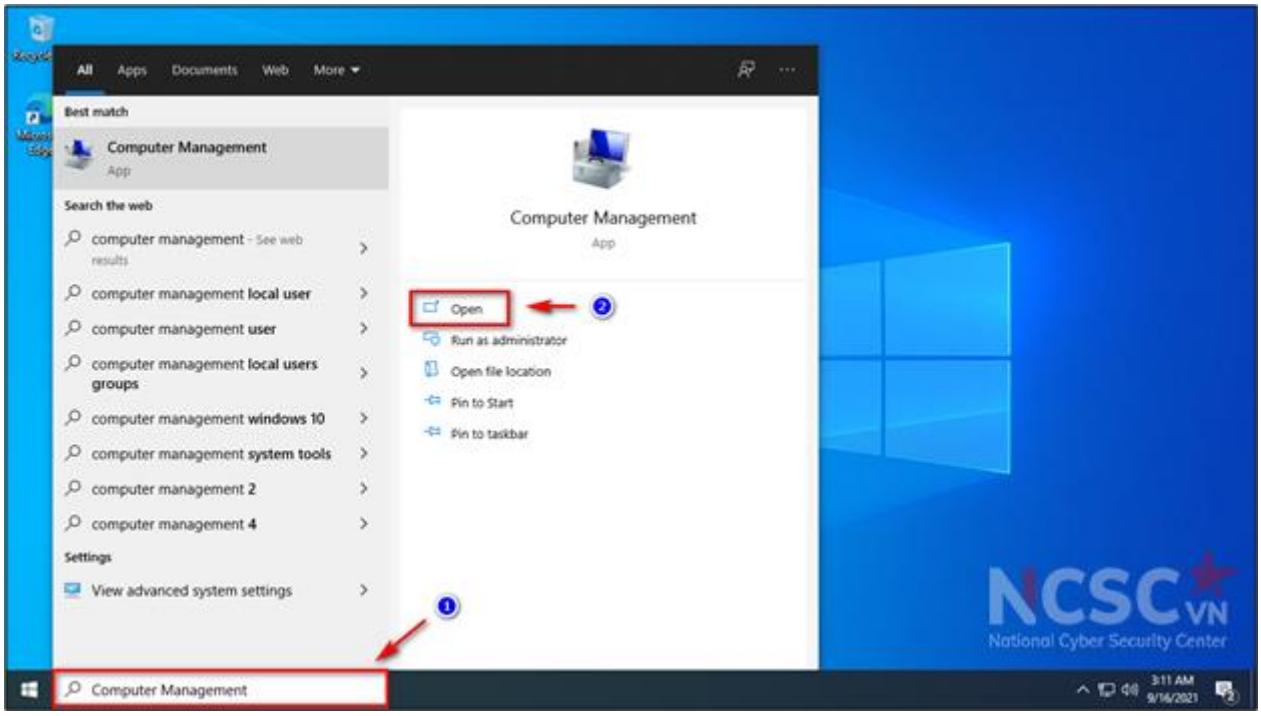
1.1. Thiết lập và cấu hình Windows 10 an toàn

1.1.1. Phân vùng ổ cứng máy tính

Việc phân vùng ổ cứng nhằm mục đích chia ổ có dung lượng lớn thành những ổ có dung lượng nhỏ hơn, thuận tiện cho việc quản lý, lưu trữ dữ liệu phục vụ các nhu cầu sử dụng khác nhau của người dùng.

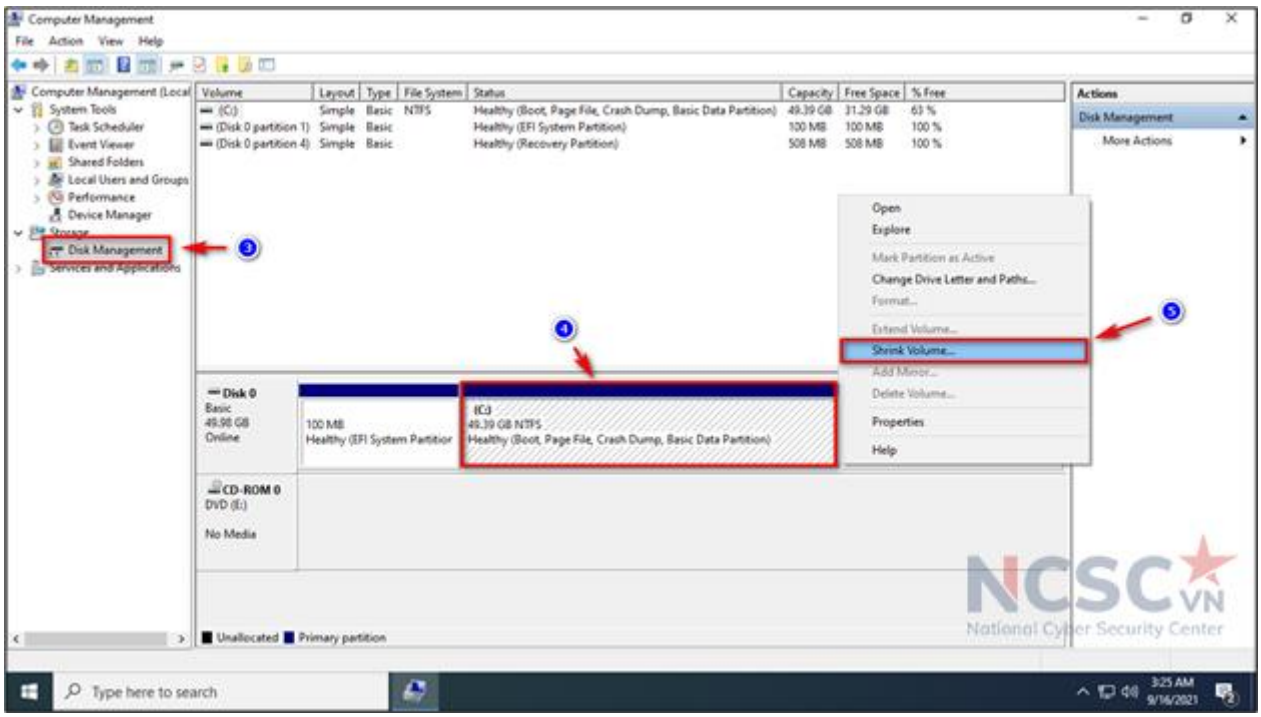
Nếu máy tính chưa phân chia thành các ổ khác nhau bạn có thể thực hiện chia ổ theo hướng dẫn dưới đây.

Bước 1: Tại biểu tượng tìm kiếm trên Windows > nhập Computer Management > Open.



Hình 6: Hướng dẫn phân vùng ổ cứng (1)

Bước 2: Chọn Disk Management > Chuột phải vào ổ muốn chia nhỏ > Shrink Volume

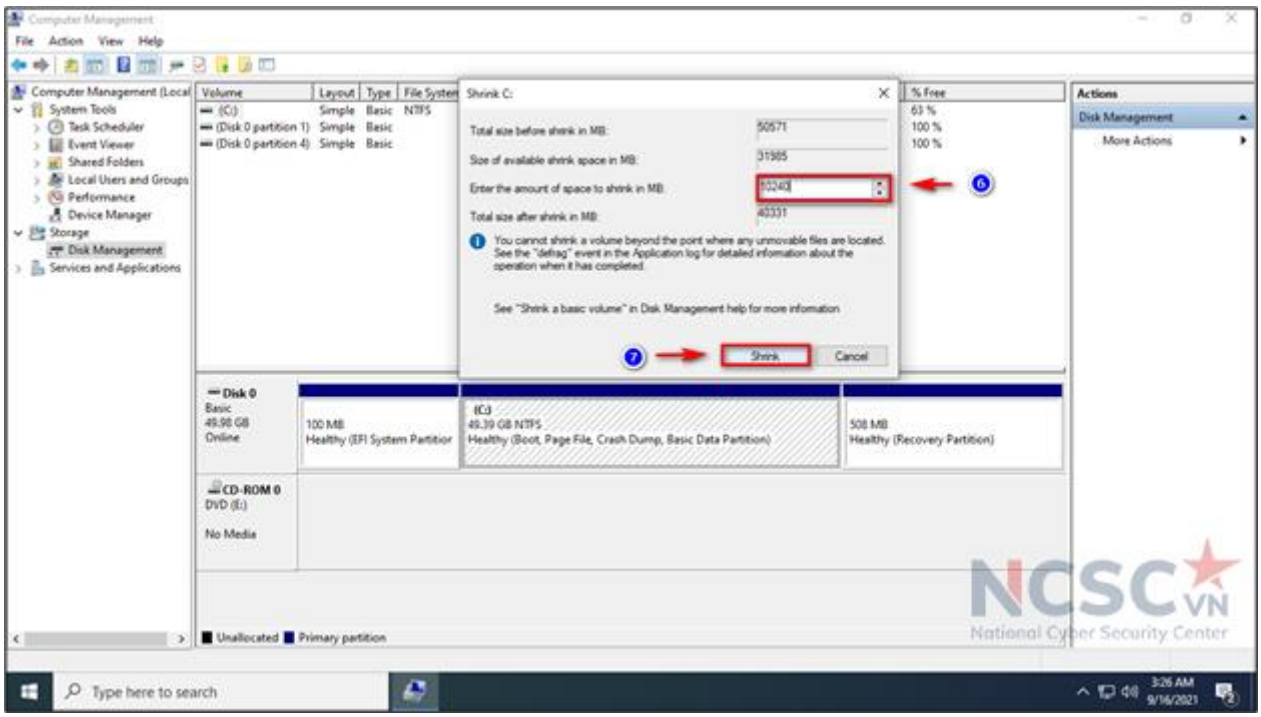


Hình 7: Hướng dẫn phân vùng ổ cứng (2)

Bước 3: Windows sẽ tính toán và hiển thị dung lượng cho phép chia nhỏ, ở bước này người dùng sẽ thấy trong bảng xuất hiện 4 thông số như sau:

- Total size before shrink in MB: tổng dung lượng của ổ, tính theo MB (1024 MB = 1GB).
- Size of available shrink space in MB: dung lượng tối đa cho phép người dùng chia ra.
- Enter the amount of space to shrink in MB: dung lượng người dùng muốn chia ra làm phân vùng mới (chúng ta sẽ gõ số theo đơn vị MB vào đây)
- Total size after shrink in MB: dung lượng còn lại khi chia nhỏ phân vùng.

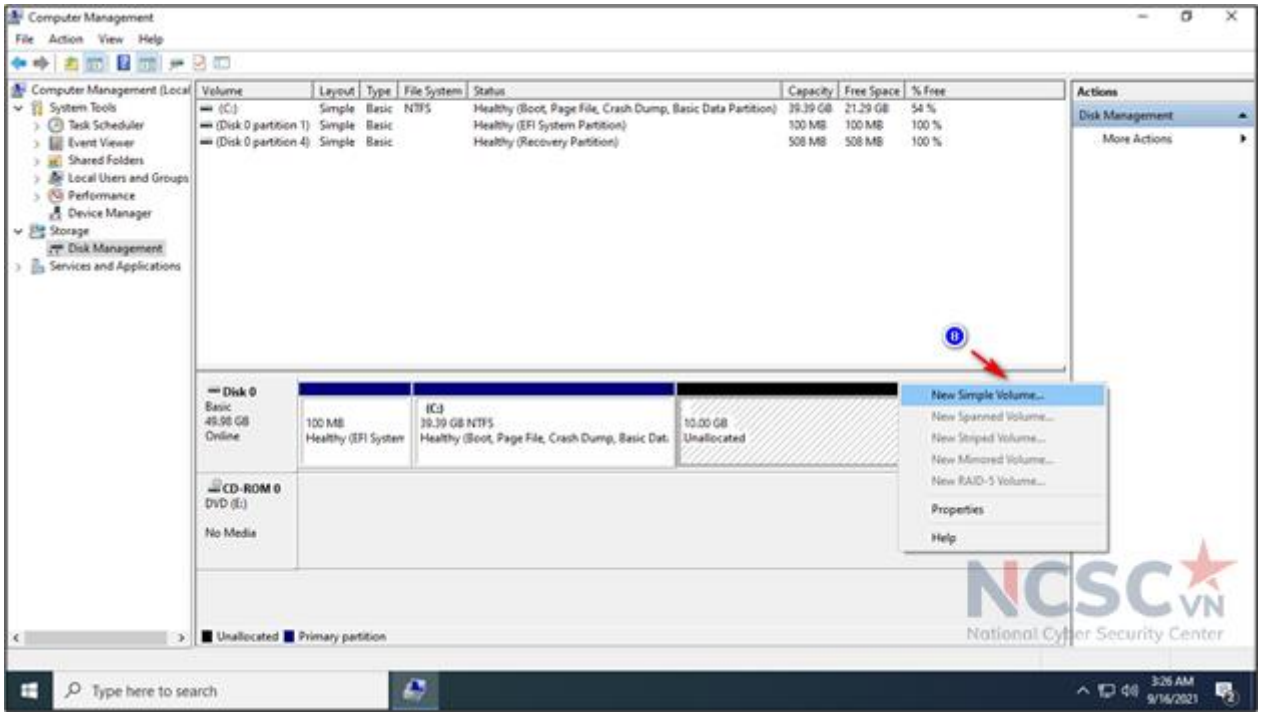
Tại đây người dùng chọn dung lượng cho phân vùng cần chia > bấm Shrink



Hình 8: Hướng dẫn phân vùng ổ cứng (3)

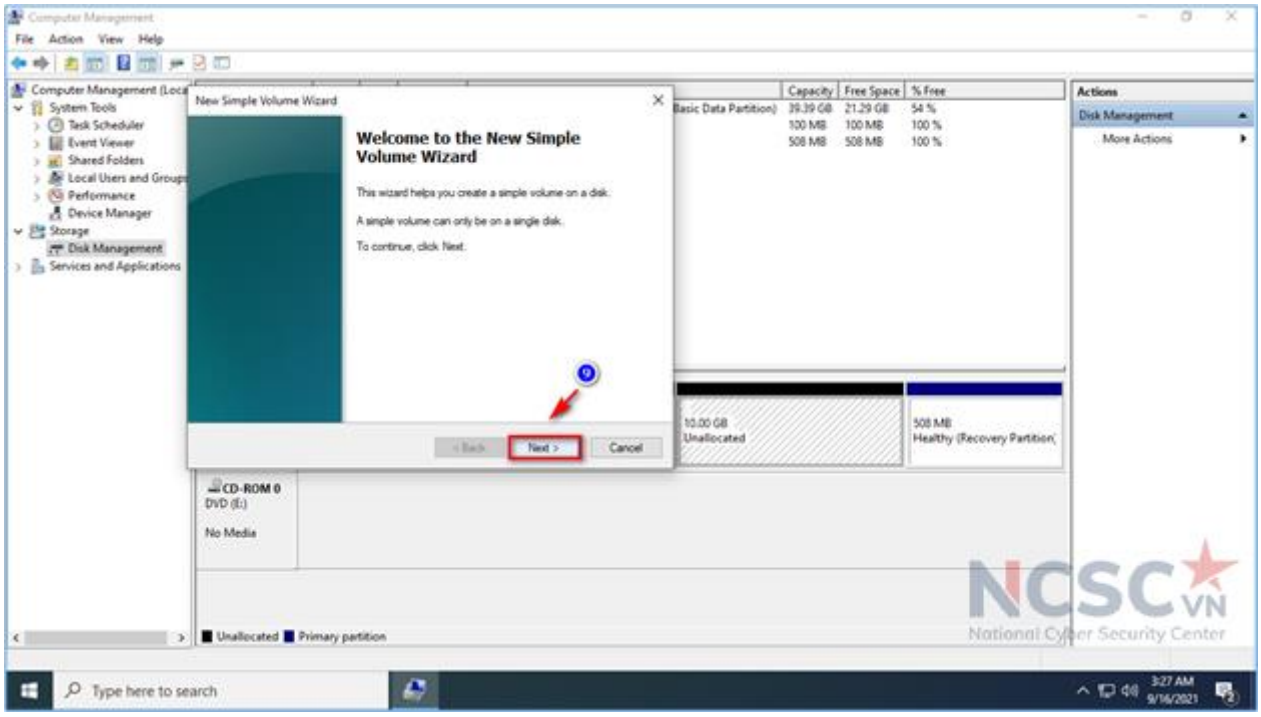
Ví dụ: từ ổ C có dung lượng 49.93 GB, người dùng muốn chia ra một phần vùng mới có dung lương 10 GB, chúng ta sẽ nhập vào mục Enter the amount of space to shrink in MB: 10240 MB ~ 10 GB (1024 MB = 1GB).

Bước 4: phân vùng mới sau khi được chia sẽ có màu đen vì nó chưa được định dạng (format), để sử dụng được phân vùng mới này, chúng ta cần format lại phân vùng đó. Nhấn chuột phải vào vùng đen đó > chọn New Simple Volume



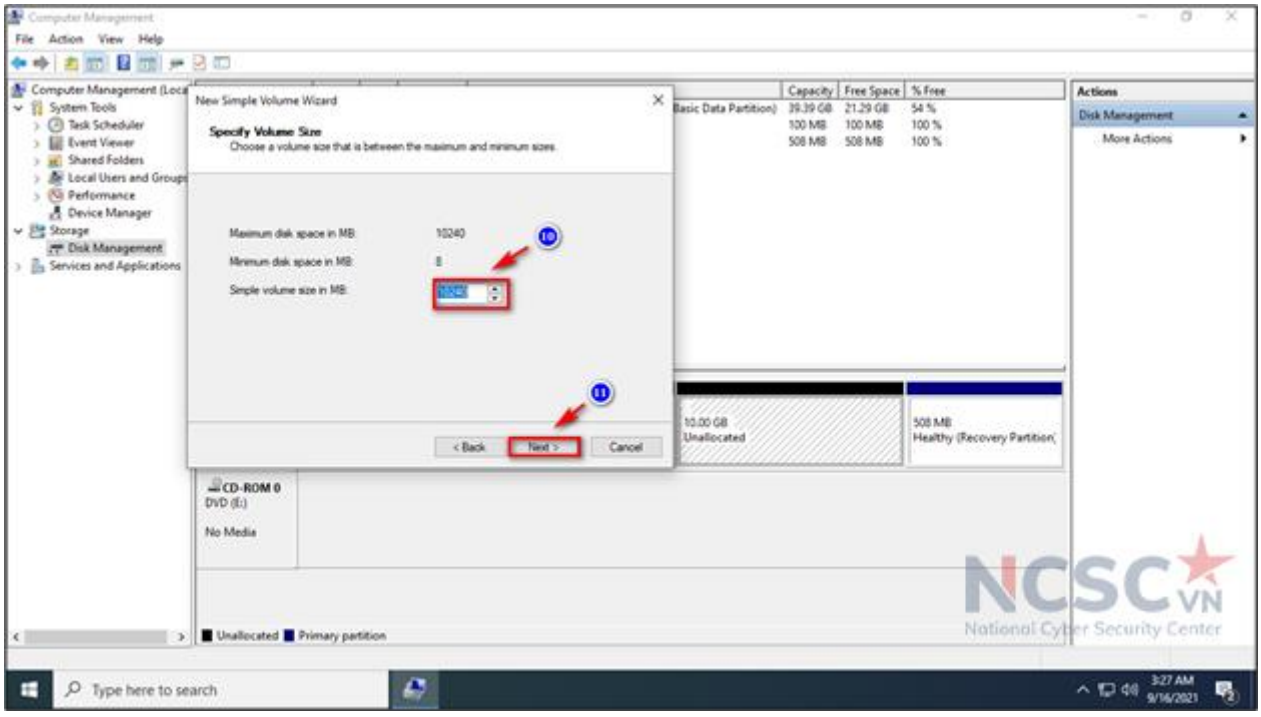
Hình 9: Hướng dẫn phân vùng ổ cứng (4)

Bước 5: Một cửa sổ mới hiện lên, chọn Next.



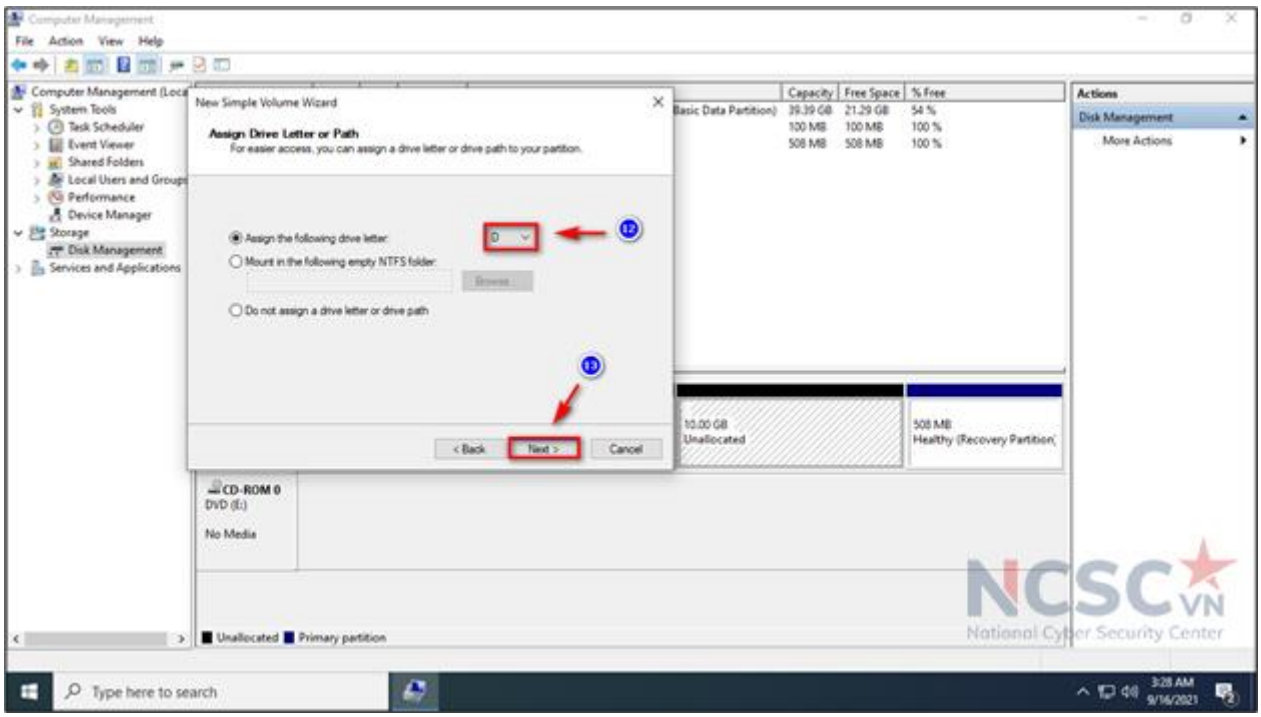
Hình 10: Hướng dẫn phân vùng ổ cứng (5)

Bước 6: Chọn dung lượng cho ổ cần chia, mặc định sẽ là dung lượng tối đa > Next để tiếp tục.



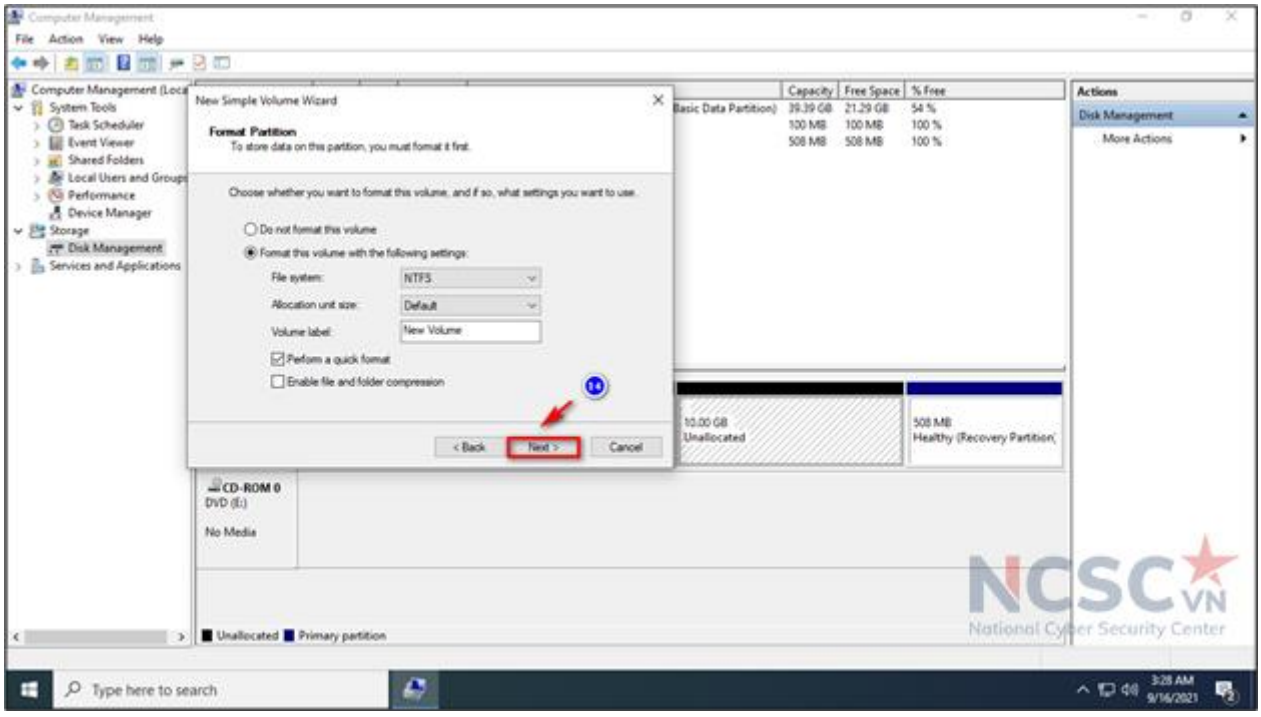
Hình 11: Hướng dẫn phân vùng ổ cứng (6)

Bước 7: Chọn tên ổ, người dùng có thể chọn A, B, C, D ... tùy theo nhu cầu. Tên ổ sẽ không được trùng so với các ổ khác đang tồn tại trên máy tính.



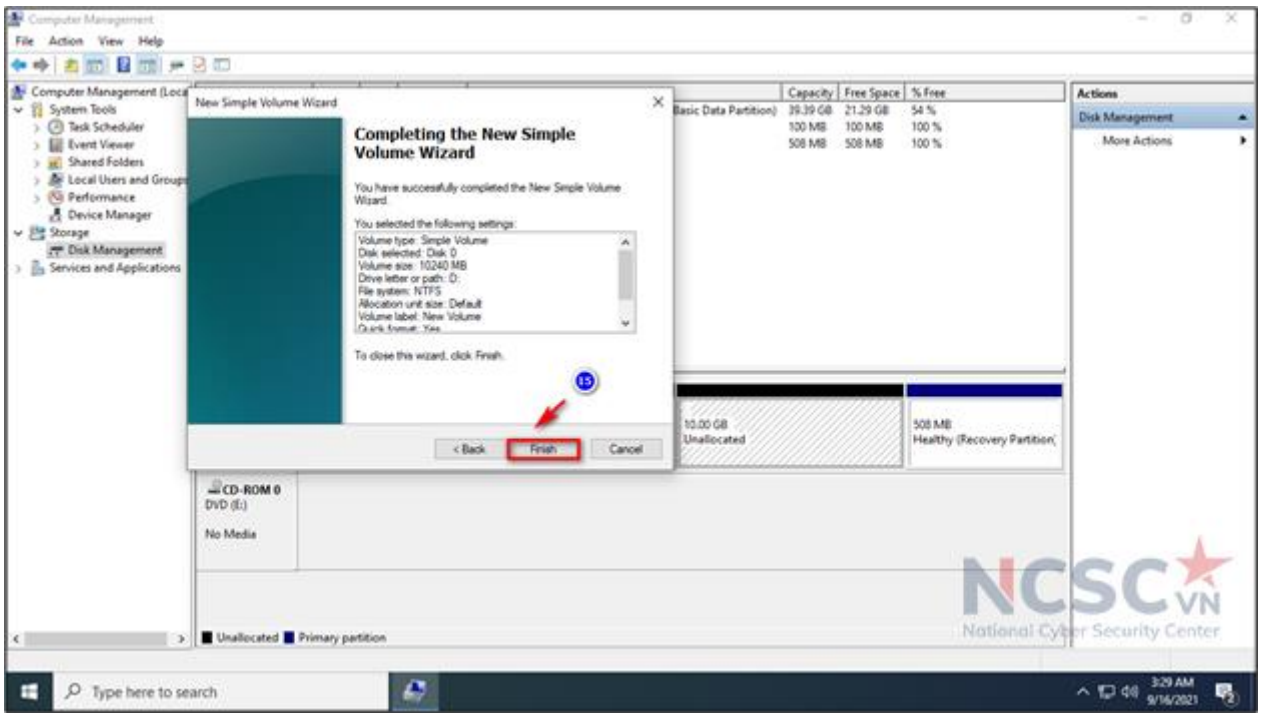
Hình 12: Hướng dẫn phân vùng ổ cứng (7)

Bước 8: Chọn vào Format this volume with ... > Chọn Perfom a quick format > Nhấn Next để xác nhận phân vùng lại ổ vừa tạo.



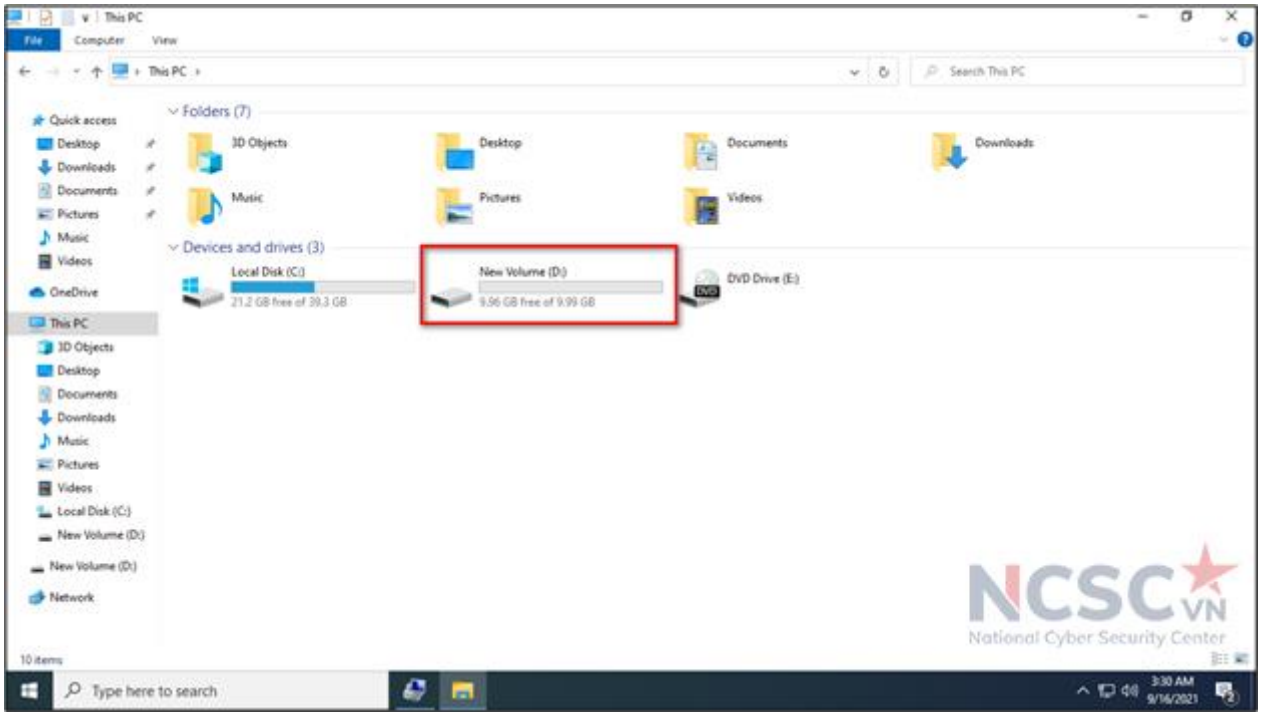
Hình 13: Hướng dẫn phân vùng ổ cứng (8)

Bước 9: Nhấn Finish để hoàn tất quá trình chia, phân vùng ổ cứng.



Hình 14: Hướng dẫn phân vùng ổ cứng (9)

Quá trình phân vùng ổ cứng thành công, ta sẽ thấy một ổ mới được tạo ra.



Hình 15: Hướng dẫn phân vùng ổ cứng (10)

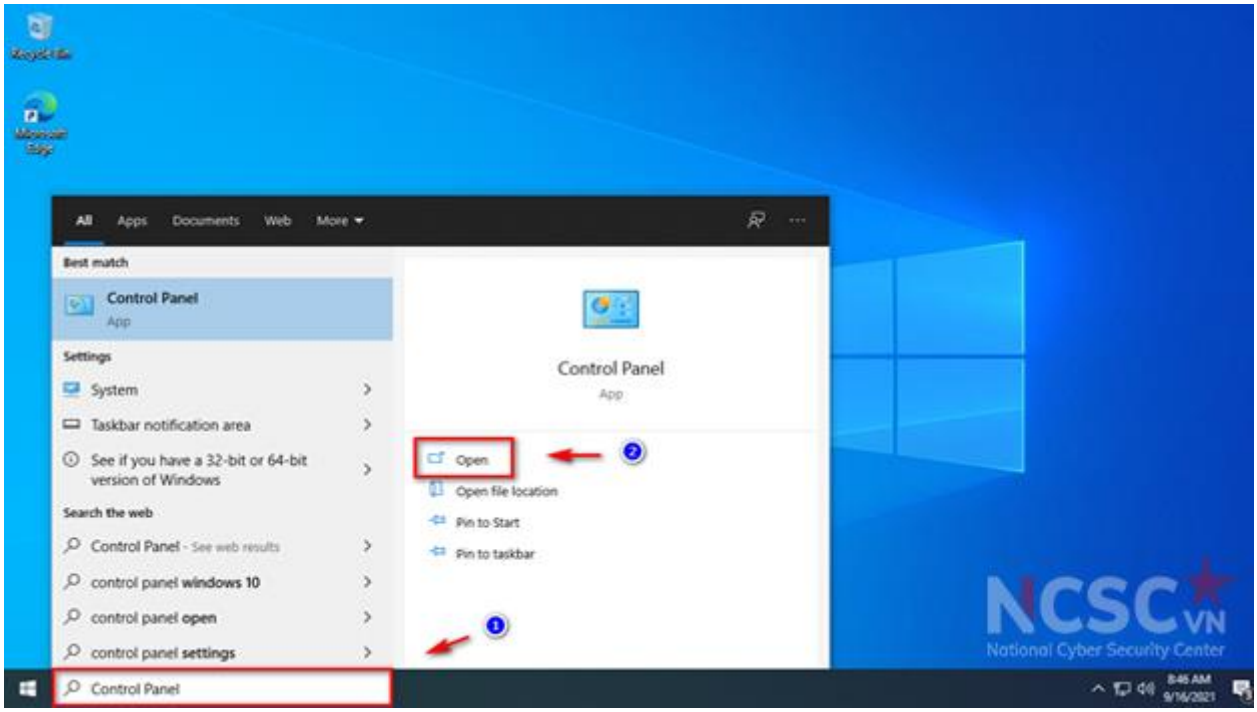
Trong thực tế máy tính người dùng có dung lượng ổ cứng hoàn toàn khác nhau có loại 128 GB, 256 GB, 500 GB, hay 1TB, 2TB. Do vậy trong quá trình phân vùng ổ cứng người dùng cân nhắc chia ổ cứng tùy theo nhu cầu sử dụng của bản thân. Dưới đây là khuyến nghị người dùng có thể tham khảo.

Phân vùng	Dung lượng khuyến nghị	Định dạng phân vùng	Ghi chú
C:\	100GB	NTFS	Phân vùng chứa hệ điều hành, profiles và các ứng dụng cài đặt của hệ thống
D:\	Tùy chỉnh theo nhu cầu sử dụng	NTFS	Chứa data, backup các ứng dụng, các dữ liệu khác

1.1.2. Sử dụng BitLocker để mã hóa dữ liệu

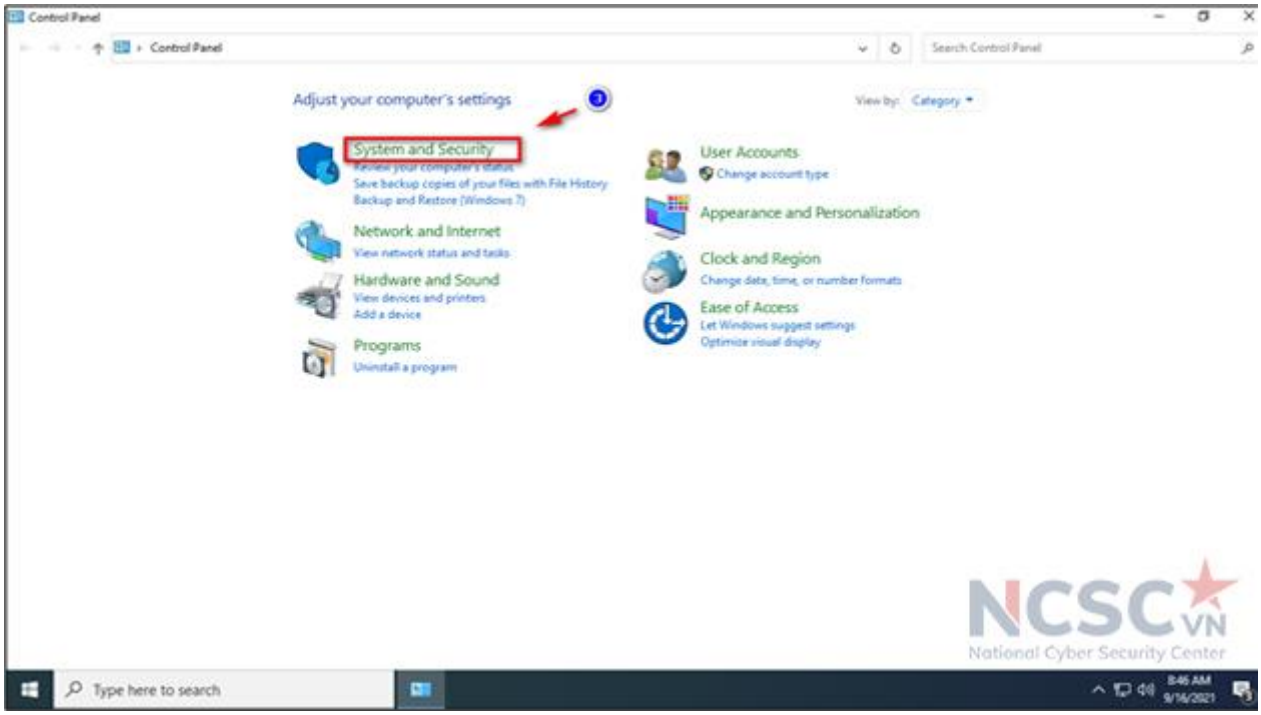
BitLocker là công cụ bảo mật giúp mã hóa ổ cứng rất hữu hiệu được Microsoft tích hợp sẵn trên hệ điều hành Windows 10. Phần này sẽ hướng dẫn người dùng mã hóa dữ liệu ổ cứng của họ bằng công cụ BitLocker, điều này giúp ngăn chặn dữ liệu quan trọng trên máy tính của người dùng có thể bị rơi vào những tay kẻ xấu khi bị mất máy tính hoặc bị đánh cắp.

Bước 1: Vào mục tìm kiếm trên Windows > nhập Control Panel và chọn Open.



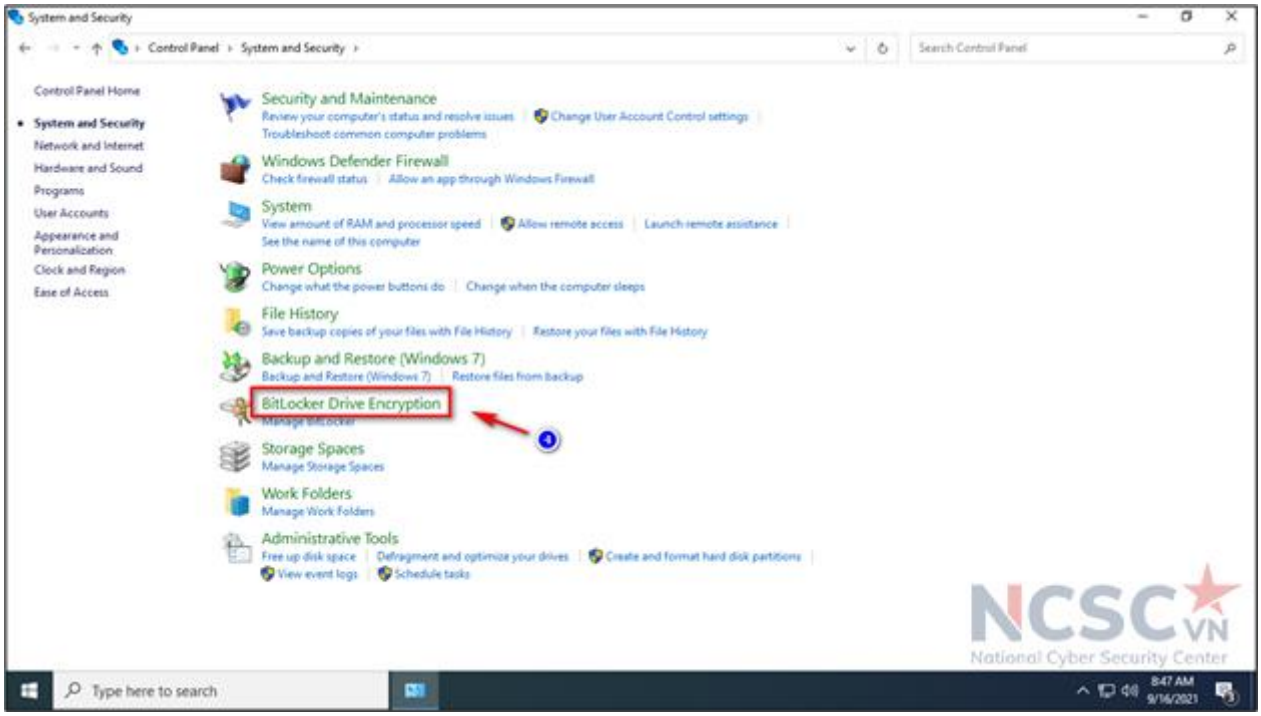
Hình 16: Mã hóa dữ liệu trên Windows 10 (1)

Bước 2: Nhấn vào System and Security.



Hình 17: Mã hóa dữ liệu trên Windows 10 (2)

Bước 3: Chọn BitLocker Drive Encryption.



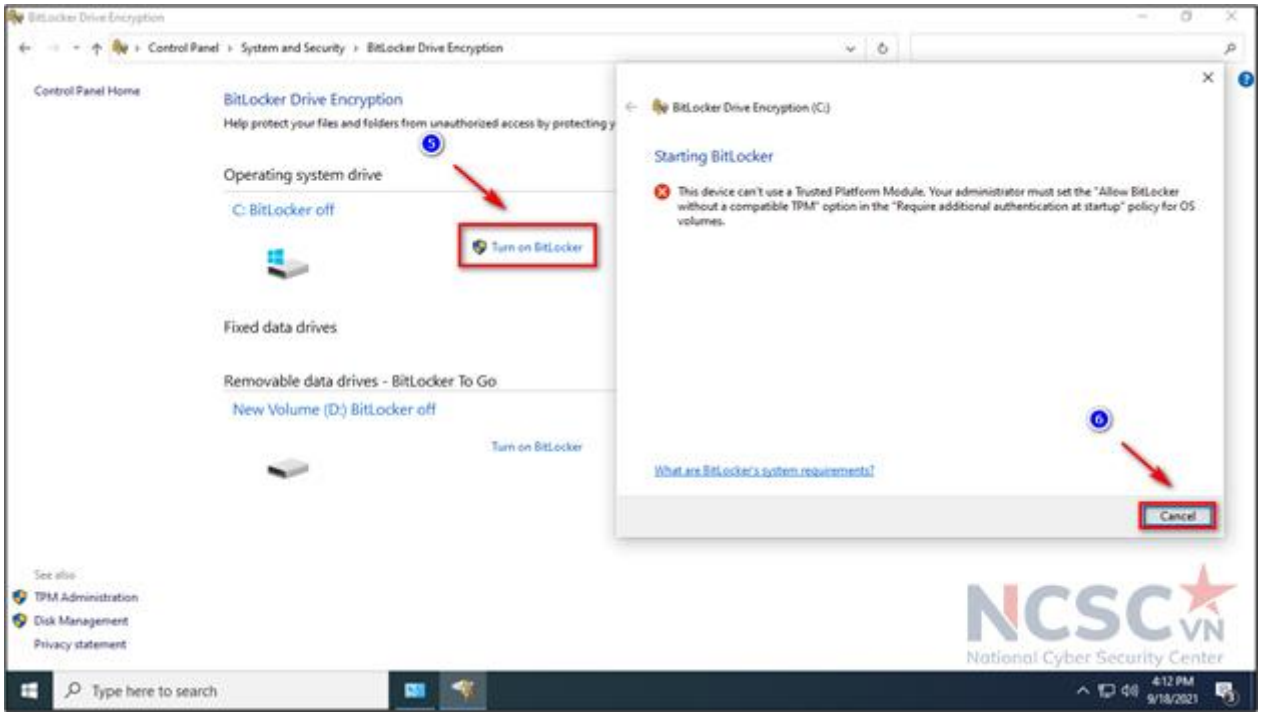
Hình 18: Mã hóa dữ liệu trên Windows 10 (3)

Lưu ý: Kể từ bước này, chúng ta sẽ phân làm hai phần để mã hóa cho từng ổ cứng:
Phần 1: mã hóa cho ổ C – yêu cầu máy phải có chip bảo mật TPM
Phần 2: mã hóa cho ổ D – không yêu cầu máy phải có chip bảo mật TPM
Người dùng có thể cân nhắc lựa chọn một trong hai phần để thực hiện theo, phù

hợp với nhu cầu sử dụng của từng người.

Phần 1: Mã hóa cho ổ C – yêu cầu máy phải có chip bảo mật TPM

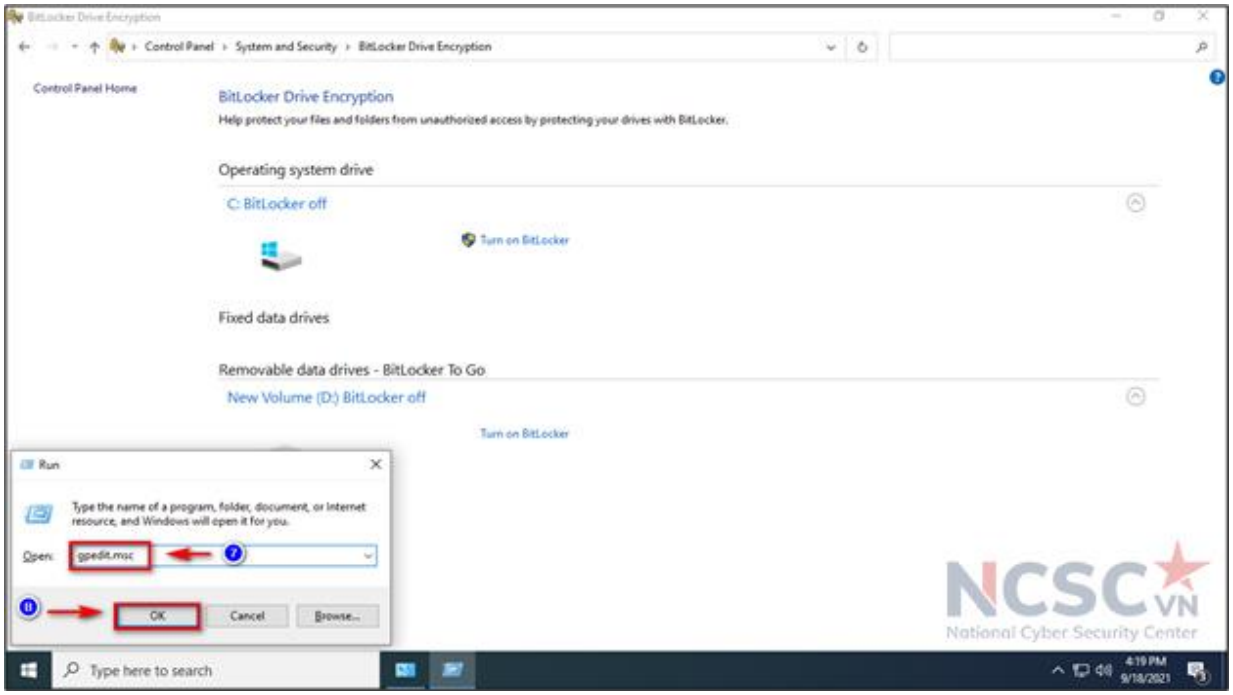
Bước 4: Trong BitLocker Drive Encryption, chọn phân vùng ổ C bấm Turn on BitLocker.



Hình 19: Mã hóa dữ liệu trên Windows 10 (4)

- Nếu người dùng không gặp thông báo như trên: chứng tỏ máy đã có tích hợp chip bảo mật TPM có thể bỏ qua bước 4 này.
- Còn nếu trường hợp người dùng gặp thông báo như trên: làm tiếp các bước phụ sau đây để kích hoạt BitLocker trên máy tính không hỗ trợ TPM.

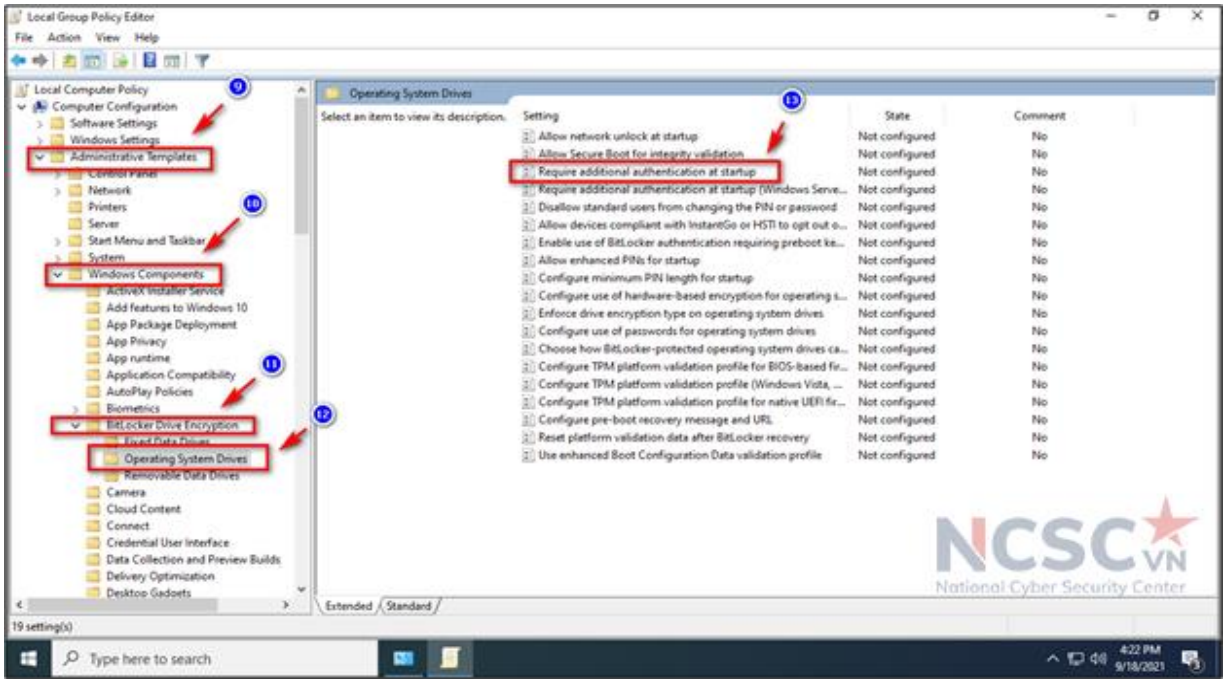
Bước 4.1: Nhấn tổ hợp phím Windows + R để mở hộp thoại Run sau đó nhập lệnh gpedit.msc và nhấn OK.



Hình 20: Mã hóa dữ liệu trên Windows 10 (5)

Bước 4.2: Cửa sổ Local Group Policy Editor hiện lên, người dùng thực hiện theo các bước chi tiết như sau:

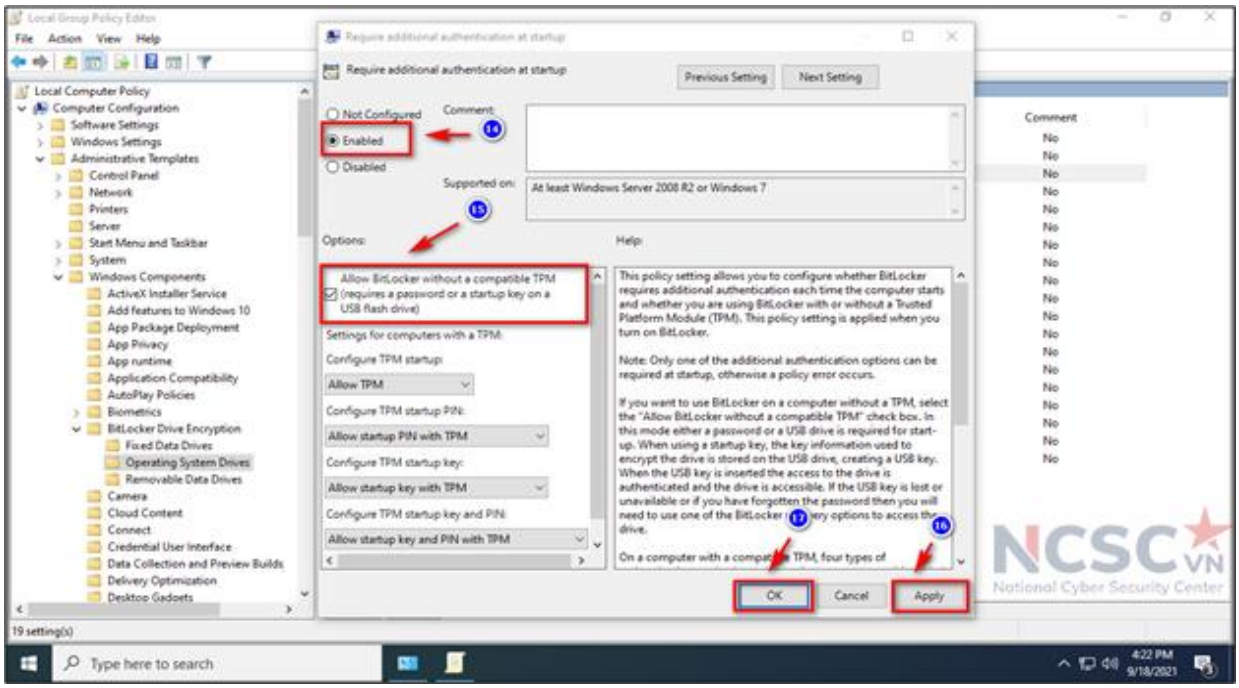
Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives



Hình 21: Mã hóa dữ liệu trên Windows 10 (6)

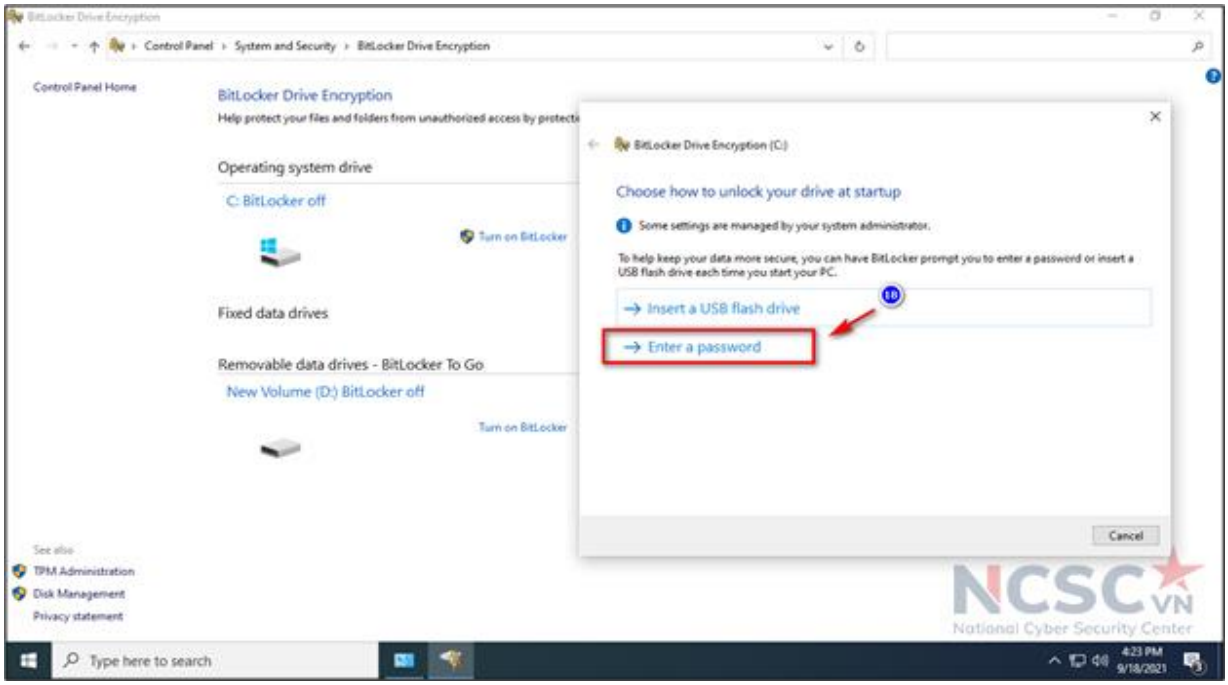
Sau đó ở cửa sổ hiện tại người dùng kích đúp vào dòng Require additional

authentication at startup. Trong cửa số mới 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.



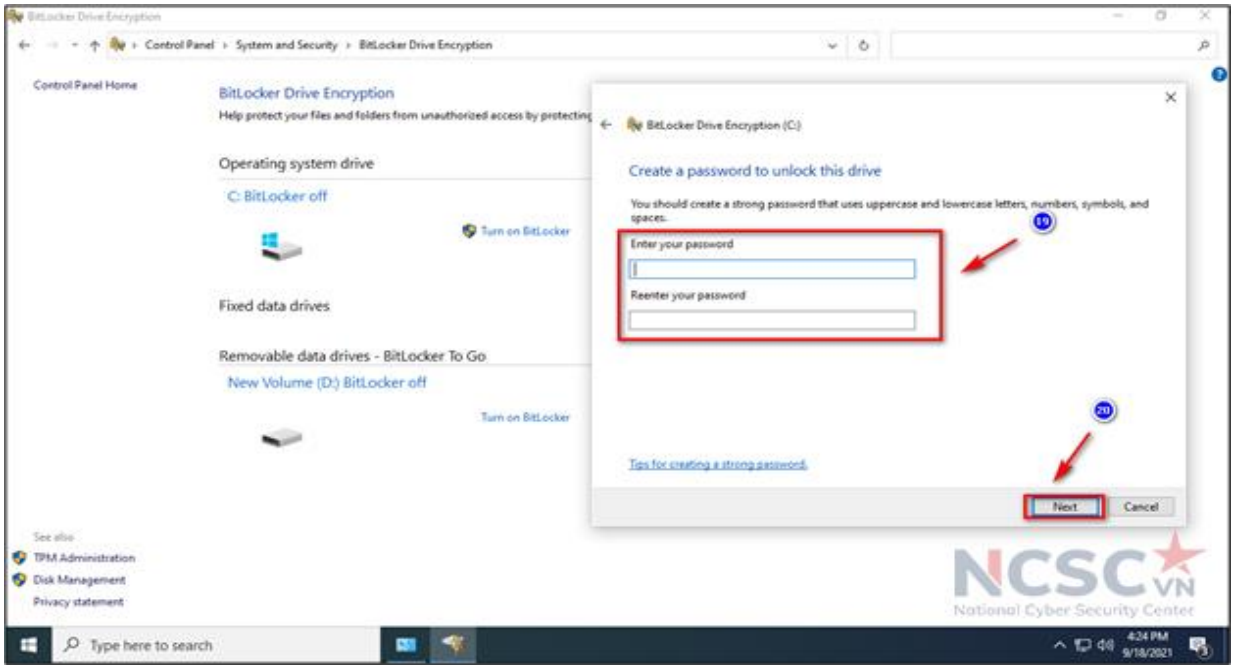
Hình 22: Mã hóa dữ liệu trên Windows 10 (7)

Bước 5: Nhấn chọn Enter a password



Hình 23: Mã hóa dữ liệu trên Windows 10 (8)

Bước 6: Nhập mật khẩu sẽ sử dụng mỗi khi người dùng khởi động Windows để mở khóa ổ cứng và nhấp vào Next để tiếp tục (đảm bảo tạo mật khẩu mạnh bao gồm chữ hoa, chữ thường, số và ký hiệu)

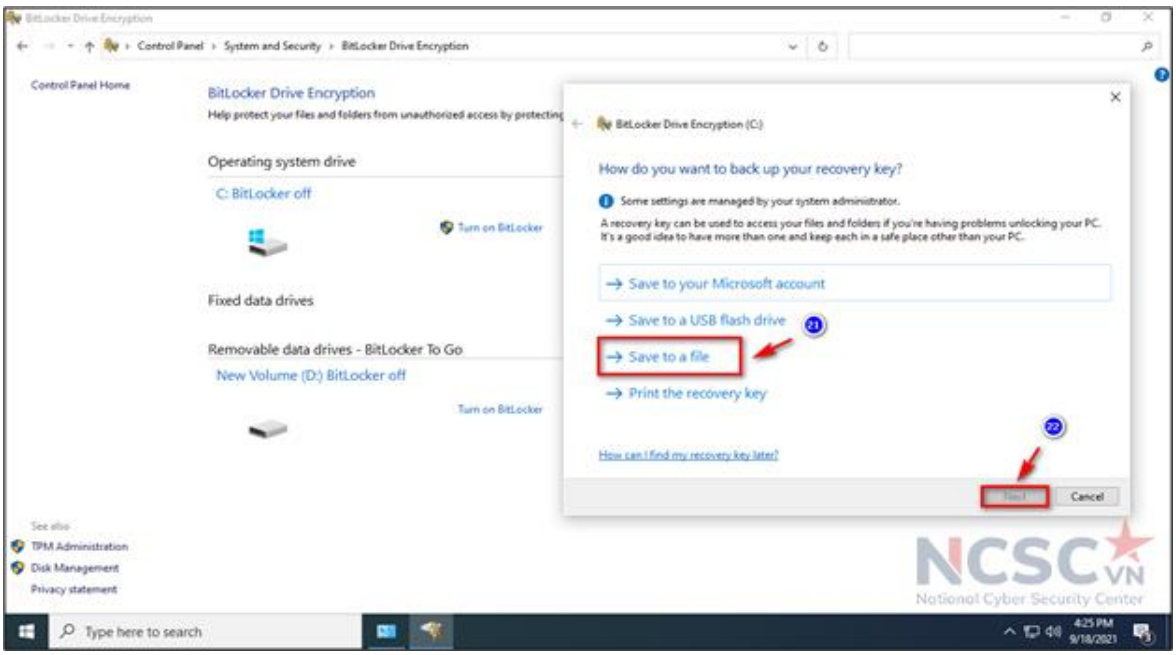


Hình 24: Mã hóa dữ liệu trên Windows 10 (9)

Bước 7: Người dùng sẽ được cung cấp các lựa chọn để lưu khóa (key) khôi phục trong trường hợp quên mật khẩu. Nếu người dùng quên mật khẩu thì khóa khôi phục là chìa khóa duy nhất để có thể mở được dữ liệu. Nếu mất cả 2 thì sẽ mất dữ liệu vĩnh viễn.

- Save to your Microsoft account (Lưu vào tài khoản Microsoft)
- Save to a USB flash drive (Lưu vào thiết bị kết nối ngoài USB, ổ cứng di động)
- Save to a file (Tạo file lưu)
- Print the recovery key (In khóa khôi phục)

Lưu ý: Khuyến nghị nên lựa chọn Save to a file, mật khẩu sẽ được lưu dưới dạng file .txt. Người dùng chọn nơi lưu khóa khôi phục, không lưu vào phân vùng đang mã hóa bitlocker. Vì khi quên mật khẩu mở bitlocker thì việc truy cập vào phân vùng đó để lấy khóa khôi phục là không thể. Để an toàn hơn có thể lưu 1 bản khóa khôi phục file .txt lên Google Drive, Onedrive ... xong bấm Next để tiếp tục

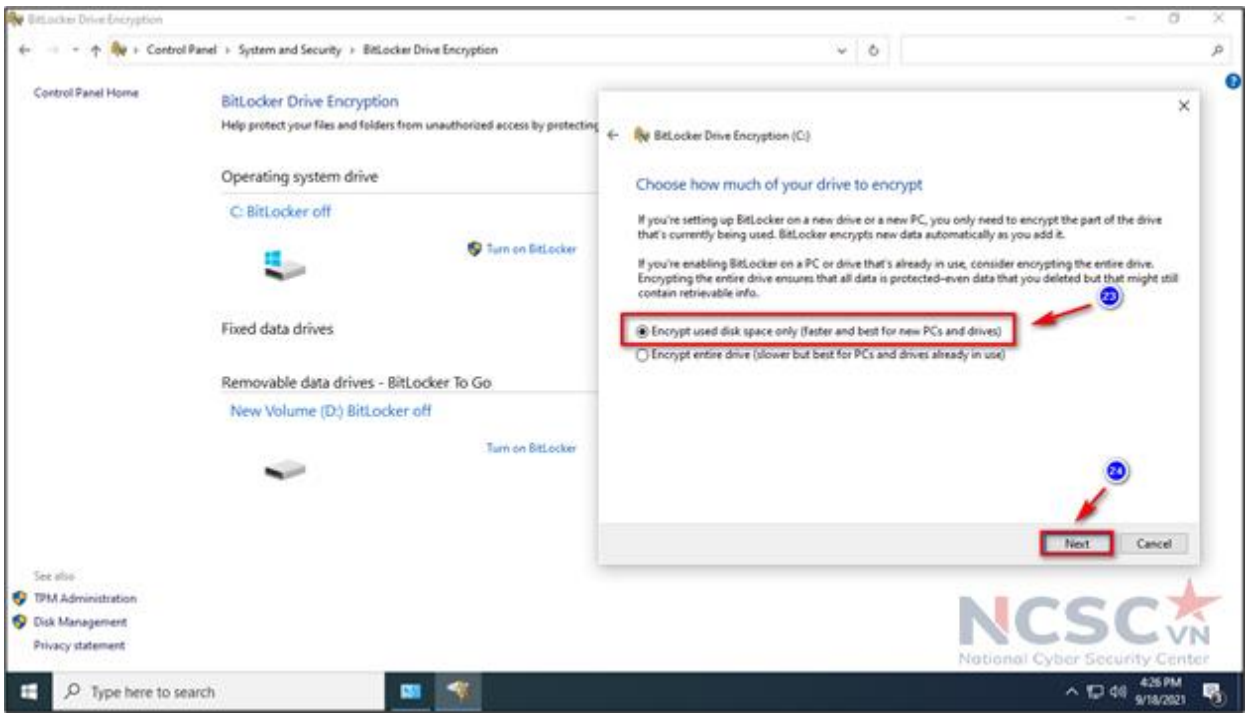


Hình 25: Mã hóa dữ liệu trên Windows 10 (10)

Bước 8: Tùy chọn kiểu mã hóa phù hợp, xong bấm Next để tiếp tục:

- Encrypt used disk space only (faster and best for new PCs and drives). Có nghĩa chỉ mã hóa dung lượng ổ cứng đã sử dụng (nhanh hơn và phù hợp cho ổ cứng mới)

- Encrypt entire drive (slower but best for PCs and drives already in use). Có nghĩa là mã hóa toàn bộ ổ cứng (chậm hơn nhưng phù hợp cho ổ cứng đã sử dụng)



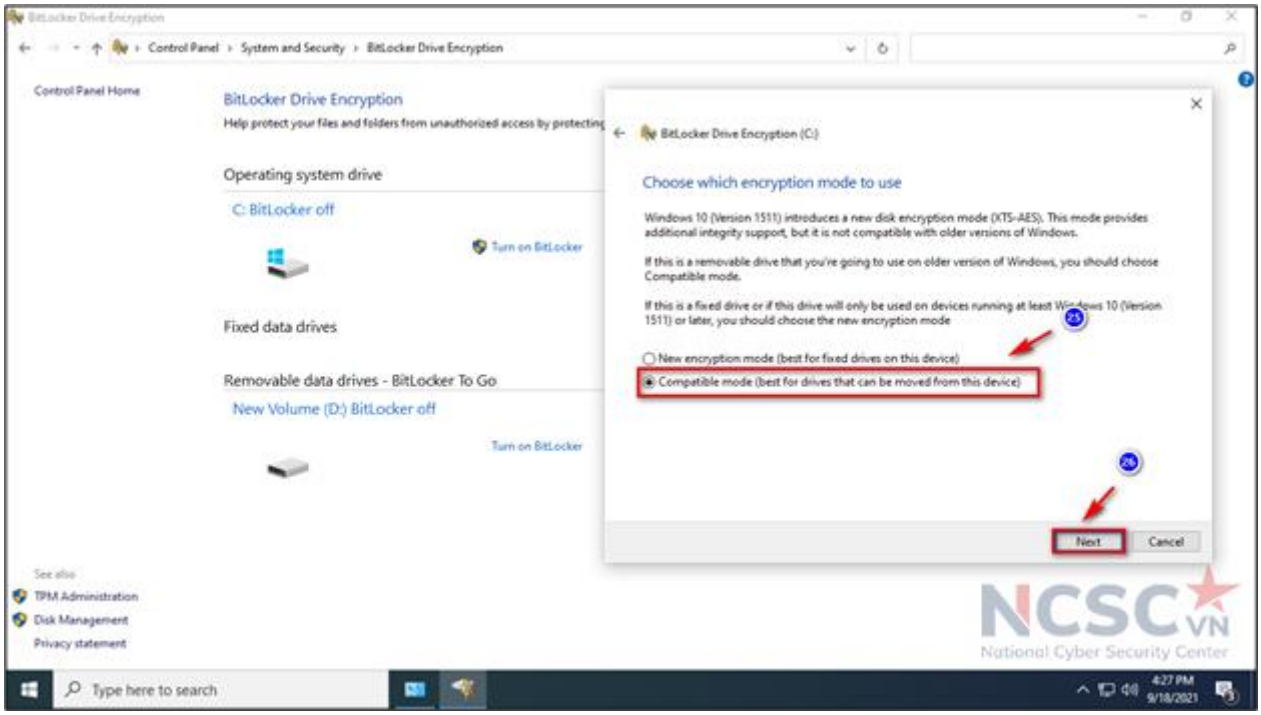
Hình 26: Mã hóa dữ liệu trên Windows 10 (11)

Bước 9: Chọn chế độ mã hóa phù hợp, xong bấm Next để tiếp tục:

- New encryption mode (best for fixed drives on this device) – Chế độ mã hóa mới (phù hợp cho các ổ cứng cố định trên máy tính). Chế độ này an toàn hơn nhưng chỉ hỗ

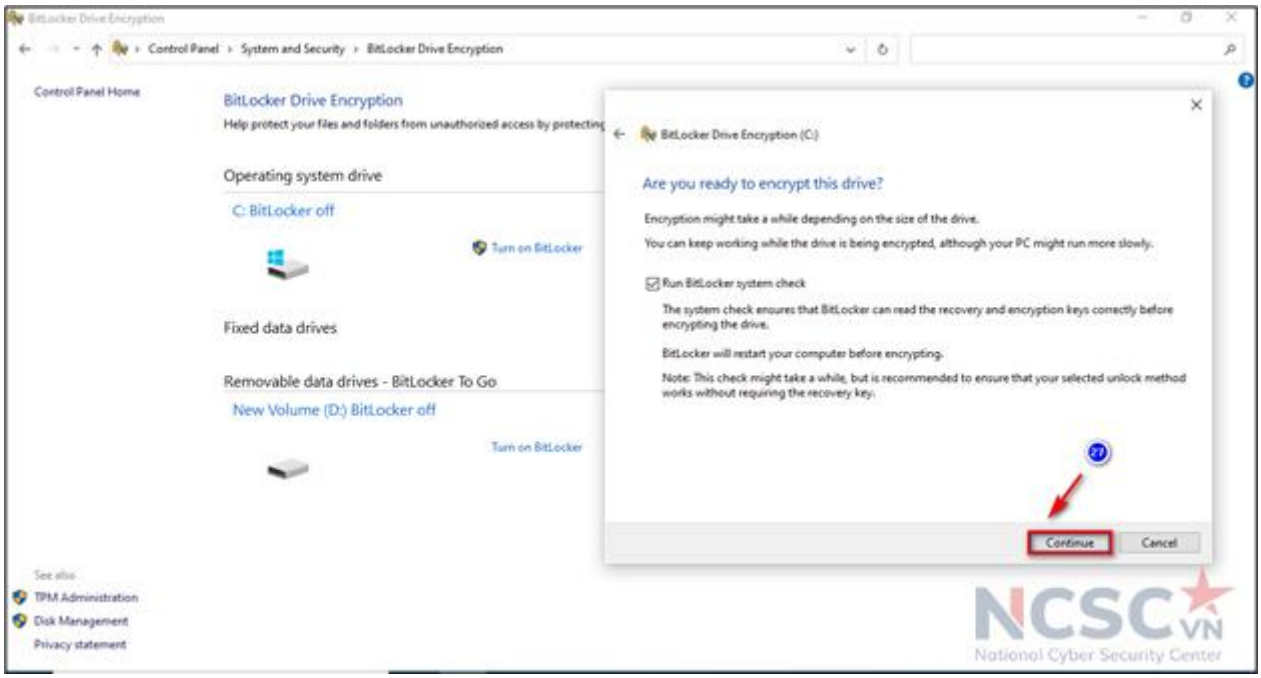
trợ trên Windows 10 phiên bản 1511 trở lên. Nếu các phiên bản Windows cũ hơn thì không hỗ trợ giải mã dữ liệu.

- Compatible mode (best for drives that can be moved from this device) – Chế độ tương thích, phù hợp với ổ cứng kết nối ngoài hoặc không nằm cố định trên máy tính, người dùng có thể chuyển ổ cứng sang máy tính khác để mở.



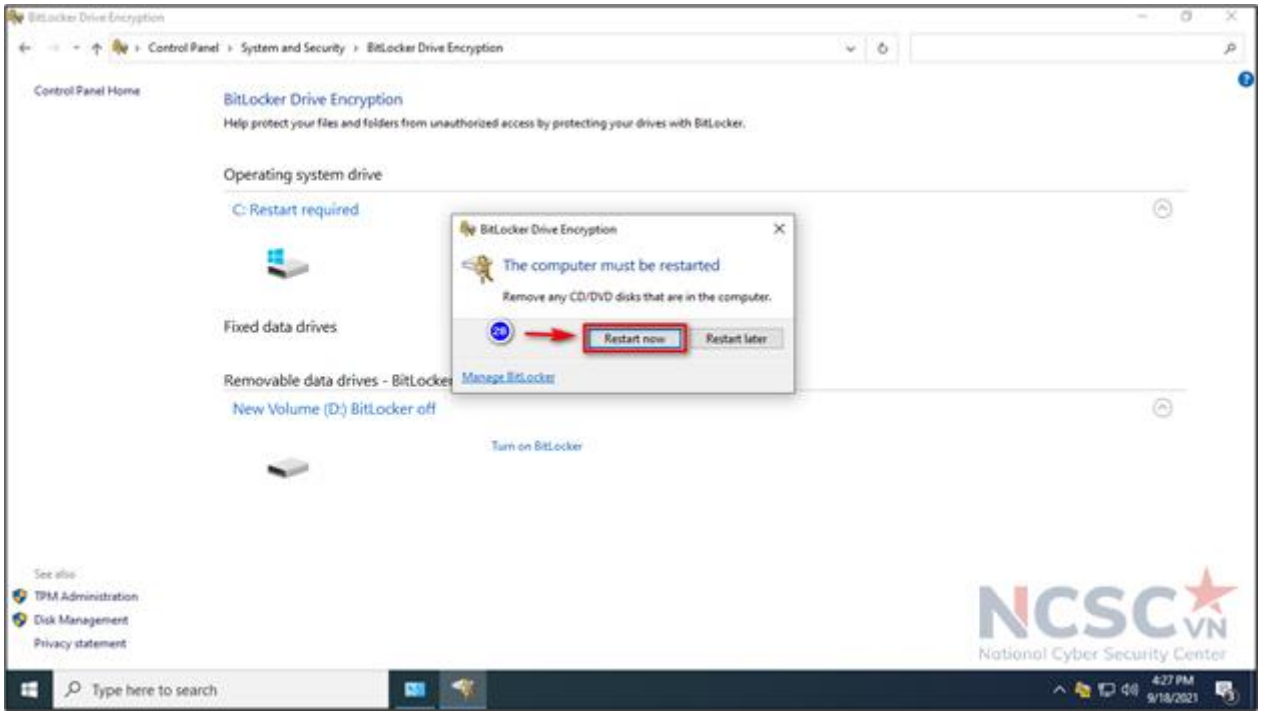
Hình 27: Mã hóa dữ liệu trên Windows 10 (12)

Bước 10: Chọn Continue để tiếp tục



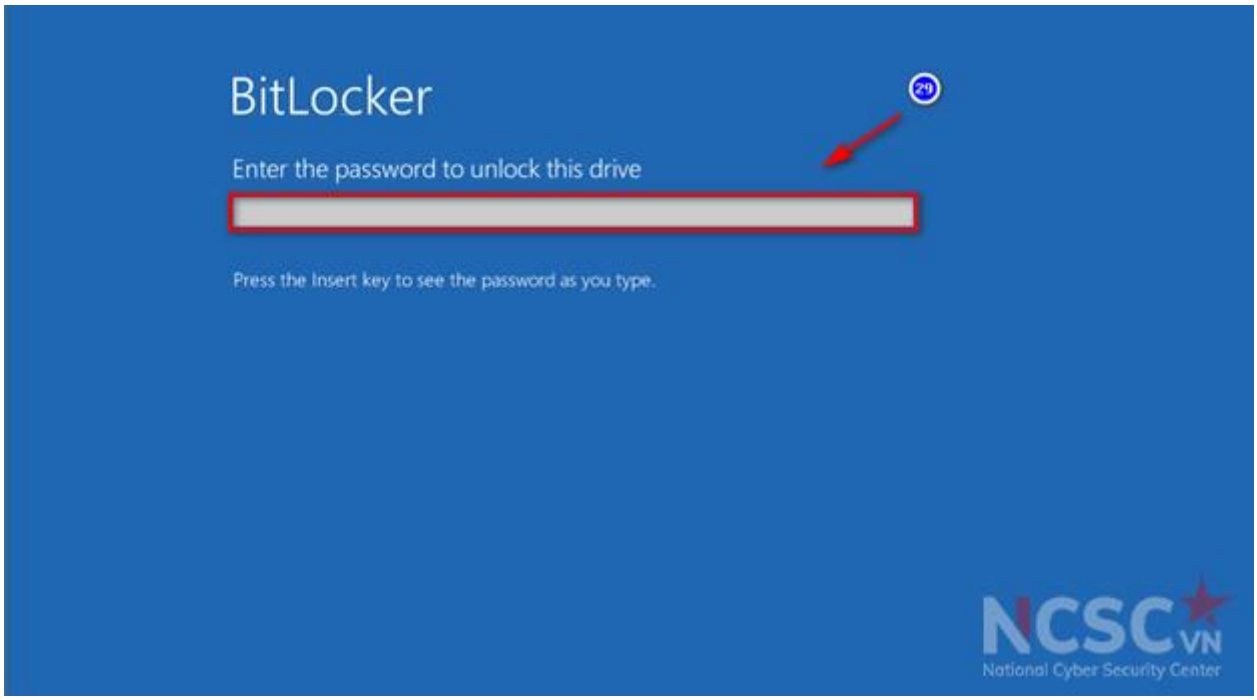
Hình 28: Mã hóa dữ liệu trên Windows 10 (12)

Bước 11: Thông báo khởi động lại máy tính, chọn Restart now để khởi động lại



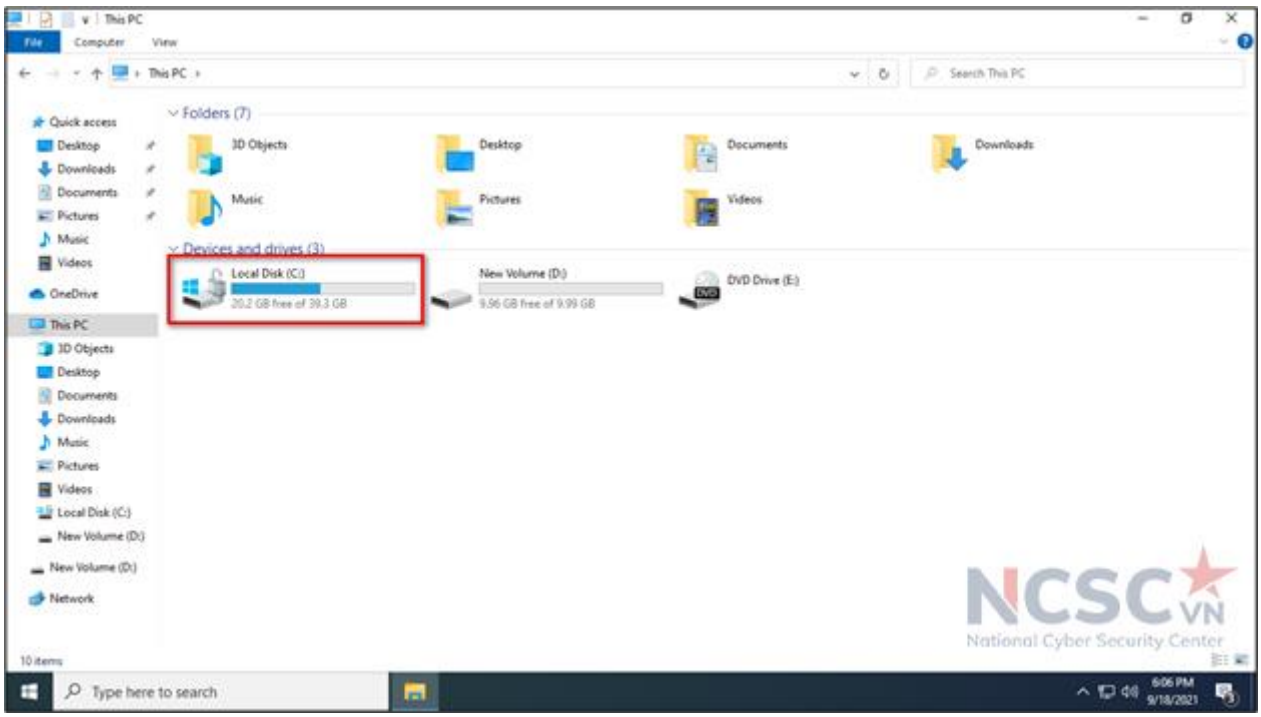
Hình 29: Mã hóa dữ liệu trên Windows 10 (13)

Bước 12: Nhập mật khẩu đã tạo để truy cập



Hình 30: Mã hóa dữ liệu trên Windows 10 (14)

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

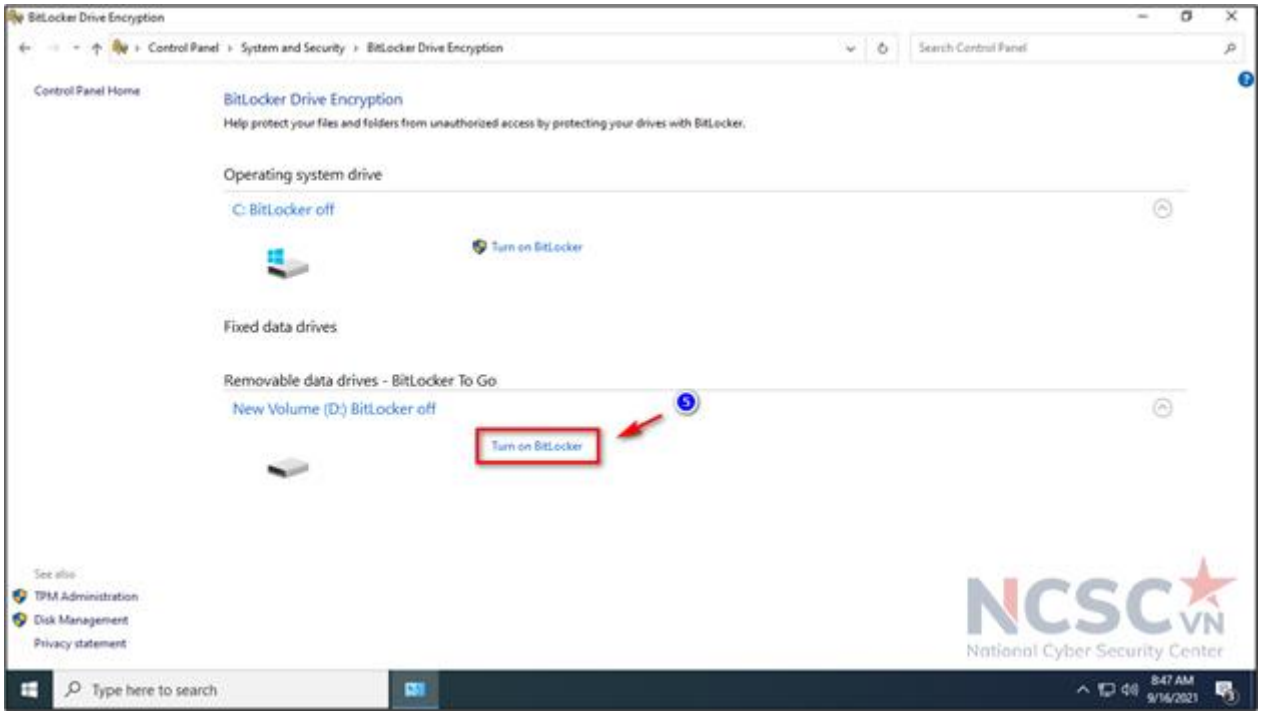


Hình 31: Mã hóa dữ liệu trên Windows 10 (15)

Phần 2: Mã hóa cho ổ D – không yêu cầu máy phải có chip bảo mật TPM

Thực hiện từ Bước 1- đến Bước 3 như hướng dẫn ở trên.

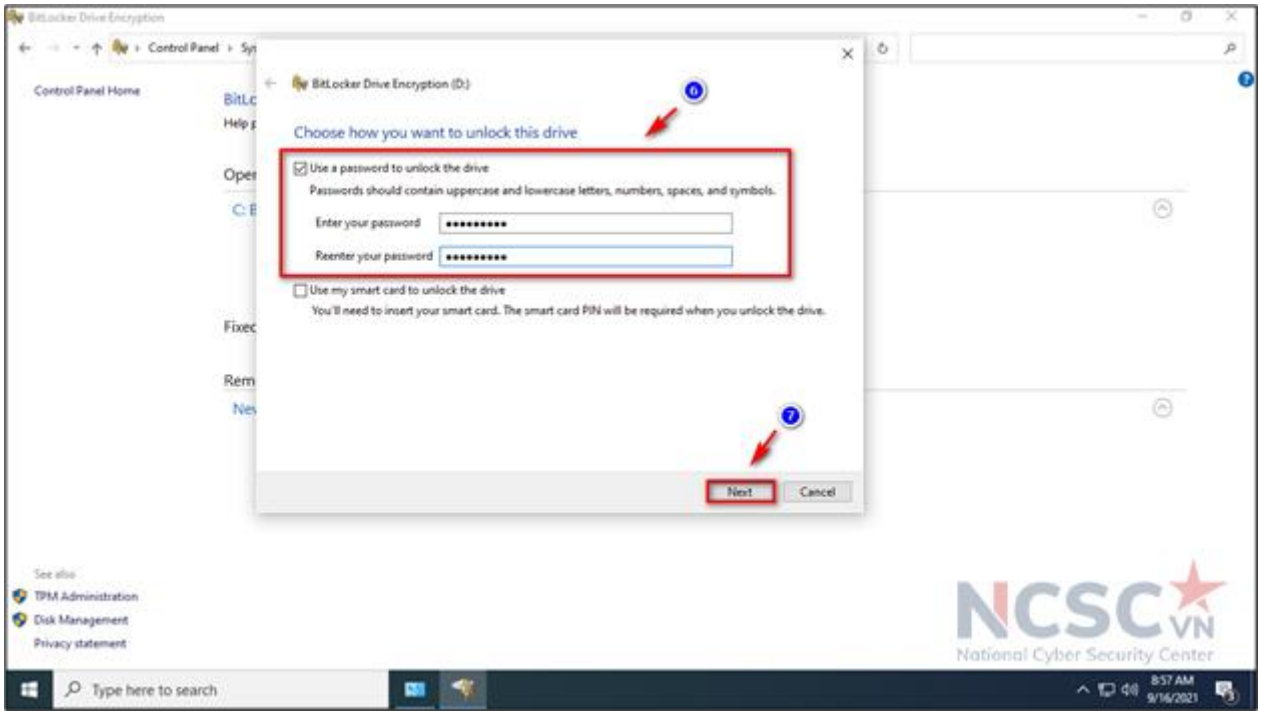
Bước 4: Trong BitLocker Drive Encryption, chọn phân vùng ổ D bấm Turn on BitLocker.



Hình 32: Mã hóa dữ liệu trên Windows 10 (16)

Bước 5: Nhập mật khẩu sẽ sử dụng mỗi khi người dùng khởi động Windows để mở khóa ổ cứng và nhấp vào Next để tiếp tục (đảm bảo tạo mật khẩu mạnh bao gồm

chữ hoa, chữ thường, số và ký hiệu).

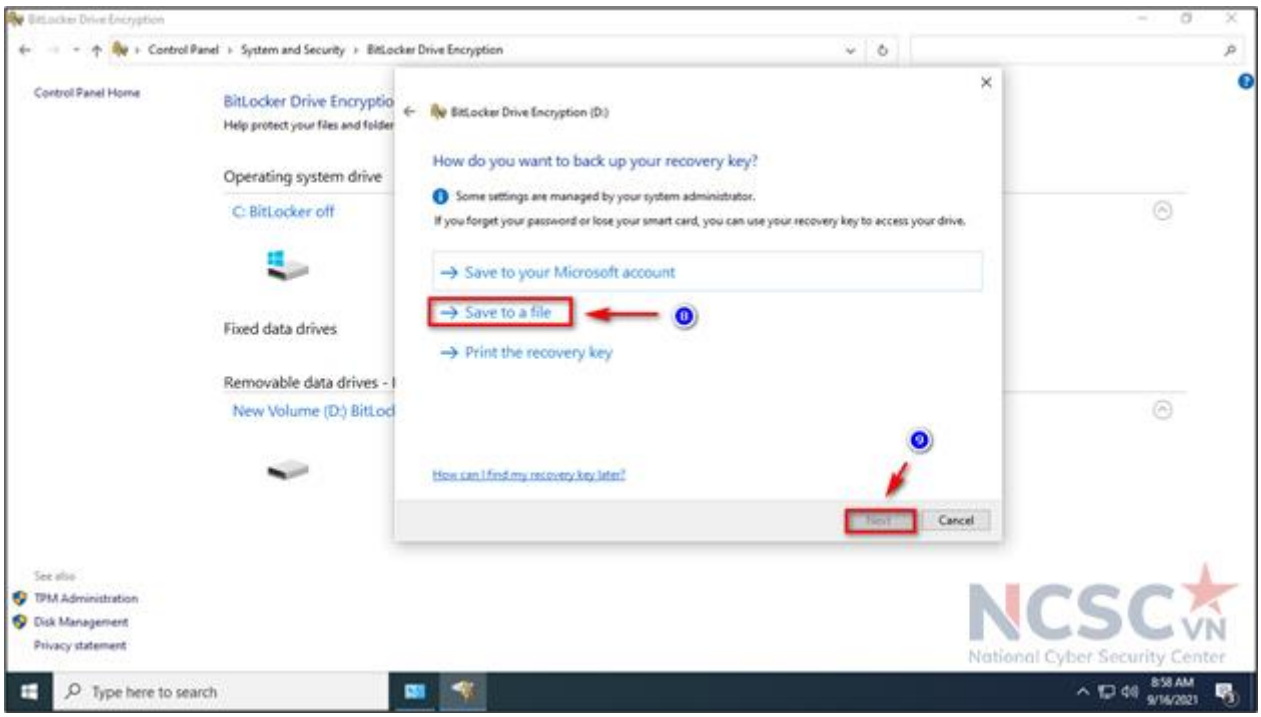


Hình 33: Mã hóa dữ liệu trên Windows 10 (17)

Bước 6: Người dùng sẽ được cung cấp các lựa chọn để lưu khóa (key) khôi phục trong trường hợp quên mật khẩu. Nếu người dùng quên mật khẩu thì khóa khôi phục là chìa khóa duy nhất để có thể mở được dữ liệu. Nếu mất cả 2 thì sẽ mất dữ liệu vĩnh viễn.

- Save to your Microsoft account (Lưu vào tài khoản Microsoft)
- Save to a USB flash drive (Lưu vào thiết bị kết nối ngoài USB, ổ cứng di động)
- Save to a file (Tạo file lưu)
- Print the recovery key (In khóa khôi phục)

Lưu ý: Khuyến nghị nên lựa chọn Save to a file, mật khẩu sẽ được lưu dưới dạng file .txt. Người dùng chọn nơi lưu khóa khôi phục, không lưu vào phân vùng đang mã hóa bitlocker. Vì khi quên mật khẩu mở bitlocker thì việc truy cập vào phân vùng đó để lấy khóa khôi phục là không thể. Để an toàn hơn có thể lưu 1 bản khóa khôi phục file .txt lên Google Drive, Onedrive ... xong bấm Next để tiếp tục

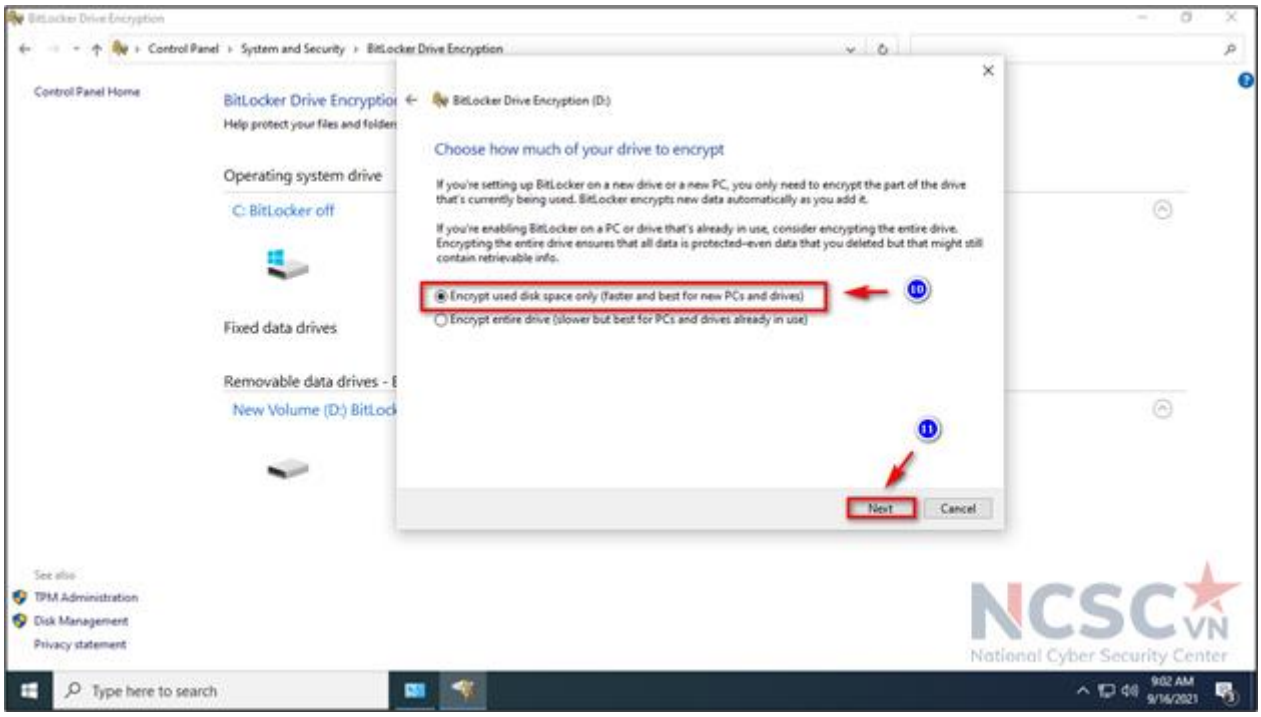


Hình 34: Mã hóa dữ liệu trên Windows 10 (18)

Bước 7: Tùy chọn kiểu mã hóa phù hợp, xong bấm Next để tiếp tục:

- Encrypt used disk space only (faster and best for new PCs and drives). Có nghĩa chỉ mã hóa dung lượng ổ cứng đã sử dụng (nhanh hơn và phù hợp cho ổ cứng mới)

- Encrypt entire drive (slower but best for PCs and drives already in use). Có nghĩa là mã hóa toàn bộ ổ cứng (chậm hơn nhưng phù hợp cho ổ cứng đã sử dụng)

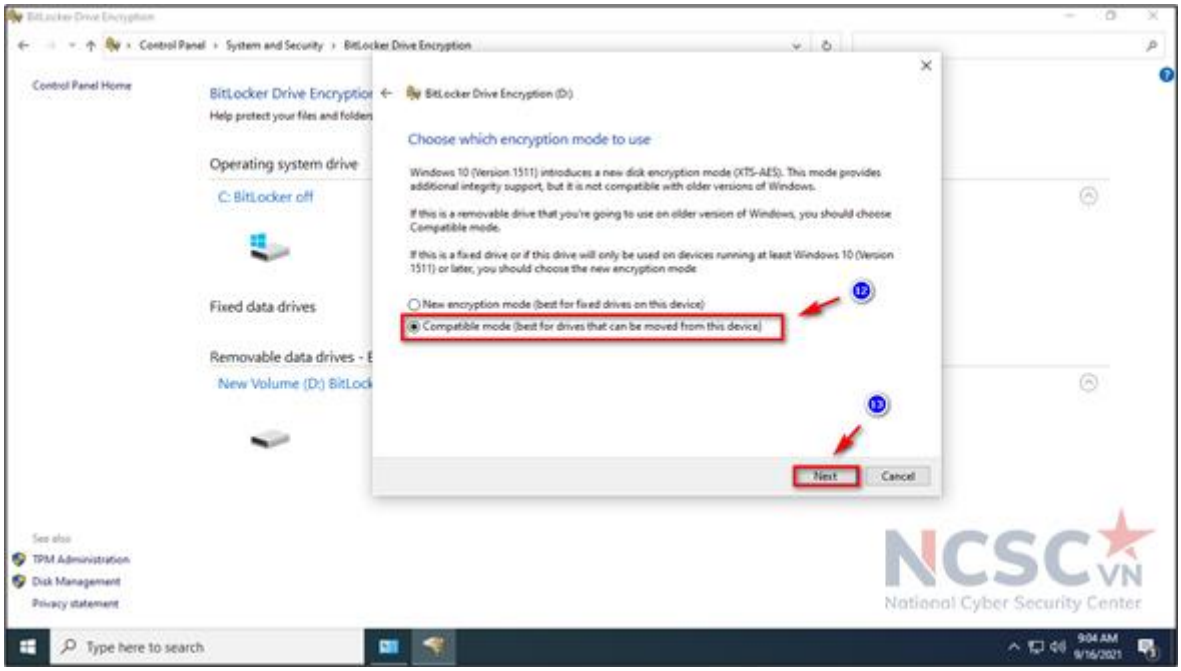


Hình 35: Mã hóa dữ liệu trên Windows 10 (19)

Bước 8: Chọn chế độ mã hóa phù hợp, xong bấm Next để tiếp tục:

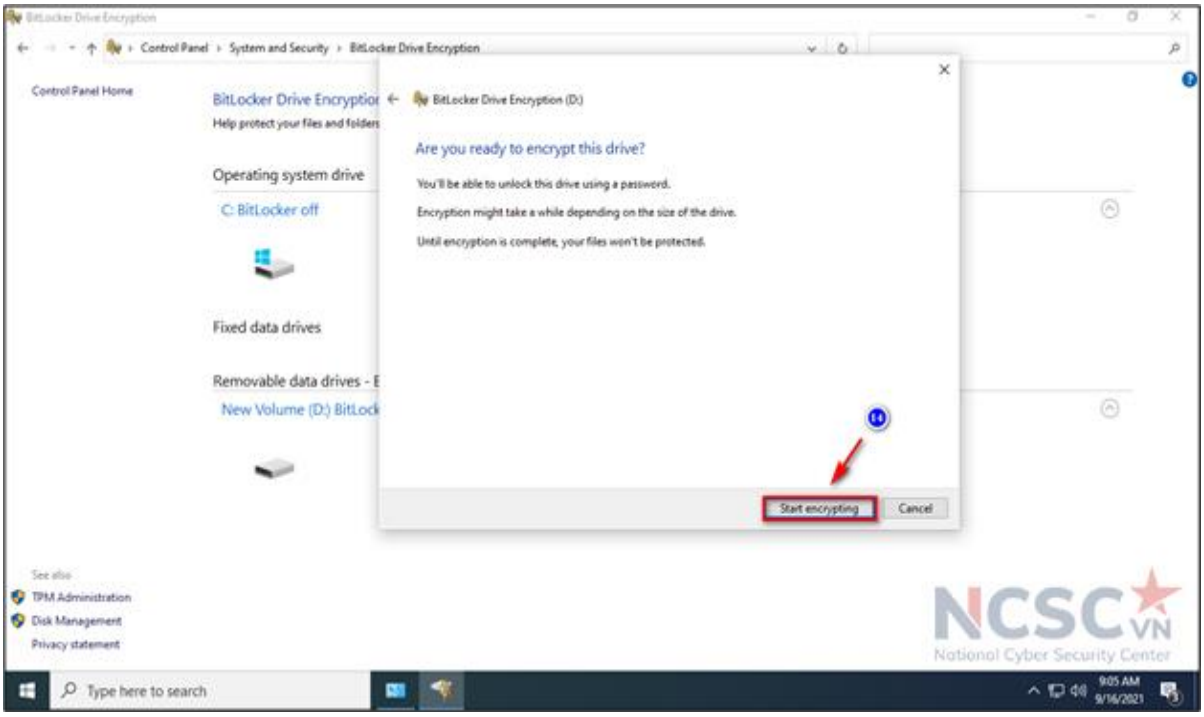
- New encryption mode (best for fixed drives on this device) – Chế độ mã hóa mới (phù hợp cho các ổ cứng cố định trên máy tính). Chế độ này an toàn hơn nhưng chỉ hỗ trợ trên Windows 10 phiên bản 1511 trở lên. Nếu các phiên bản windows cũ hơn thì không hỗ trợ giải mã dữ liệu.

- Compatible mode (best for drives that can be moved from this device) – Chế độ tương thích, phù hợp với ổ cứng kết nối ngoài hoặc không nằm cố định trên máy tính, người dùng có thể chuyển ổ cứng sang máy tính khác để mở.



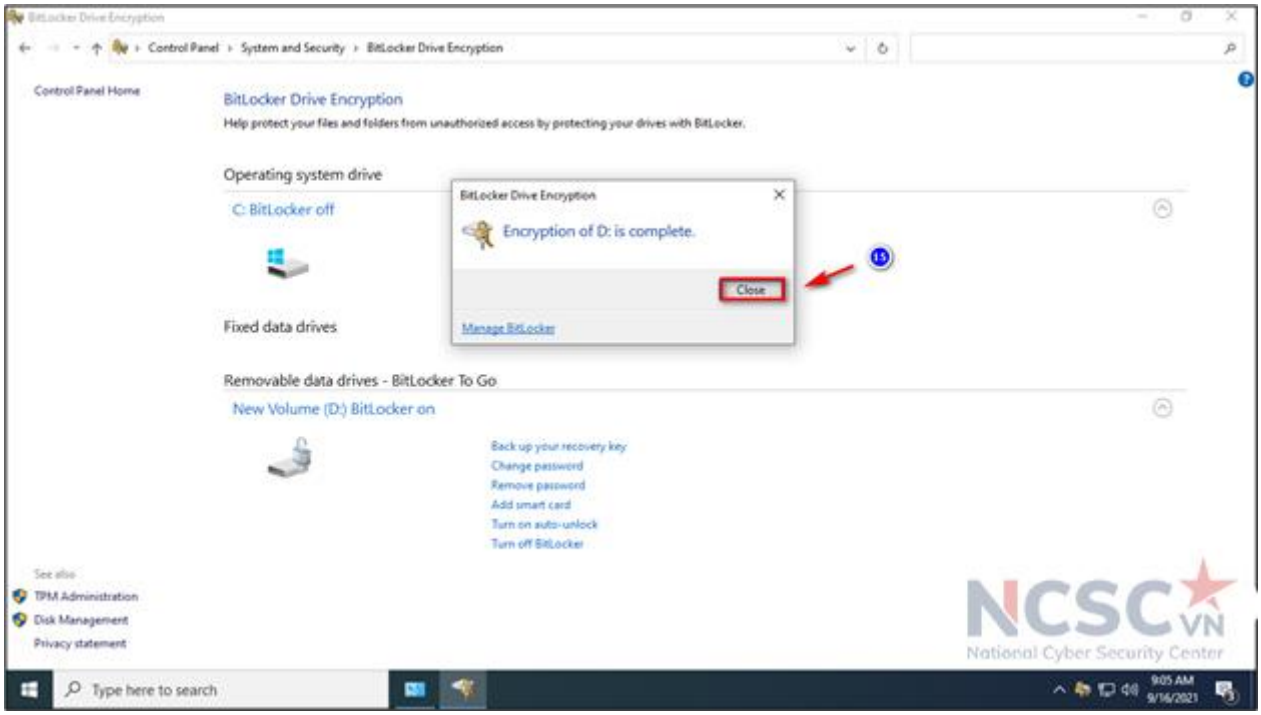
Hình 36: Mã hóa dữ liệu trên Windows 10 (20)

Bước 9: Chọn Start encrypting để tiến hành mã hóa.



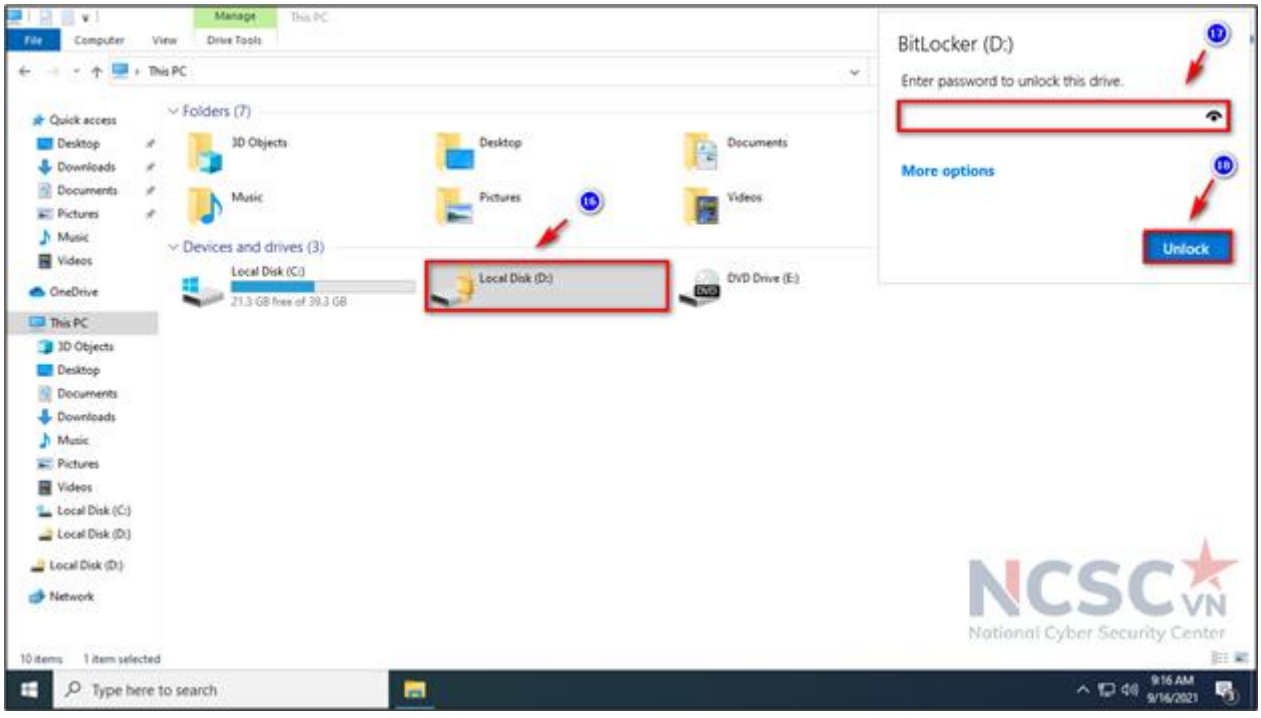
Hình 37: Mã hóa dữ liệu trên Windows 10 (21)

Bước 10: Quá trình mã hóa kết thúc > Close > khởi động lại máy tính



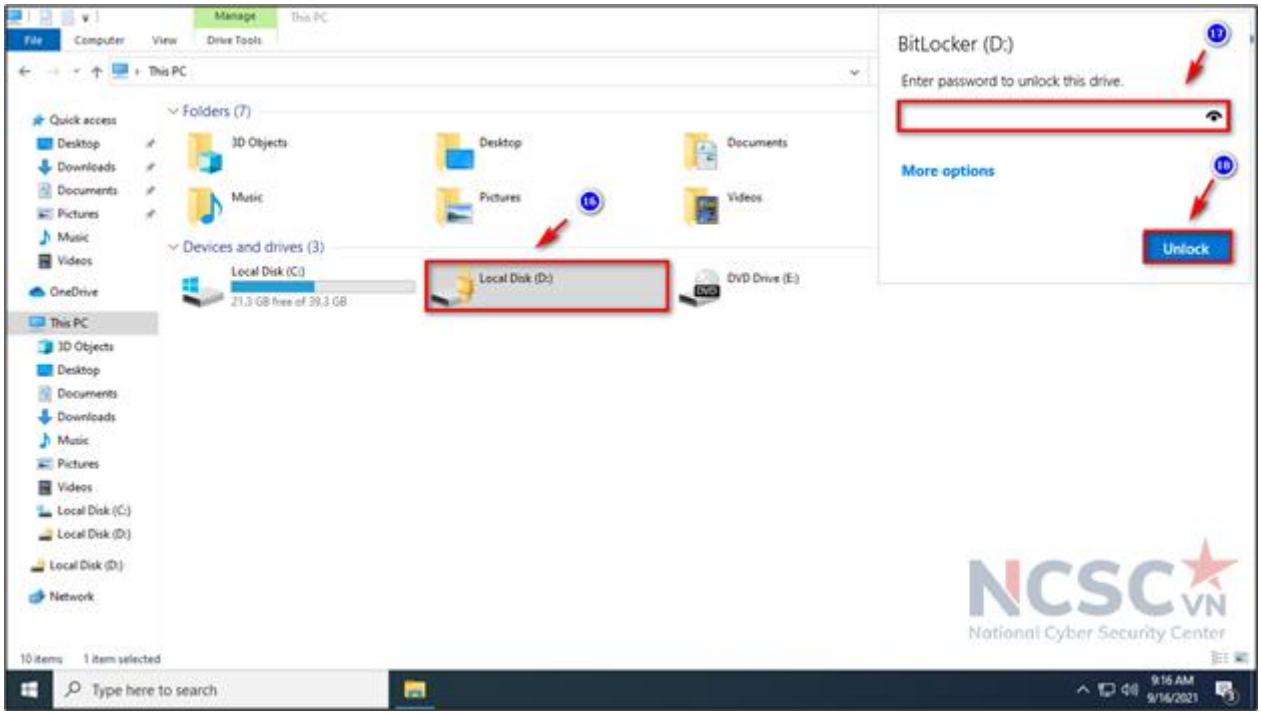
Hình 38: Mã hóa dữ liệu trên Windows 10 (22)

Bước 11: Sau khi khởi động lại máy tính, tìm kiếm ổ đĩa đã thực hiện mã hóa ta sẽ thấy biểu tượng ổ khóa (đang đóng). Nhấn chọn ổ đĩa, tiến hành nhập mật khẩu đã thiết lập xong bấm Unlock, để truy cập dữ liệu bên trong ổ đĩa.



Hình 39: Mã hóa dữ liệu trên Windows 10 (23)

Sau Unlock ổ đĩa, ta sẽ thấy biểu tượng ổ khóa (đang mở).

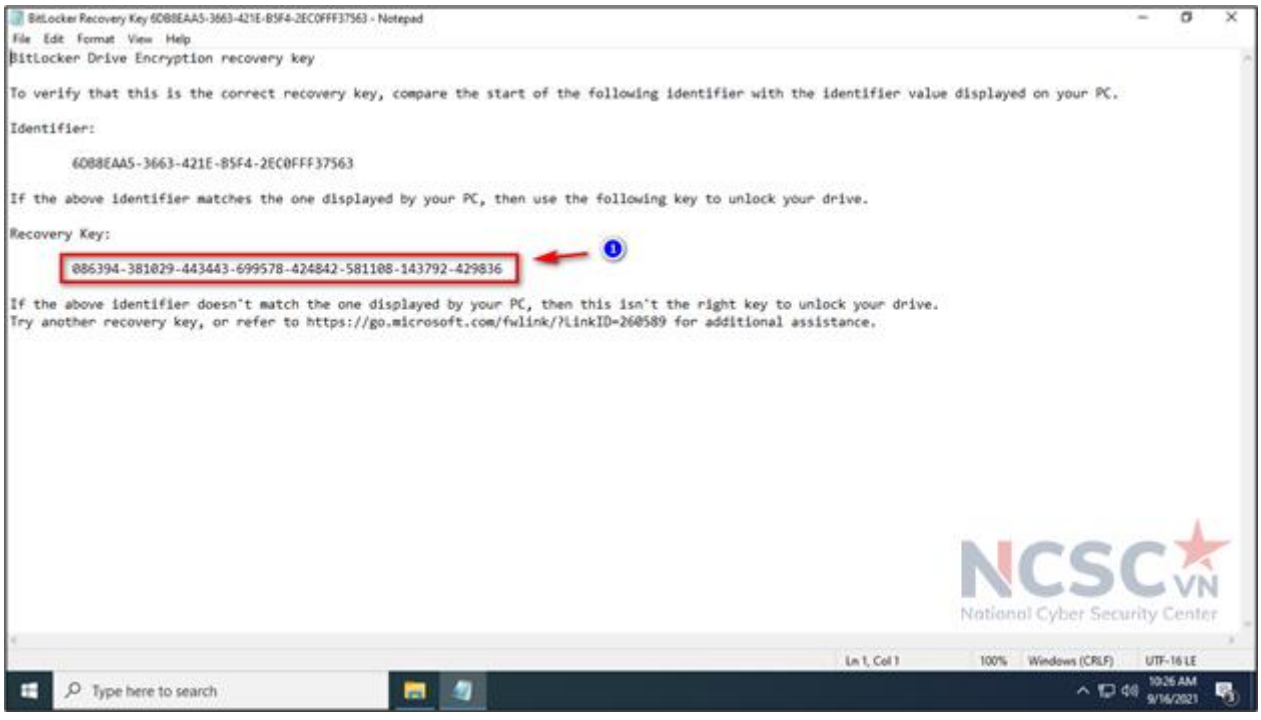


Hình 40: Mã hóa dữ liệu trên Windows 10 (24)

Sử dụng khóa khôi phục để mở khóa ổ

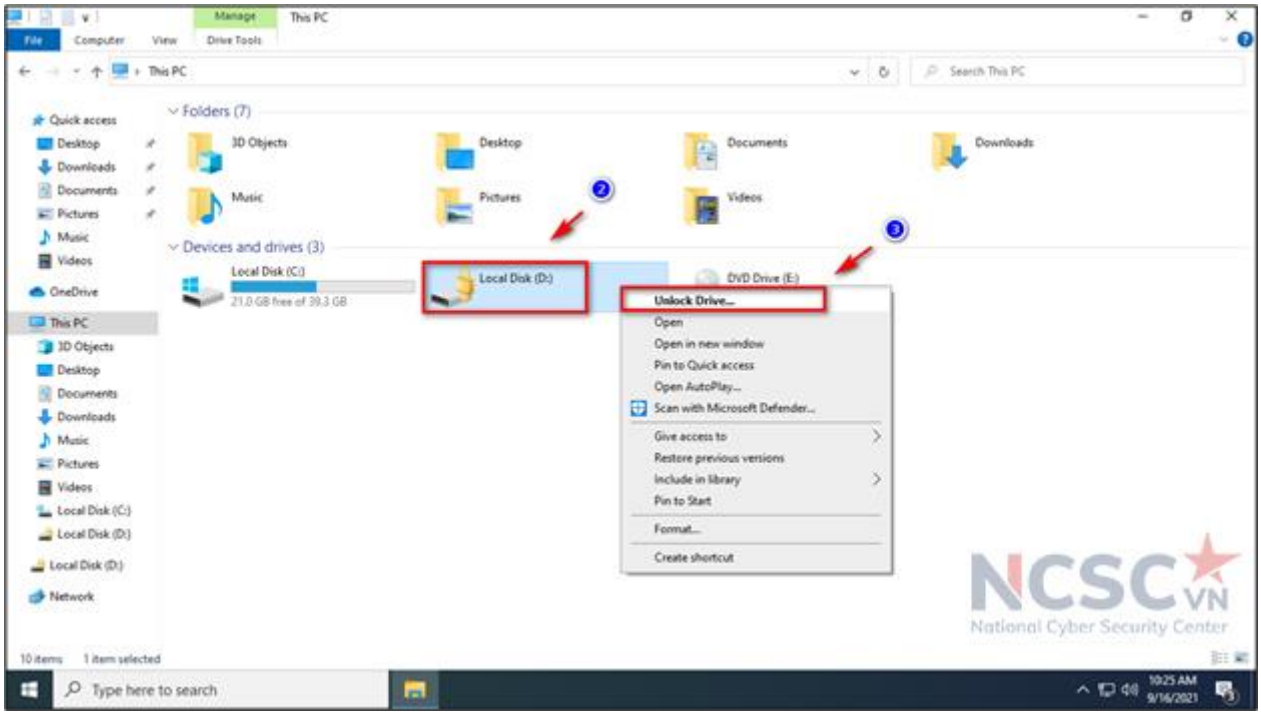
Trong trường hợp người dùng quên mật khẩu mở khóa hoặc vì bất kỳ lý do gì mà không thể truy cập vào ổ được mã hóa, người dùng có thể mở khóa ổ bằng khóa khôi phục.

Bước 1: Mở file chứa khóa khôi phục sau đó copy khóa Recovery key.



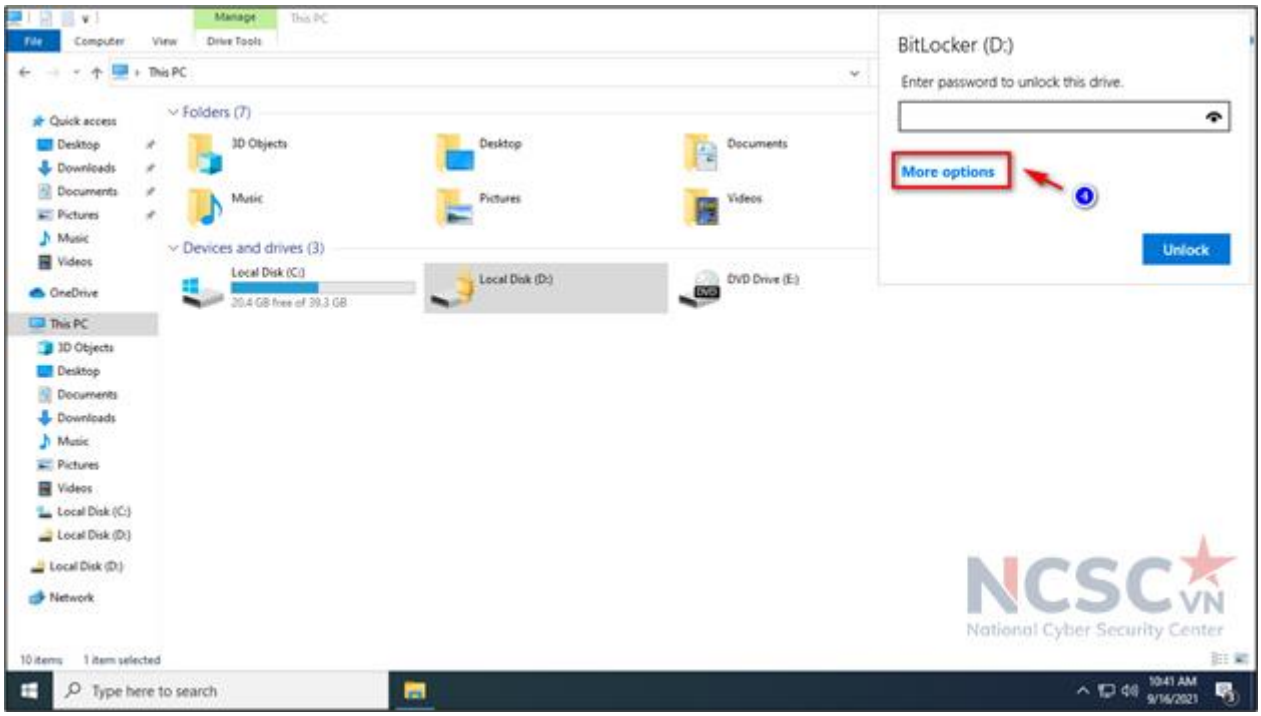
Hình 41: Sử dụng khóa khôi phục để mở khóa ổ (1)

Bước 2: Chuột phải vào ổ được mã hóa từ File Explorer, sau đó chọn Unlock Drive.



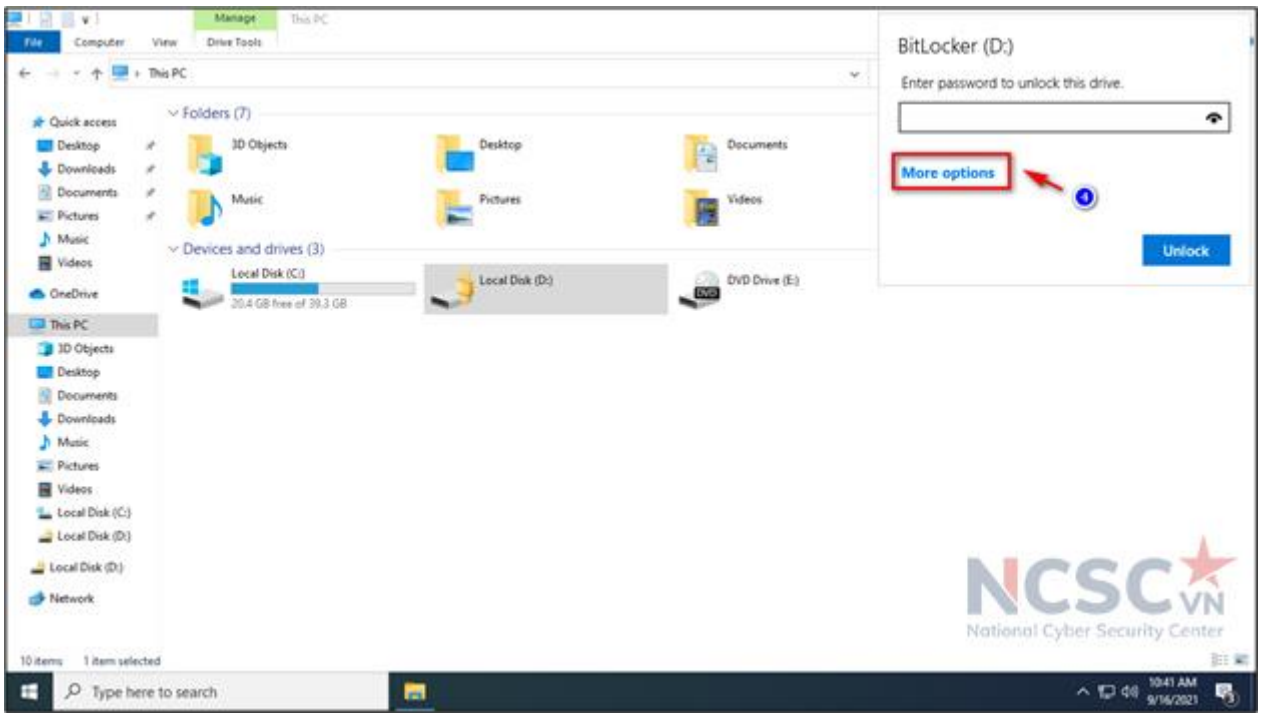
Hình 42: Sử dụng khóa khôi phục để mở khóa ổ (2)

Bước 3: Cửa sổ Bitlocker xuất hiện chọn More options



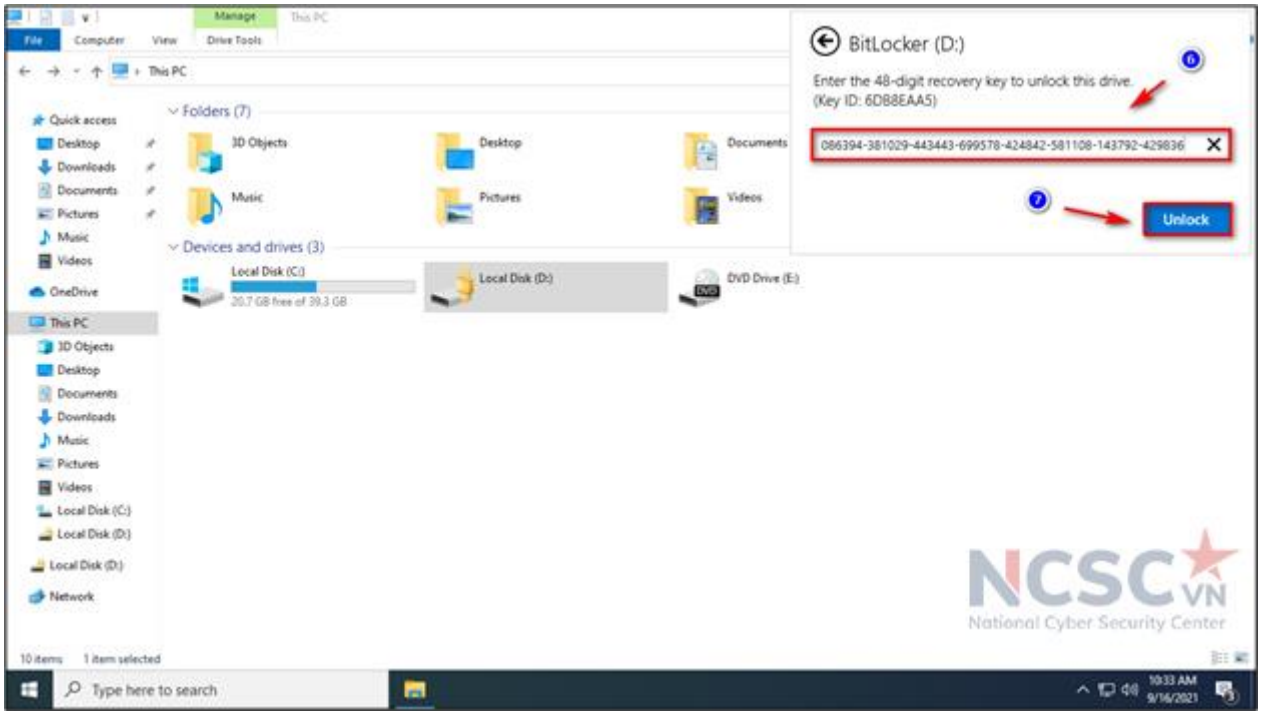
Hình 43: Sử dụng khóa khôi phục để mở khóa ổ (3)

Bước 4: Chọn tiếp Enter recovery key.



Hình 44: Sử dụng khóa khôi phục để mở khóa ổ (4)

Bước 5: Nhập key đã copy vào ô chứa, nhấn Unlock để mở khóa.



Hình 45: Mã hóa dữ liệu trên Windows 10

1.1.3. Thiết lập chính sách đối với tài khoản và mật khẩu

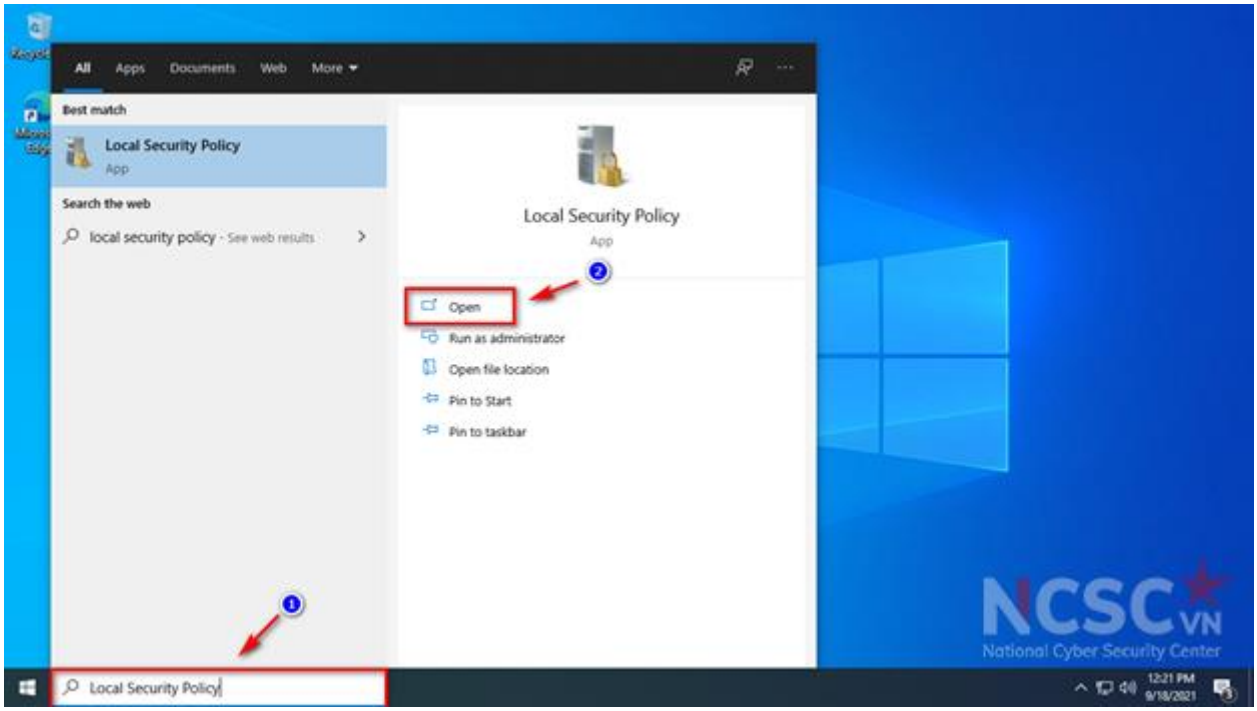
Thiết lập chính sách tài khoản và mật khẩu giúp bạn quản lý được tài khoản đã cấp trên máy tính như số lần đăng nhập sai, thời gian bị khóa tài khoản sau khi nhập sai quá nhiều…Ngoài ra, nó giúp giảm thiểu được các mối đe dọa đối với mật khẩu như mật

khẩu quá ngắn, độ phức tạp của mật khẩu không nhiều.

Tuy nhiên đối với máy tính cá nhân, việc thiết lập chính sách đối với tài khoản và mật khẩu không thực sự quá cần thiết, do vậy bạn cũng có thể bỏ qua mục này.

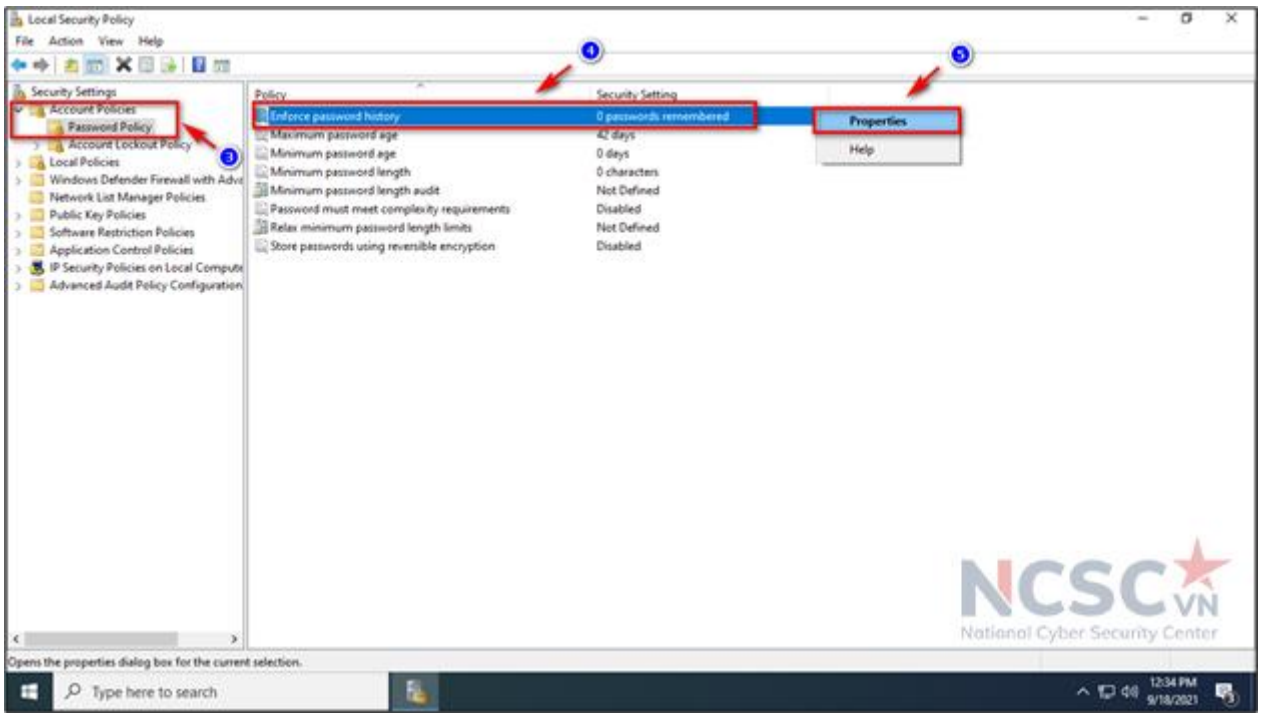
Cấu hình chính sách về mật khẩu:

Bước 1: Tại biểu tượng tìm kiếm trên Windows > nhập Local Security Policy.



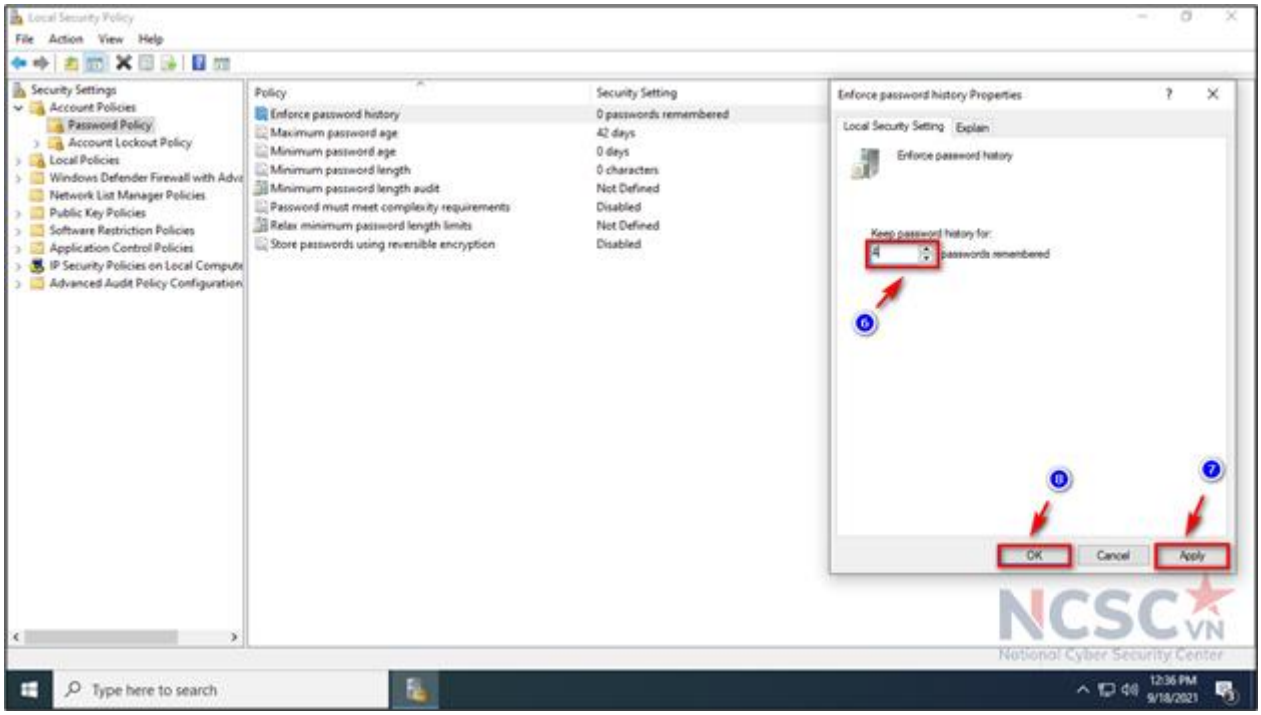
Hình 46: Cấu hình chính sách về mật khẩu (1)

Bước 2: Tại mục Local Security Policy, Security Settings > chọn Account Policies > chọn Password Policy > bấm chuột phải vào chính sách mật khẩu cần thiết lập > chọn Properties



Hình 47: Cấu hình chính sách về mật khẩu (2)

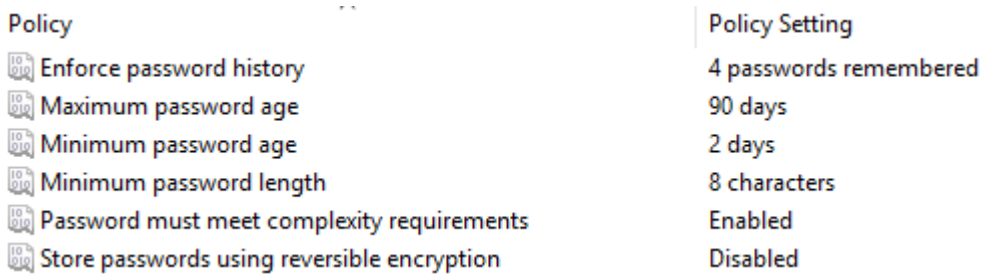
Bước 3: Chỉnh sửa các thông số thiết lập > xong bấm Apply > chọn OK



Hình 48: Cấu hình chính sách về mật khẩu (3)

Ví dụ: Chính sách người dùng không được sử dụng lại 4 mật khẩu cũ

Tham khảo thông số thiết lập theo chính sách an toàn thông tin trong mục Password Policy



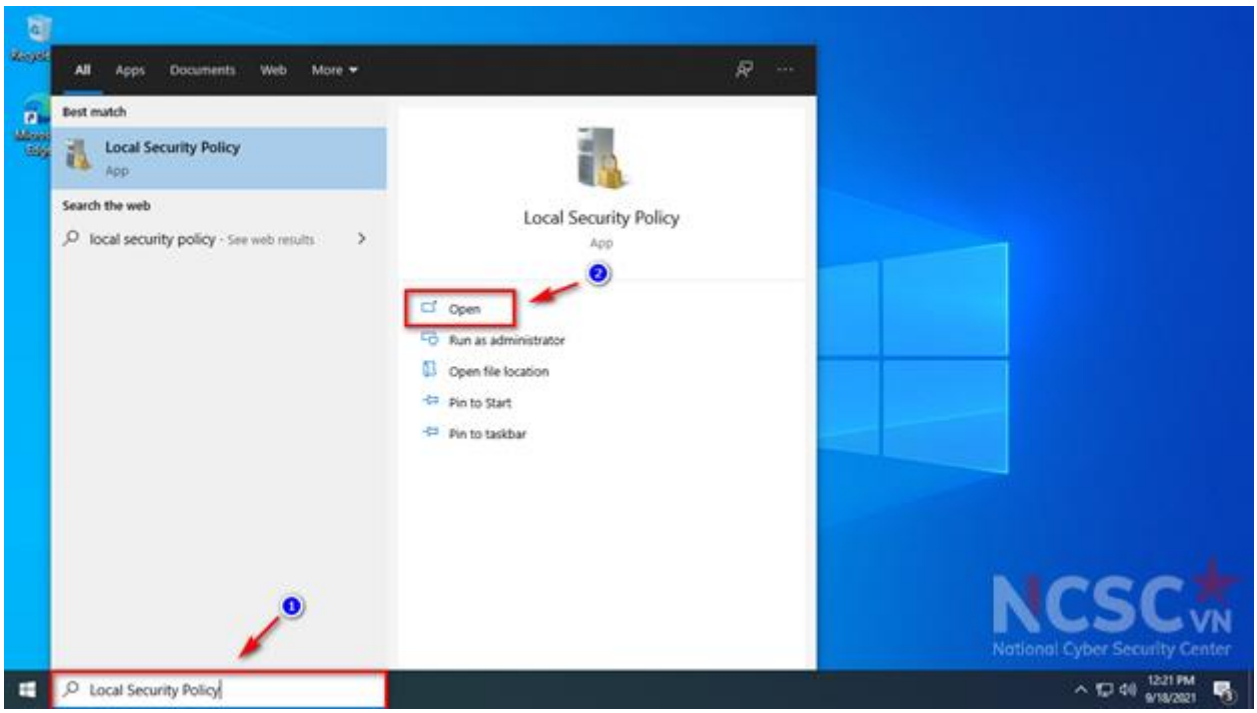
Hình 49: Thông số nên thiết lập đối với chính sách mật khẩu

Trong đó:

TT	Policy	Setting	Ghi chú
1	Enforce password history	4	Người dùng không được sử dụng lại 4 mật khẩu cũ
2	Maximum password age	90	Thời gian sử dụng mật khẩu trước khi bị yêu cầu thay đổi
3	Minimum password age	2	Thời gian có thể thay đổi mật khẩu sau lần đổi mật khẩu gần nhất
4	Minimum password length	8	Độ dài tối thiểu cho mật khẩu
5	Password must meet complexity requirements	Enable	Mật khẩu phải có độ phức tạp (chữ hoa, thường, ký tự đặc biệt)
6	Store passwords using reversible encryption	Disable	Lưu trữ mật khẩu bằng mã hóa ngược

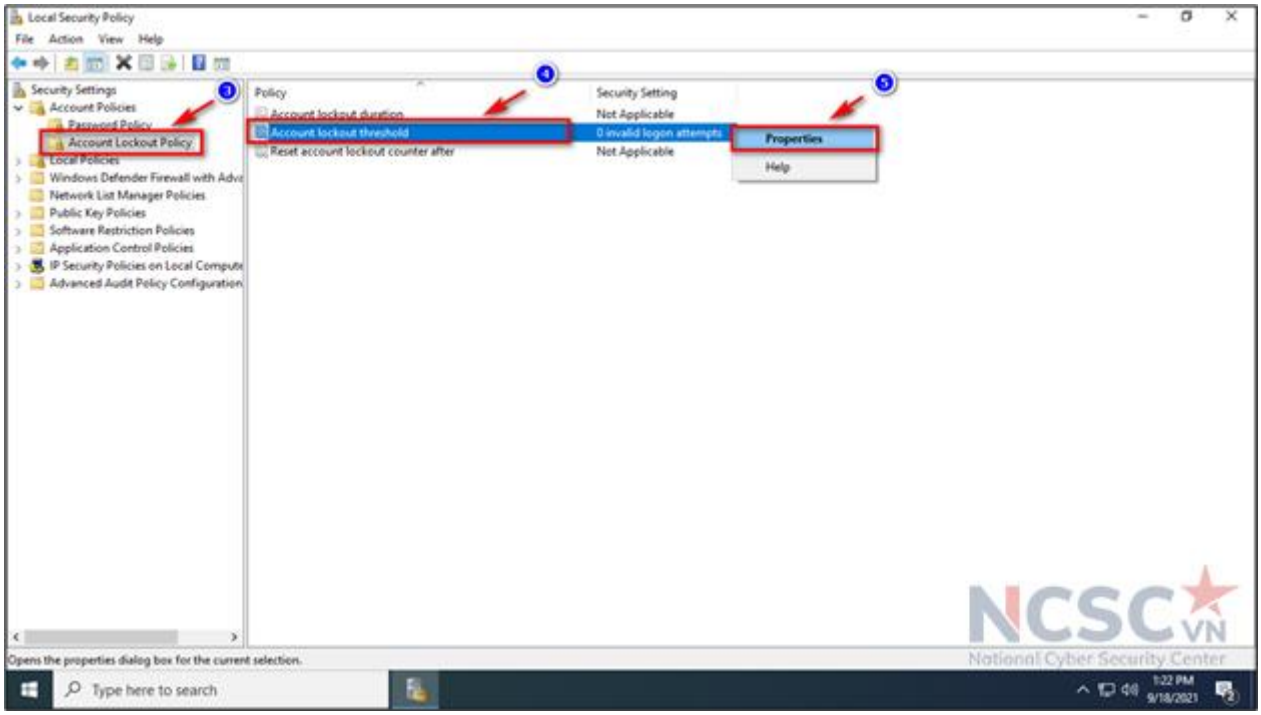
Cấu hình chính sách về tài khoản:

Bước 1: Tại biểu tượng tìm kiếm trên Windows > nhập Local Security Policy.



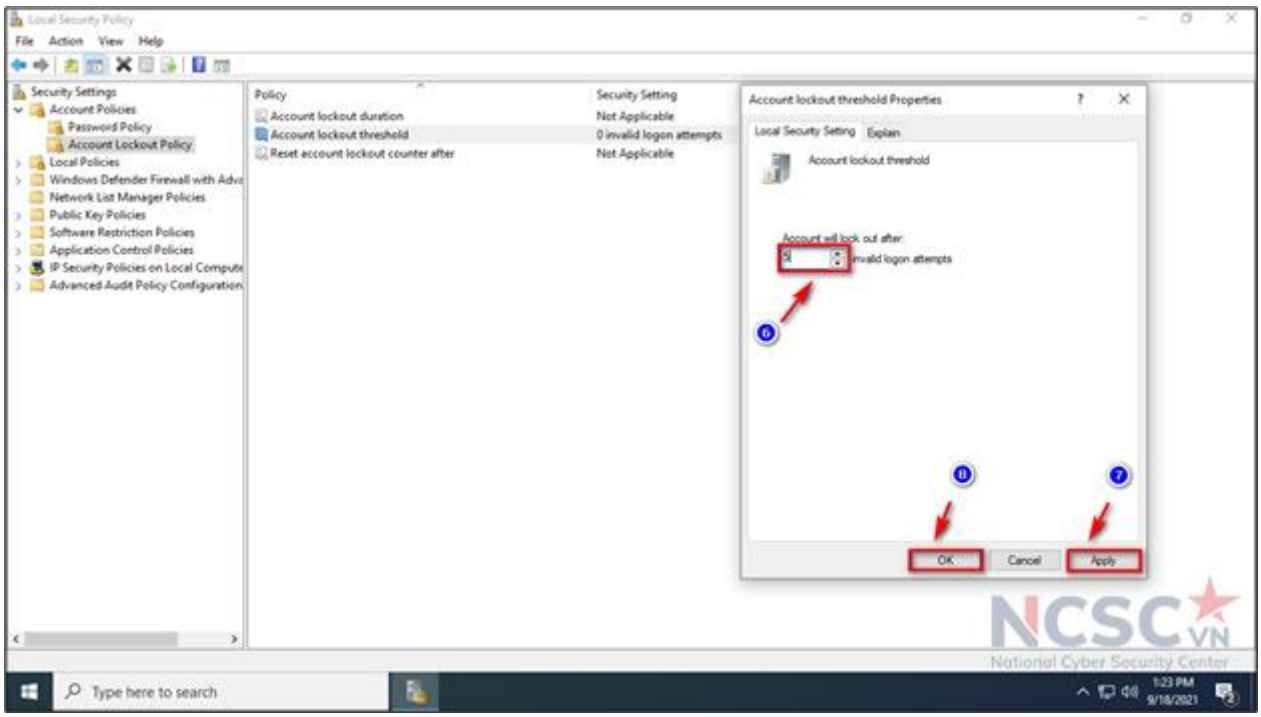
Hình 50: Cấu hình chính sách về tài khoản (1)

Bước 2: Tại mục Local Security Policy, Security Setttings > Account Policies > Account Lockout Policy > bấm chuột phải vào chính sách tài khoản cần thiết lập > chọn Properties



Hình 51: Cấu hình chính sách về tài khoản (2)

Bước 3: Chỉnh sửa các thông số thiết lập > xong bấm Apply > chọn OK



Hình 52: Cấu hình chính sách về tài khoản (3)

Ví dụ: Chính sách người dùng đăng nhập thất bại 5 lần sẽ bị khóa tài khoản

Tham khảo thông số thiết lập theo chính sách an toàn thông tin trong mục Account Lockout Policy:

Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Hình 53: Cấu hình chính sách tài khoản (4)

Trong đó:

TT	Policy	Setting	Ghi chú
1	Account lockout duration	30	Thời gian khóa tài khoản sau khi nhập sai quá số lần cho phép
2	Account lockout threshold	5	Số lần đăng nhập thất bại dẫn đến khóa tài khoản
3	Reset account lockout counter after	30	Thời gian thiết lập lại số lần đăng nhập thất bại

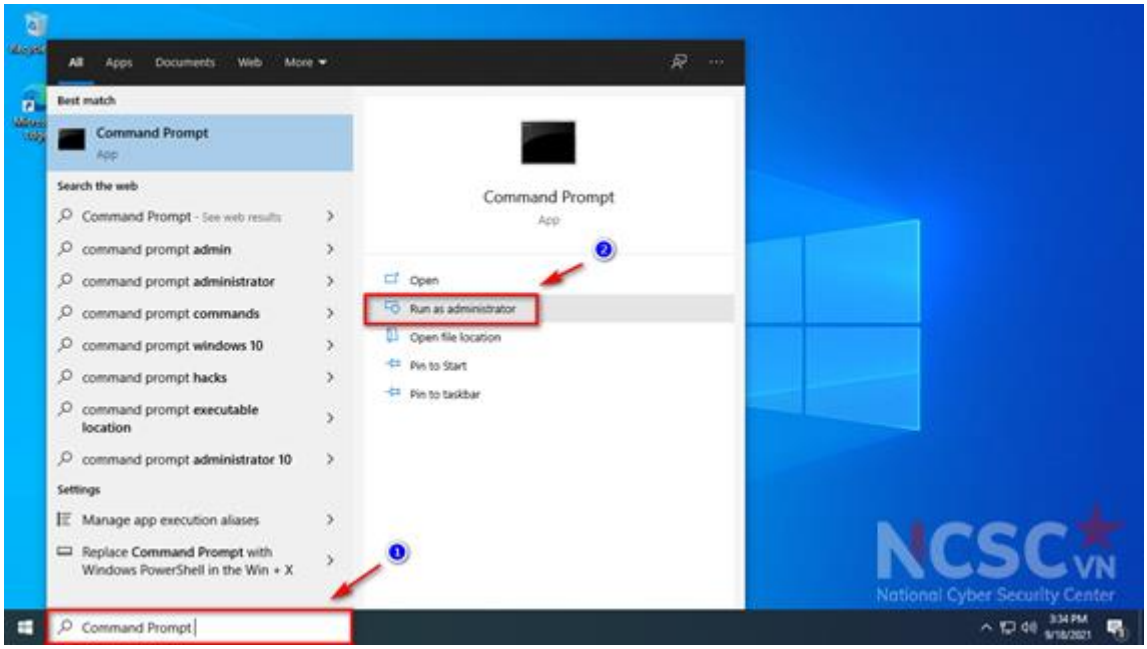
1.1.4. Vô hiệu hóa các thư mục chia sẻ không cần thiết

Chia sẻ thư mục trên máy tính là cách tuyệt vời để chia sẻ dữ liệu với máy tính khác trong cùng một mạng thay vì phải gửi qua email hoặc sử dụng USB. Tuy nhiên cách này tồn tại rất nhiều mối nguy hiểm, bởi vì thư mục được chia sẻ trong mạng nên bất kỳ ai cũng có thể truy cập để xem. Hơn nữa các thư mục chia sẻ trên máy tính có thể là lý do làm lộ lọt dữ liệu trên máy tính hoặc Hacker có thể tấn công vào máy tính của

bạn qua các thư mục chia sẻ này. Nếu không sử dụng bạn có thể vô hiệu hóa các thư mục chia sẻ đi.

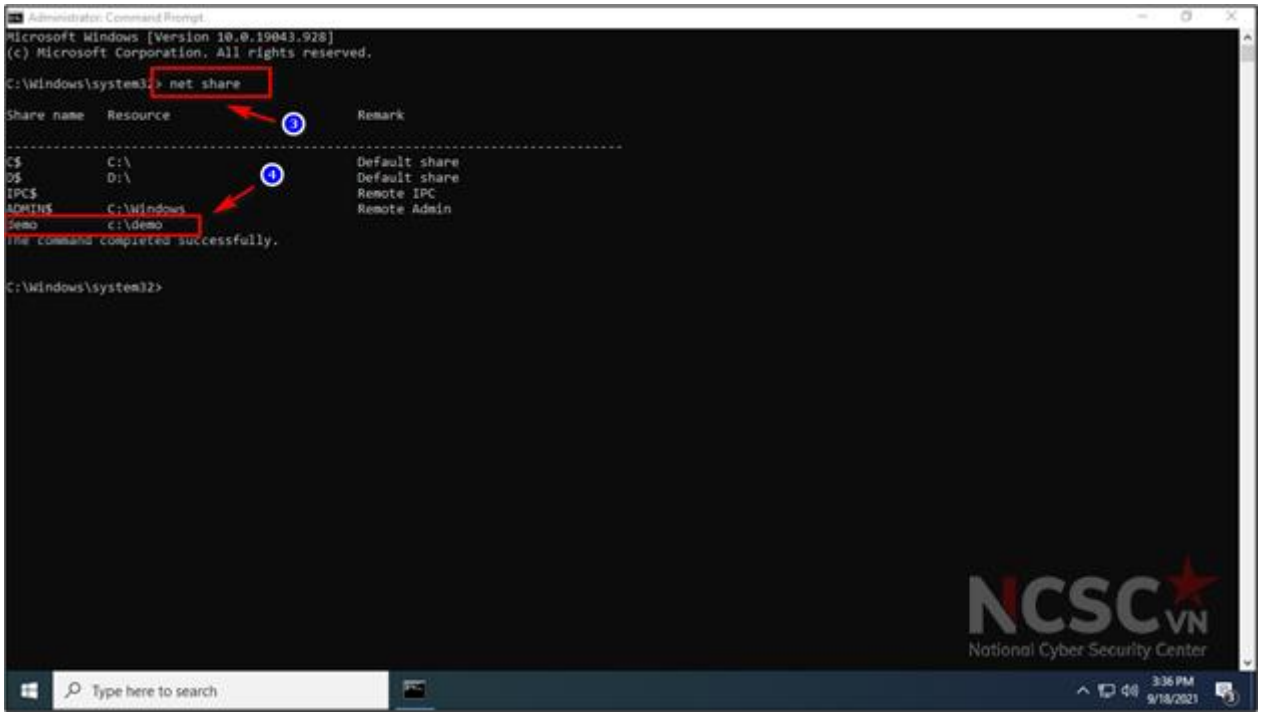
Các bước thực hiện như sau:

Bước 1: Tại biểu tượng tìm kiếm trên Windows > nhập Command Prompt và chọn Run as administrator.



Hình 54: Vô hiệu hóa các thư mục chia sẻ không cần thiết (1)

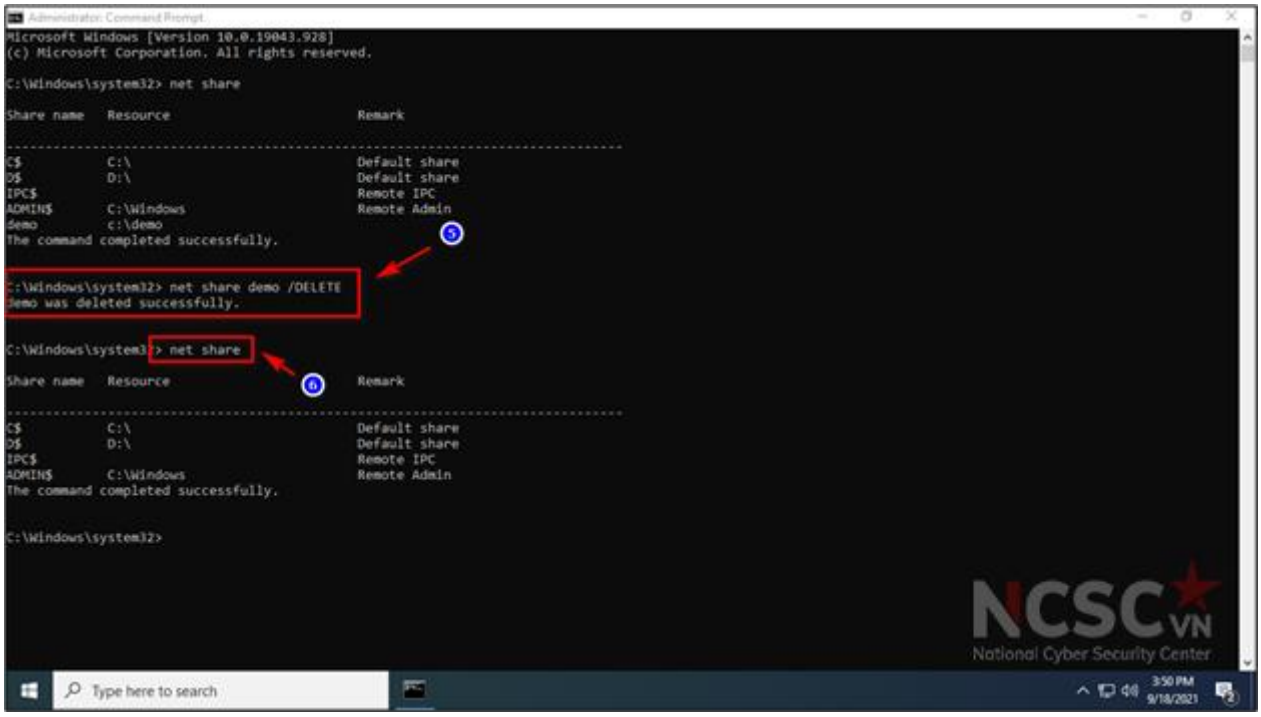
Bước 2: Nhập net share để tìm kiếm các thư mục được chia sẻ trên máy tính



Hình 55: Vô hiệu hóa các thư mục chia sẻ không cần thiết (2)

Ví dụ: Trên máy tính này có thư mục demo đang được chia sẻ

Bước 3: Tiến hành vô hiệu hóa thư mục được chia sẻ với cú pháp như sau: NET SHARE sharename /DELETE

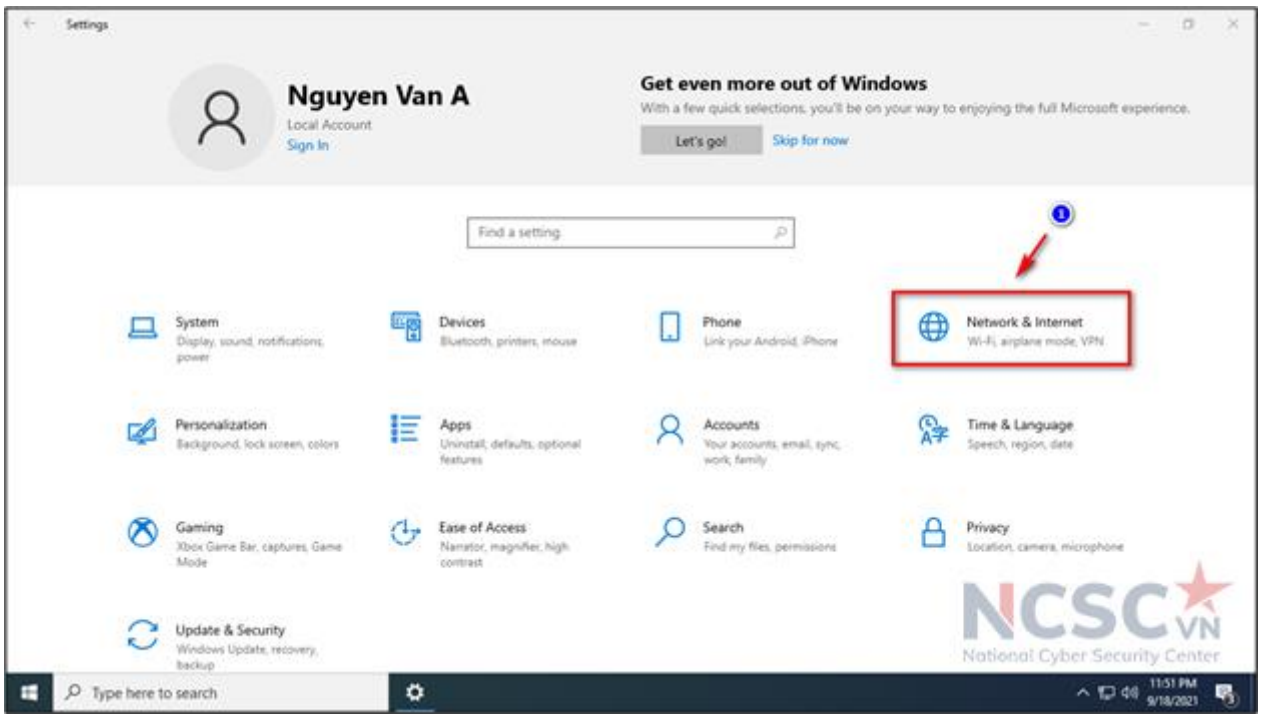


Hình 56: Vô hiệu hóa các thư mục chia sẻ không cần thiết (3)

Ví dụ: Cú pháp xóa thư mục chia sẻ demo: net share demo /DELETE

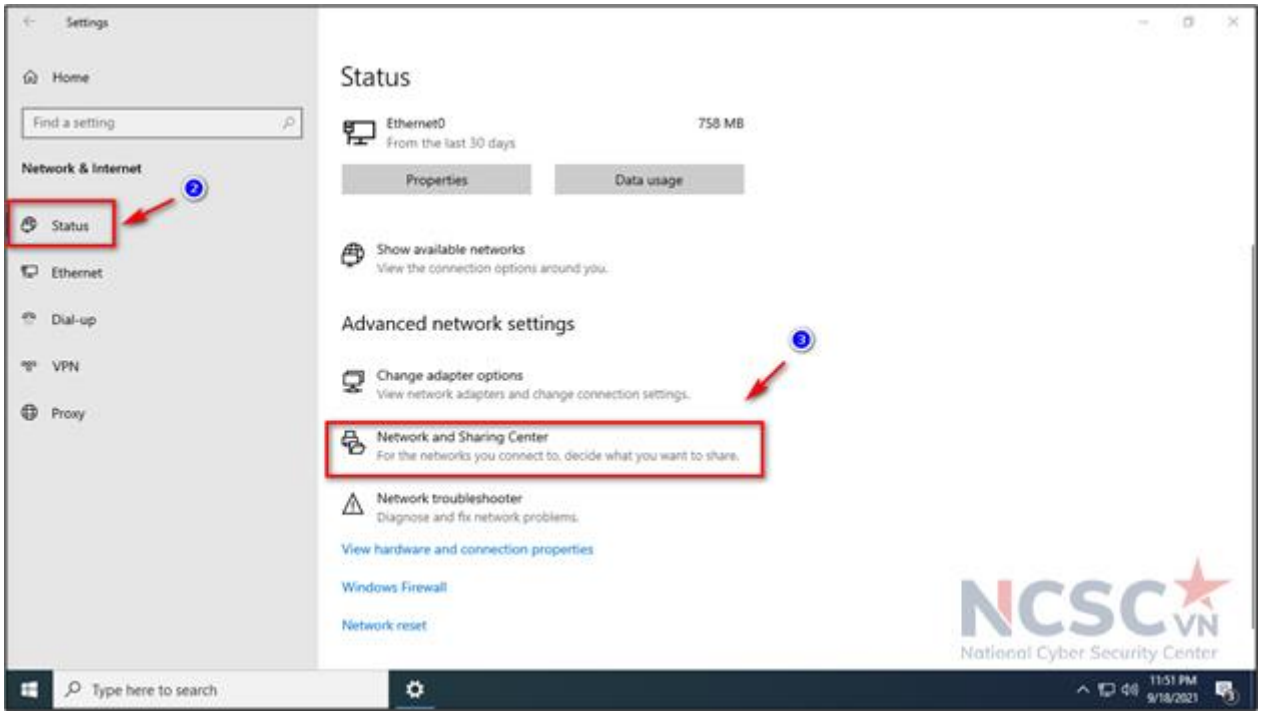
Lưu ý: Trong trường hợp người dùng cần phải chia sẻ thư mục cần bật tính năng Password protected Sharing (Chia sẻ được bảo vệ bằng mật khẩu), để những người có tài khoản, mật khẩu đăng nhập mới có thể truy cập được thư mục chia sẻ.

Bước 1: Nhấn phím Windows + I để mở Settings và click vào Network & Internet



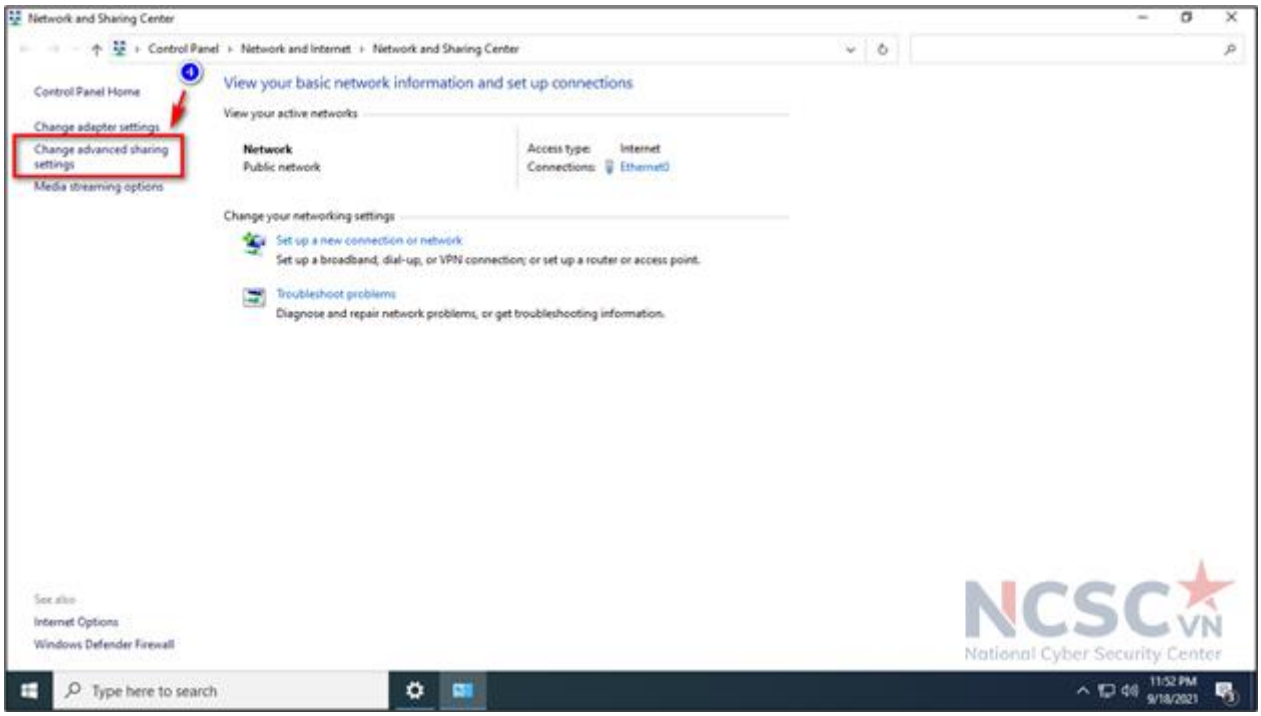
Hình 57: Vô hiệu hóa các thư mục chia sẻ không cần thiết (4)

Bước 2: Trong mục Status > chọn Network and Sharing Center



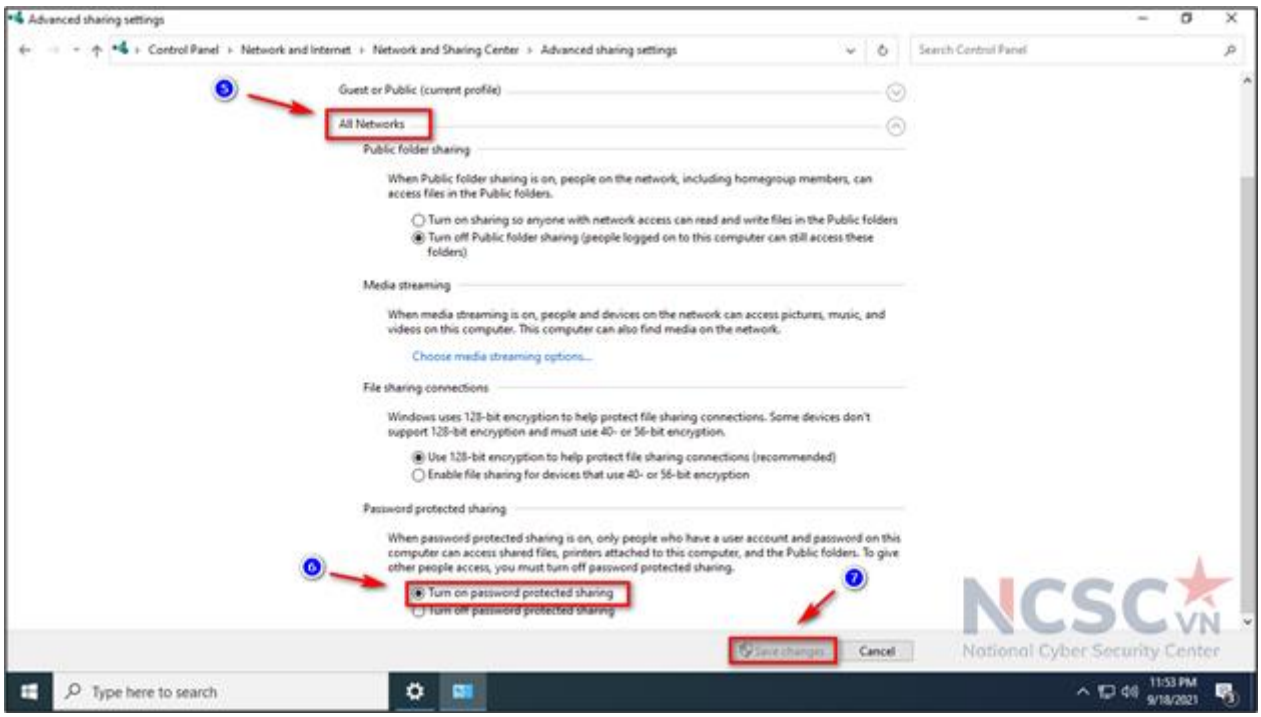
Hình 58: Vô hiệu hóa các thư mục chia sẻ không cần thiết (5)

Bước 3: Chọn Change advanced sharing settings



Hình 59: Vô hiệu hóa các thư mục chia sẻ không cần thiết (6)

Bước 4: Chọn All Networks > trong mục Password protected Sharing > chọn Turn on password protected sharing > chọn Save changes để lưu thay đổi.



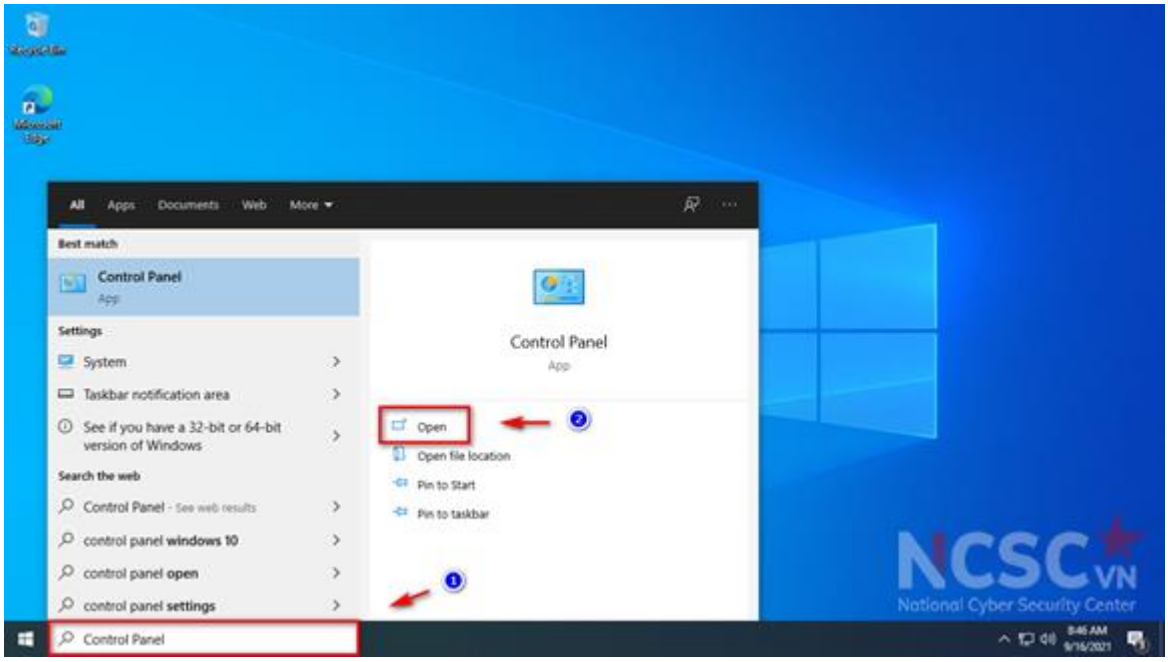
Hình 60: Vô hiệu hóa các thư mục chia sẻ không cần thiết (7)

1.1.5. Kích hoạt tường lửa bảo vệ trên thiết bị

Một trong các tác vụ đầu tiên cần thực hiện sau khi cài đặt máy tính là thiết lập các cơ chế bảo vệ cơ bản cho thiết bị. 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 máy tính 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.

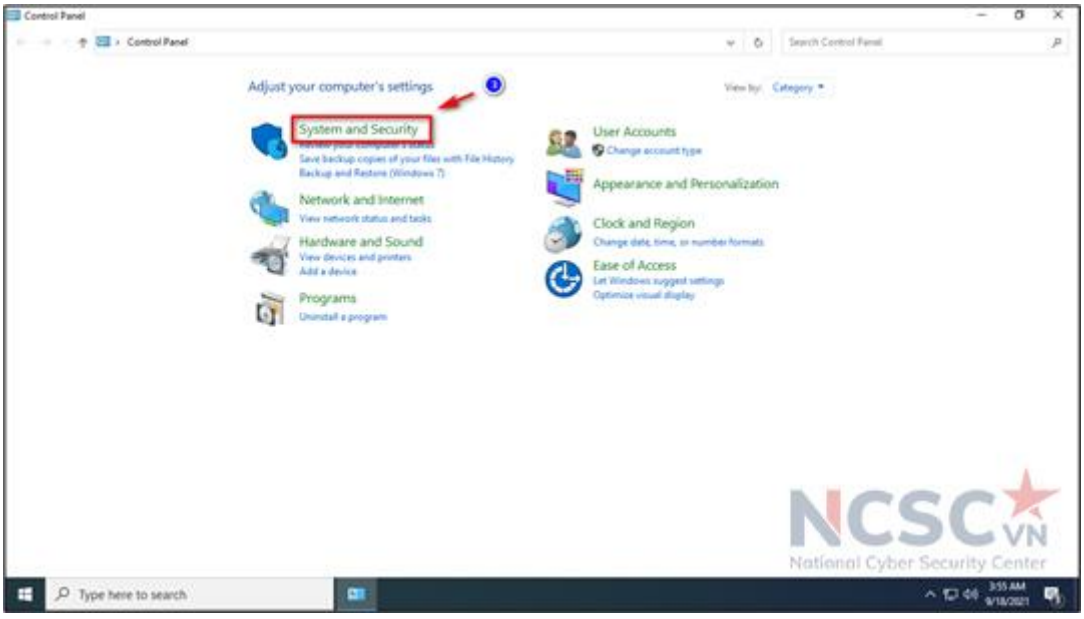
Để kích hoạt tường lửa thực hiện như sau

Bước 1: Tại biểu tượng tìm kiếm trên Windows > Control Panel và chọn Open.



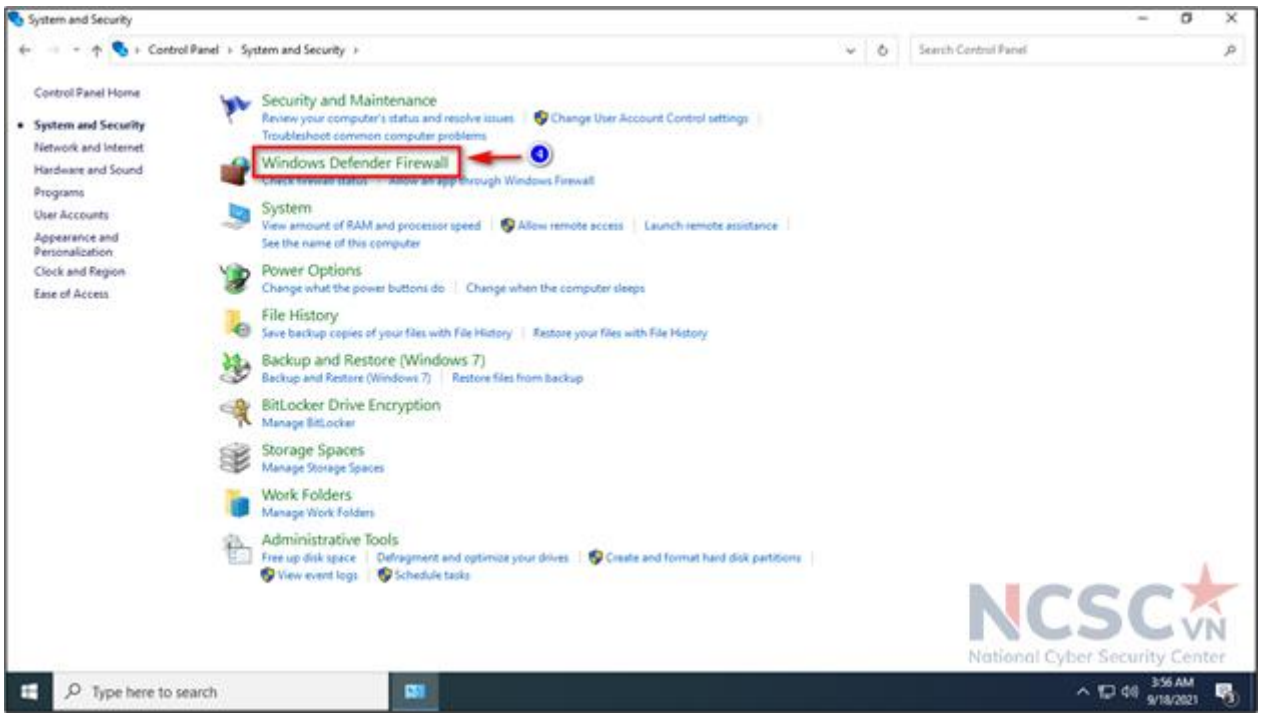
Hình 61: Kích hoạt tường lửa (1)

Bước 2: Chọn System and Security.



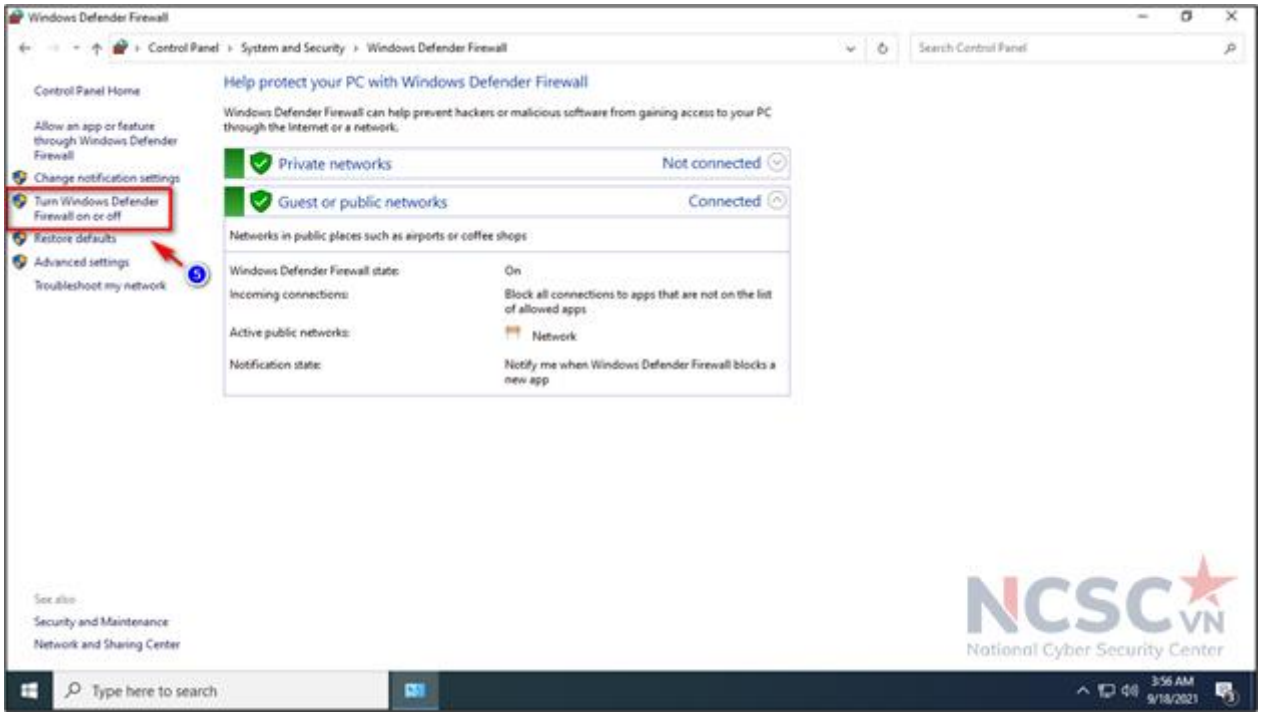
Hình 62: Kích hoạt tường lửa (2)

Bước 3: Chọn tiếp vào mục Windows Defender Firewall.



Hình 63: Kích hoạt tường lửa (3)

Bước 4: Sau đó, chọn tiếp vào mục Turn Windows Defender Firewall on or off ở bên trái màn hình.

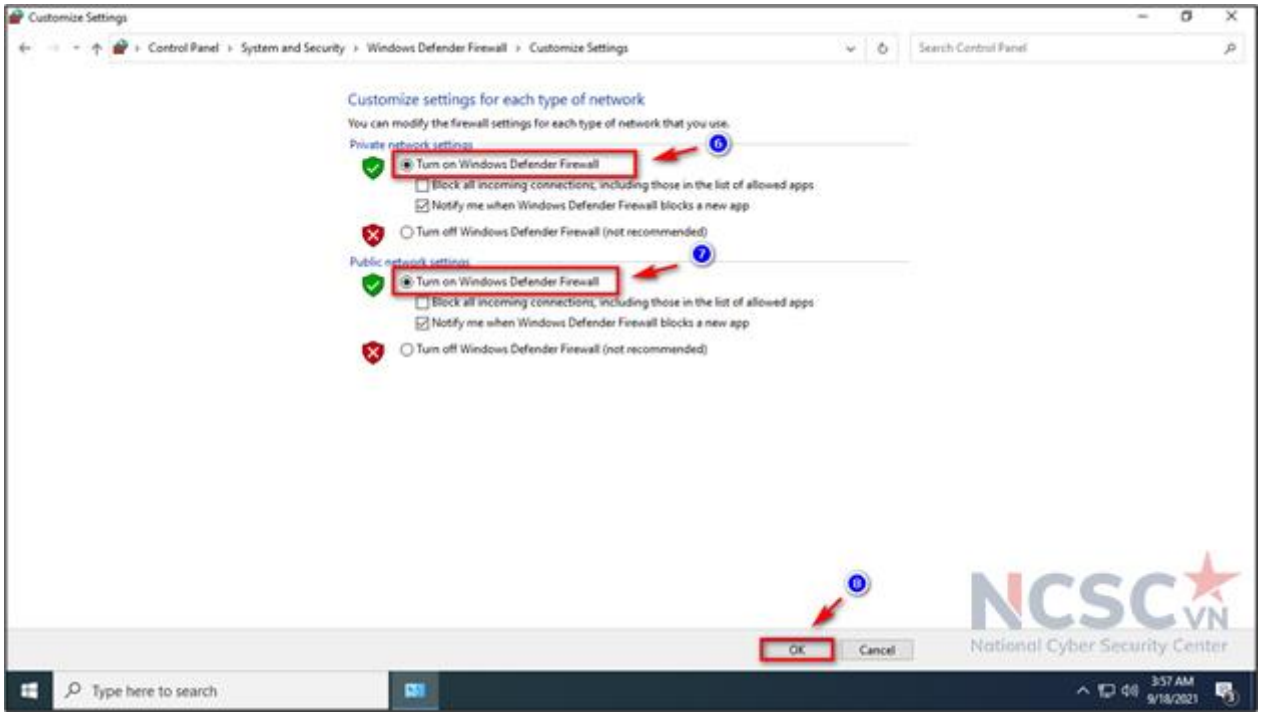


Hình 64: Kích hoạt tường lửa (4)

Bước 5: Lựa chọn bật hoặc tắt tường lửa trên thiết bị cá nhân

- Turn on Windows Defender Firewall: bật tường lửa
- Turn off Windows Defender Firewall: tắt tường lửa

Lựa chọn bật tường lửa và nhấn OK để hoàn tất cài đặt.



Hình 65: Kích hoạt tường lửa (5)

1.1.6. Gỡ bỏ các chương trình không cần thiết

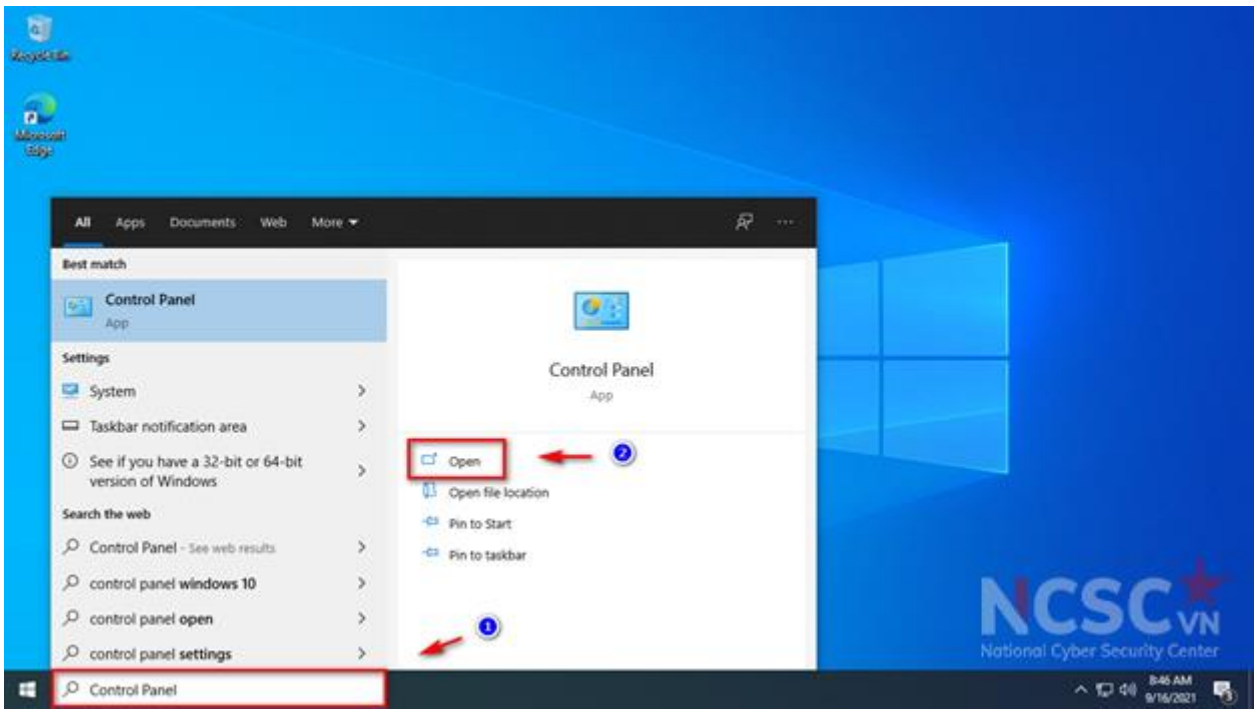
Các thiết bị cá nhân thường được nhà sản xuất cài đặt sẵn các chương trình quảng cáo, giới thiệu hoặc bản dùng thử của các phần mềm khác. Các chương trình này có thể ẩn chứa các nguy cơ gây mất an toàn thông tin mà Hacker có thể lợi dụng ngay trong quá trình sử dụng lần đầu tiên hoặc làm giảm hiệu năng của thiết bị.

Ngoài ra có nhiều ứng dụng bạn chỉ sử dụng một thời gian, sau đó không dùng nữa. Bạn nên tháo gỡ các chương trình không cần thiết trên máy tính 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.

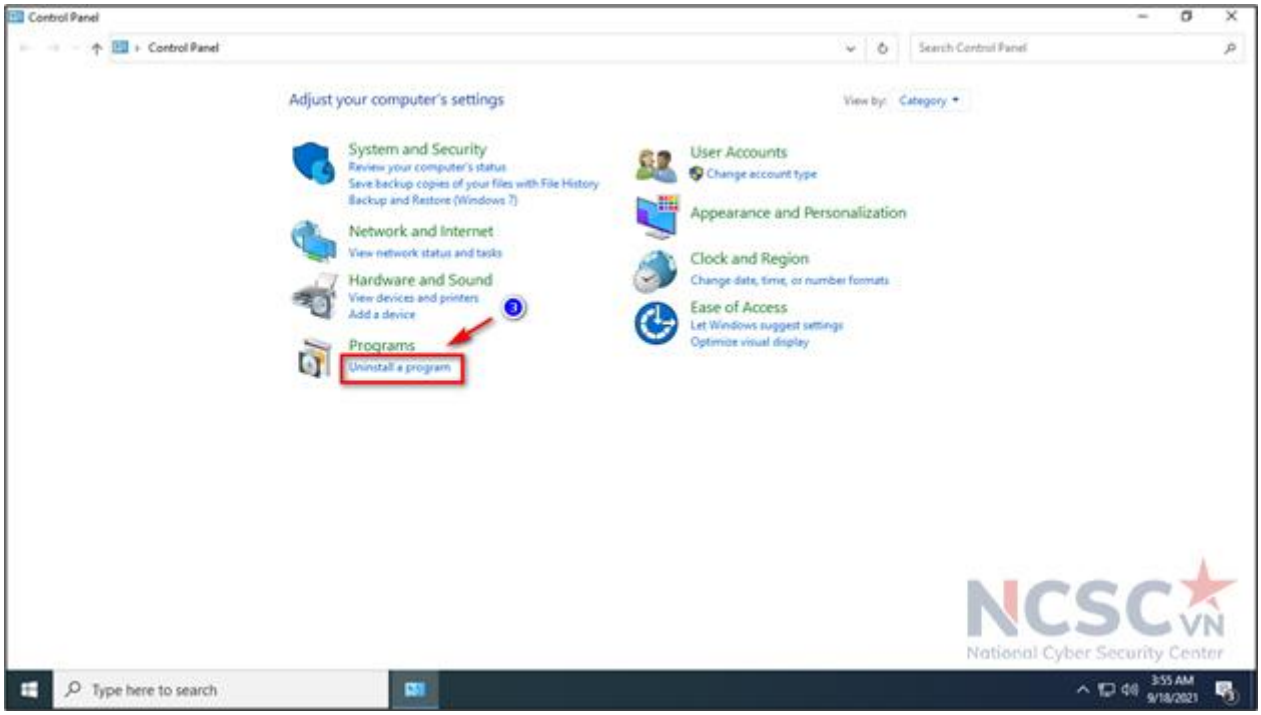
Bạn có thể làm theo các bước sau:

Bước 1: Vào mục tìm kiếm trên Windows > Control Panel và chọn Open.



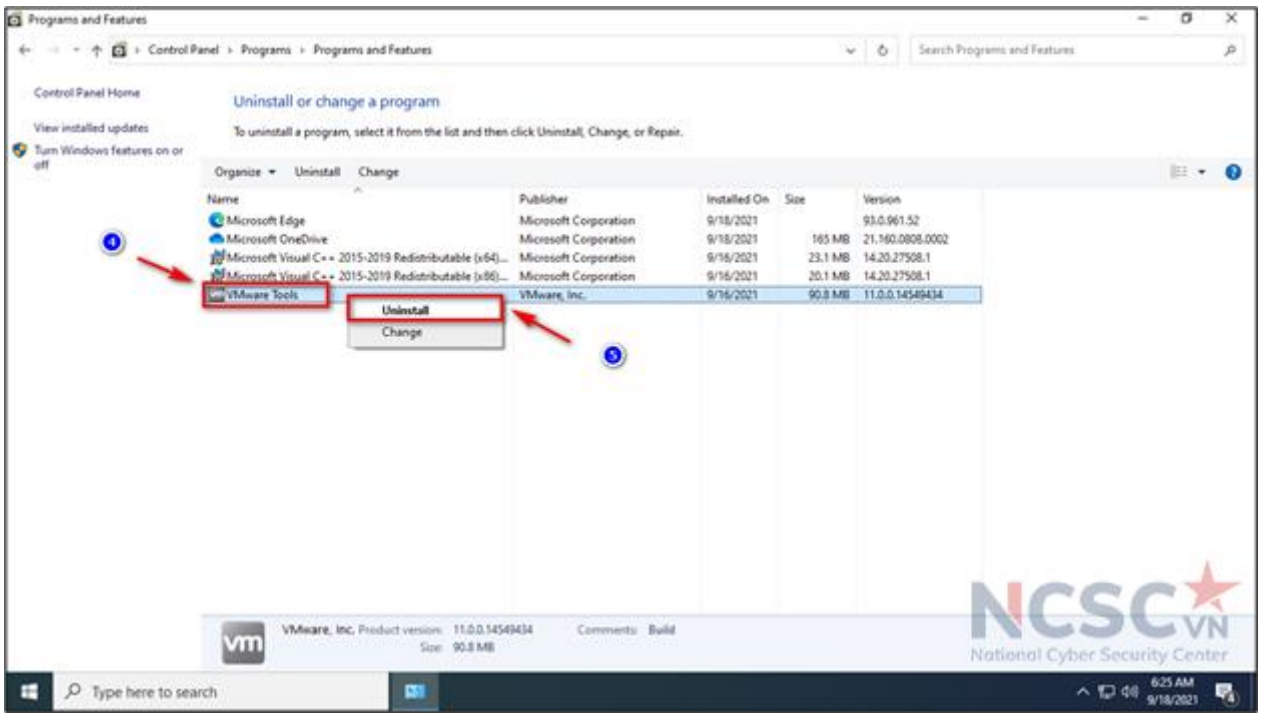
Hình 66: Gỡ bỏ các chương trình không cần thiết (1)

Bước 2: Chọn vào mục Uninstall a program.



Hình 67: Gỡ bỏ các chương trình không cần thiết (2)

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

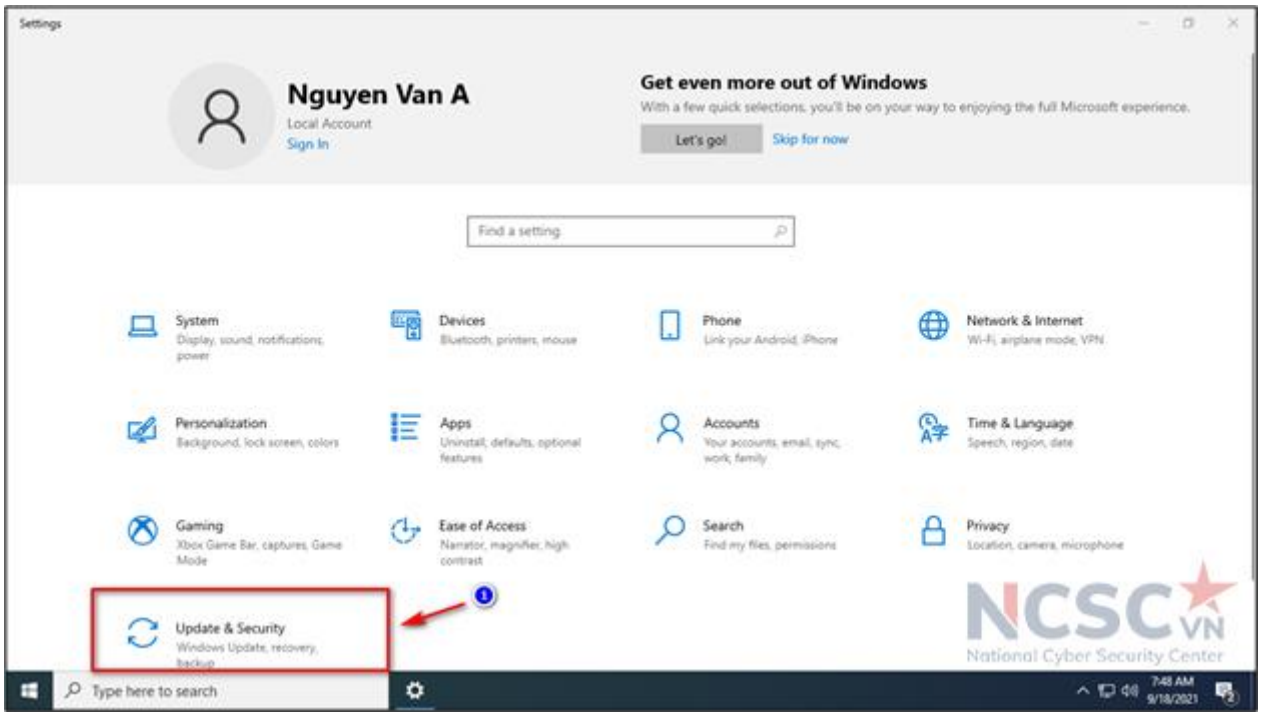


Hình 68: Gỡ bỏ các chương trình không cần thiết (3)

1.1.7. Cập nhật hệ điều hành

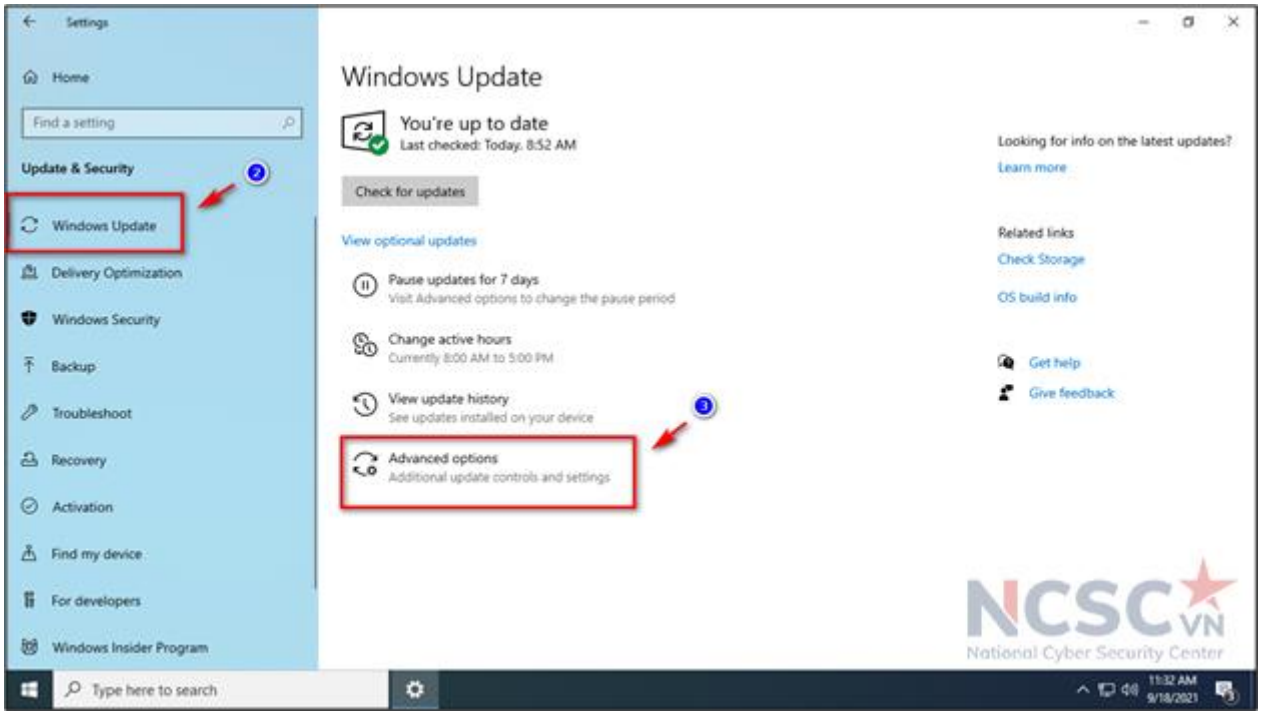
Máy tính có thể sử dụng phiên bản hệ điều hành có nhiều lỗ hổng bảo mật chưa được cập nhật bản vá, bạn có thể thiết lập chế độ tự động cập nhật hệ điều hành và các phần mềm khác. Bạn có thể chọn chế độ tự động cập nhật theo nhu cầu để đảm bảo không bị gián đoạn công việc. Các bước thực hiện cụ thể như sau:

Bước 1: Mở Settings và click vào Update & Security (Windows + I để mở)



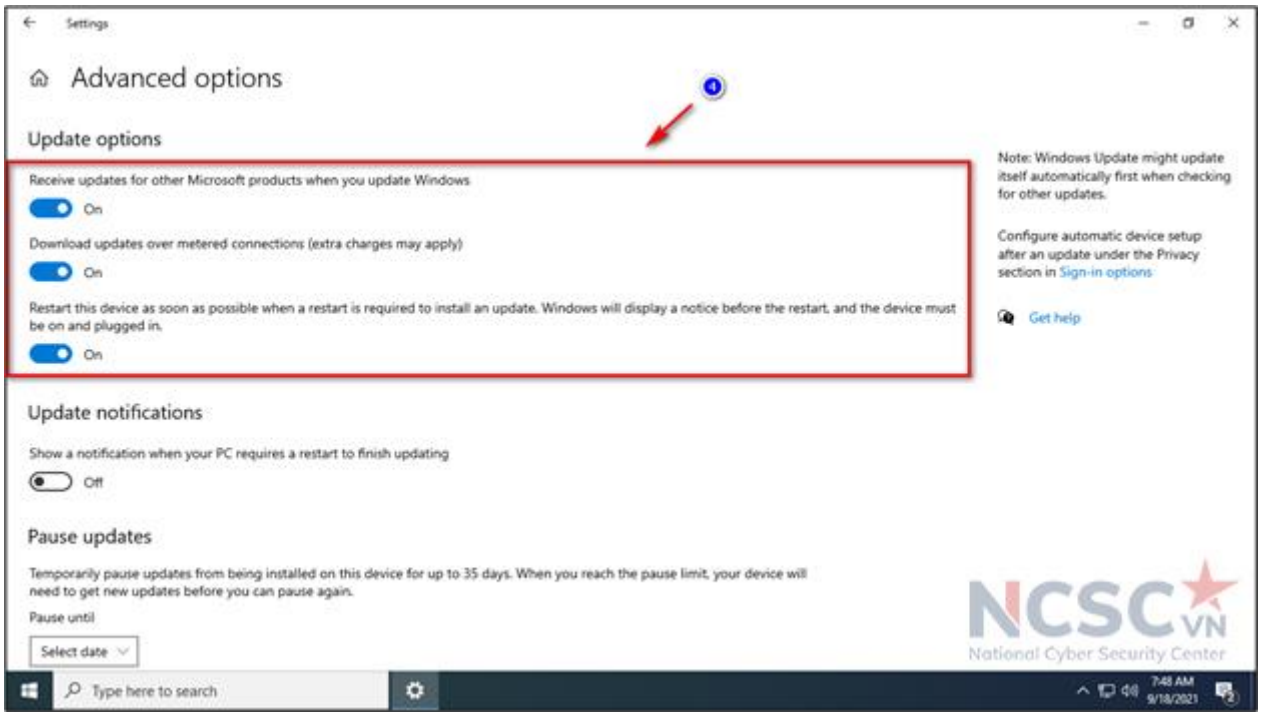
Hình 69: Cập nhật hệ điều hành (1)

Bước 2: Trong Windows Update > Chọn Advanced options



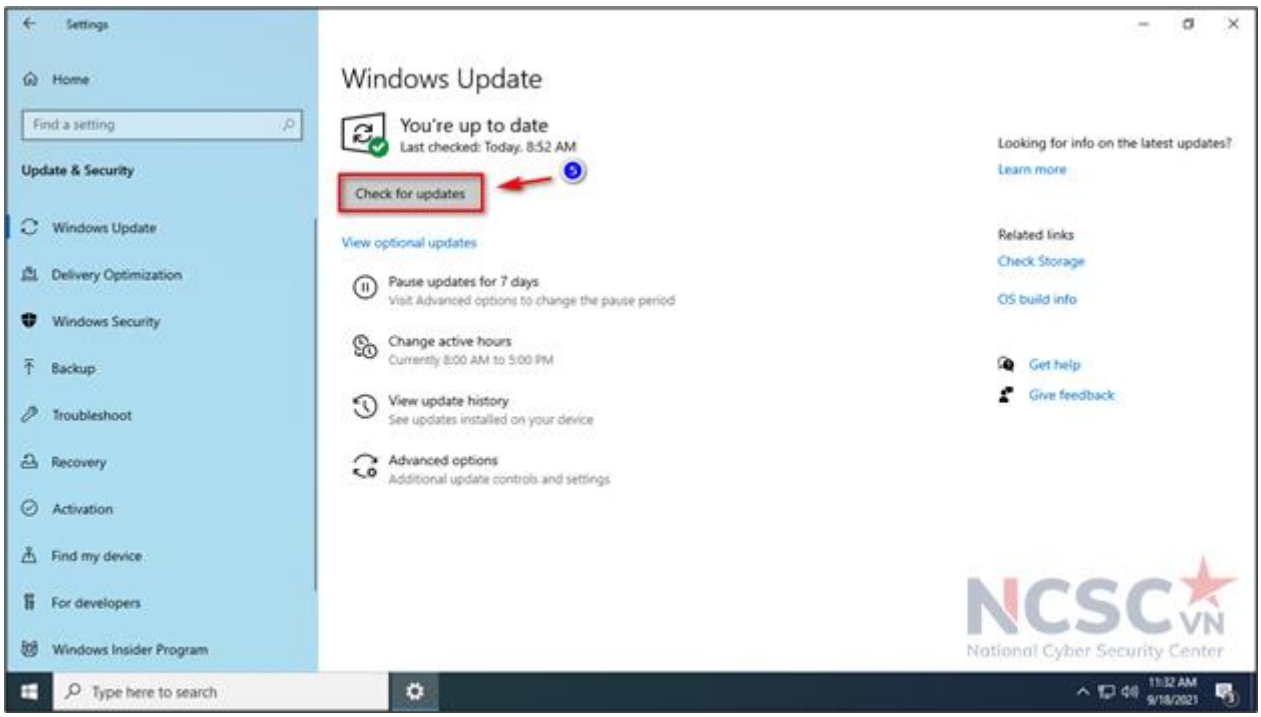
Hình 70: Cập nhật hệ điều hành (2)

Bước 3: Bật các option để tự động cập nhật hệ điều hành và các phần mềm



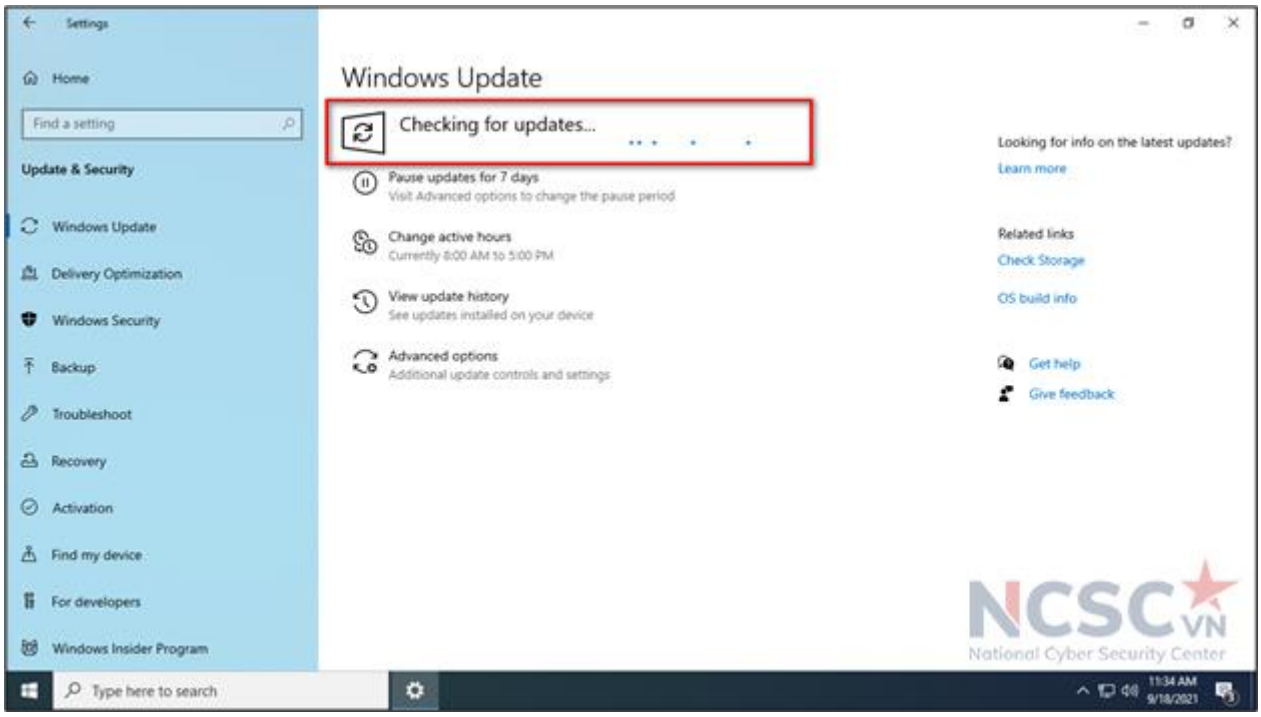
Hình 71: Cập nhật hệ điều hành (3)

Bước 4: Quay lại Windows Update > Check for Updates



Hình 72: Cập nhật hệ điều hành (4)

Lúc này, hệ thống sẽ kiểm tra phiên bản hiện tại mà Microsoft đưa ra với phiên bản hiện tại trên máy tính của người dùng, đồng thời tự động tải về bản cập nhật cần thiết.



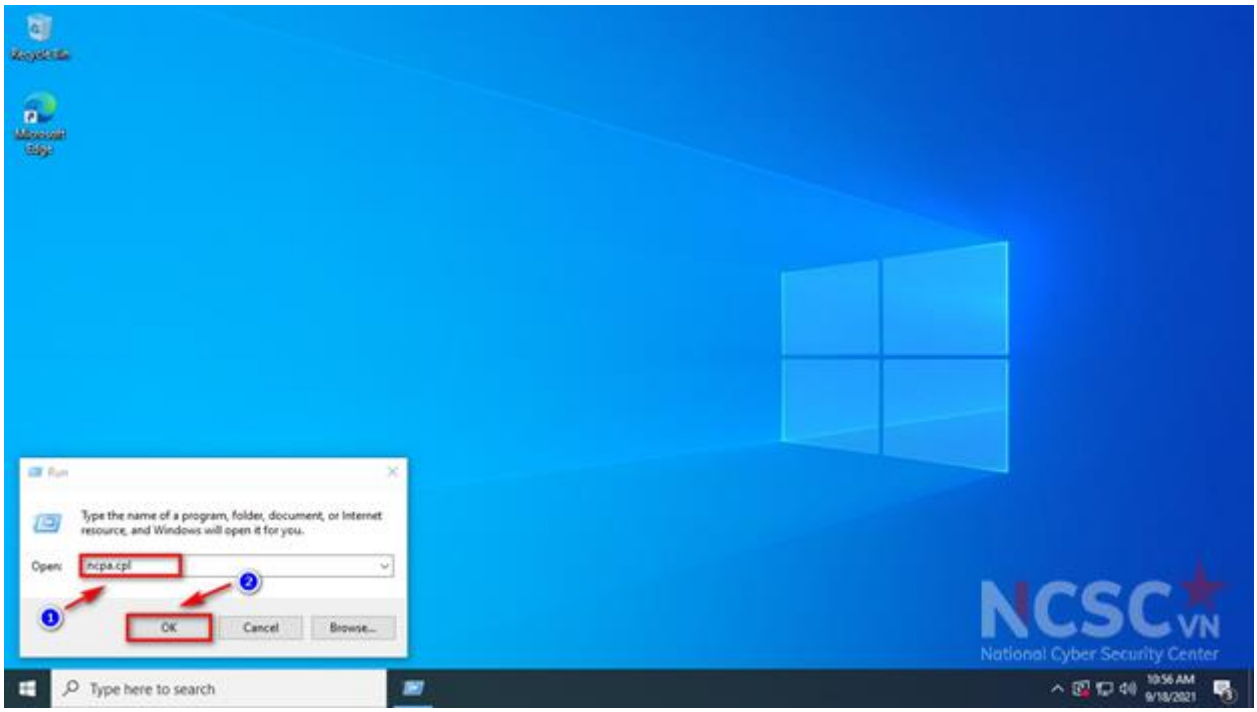
Hình 73: Cập nhật hệ điều hành (5)

Sau khi cập nhật xong, bấm Restart để khởi động lại máy tính.

1.1.8. Cấu hình mạng

Hiện nay địa chỉ IPv4 đang dần cạn kiệt, do đó địa chỉ IPv6 ra đời nhằm mục đích thay thế dần địa chỉ IPv4. Kể từ Windows Vista trở đi IPv6 được kích hoạt theo mặc định, tuy nhiên nhiều thiết bị, hệ thống mạng không hỗ trợ IPv6. Ngoài ra, giao thức IPv6 được sử cũng tồn tại nhiều lỗ hổng bảo mật gây mất an toàn thông tin cho thiết bị. Do vậy người dùng có thể vô hiệu hóa giao thức IPv6 trên máy tính.

Bước 1: Nhấn tổ hợp phím Windows + R, sau đó nhập ncpa.cpl và nhấn OK.

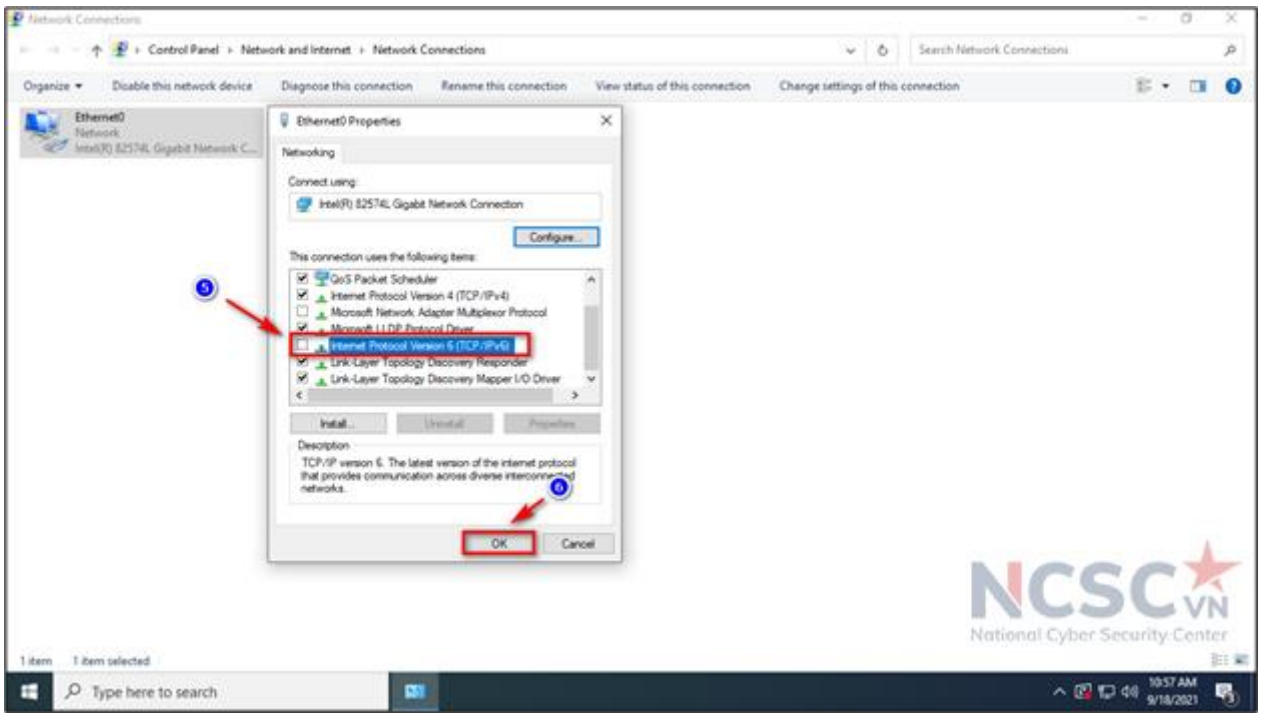


Hình 74: Cấu hình mạng (1)

Bước 2: Chuột phải vào Network Adapter đang sử dụng, chọn Properties

Hình 75: Cấu hình mạng (2)

Bước 3: Tiếp theo trên cửa sổ Properties, click chọn thẻ Networking, tại đây bạn bỏ tích tùy chọn Internet Protocol Version 6 (TCP/Ipv6), xong bấm OK.



Hình 76: Cấu hình mạng (3)

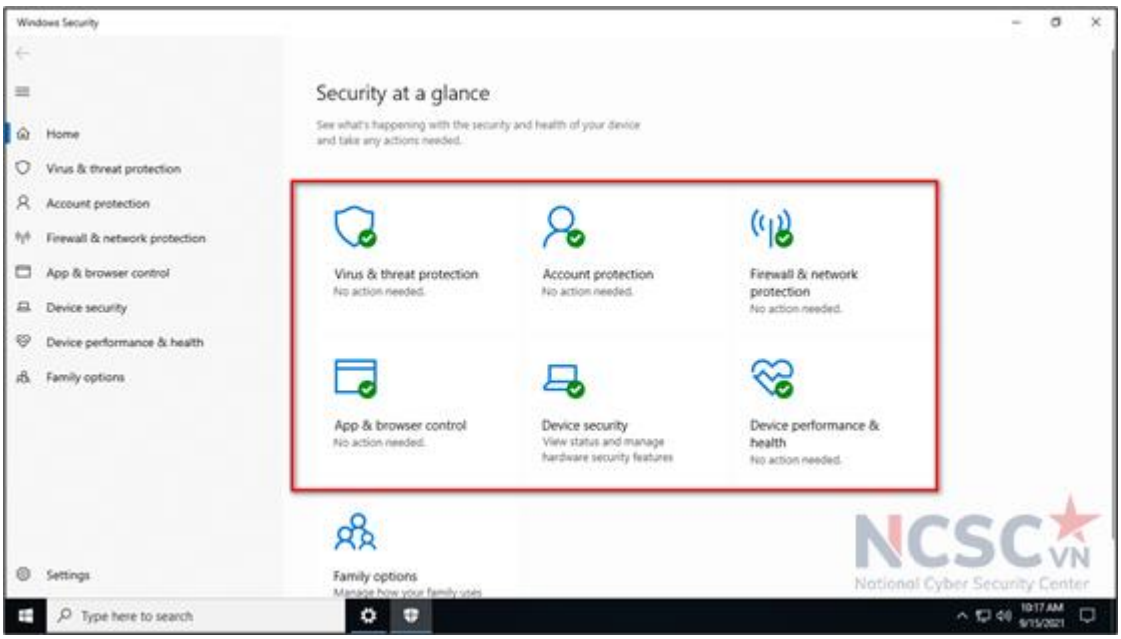
1.1.9. Sử dụng tính năng cơ bản của Windows Defender

Windows Defender là một trình diệt virus miễn phí đi kèm với Windows 10, phiên bản mới hiện nay có tên gọi Windows Security

Khi người dùng khởi động Windows 10, Windows Security sẽ được bật và chủ động bảo vệ máy tính bằng cách quét các phần mềm độc hại, virus, cũng như các mối đe dọa bảo mật khác.

Bật Window security để bảo vệ máy tính:

Nhấm Start > chọn Setting > chọn Update & Security > chọn Windows Security > chọn Open Windows Security.



Hình 77: Bật Windows Security để bảo vệ máy tính

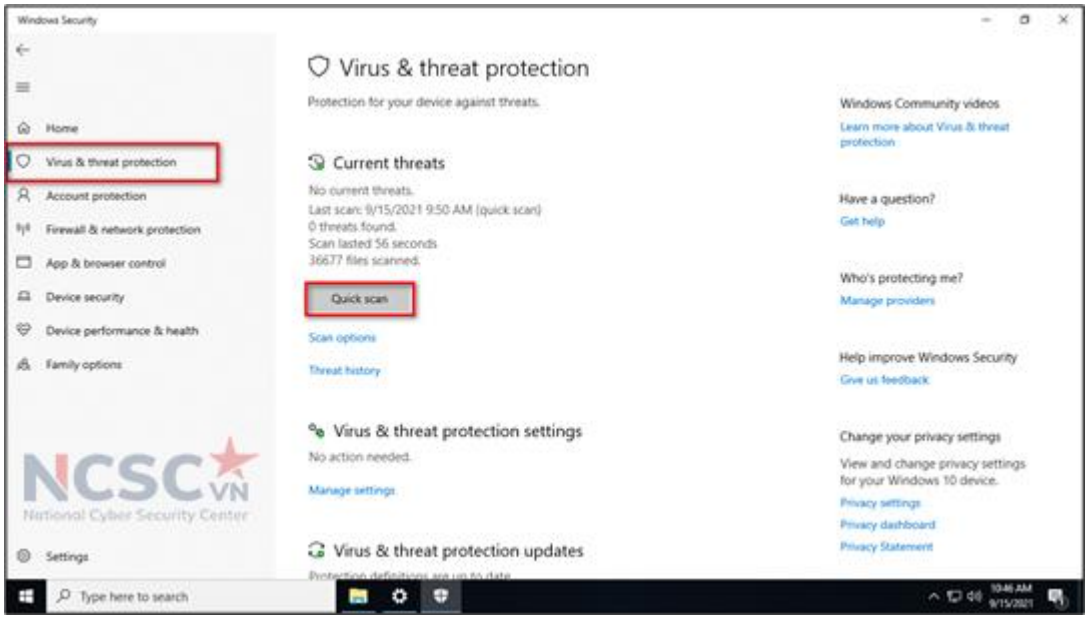
Kiểm tra khả năng bảo mật của máy tính:

Windows Security đánh giá khả năng bảo mật trên máy tính thông qua ba màu sắc tương ứng với từng cấp độ cảnh báo khác nhau:

- Màu xanh lục: máy tính đang được bảo vệ đầy đủ cũng như không có bất kỳ mối đe dọa nào. Bạn không phải triển khai thêm bất cứ thiết lập bảo mật nào.
- Màu vàng: máy tính thiết lập thêm các cài đặt an toàn
- Màu đỏ: cảnh báo có sự xuất hiện của rủi ro bảo mật, cần phải kiểm tra lại ngay.

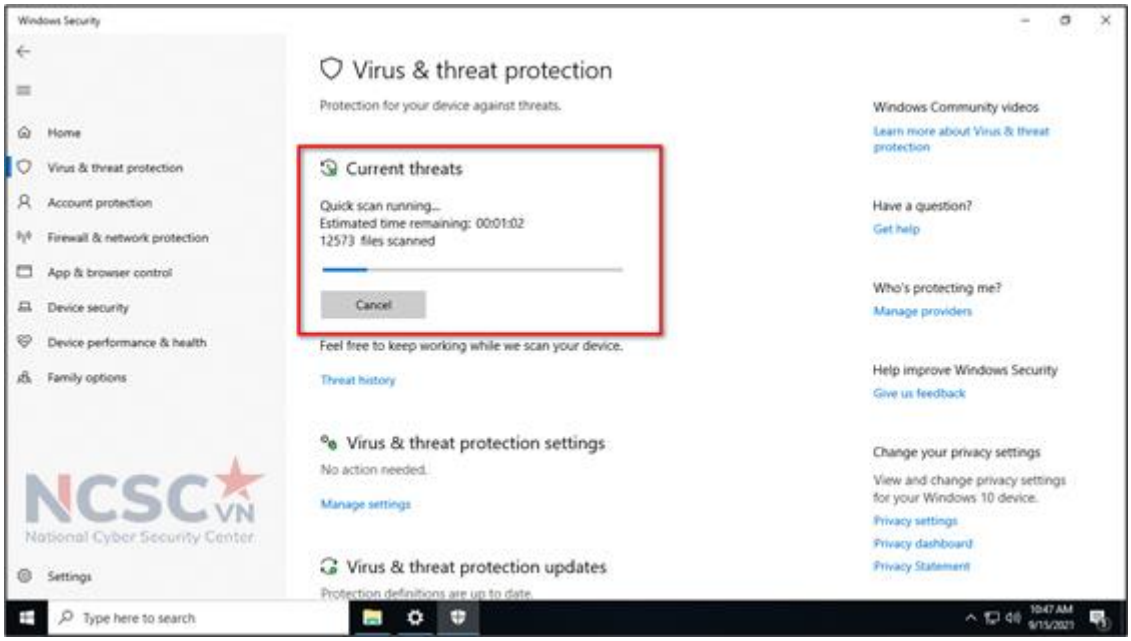
Quét mã độc bằng Windows Security:

Trong Window security, chọn Virus & threat protection > trong mục Current Threats, chọn Quick scan



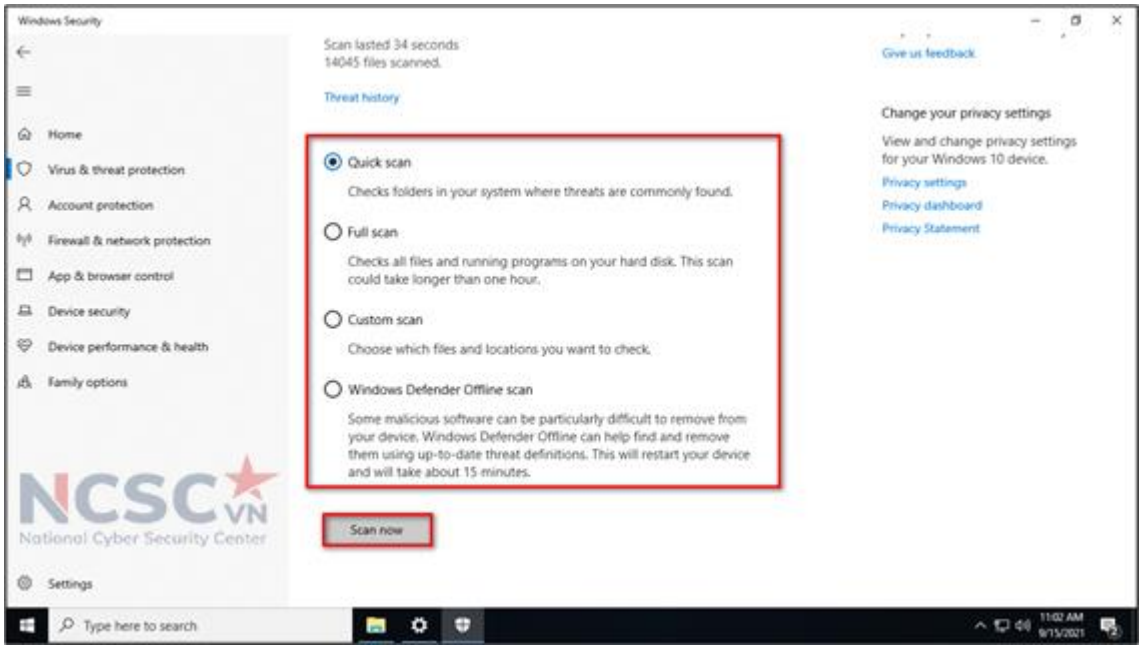
Hình 78: Quét mã độc bằng Windows Security (1)

Tiến trình quét Virus đang diễn ra



Hình 79: Quét mã độc bằng Windows Security (2)

Ngoài ra, chúng ta có thể lựa chọn các tùy chọn chuyên sâu hơn để quét Virus ở mục Scan option.



Hình 80: Quét mã độc bằng Windows Security (3)

- Quick scan: Chỉ kiểm tra các thư mục trong hệ thống nơi mà thường bị đe dọa tấn công.

- Full scan: Quét toàn bộ file trong hệ thống. Sẽ mất nhiều thời gian để quét.

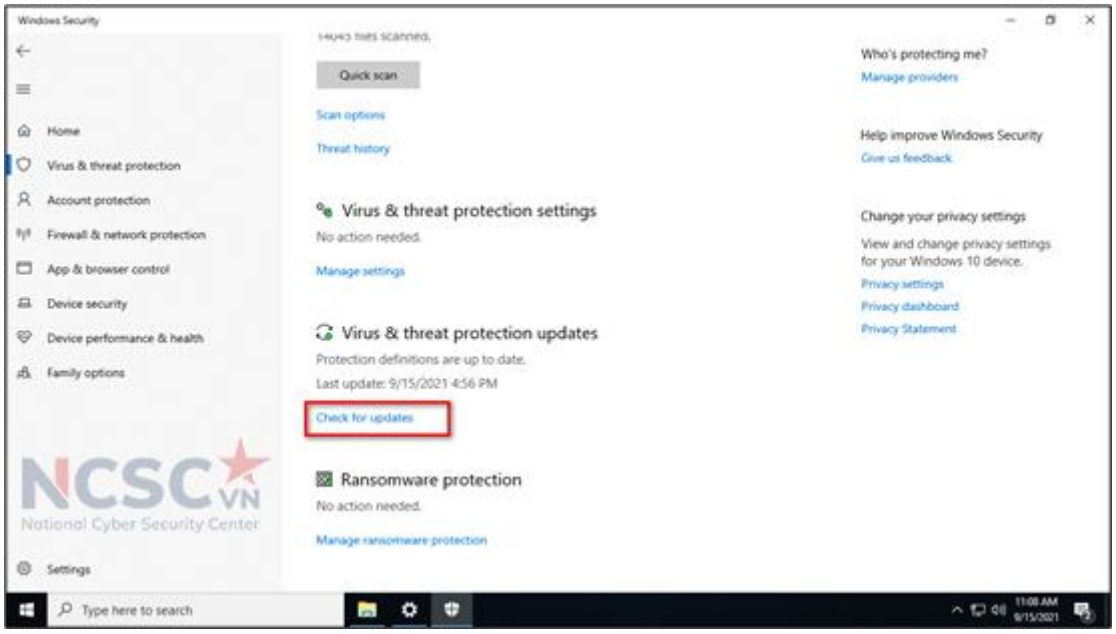
- Custom Scan: Chỉ quét file hoặc thư mục bạn muốn.

- Windows Defender Offline scan: quét và gỡ bỏ một số phần mềm độc hại đặc biệt. Cần một khoảng thời gian đủ lâu và sẽ cần khởi động lại máy tính.

Sau khi lựa chọn cách quét Virus, click vào “Scan now” để quét.

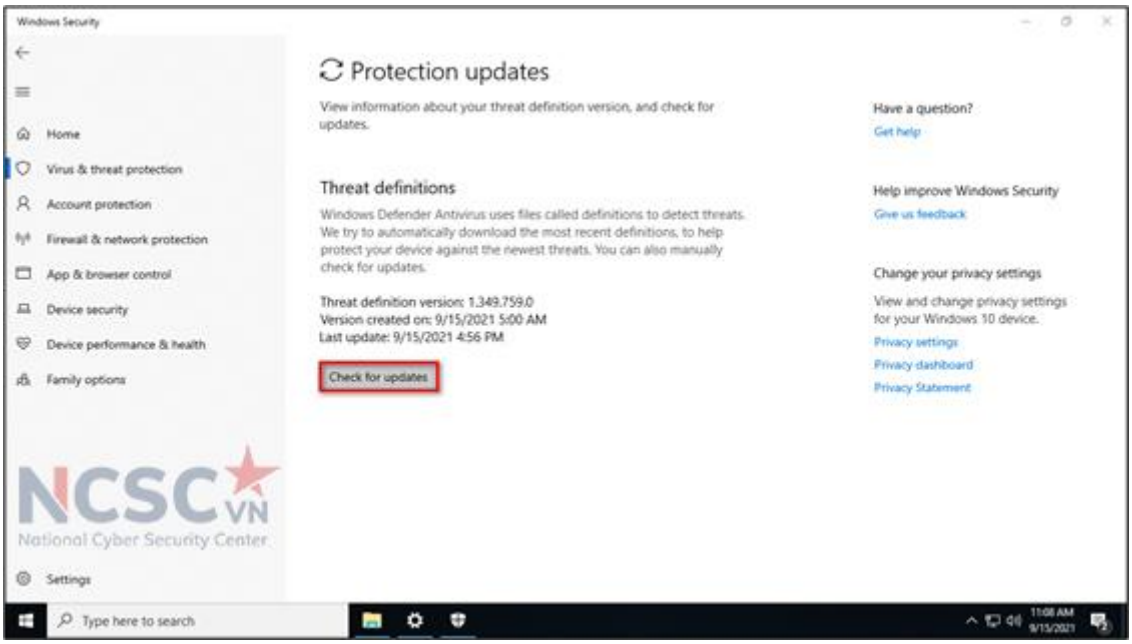
1.1.10. Cập nhật Virus và các mối đe dọa bằng Window Security

Trong Window Security, chọn Virus & threat protection > trong Virus & threat protection updates, chọn Check for updates



Hình 81: Cập nhật virus và các mối đe dọa bằng Windows Security (1)

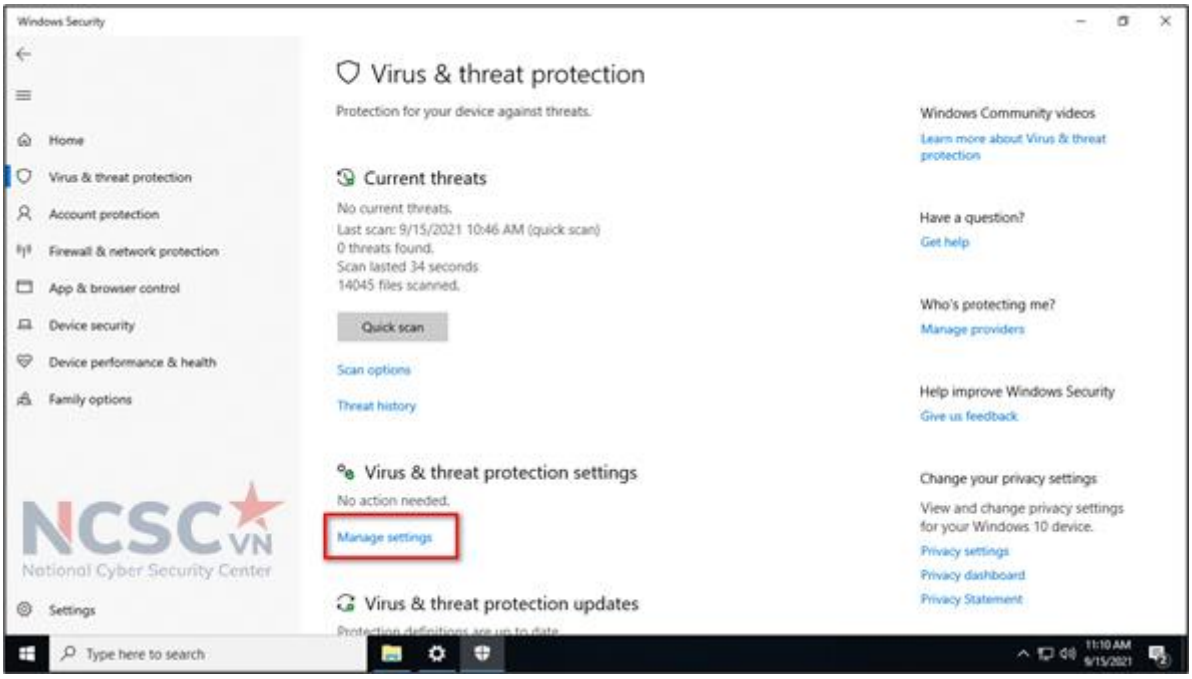
Chọn tiếp Check for updates, để tiến hành cập nhật



Hình 82: Cập nhật virus và các mối đe dọa bằng Windows Security (2)

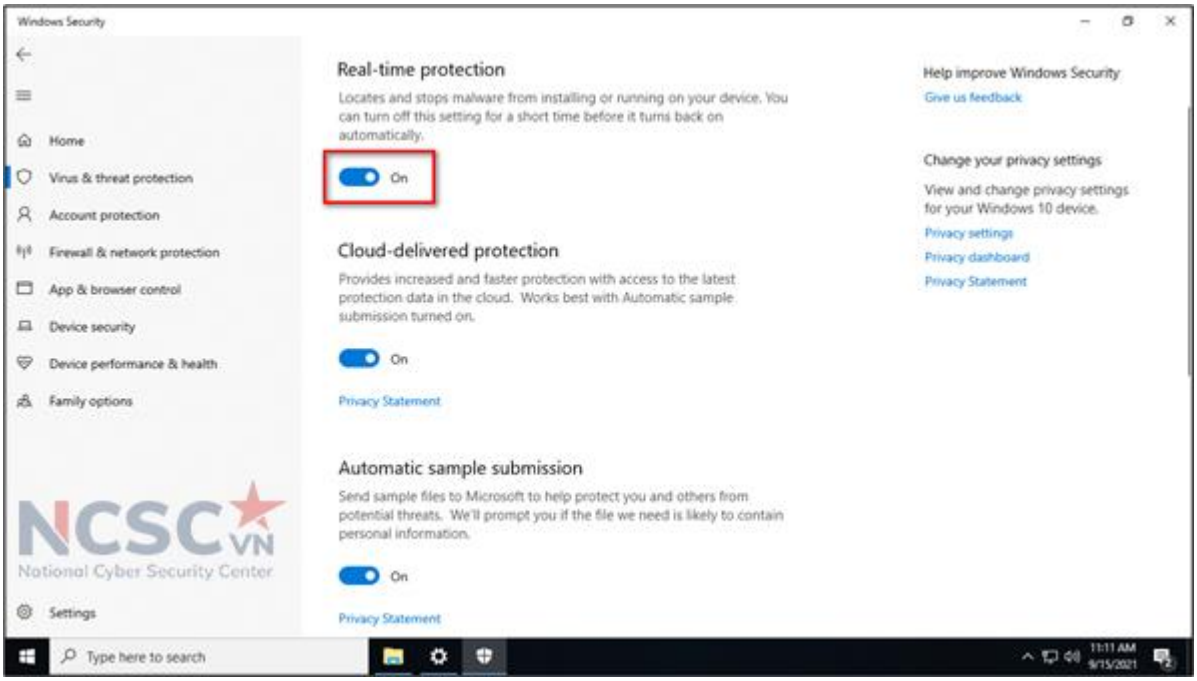
1.1.12. Bật tính năng tự động bảo vệ thiết bị theo thời gian thực trên Window Security

Trong Window Security, chọn Virus & threat protection > trong Virus & threat protection settings, chọn Manage settings



Hình 83: Bật tính năng bảo vệ thiết bị theo thời gian thực trên Windows Security (1)

Bật tính năng, ON trong mục Real-time protection



Hình 84: Bật tính năng bảo vệ thiết bị theo thời gian thực trên Windows Security (2)

1.2. Quản lý tài khoản trên máy người dùng

1.2.1. Tạo tài khoản riêng trên Windows cho mục đích giảng dạy, học tập

Windows 10 cho phép tạo hai loại tài khoản: tài khoản quản trị viên

(Administrator) và tài khoản người dùng tiêu chuẩn (Standard).

Bạn nên tạo riêng tài khoản (Standard) cho mục đích giảng dạy, học tập. Đặc biệt với máy tính có nhiều người dùng (ví dụ các giáo viên sử dụng chung máy tính của nhà trường để giảng dạy, cha mẹ có 2 con em cùng học trên một máy tính trong các khung giờ khác nhau).

Tại sao nên tạo riêng tài khoản cho mục đích giảng dạy?

- Người dùng không nên sử dụng tài khoản quản trị viên trong quá trình học tập, giảng dạy, vì việc học tập, giảng dạy trực tuyến không yêu cầu phải có quyền quản trị viên. Đặc biệt các em học sinh nếu không cẩn thận trong quá trình sử dụng tài khoản quản trị viên có thể vô tình tải và cài đặt mã độc cài cắm trong các ứng dụng không tin cậy.

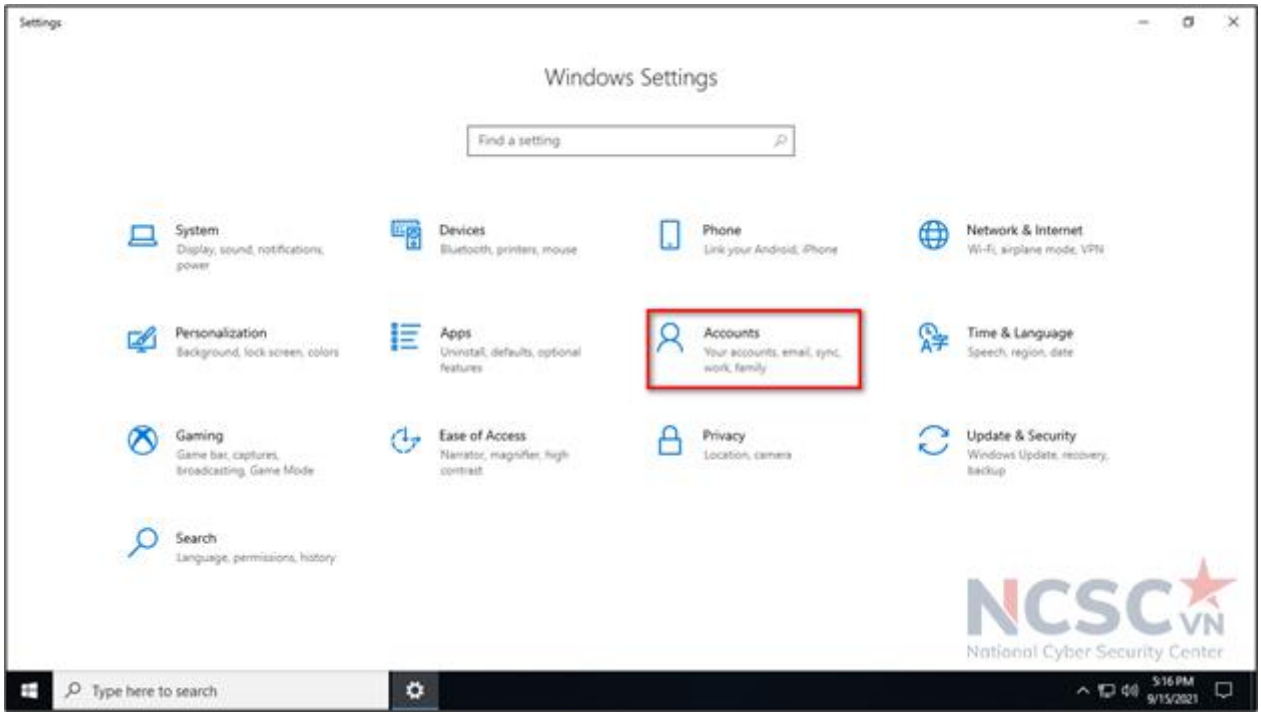
- Nếu để máy tính không khóa, bất cứ ai cũng có thể truy cập vào máy tính và thực hiện thay đổi trái phép mà không có sự cho phép của chủ sở hữu.

- Mỗi người có thể tự sắp xếp dữ liệu của mình mà cơ bản không bị người khác làm thay đổi.

- Không làm ảnh hưởng đến các ứng dụng, dữ liệu của cha mẹ lưu trên máy tính.

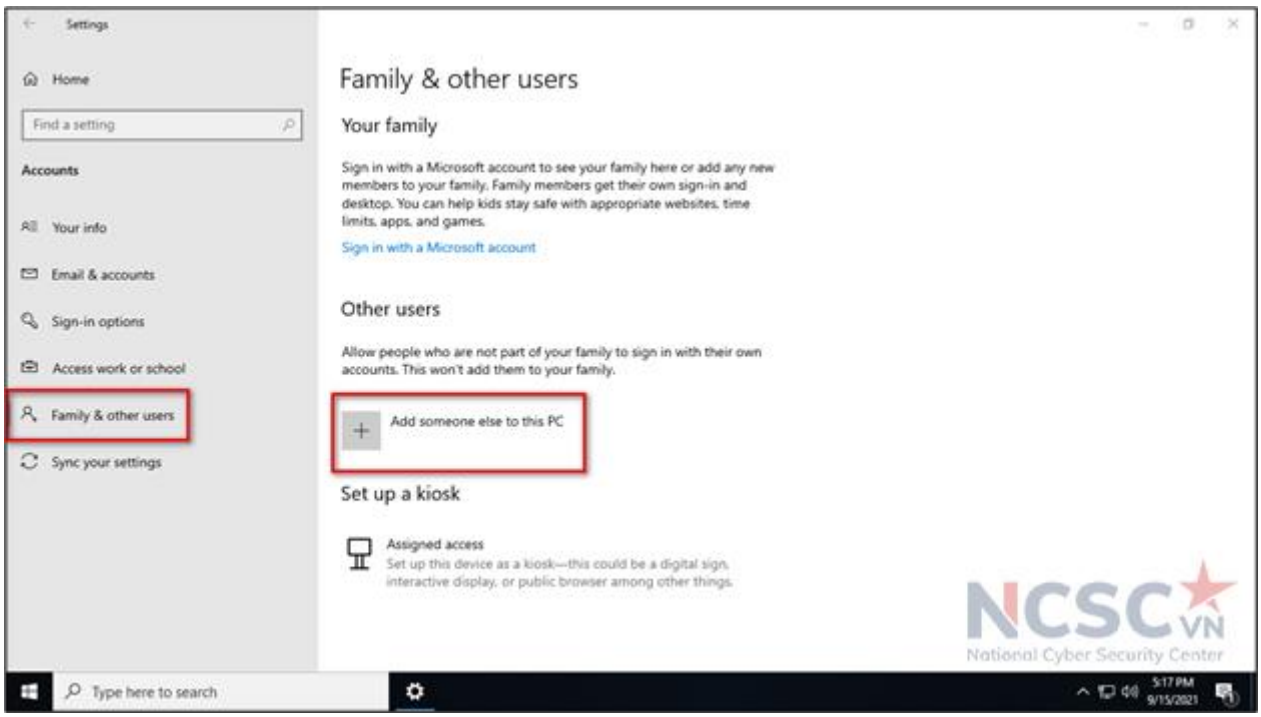
Cách 1: Tạo tài khoản bằng Windows Settings.

Bước 1: Nhấn phím Windows + I để mở Settings và click vào Accounts.



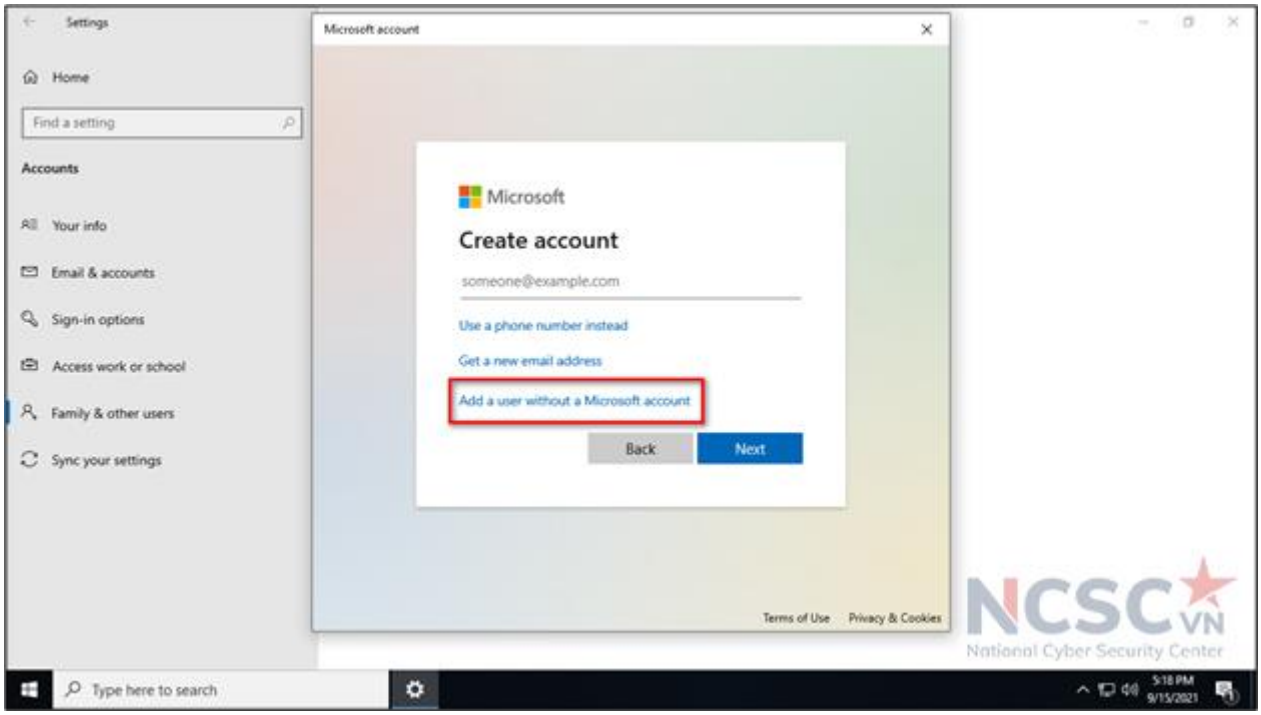
Hình 85: Tạo tài khoản người dùng tiêu chuẩn (1)

Bước 2. Chọn Add a family member, trong mục Other Users chọn Add someone else to this PC.



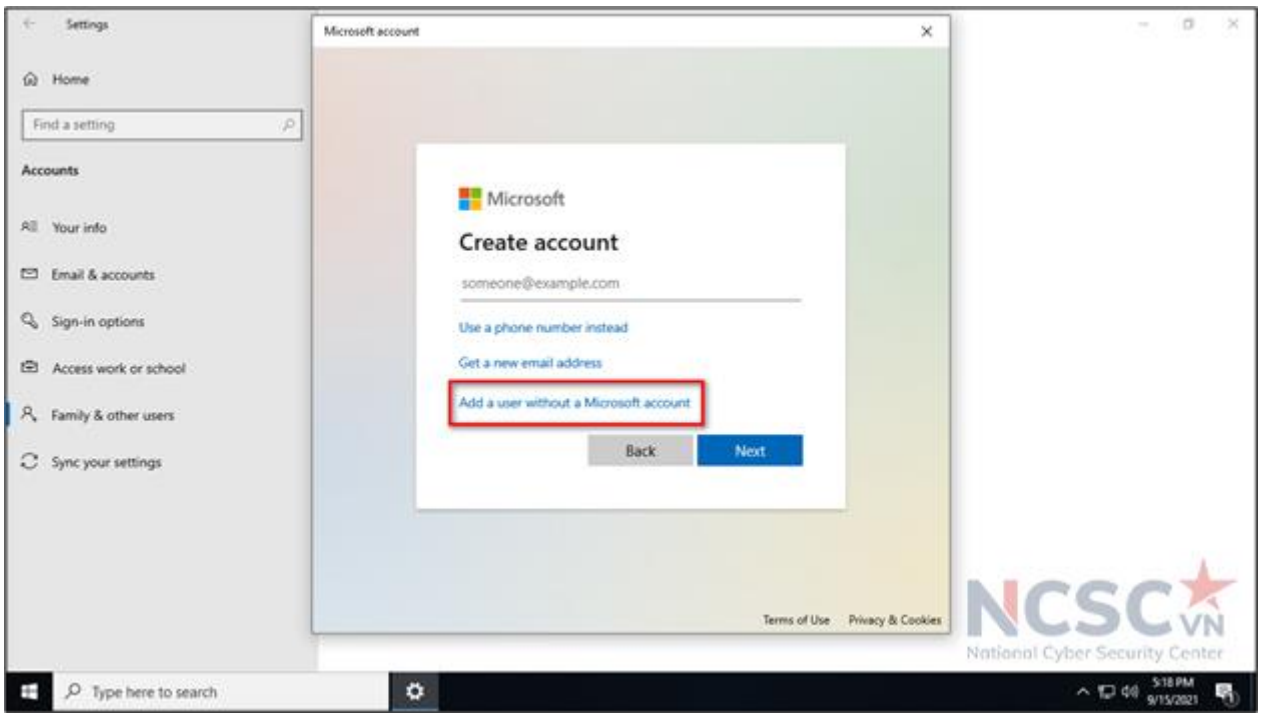
Hình 86: Tạo tài khoản người dùng tiêu chuẩn (2)

Bước 3. Click vào I don’t have this person’s sign-in information và chọn Next



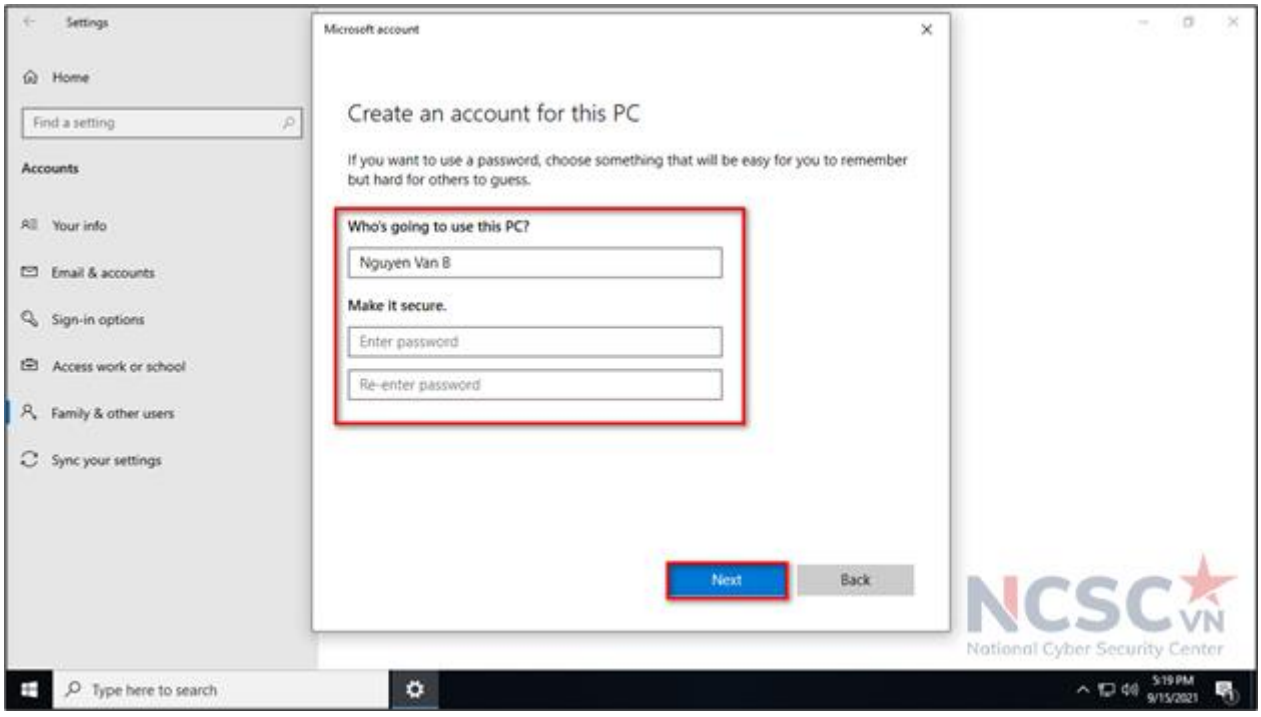
Hình 87: Tạo tài khoản người dùng tiêu chuẩn (3)

Bước 4. Click vào Add a user without Microsoft account.



Hình 88: Tạo tài khoản người dùng tiêu chuẩn (4)

Bước 5. Nhập tên người dùng và mật khẩu, trả lời 3 câu hỏi bí mật, sau đó bấm Next để tiếp tục.

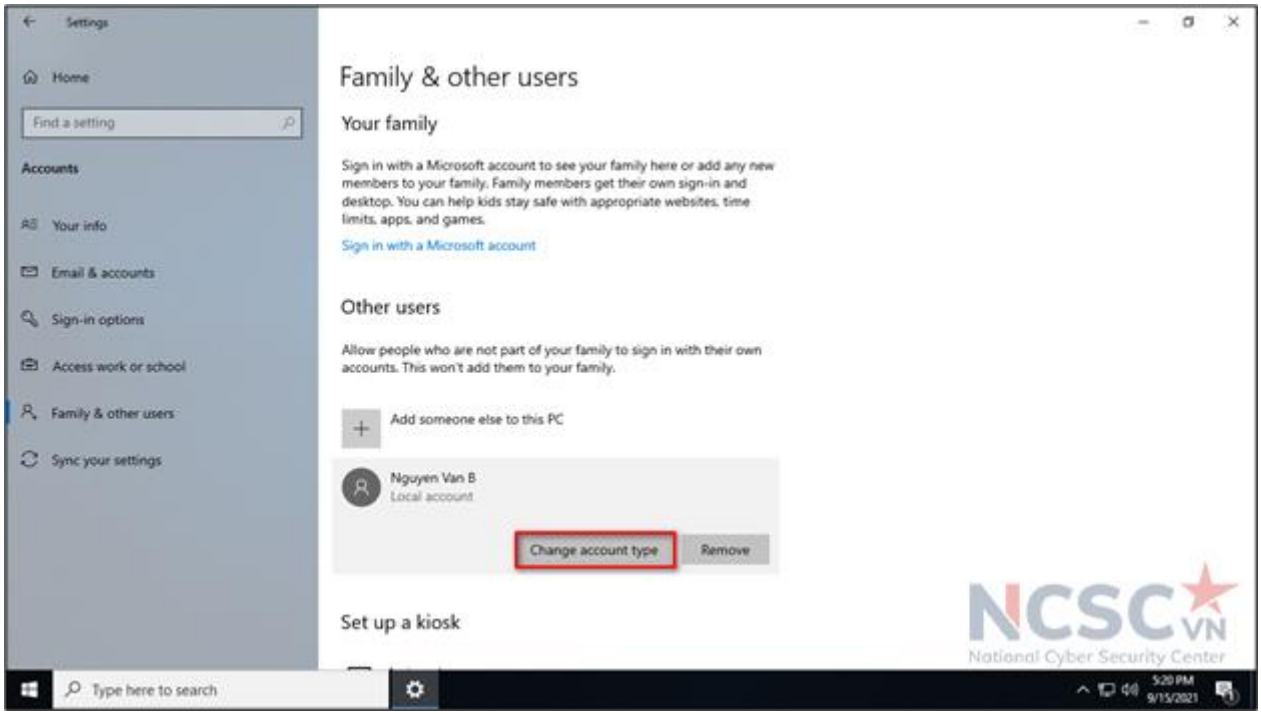


Hình 89: Tạo tài khoản người dùng tiêu chuẩn (5)

Bạn có thể bỏ qua Bước 6 và bước 7 nếu không muốn cấp quyền quản trị viên cho tài khoản giảng dạy, học tập. Vì thông thường chỉ cần dùng đến tài khoản quản trị khi cần cài đặt, hoặc gỡ bỏ phần mềm, ứng dụng khỏi máy tính.

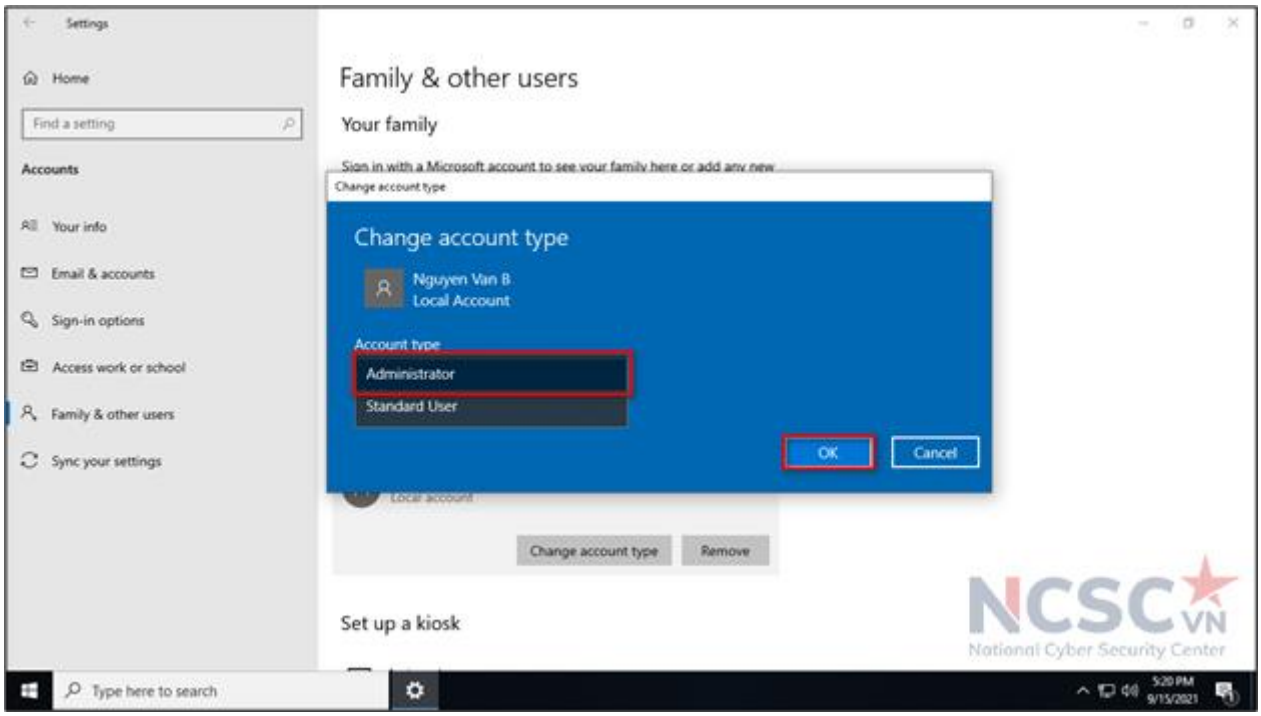
Bước 6 (có thể bỏ qua bước này). Thay đổi tài khoản này từ người dùng tiêu chuẩn

sang quản trị viên: Chọn tên tài khoản > Change account type.



Hình 90: Tạo tài khoản người dùng tiêu chuẩn (6)

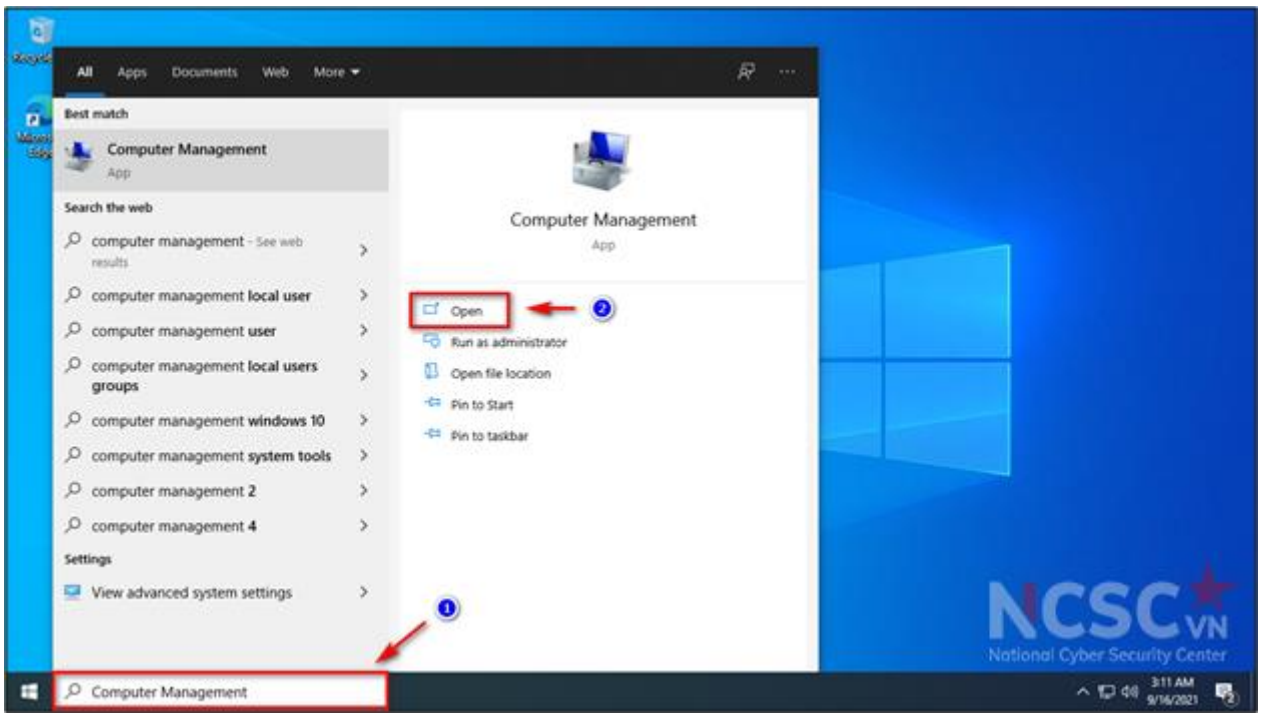
Bước 7. Cấp quyền quản trị cho tài khoản này.



Hình 91: Tạo tài khoản người dùng tiêu chuẩn (7)

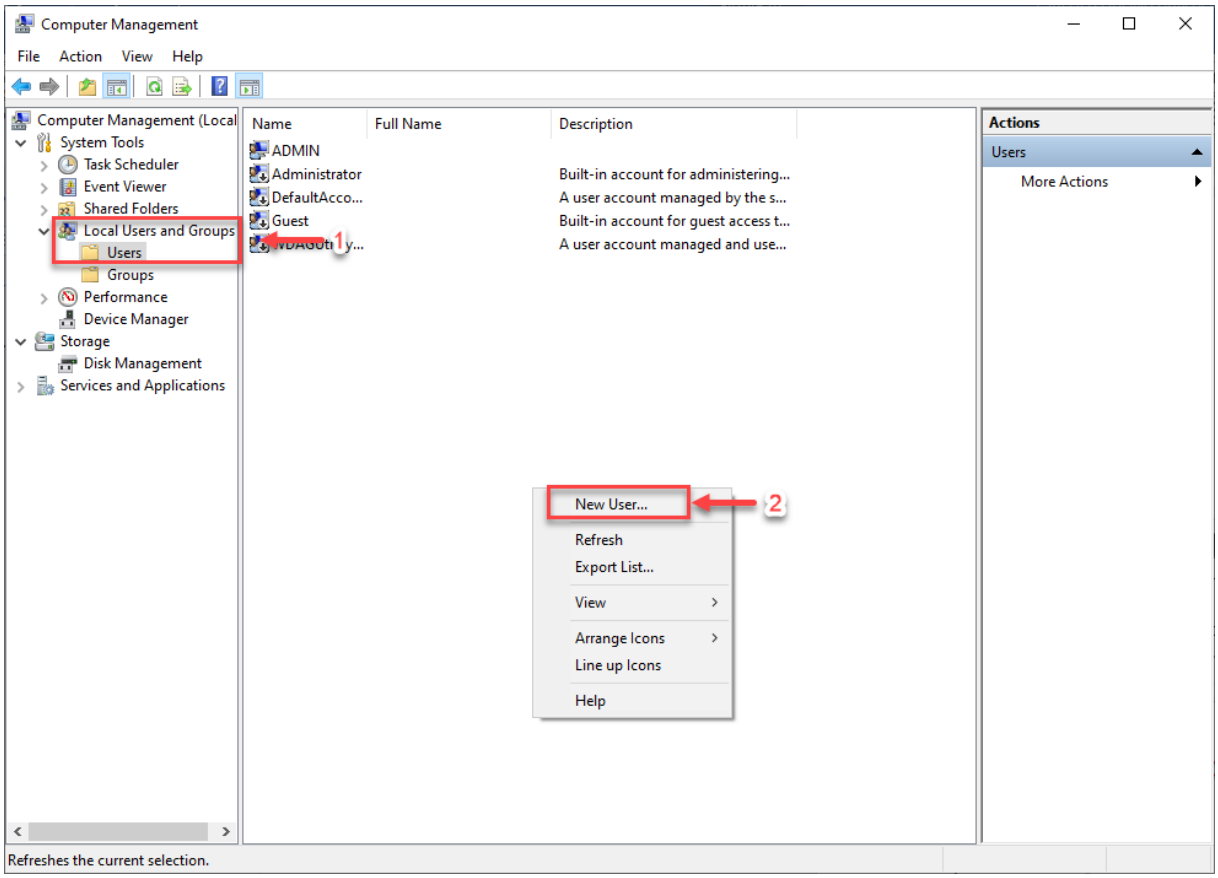
Cách 2: Tạo tài khoản bằng Computer Management.

Bước 1: Tại biểu tượng tìm kiếm trên Windows > nhập Computer Management và chọn Open.



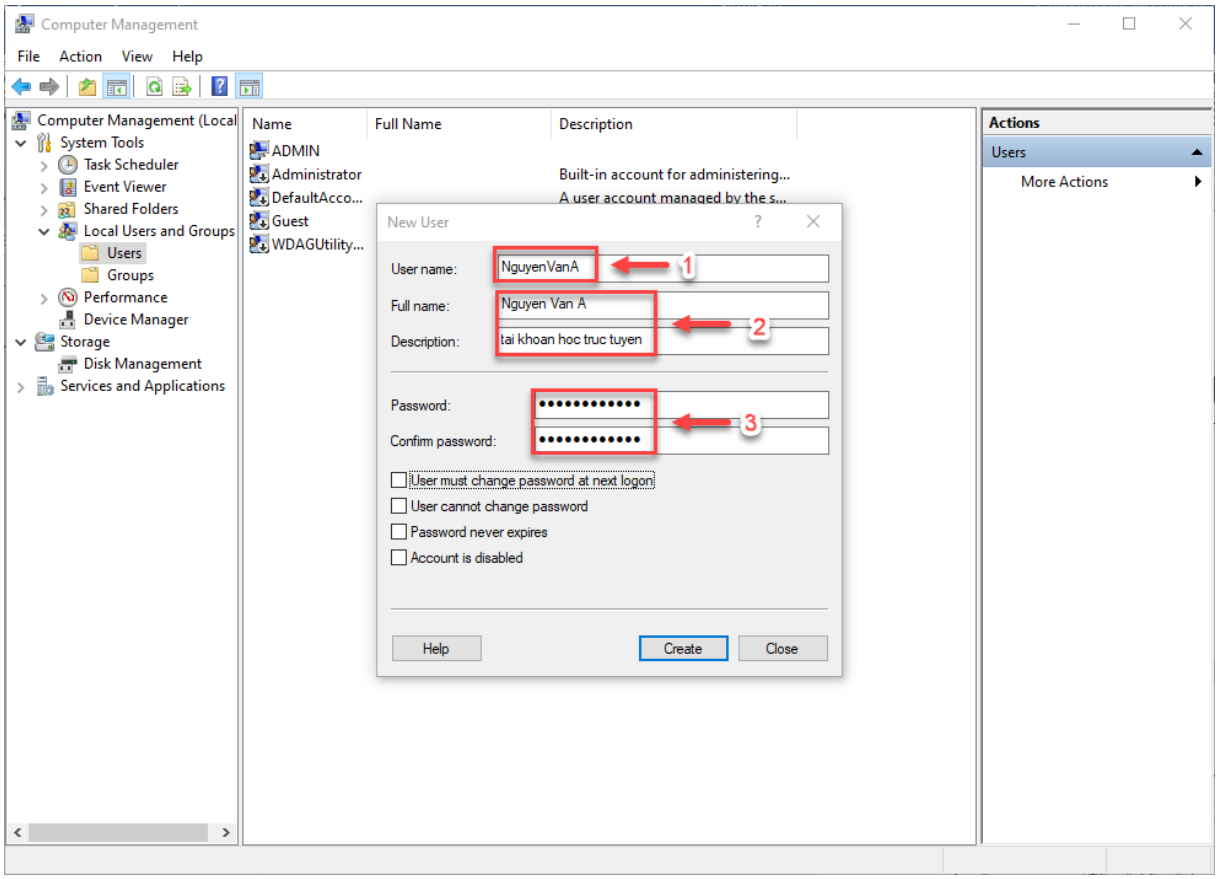
Hình 92: Tạo tài khoản người dùng tiêu chuẩn (7)

Bước 2: Tại System Tools > chọn Local Users and Groups > Users > màn hình bên phải xuất hiện các tài khoản người dùng trong Windows > bấm chuột phải chọn New User.



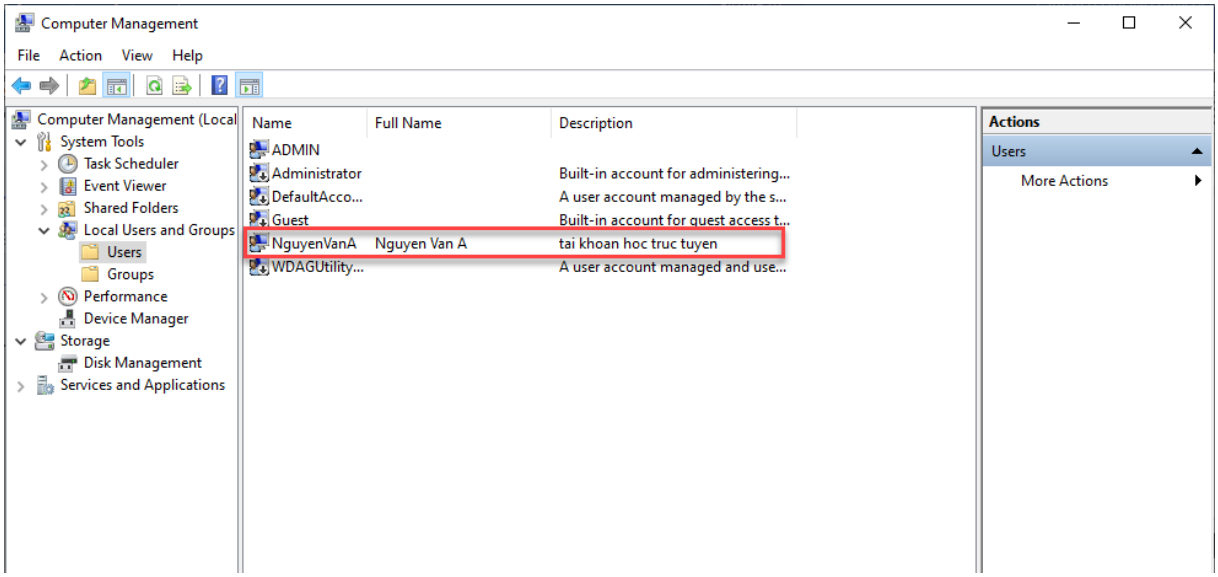
Hình 93: Tạo tài khoản người dùng tiêu chuẩn (8)

Bước 3: Nhập đầy đủ các thông tin cần thiết cho tài khoản muốn tạo (tài khoản (1), ghi chú tài khoản sử dụng (2), mât khẩu cho tài khoản (3)) > Nhấn Create để tạo tài khoản.



Hình 94: Tạo tài khoản người dùng tiêu chuẩn (9)

Nhấn tiếp Close, để quá trình tạo tài khoản kết thúc.

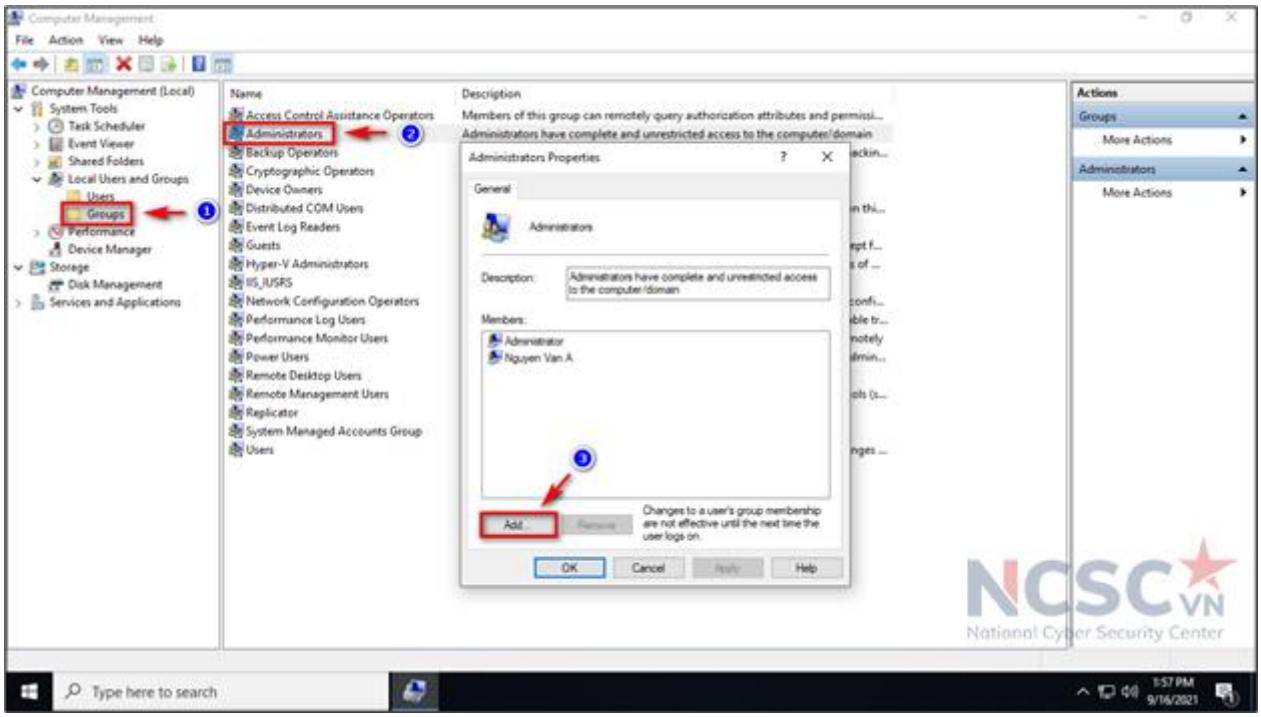


Hình 95: Tạo tài khoản người dùng tiêu chuẩn (10)

Bạn có thể bỏ qua Bước 4 đến Bước 6 nếu không muốn cấp quyền quản trị viên cho tài khoản giảng dạy, học tập. Vì thông thường chỉ cần dùng đến tài khoản quản trị

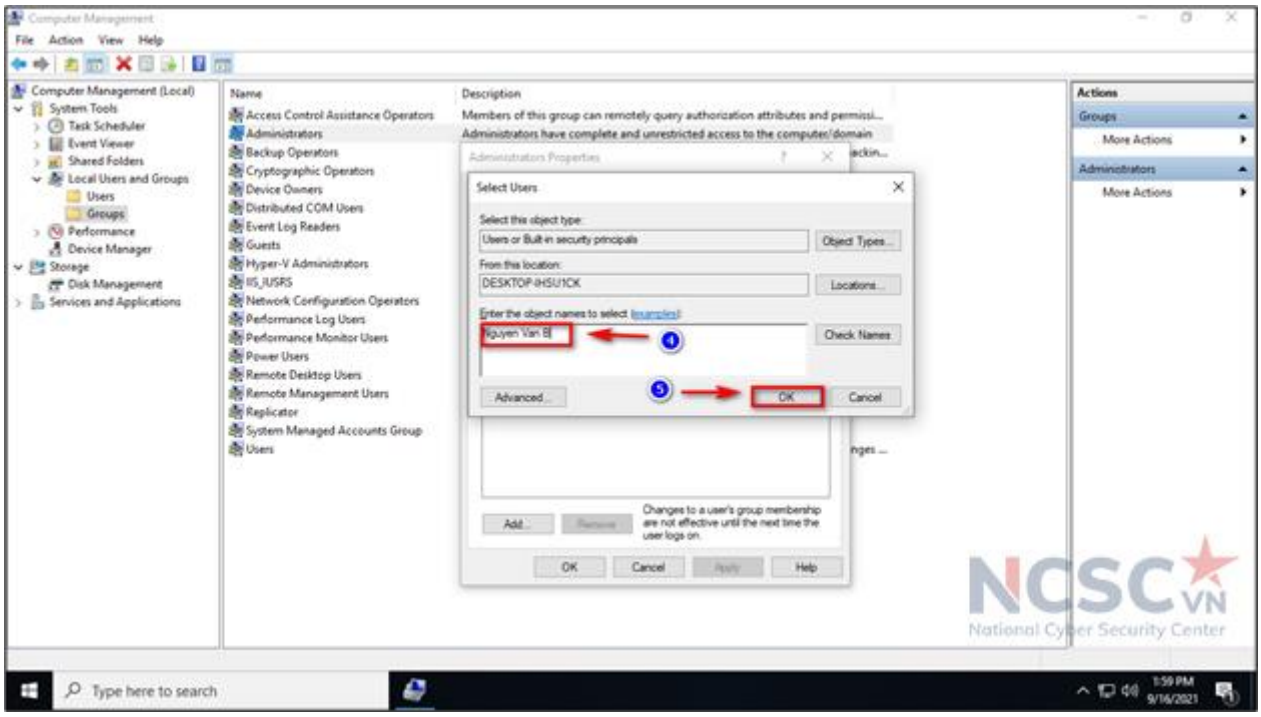
khi cần cài đặt, hoặc gỡ bỏ phần mềm, ứng dụng khỏi máy tính.

Bước 4: Để thêm quyền quản trị viên cho tài khoản vừa tạo, trong Local Users and Groups > chọn Groups > chọn Administrators > chọn Add



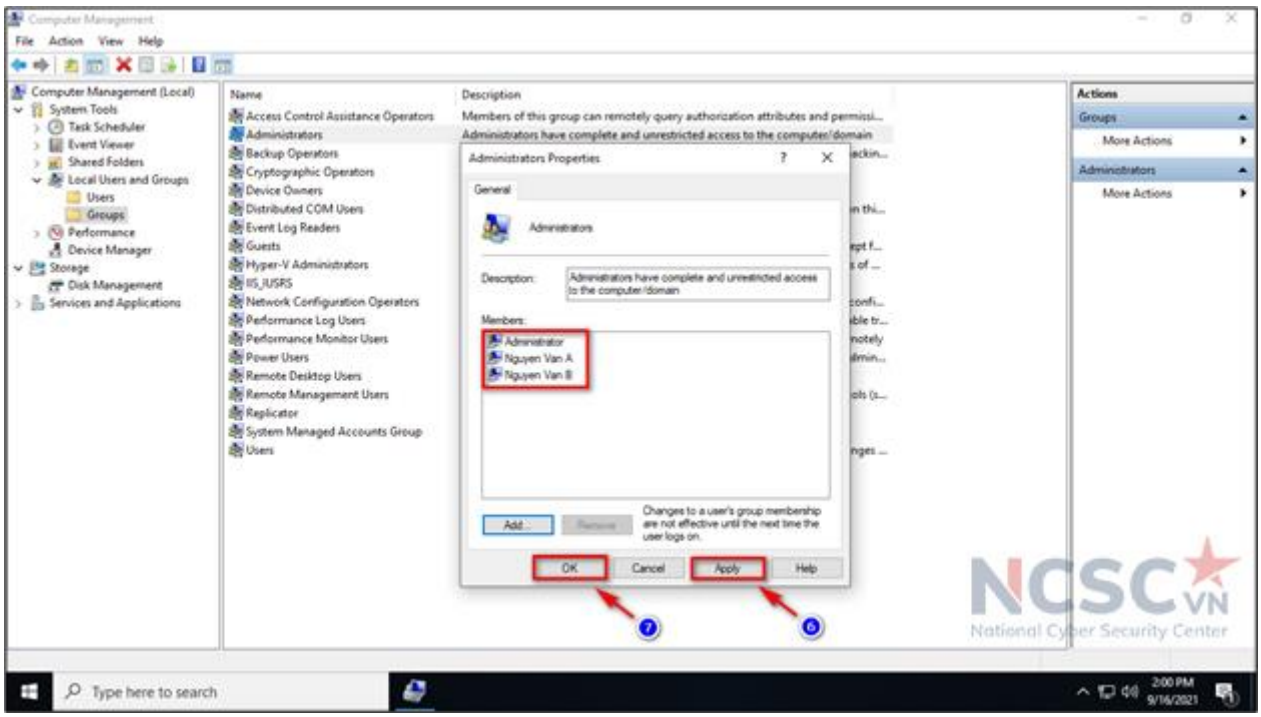
Hình 96: Tạo tài khoản người dùng tiêu chuẩn (11)

Bước 5: Nhập tên tài khoản vừa tạo > bấm OK



Hình 97: Tạo tài khoản người dùng tiêu chuẩn (12)

Bước 6: Bấm Apply > chọn OK để tài khoản được thêm quyền quản trị viên



Hình 98: Tạo tài khoản người dùng tiêu chuẩn (13)

1.2.2. Vô hiệu hóa các tài khoản không cần thiết

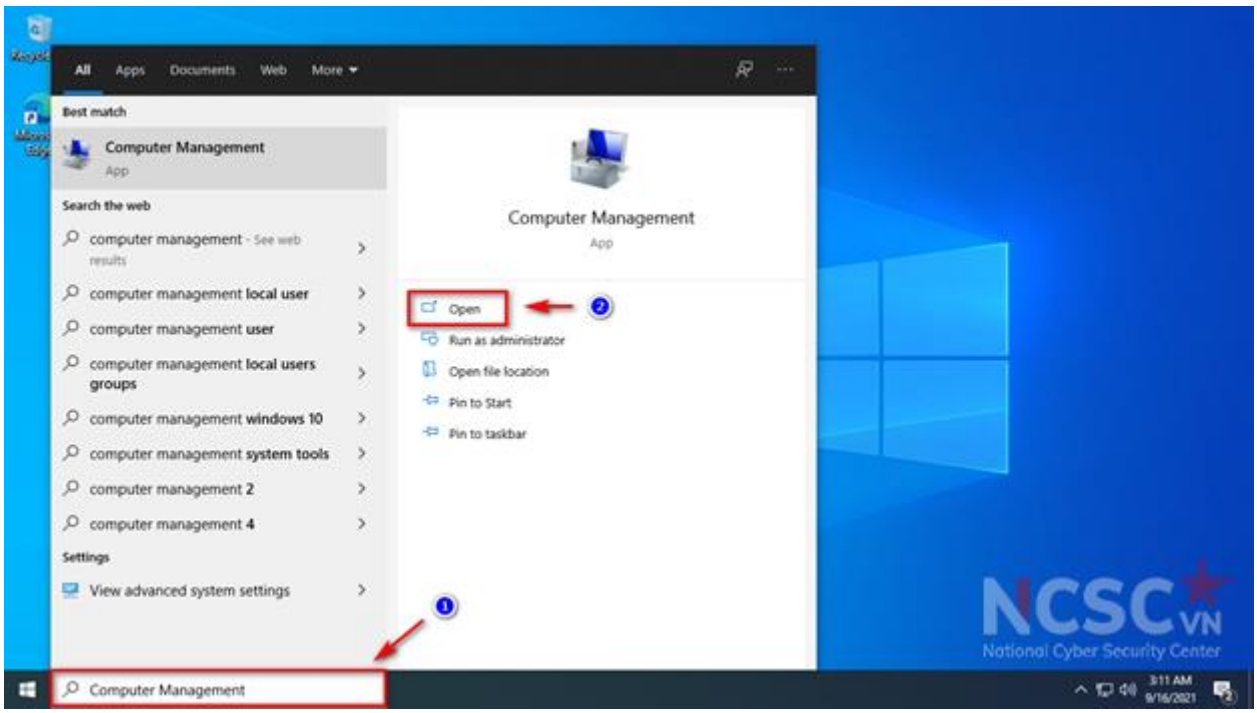
Để đảm bảo vấn đề an toàn thông tin, các tài khoản không cần thiết hoặc không được sử dụng đến nên được vô hiệu hóa. Phần này sẽ hướng dẫn bạn vô hiệu hóa những tài khoản không sử dụng thay vì phải xóa chúng đi. Vì việc xóa tài khoản sẽ làm mất dữ liệu và không thể khôi phục.

Ví dụ với trường hợp các em học sinh quay trở lại cơ sở giáo dục để học bình thường thì cha mẹ có thể tạm thời vô hiệu hóa tài khoản đã cấp cho các em để học trực tuyến trước đây.

Để vô hiệu hóa tài khoản đã tạo, thực hiện các bước dưới đây.

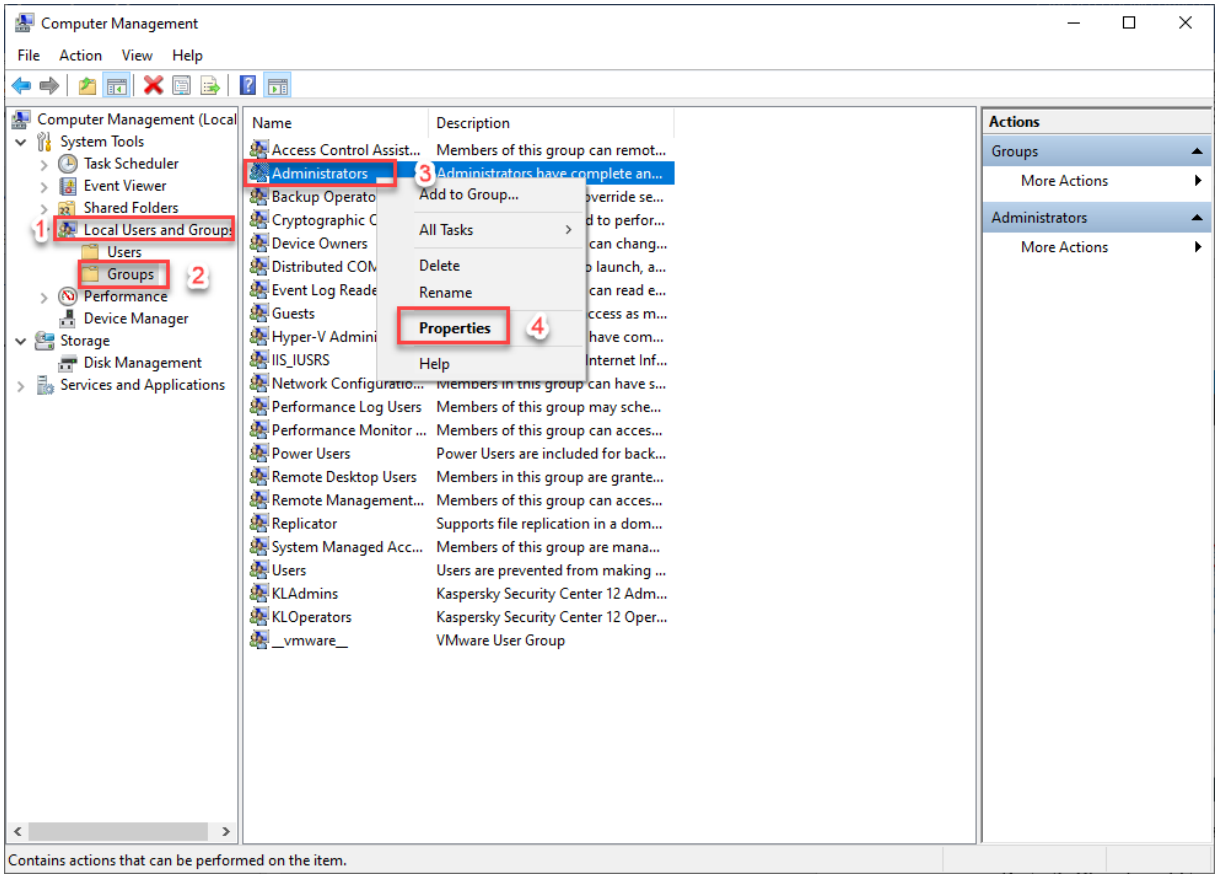
Bước 1: Đảm bảo tài khoản bị disable không phải là tài khoản nằm trong nhóm quản trị administrators (cần có ít nhất 1 tài khoản được cấp quyền trong nhóm administrator để quản trị, cài đặt ứng dụng trên máy tính).

- Vào mục tìm kiếm trên Windows > Computer Management > Open.



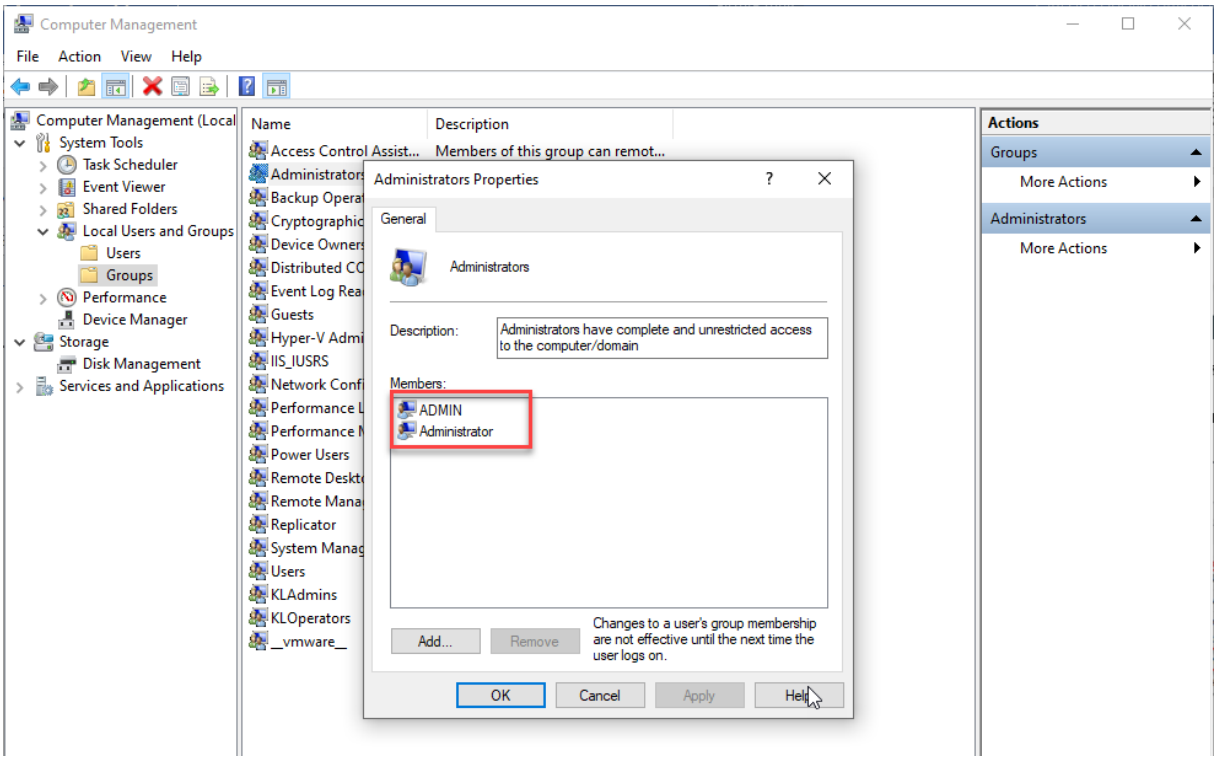
Hình 99: Vô hiệu hóa các tài khoản không cần thiết (1)

Bước 2: Chọn Local User and Groups > Group > bấm chuột phải vào nhóm có tên Administrators > Properties



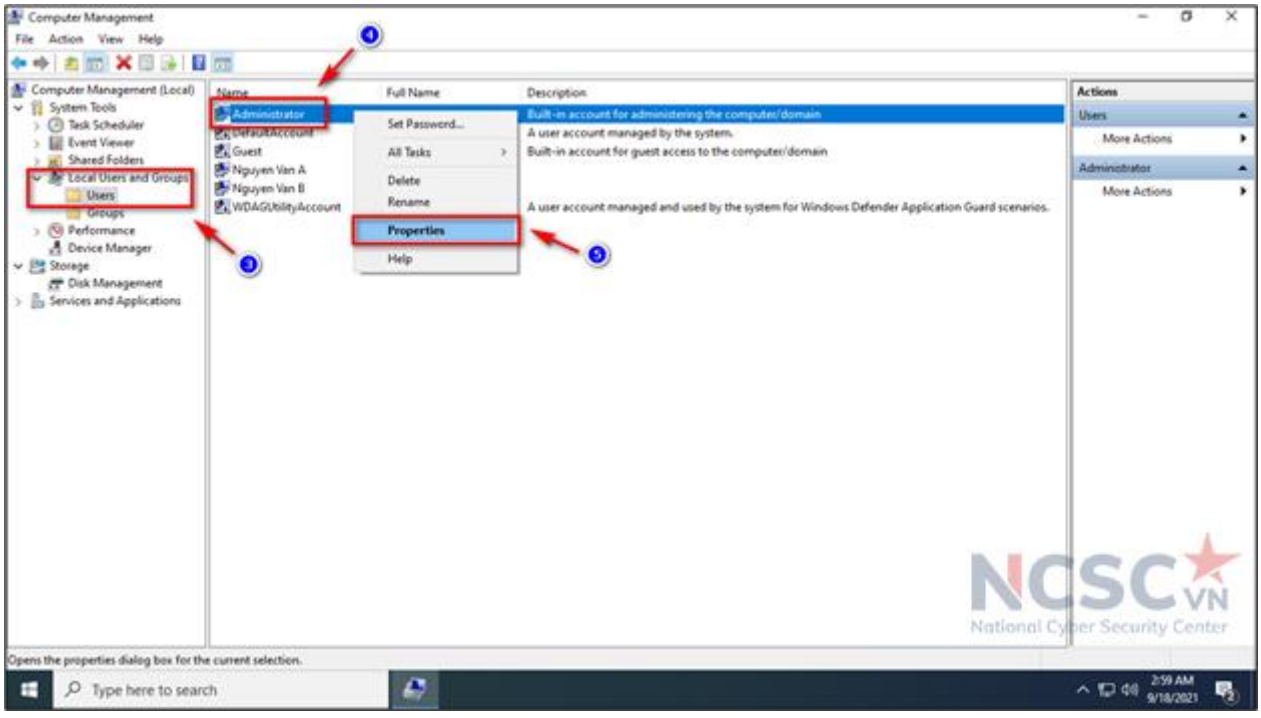
Hình 100: Vô hiệu hóa các tài khoản không cần thiết (2)

- Kiểm tra các tài khoản cần disable có thuộc nhóm quản trị hay không. Nếu tài khoản không sử dụng nằm trong nhóm quản trị, có thể phân quyền cho 1 tài khoản khác đang sử dụng làm tài khoản quản trị cho máy tính (**Bước 4 đến 6 Mục 1.2.1**)



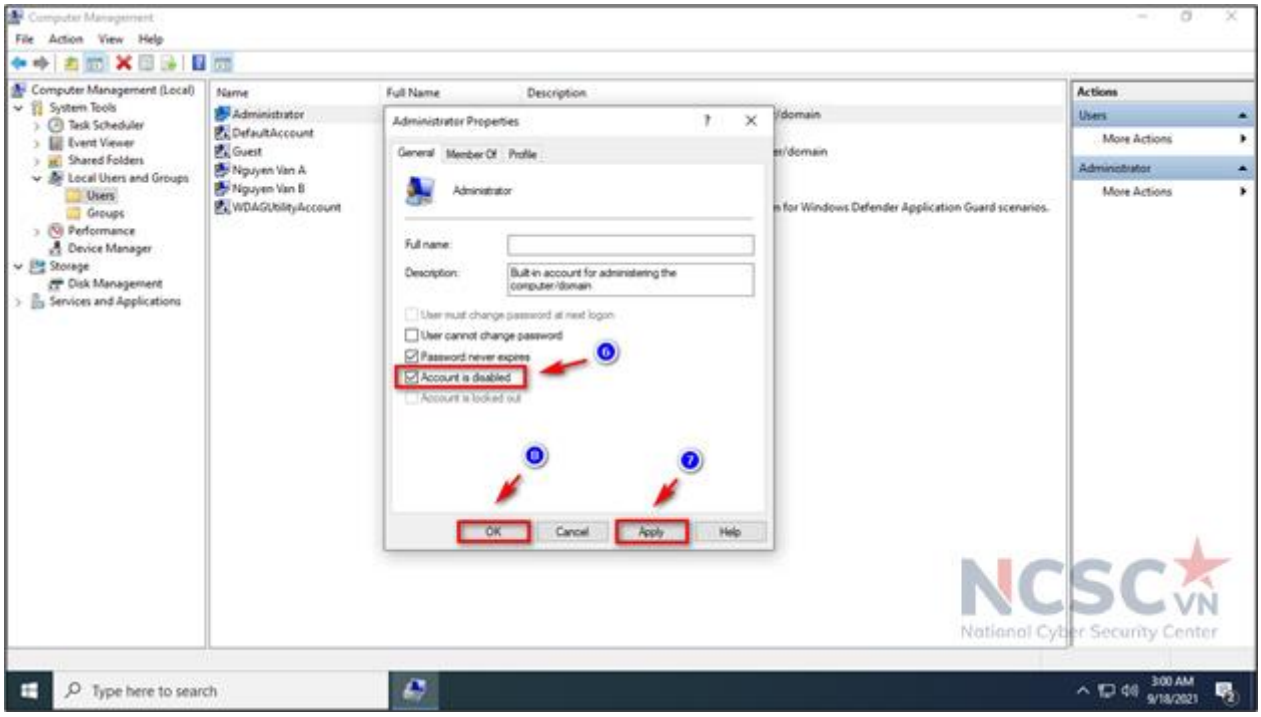
Hình 101: Vô hiệu hóa các tài khoản không cần thiết (3)

Bước 3: Chọn Local User and Groups > Users > bấm chuột phải vào tài khoản muốn vô hiệu hóa (Ví dụ: Administrator) > Properties



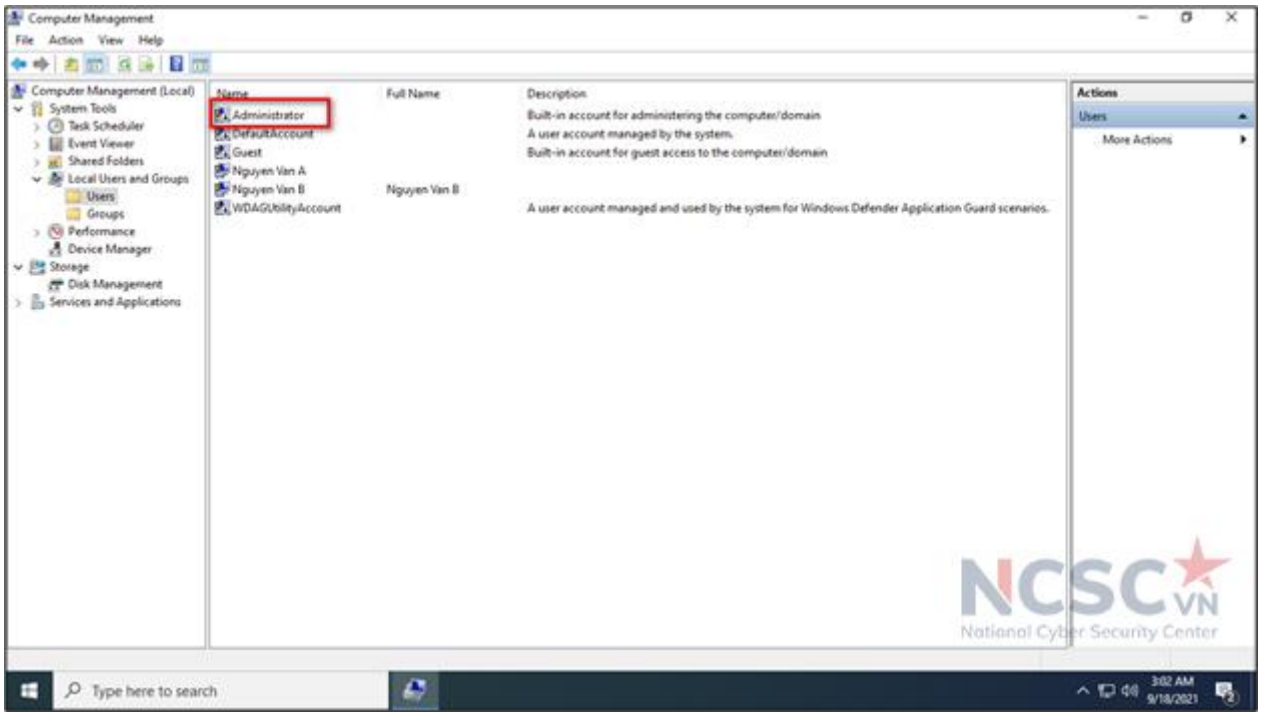
Hình 102: Vô hiệu hóa các tài khoản không cần thiết (2)

Bước 4: Tại Mục General tích chọn Account is disable (Tài khoản bị vô hiệu hóa) > Apply > OK, để vô hiệu hóa tài khoản



Hình 103: Vô hiệu hóa các tài khoản không cần thiết (3)

Tài khoản sau khi đã bị vô hiệu hóa, sẽ có thêm biểu tượng mũi tên đi xuống, điều này thể hiện tài khoản đấy đã bị vô hiệu hóa thành công.



Hình 104: Vô hiệu hóa các tài khoản không cần thiết (4)

Làm tương tự để vô hiệu hóa các tài khoản khác (Ví dụ: DefaultAccount, Guest…)

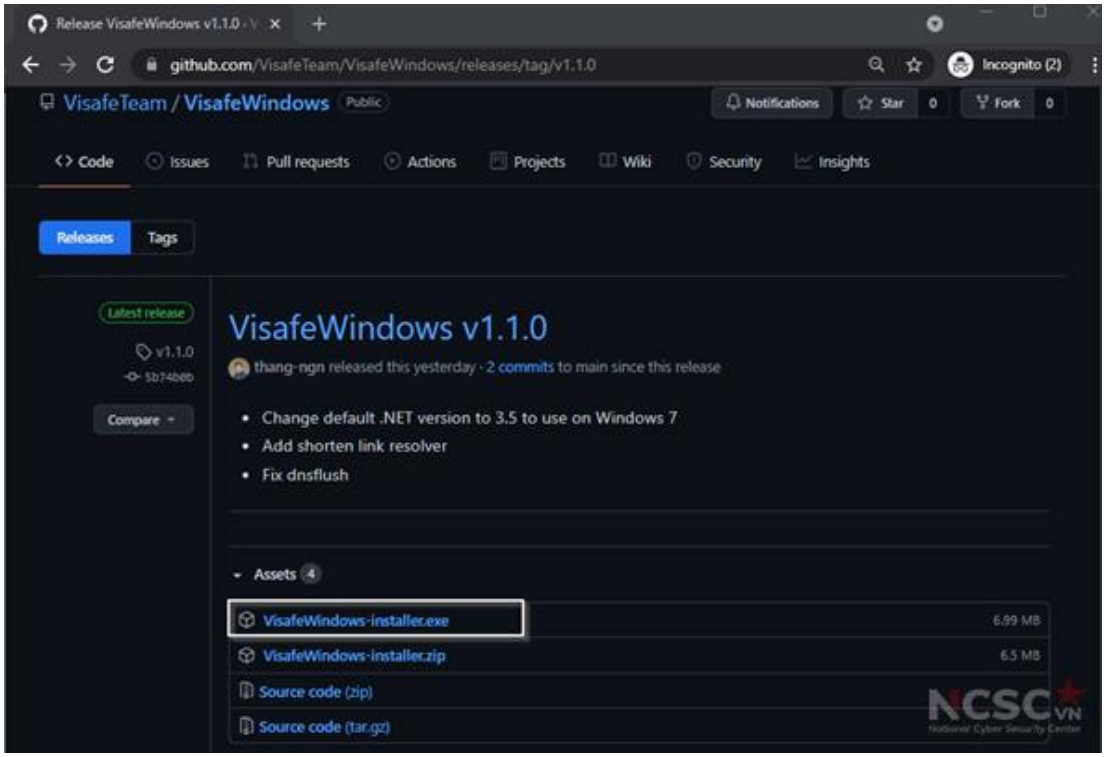
1.3. Sử dụng ứng dụng Internet an toàn trên máy tính Windows

Ứng dụng Internet an toàn (Visafe) là ứng dụng miễn phí dành cho người dùng Internet Việt Nam để tự bảo vệ mình trên không gian mạng trước các trang web lừa đảo, trang web có chứa mã độc, các quảng cáo và đường dẫn nguy hiểm, độc hại. Ngoài ra khi sử dụng Visafe, người dùng có thể sử dụng chức năng bảo vệ trẻ em để hạn chế các trang web không lành mạnh, các quảng cáo, đường link nguy hiểm không phù hợp với lứa tuổi.

Visafe do Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) xây dựng, vận hành và triển khai miễn phí hướng đến cảnh báo và bảo vệ mọi người dân trên không gian mạng trước các nguy cơ, trang web độc hại đã phát hiện ra.

Để sử dụng Visafe trên máy tính chạy hệ điều hành Windows thực hiện theo các bước sau:

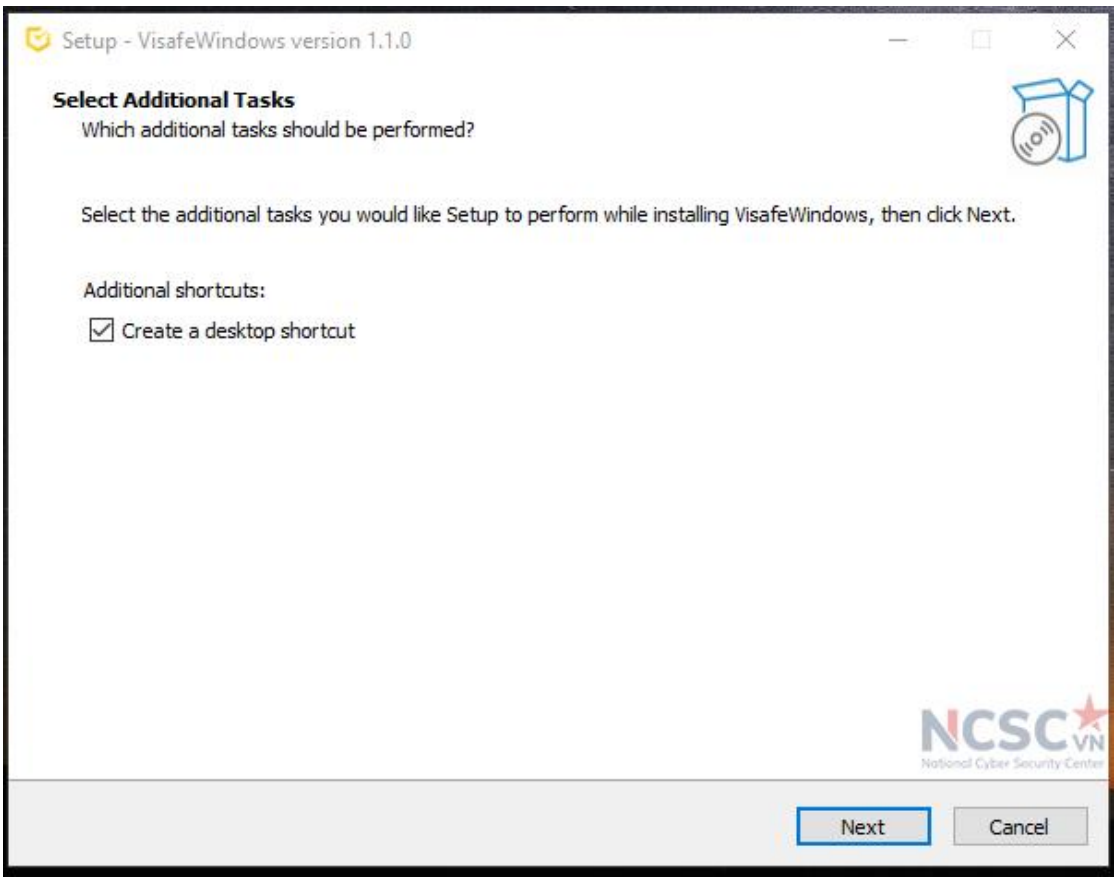
Bước 1: Tải xuống bản mới nhất của Visafe trên trang chủ https://visafe.vn hoặc tại Github https://github.com/VisafeTeam/VisafeWindows/releases/latest



Hình 105: Cài đặt ứng dụng Visafe trên Windows (1)

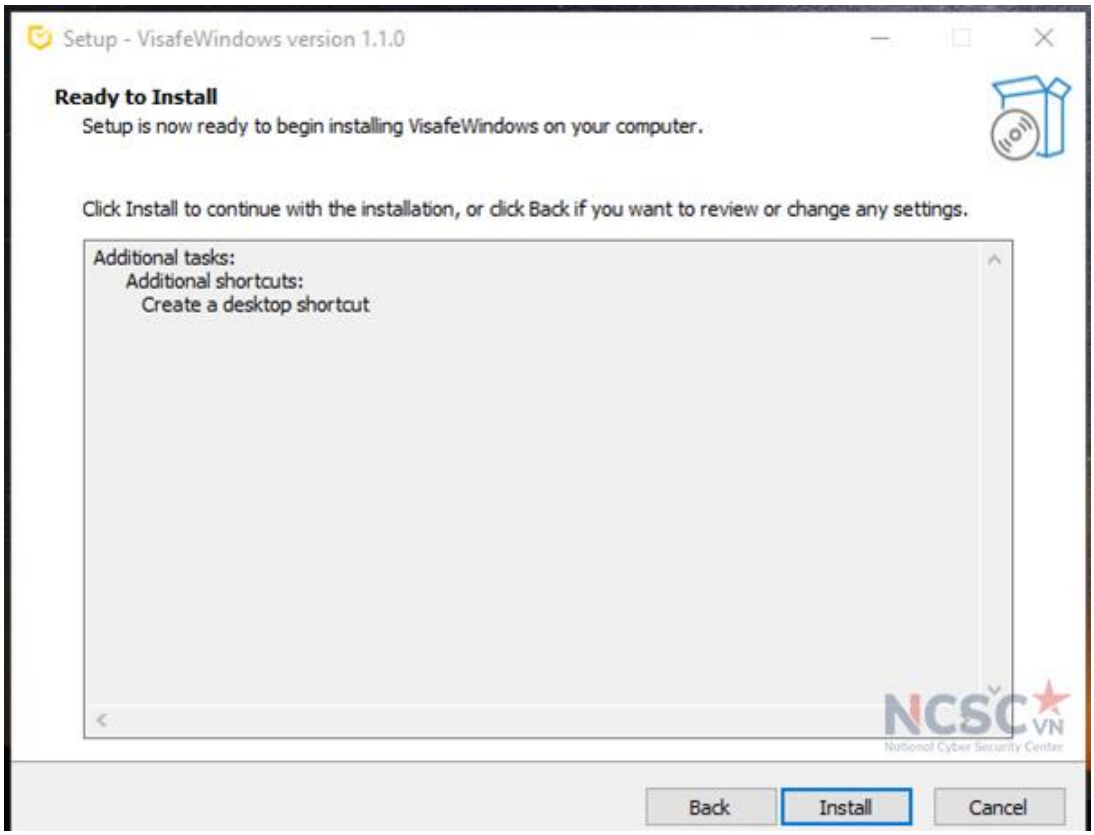
Bước 2: Chạy file cài đặt **VisafeWindows-installer.exe** và làm theo hướng dẫn dưới đây:

- Tích chọn "Create a desktop shortcut" nếu muốn tạo shortcut **Visafe.** Chọn **Next** để tiếp tục.



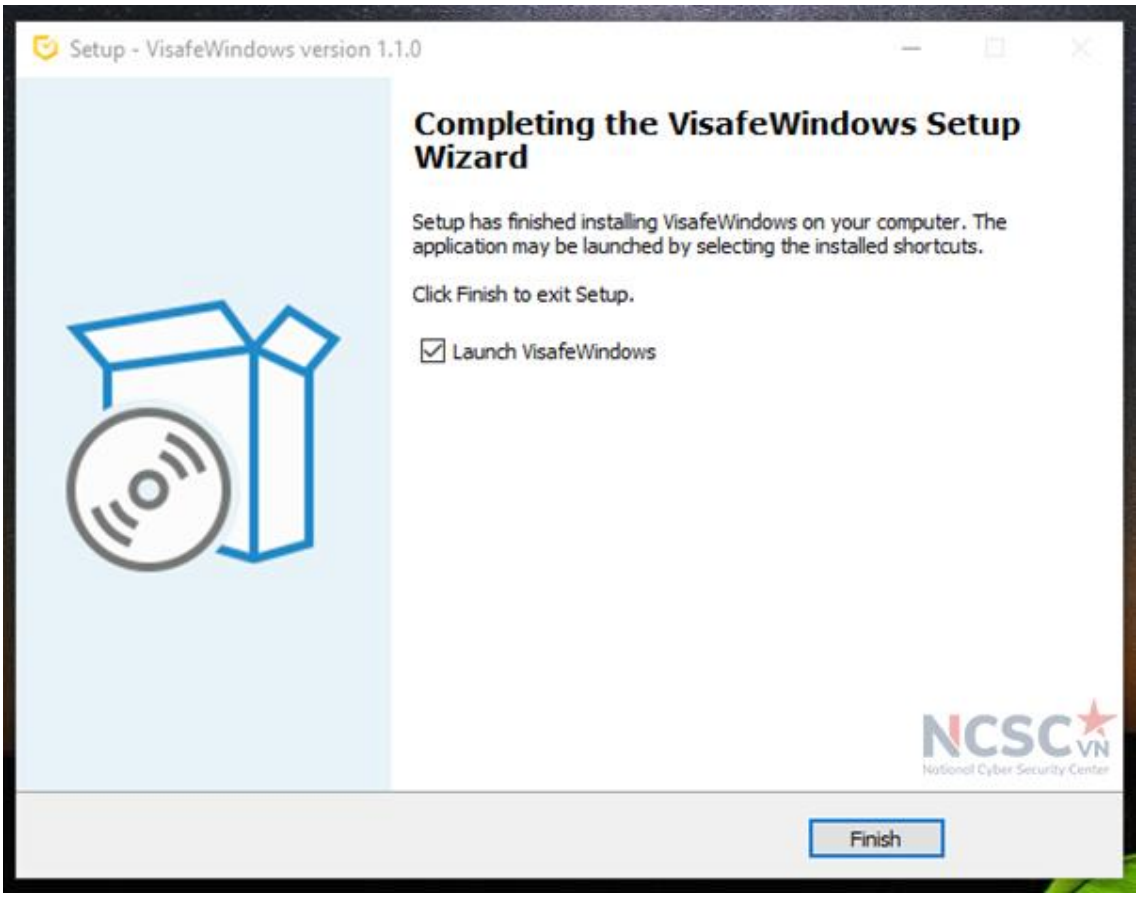
Hình 106: Cài đặt ứng dụng Visafe trên Window (2)

- Tiếp theo, chọn **Install** để bắt đầu cài đặt **Visafe.**



Hình 107: Cài đặt ứng dụng Visafe trên Windows (3)

- Sau khi hoàn tất quá trình cài đặt, chọn **Finish** để kết thúc.



Hình 108: Cài đặt ứng dụng Visafe trên Windows (3)

Quá trình cài đặt hoàn tất, **Visafe** sẽ được kích hoạt và hiện thông báo như sau:

Hình 109: Cài đặt ứng dụng Visafe trên Windows (4)

2. Máy tính sử dụng hệ điều hành MacOS

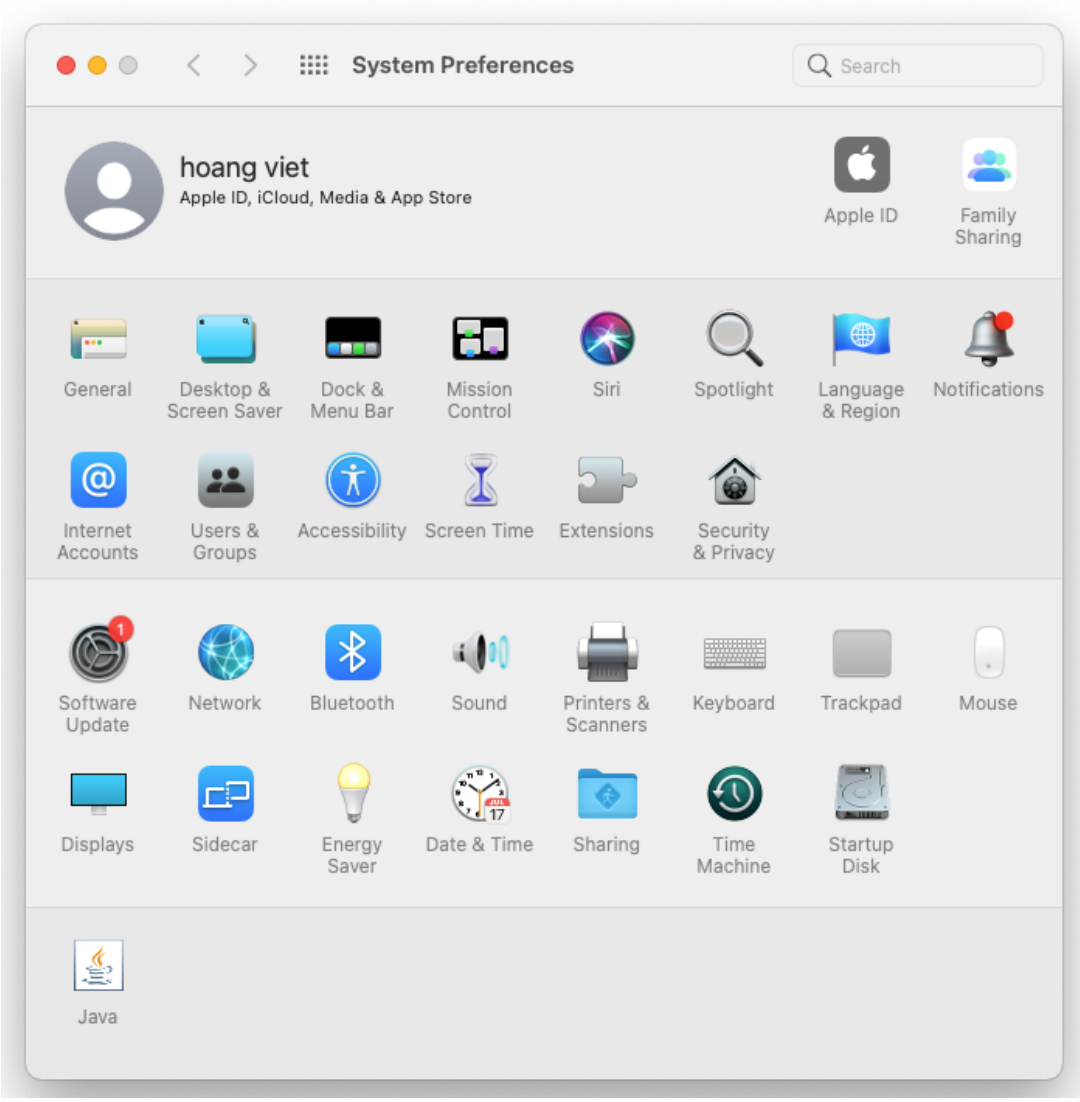
2.1. Sử dụng tính năng bảo mật có sẵn trên MacOS

2.1.1. Vô hiệu hóa tính năng đăng nhập tự động

Mặc định, khi bạn khởi động lại hoặc bật máy, bạn sẽ được hỏi thông tin đăng nhập trước khi cho phép bạn sử dụng macOS. Với tính năng đăng nhập tự động, bạn có thể

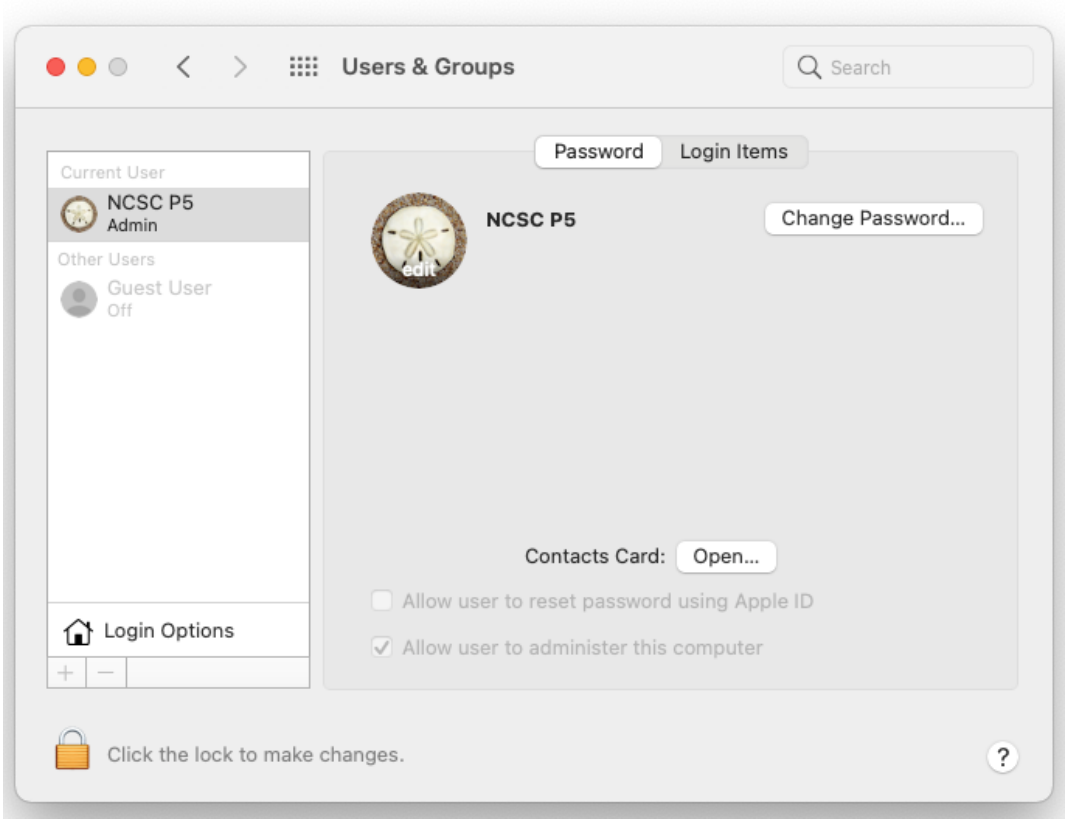
bỏ qua bước này, nhưng điều này đồng nghĩa với việc bất kỳ ai cũng có thể truy cập vào máy tính của bạn. Để vô hiệu hóa tính năng thực hiện như sau:

Bước 1: Vào *System Preferences* > *Users & Groups*



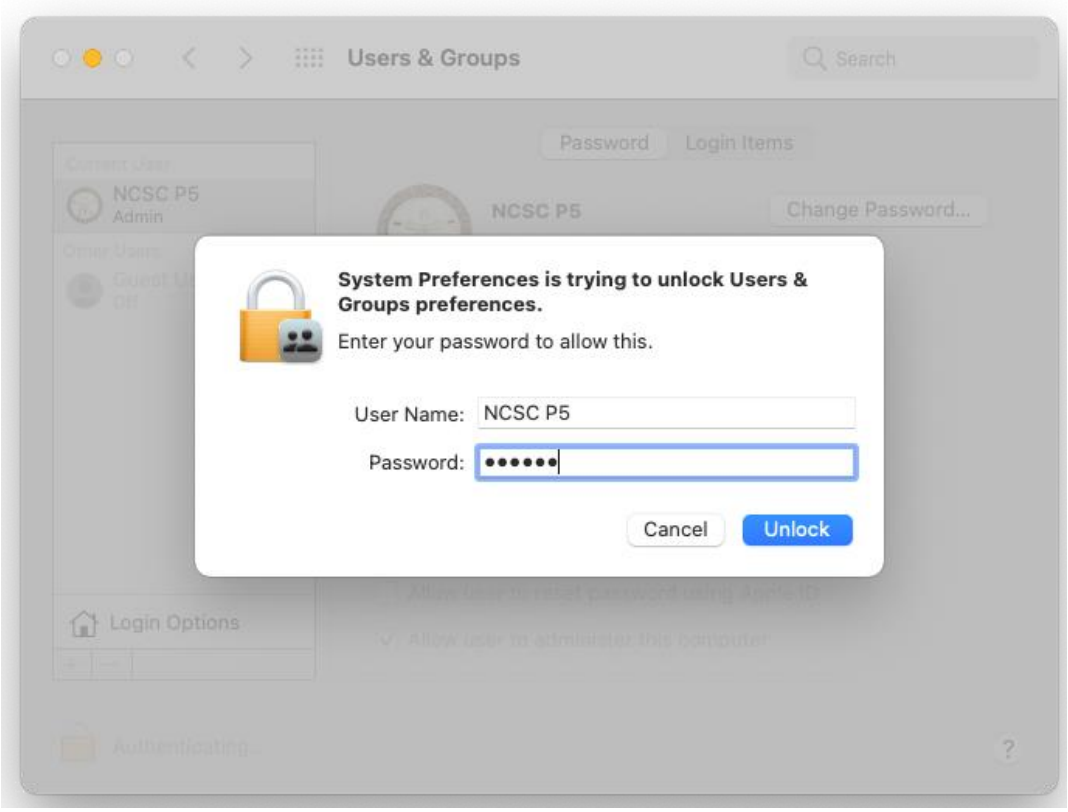
Hình 110: Vô hiệu hóa tính năng đăng nhập tự động (1)

Bước 2: Nhấp vào ổ khóa ở dưới cùng bên trái



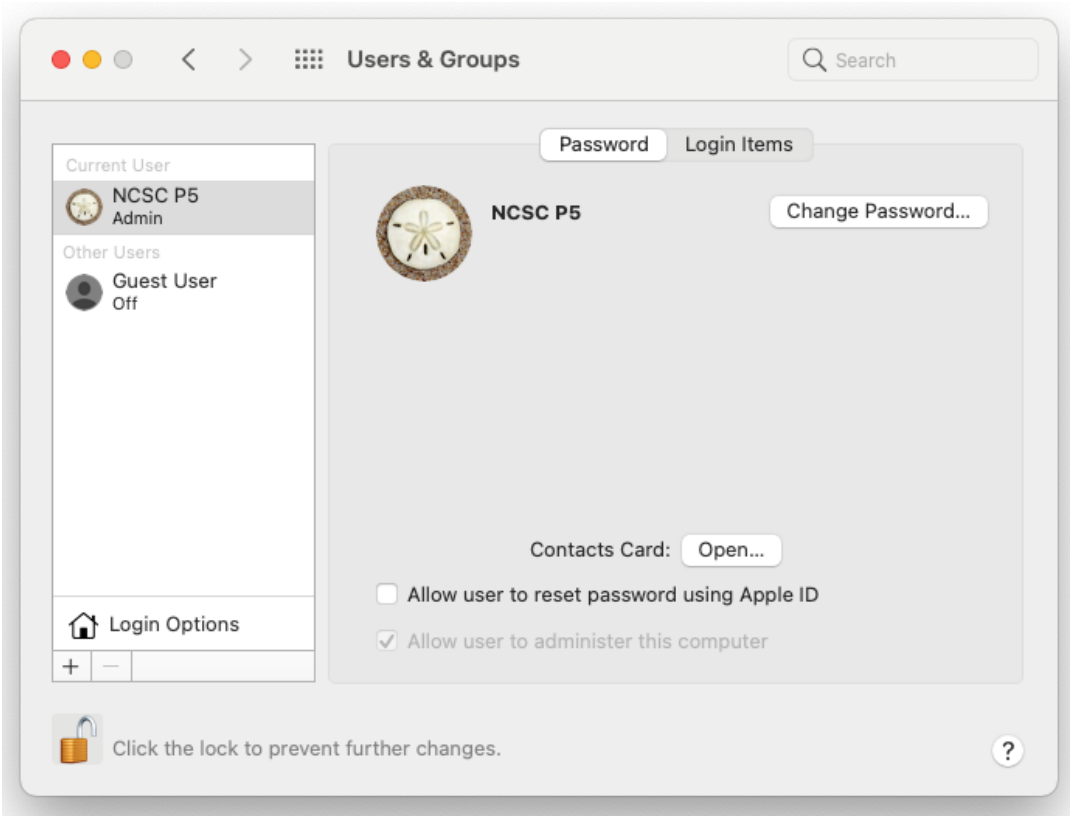
Hình 111: Vô hiệu hóa tính năng đăng nhập tự động (2)

Bước 3: Nhập thông tin đăng nhập, và chọn *Unlock*



Hình 112: Vô hiệu hóa tính năng đăng nhập tự động (3)

Bước 4: Chọn *Login Options* trong danh sách người dùng



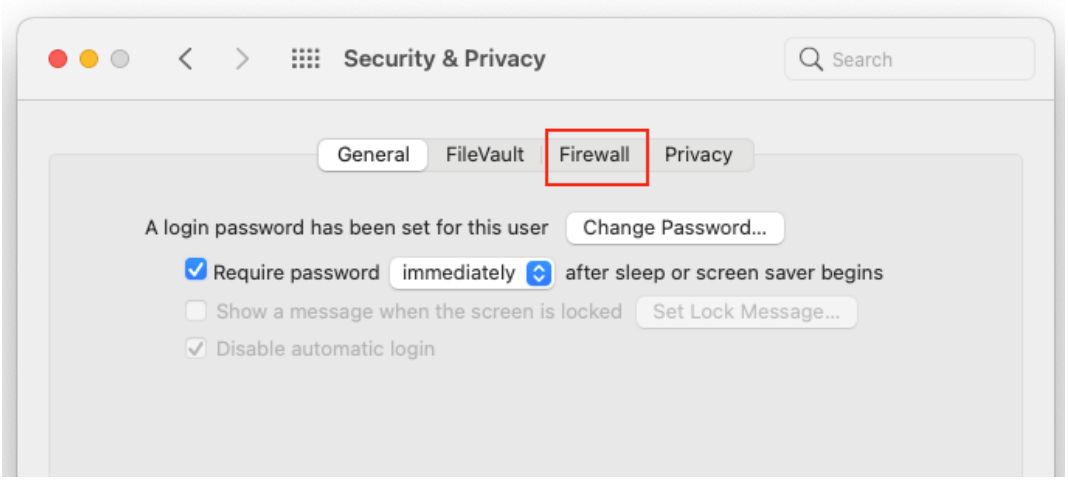
Hình 113: Vô hiệu hóa tính năng đăng nhập tự động (4)

Bước 5: Từ menu thả xuống *Automatic login,* chọn *Off* để tắt tính năng đăng nhập tự động.

2.1.2 Kích hoạt tường lửa trên MacOS

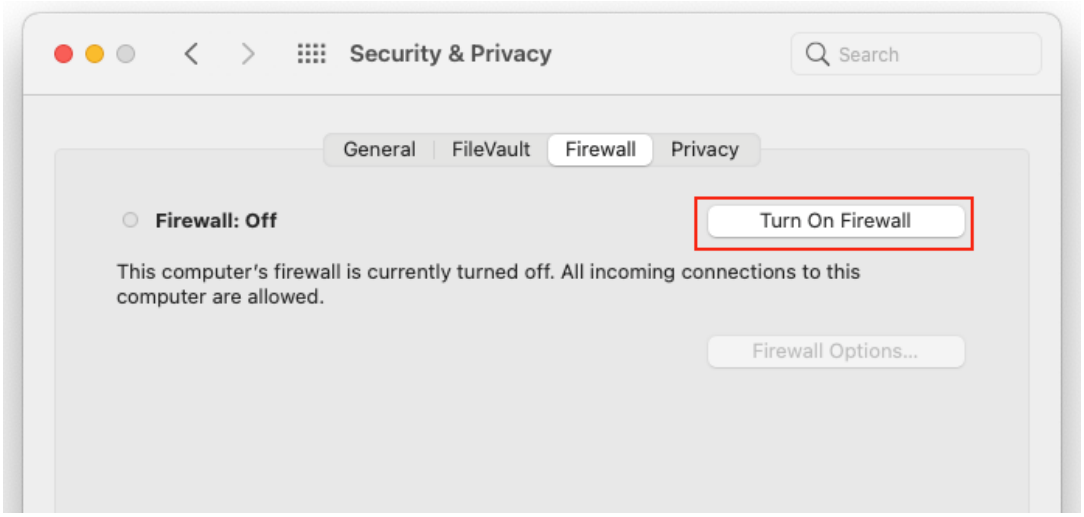
Hệ điều hành MacOS có tường lửa nhưng mặc định không bật. Để kích hoạt tường lửa thực hiện như sau:

Bước 1: Vào *System Preferences* > *Security& Privacy* > Nhấp chọn *Firewall*



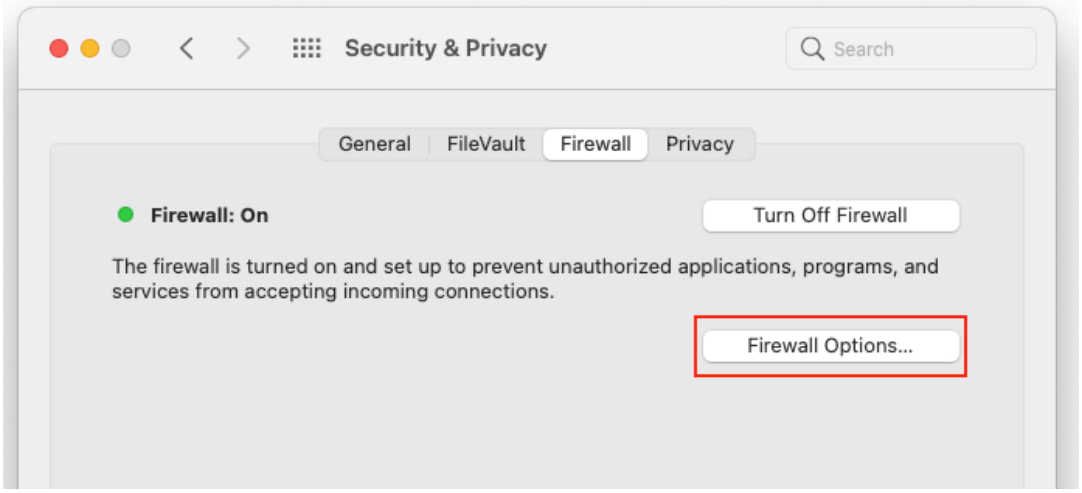
Hình 114: Kích hoạt tường lửa trên MacOS (1)

Bước 2: Nhấp vào vào ổ khóa ở dưới cùng > Nhập thông tin đăng nhập > Turn on Firewall



Hình 115: Kích hoạt tường lửa trên MacOS (2)

Nhấp vào *Firewall Options* nếu bạn muốn điều chỉnh cài đặt tường lửa



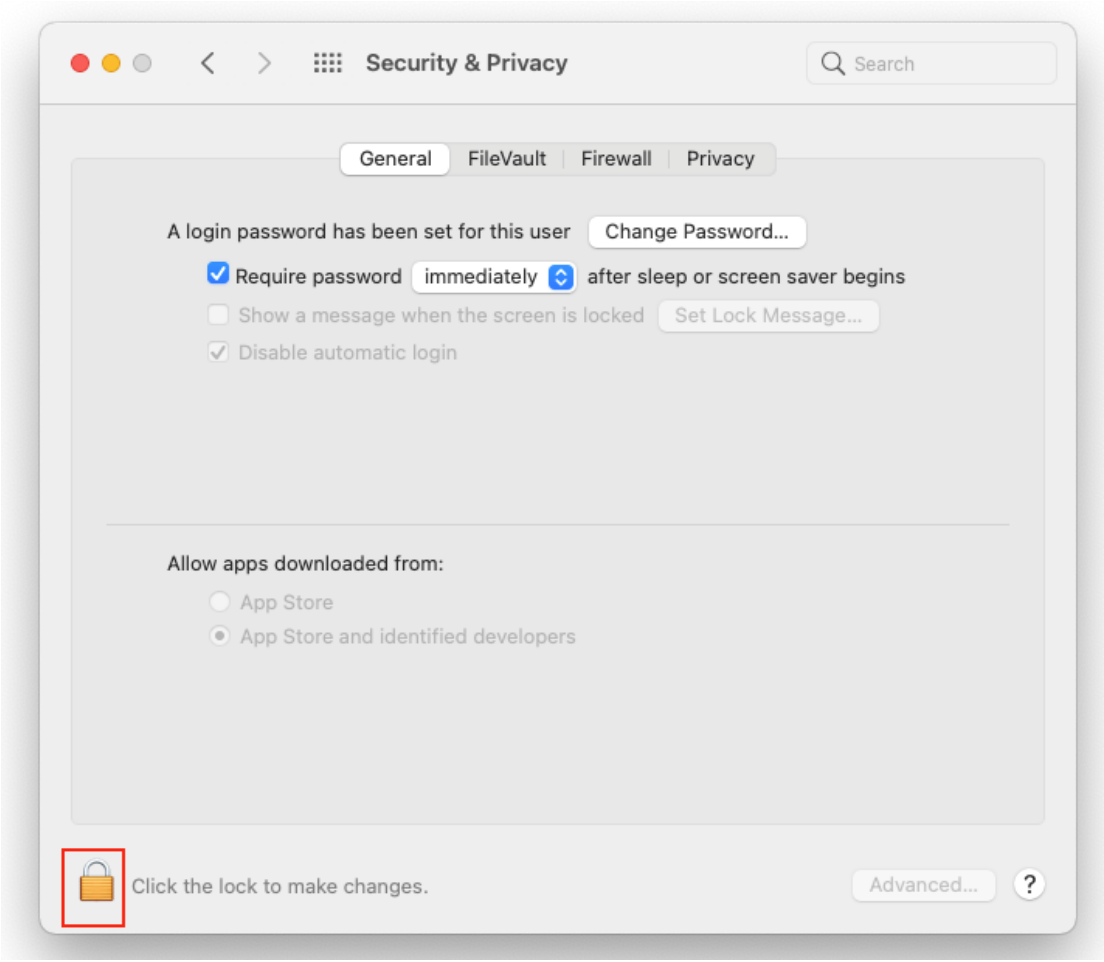
Hình 116: Kích hoạt tường lửa trên MacOS (3)

2.1.2. Kiểm soát việc cài đặt ứng dụng

Apple có toàn quyền kiểm soát những ứng dụng đưa vào App Store, nên việc chỉ cài đặt ứng dụng trên App Store giảm được khá nhiều rủi ro cài đặt phần mềm giả mạo, độc hại. Tuy nhiên có nhiều ứng dụng (thường là các ứng dụng mà nhà phát triển không phổ biến rộng rãi) vì nhiều lý do có thể sẽ không đưa lên App Store, mà người dùng vẫn muốn sử dụng, thì khi cài đặt ứng dụng đó có thể thay đổi lại thiết lập để cài đặt.

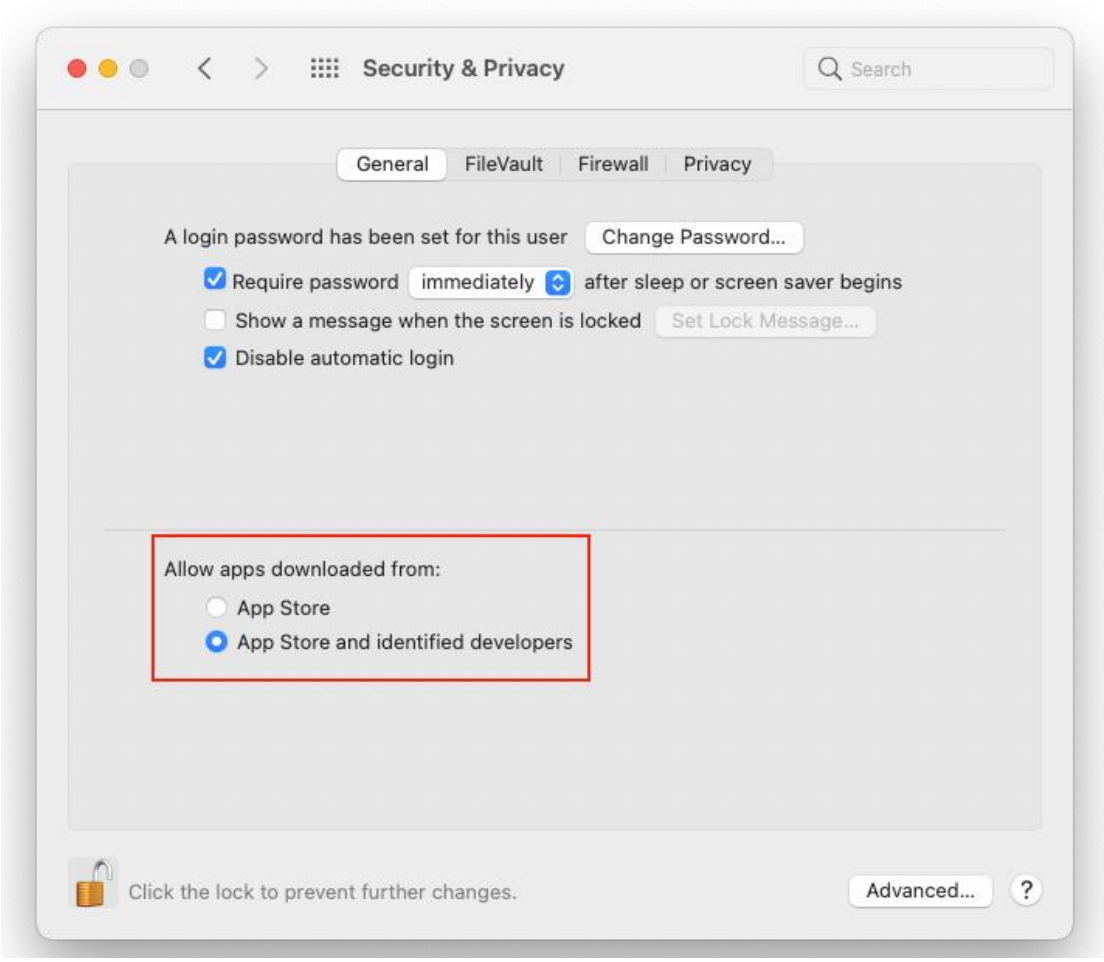
Để kiểm soát mặc định chỉ cài đặt ứng dụng trên App Store thực hiện như sau:

Bước 1: Vào *System Preferences* >*Security & Privacy* > *General*> Bấm vào ổ khóa



Hình 117: Kiểm soát việc cài đặt ứng dụng trên MacOS (1)

Bước 2: Nhập thông tin đăng nhập > Chọn *Unlock* > *Dưới Allow apps downloaded from, chọn App Store*



Hình 118: Kiểm soát việc cài đặt ứng dụng trên MacOS (2)

Cài đặt ứng dụng không có trên App Store: người dùng cần hết sức cân nhắc khi cài đặt ứng dụng không có trên App Store. Khi cài đặt ứng dụng không có trên App Store cần lưu ý:

- Tải ứng dụng từ trang chính thống của nhà phát triển. Ví dụ đối với Microsoft Team chỉ tải ứng dụng từ website của Microsoft Team tại https://www.microsoft.com/en-us/microsoft-teams/download-app

- Chuyển chế độ cho phép cài đặt từ "App Store and identified developers". Sau khi hoàn tất cài đặt ứng dụng chuyển về chế độ "App Store"

Dưới đây là hướng dẫn cài đặt ứng dụng Microsoft Team

Bước 1: Tải ứng dụng từ nguồn tin cậy

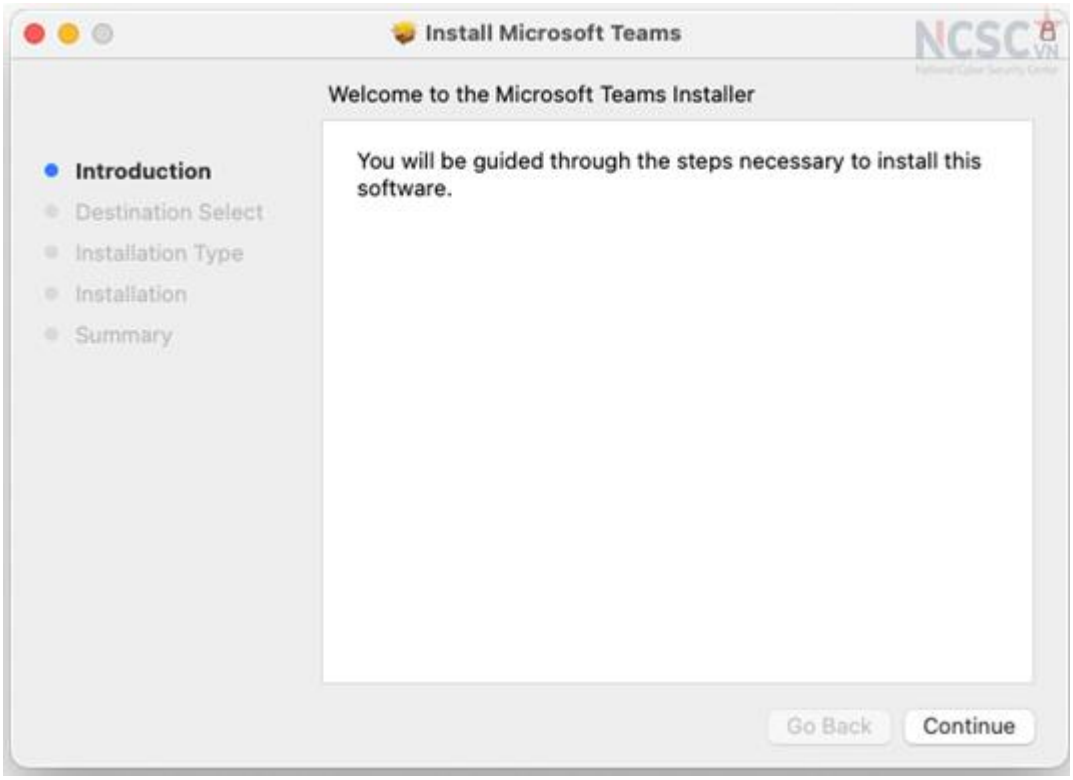
https://www.microsoft.com/en-us/microsoft-teams/download-app

Bước 2: Chuyển chế độ cho phép cài đặt "App Store and identified developers"

System Preferences >Security & Privacy > General> Bấm vào ổ khóa>Nhập thông tin đăng nhập > Chọn *Unlock > Dưới Allow apps downloaded from, chọn App Store and identified developers*

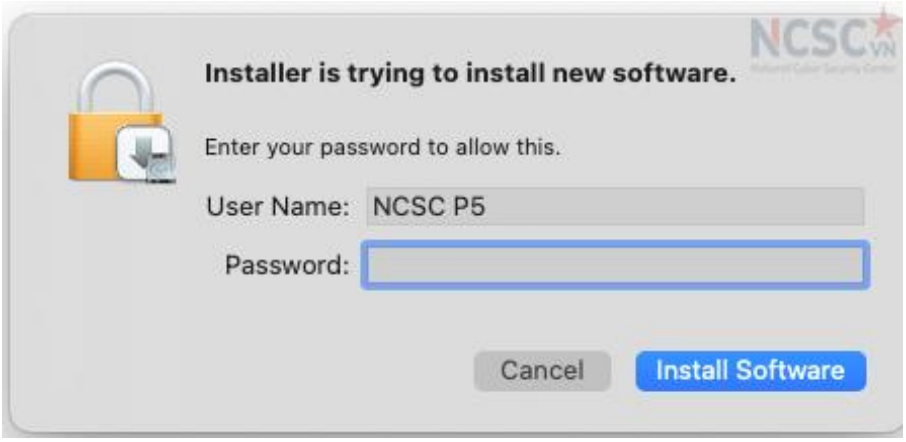
Hình 119: Cài đặt ứng dụng không có trên App Store (1)

Bước 3: Mở file cài đặt ứng dụng đã tải về (trong bước 1) > Continue và theo từng bước để hoàn thành quá trình cài đặt.



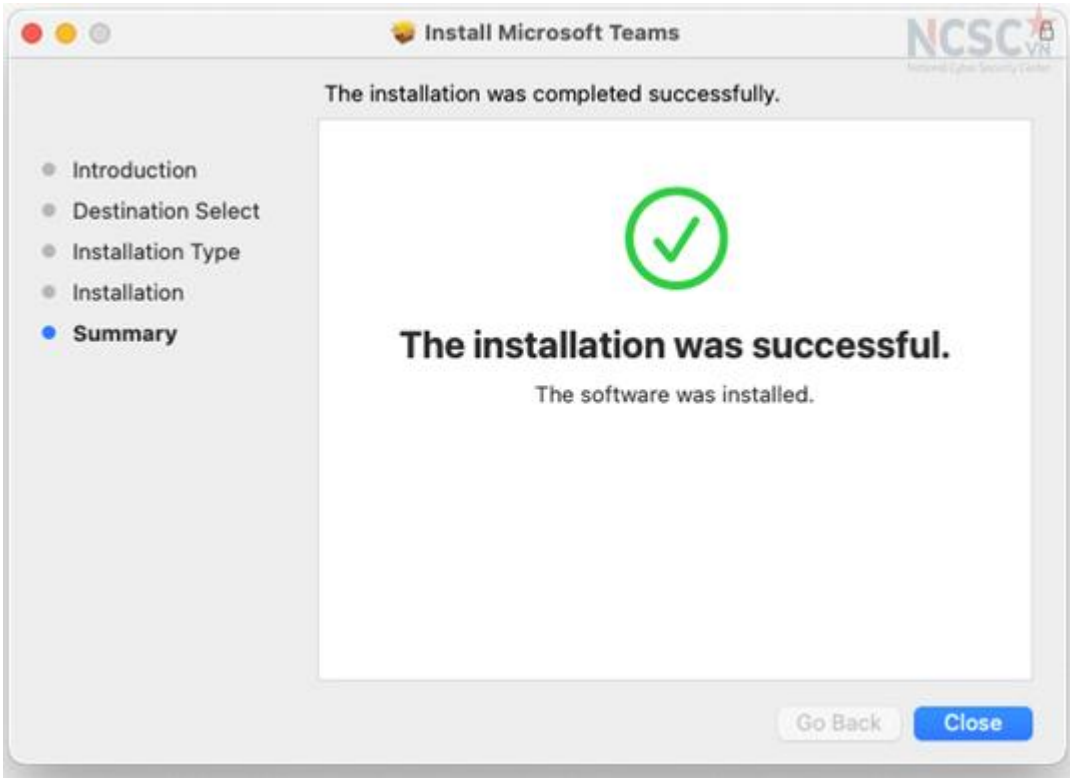
Hình 120: Cài đặt ứng dụng không có trên App Store (2)

Bước 4: Chọn *Install for all users of this computer > Continues> Install> Nhập thông tin đăng nhập, và chọn Install Software*



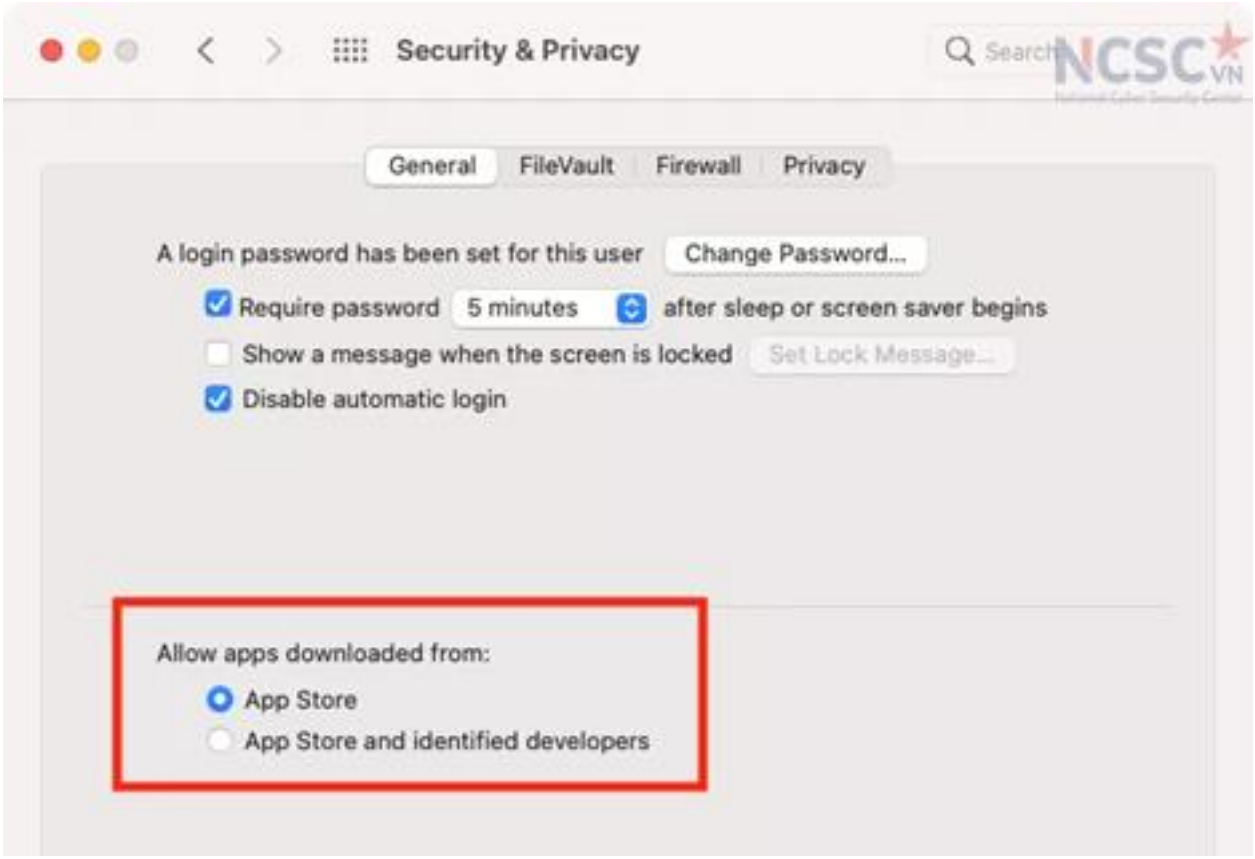
Hình 121: Cài đặt ứng dụng không có trên App Store (3)

Bước 5: Chọn *Close* để kết thúc quá trình cài đặt



Hình 122: Cài đặt ứng dụng không có trên App Store (4)

Bước 6: Sau khi hoàn tất cài đặt ứng dụng chuyển về chế độ "App Store"



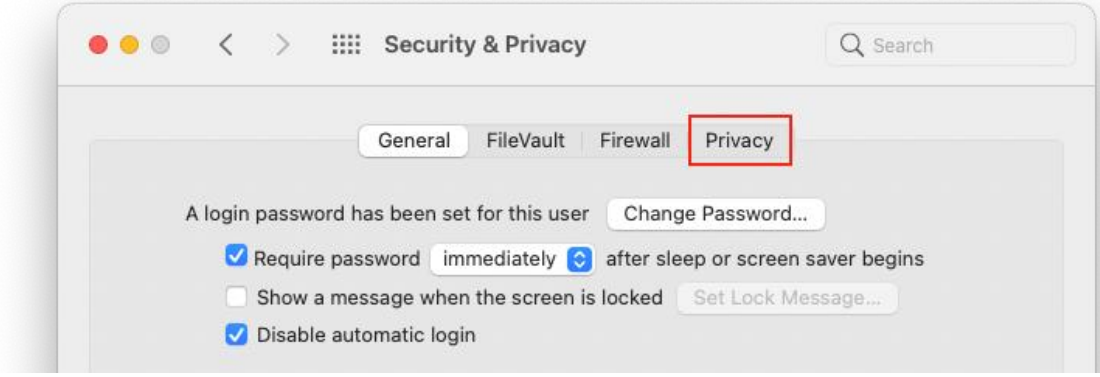
Hình 123: Cài đặt ứng dụng không có trên App Store (5)

2.1.3. Cấu hình quyền riêng tư

Quyền riêng tư trong cài đặt bảo mật của hệ điều hành MacOS là một bảng điều khiển quyền. Tại đây, bạn có thể xác định ứng dụng nào có thể thực hiện một số việc nhất định, chẳng hạn như truy cập micro, xem vị trí hiện tại của bạn.

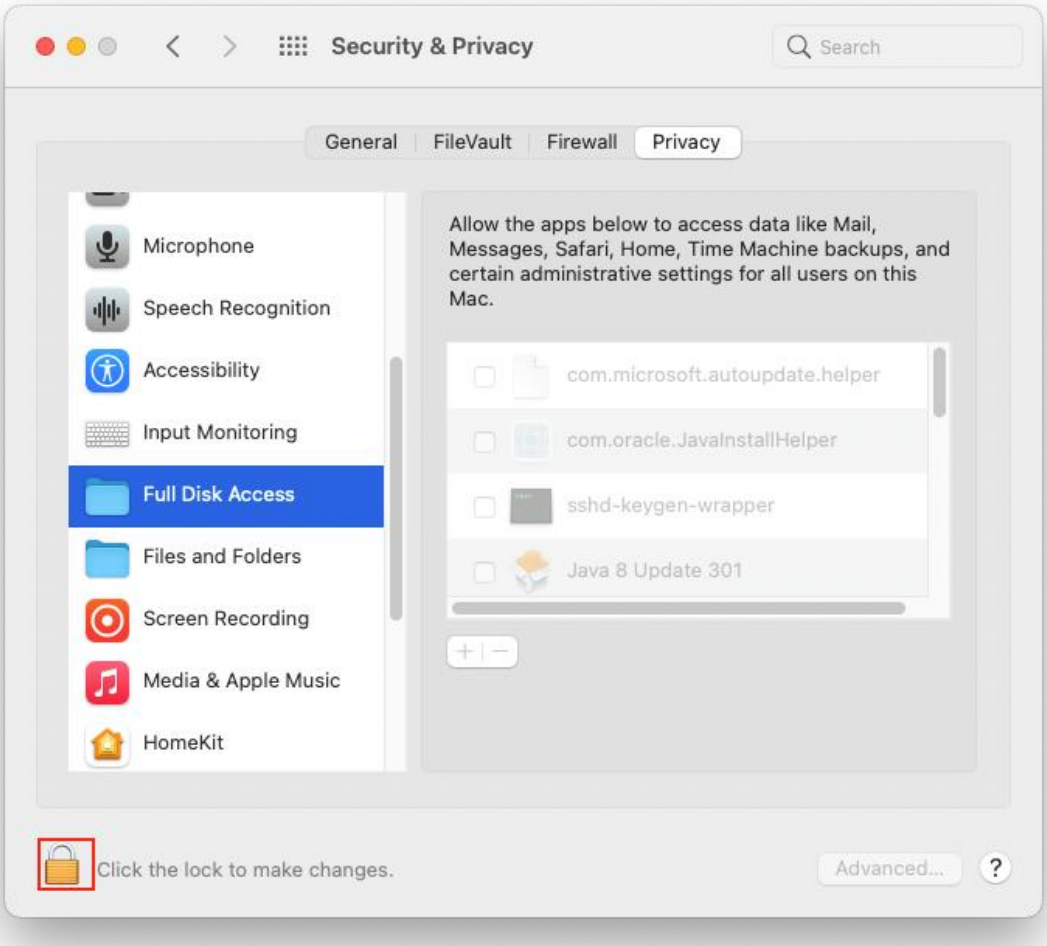
Để cấu hình quyền riêng tư thực hiện như sau:

Bước 1: Mở *System Preferences* > Chọn tab *Privacy*



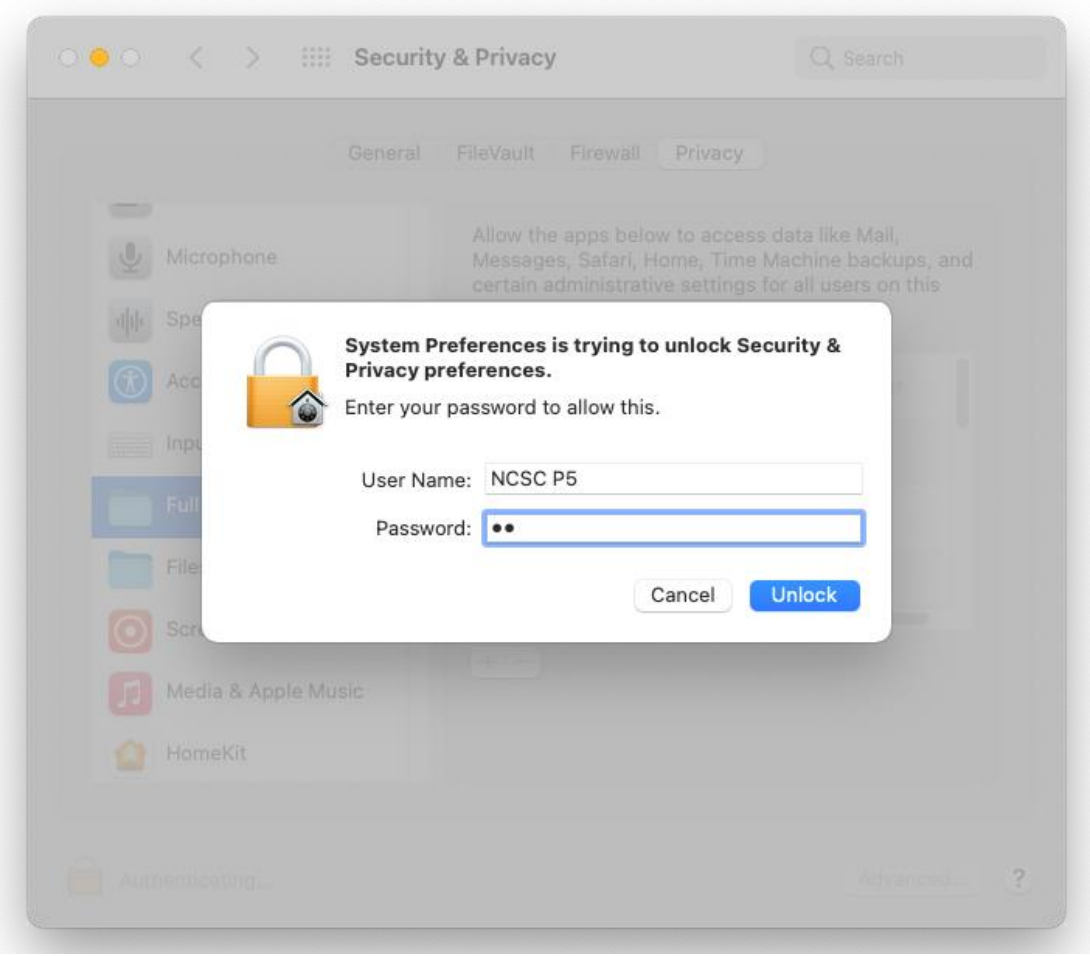
Hình 124: Cấu hình quyền riêng tư (1)

Bước 2: Trong menu bên trái, cuộn qua các danh mục khác nhau và chọn một tính năng để thiết lập > Chọn vào ổ khóa



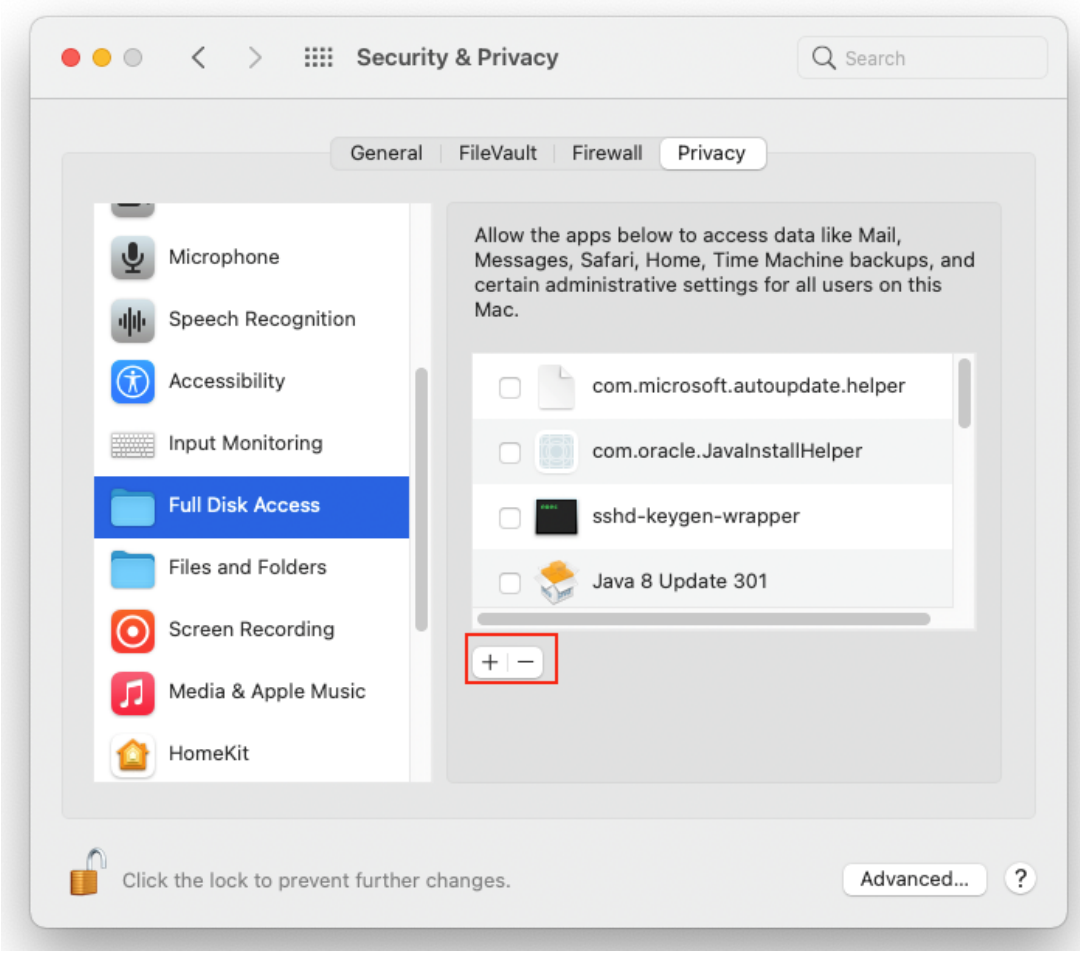
Hình 125: Cấu hình quyền riêng tư (2)

Bước 2: Nhập thông tin đăng nhập, và chọn *Unlock*



Hình 126: Cấu hình quyền riêng tư (3)

Bước 3: Sử dụng các nút cộng và trừ để thêm hoặc xóa quyền



Hình 127: Cấu hình quyền riêng tư (4)

2.2. Tạo tài khoản riêng trên MacOS cho mục đích giảng dạy, học tập

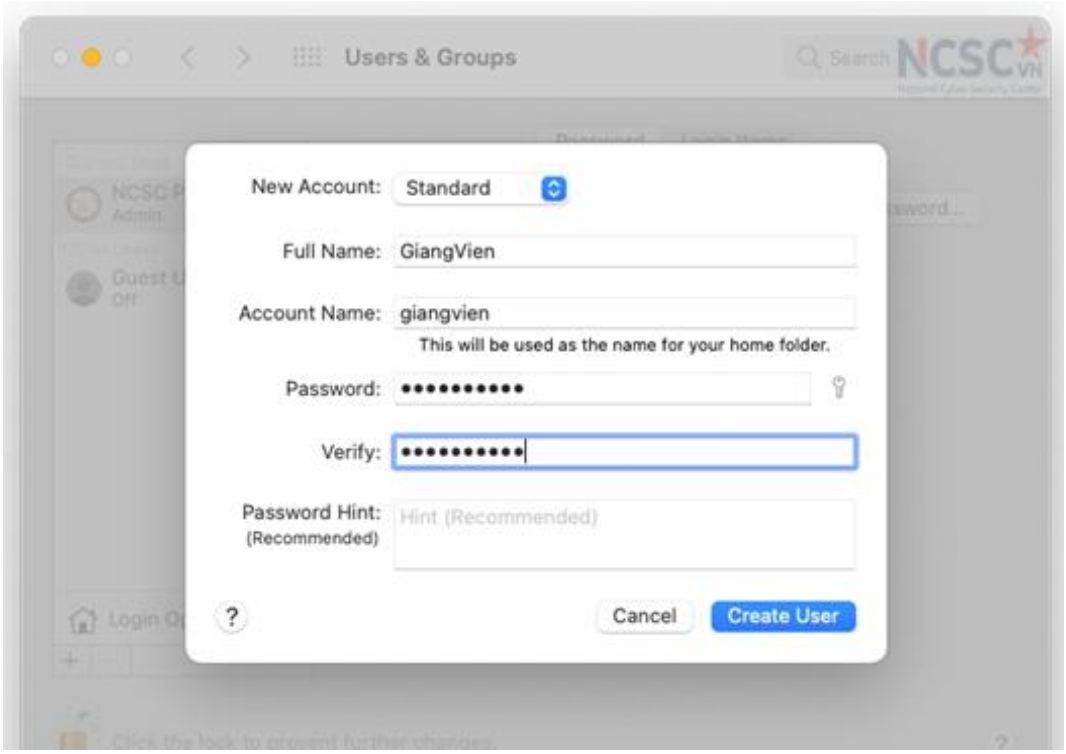
Để tạo tài khoản tiêu chuẩn mới thực hiện theo các bước sau:

Bước 1: Truy cập vào *System Preferences* > *Users & Groups* > Nhấp vào ổ khóa ở dưới cùng bên trái >Nhập thông tin đăng nhập > *Unlock* > Nhấp vào nút dấu cộng dưới danh sách người dùng để thêm tài khoản

Hình 128: Tạo tài khoản mới cho mục đích học tập (1)

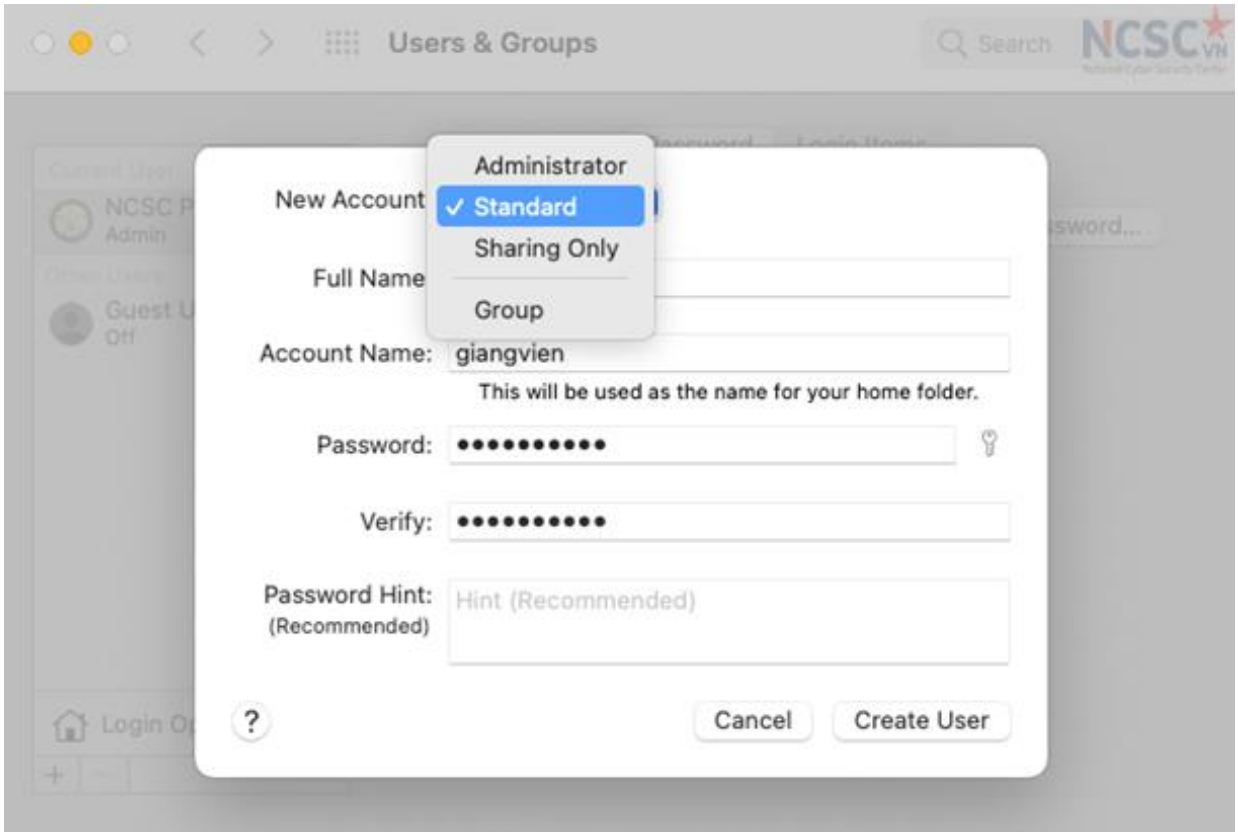
Bước 2: Điền thông tin người dùng vào các trường *Full Name, Account Name,* and *Password*, và chọn *Create User.*

Nên đặt tên theo từng người sử dụng



Hình 129: Tạo tài khoản mới cho mục đích học tập (2)

Bước 3: Lựa chọn loại tài khoản. Đảm bảo trong menu thả xuống *New Account* có hiện *Standard*



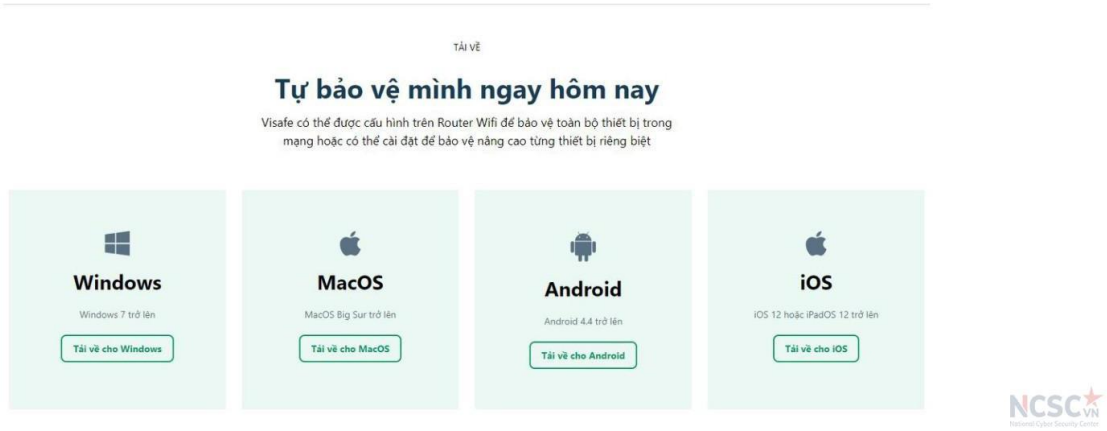
Hình 130: Tạo tài khoản mới cho mục đích học tập (3)

2.3. Sử dụng ứng dụng Internet an toàn trên hệ điều hành MacOS

Để thiết lập ứng dụng Internet an toàn (Visafe) trên hệ điều hành MacOS bạn không cần cài đặt phần mềm riêng chỉ cần thực hiện cấu hình trên máy tính như sau:

Bước 1: Tải ứng dụng Visafe từ trang chủ: https://visafe.vn.

Dùng trình duyệt web truy cập vào trang chủ > Tìm đến phần Tải về> Chọn mục MacOS để tải về tập tin cấu hình.

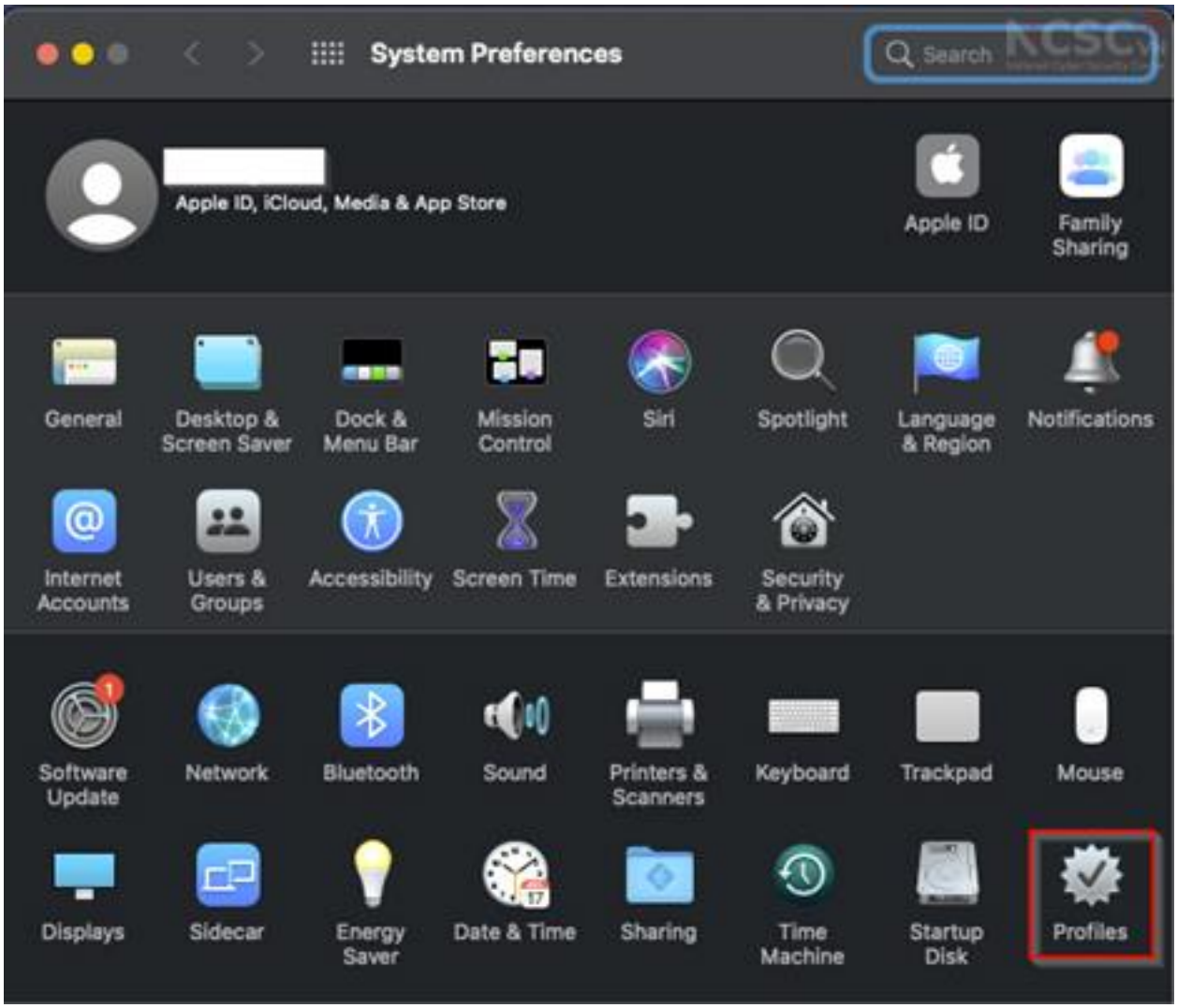


Hình 131: Tải file cài đặt Visafe trên MacOS

Bước 2: Kích đúp chuột vào file vừa tải về

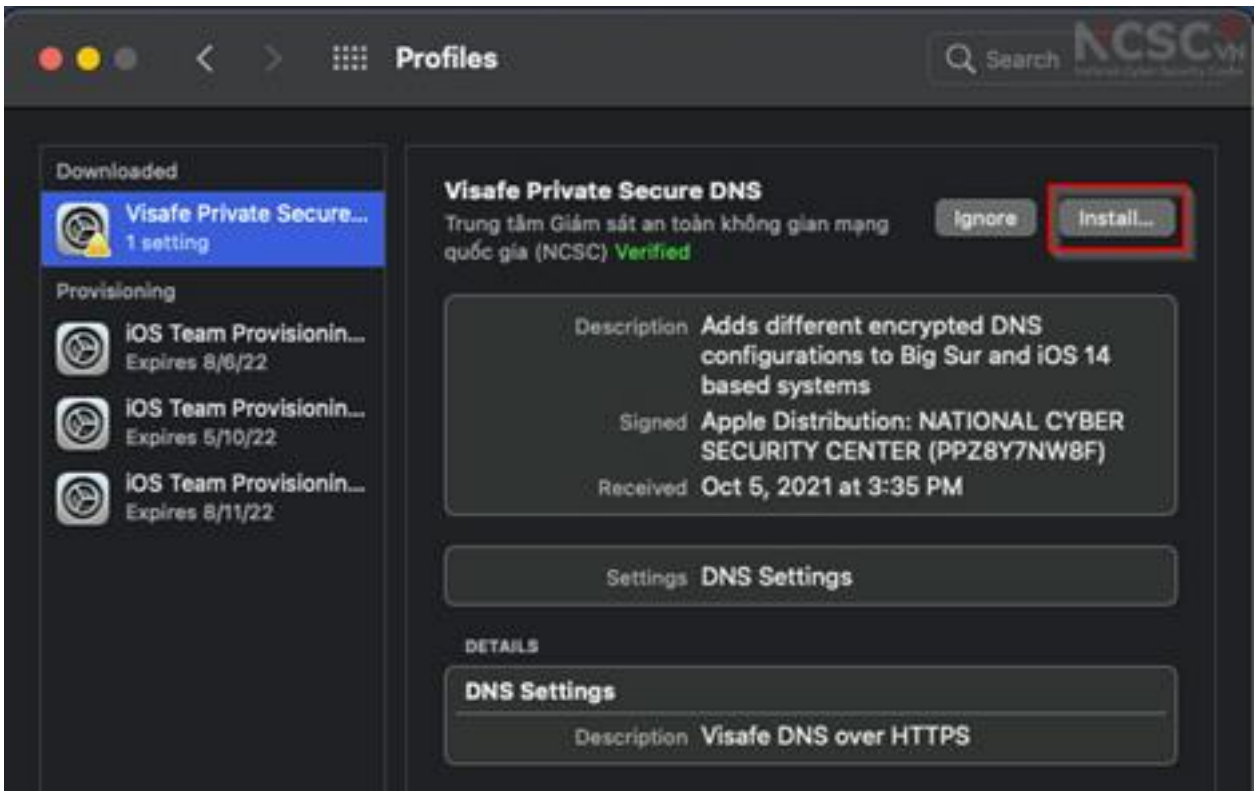
Bước 3: Cấu hình để sử dụng Visafe.

Vào System Preferences > Profile



Hình 132: Cài đặt Visafe trên MacOS (1)

Bước 4: Chọn *Install* để cài đặt Visafe

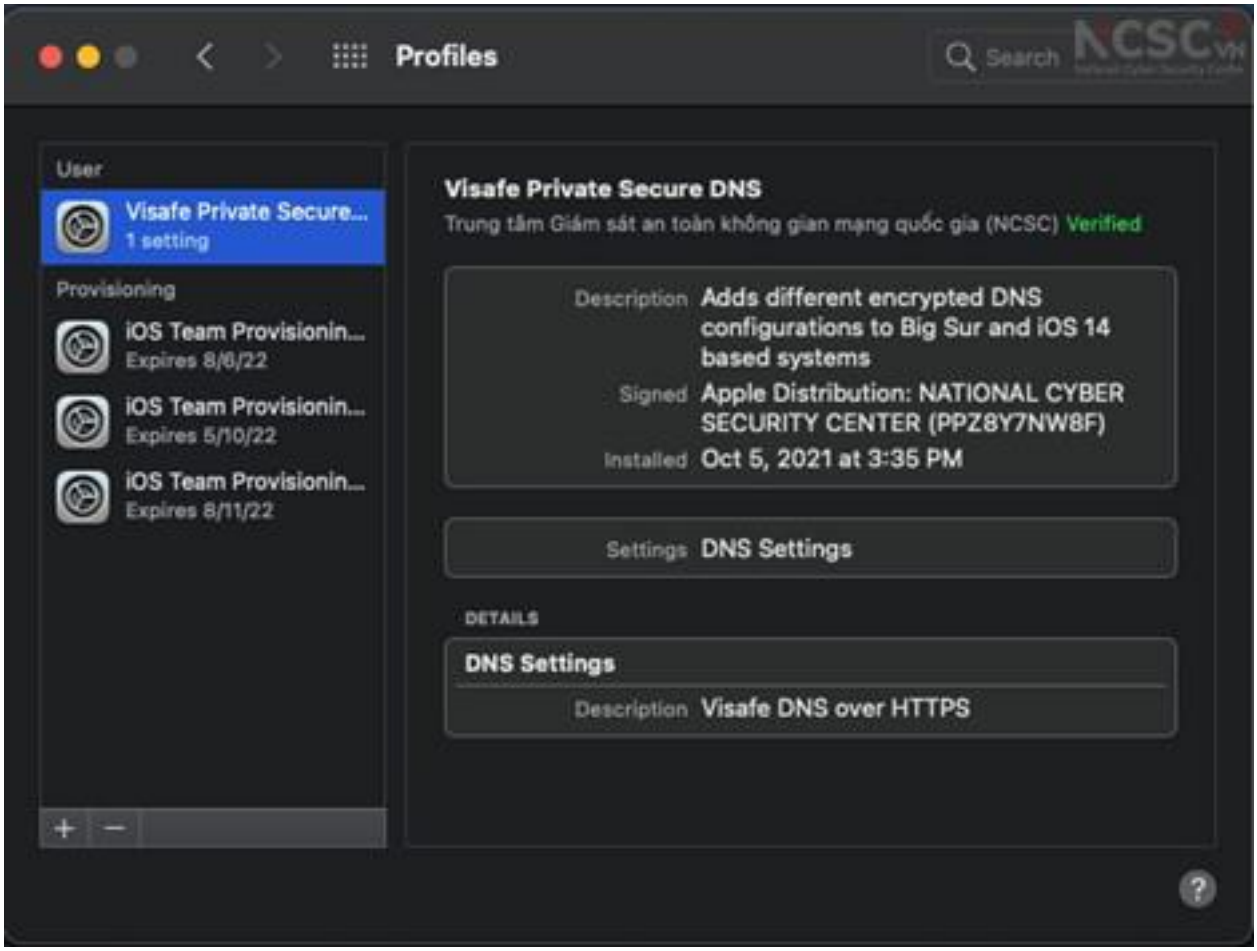


Hình 133: Cài đặt Visafe trên MacOS (2)

Bước 5: Nhập thông tin đăng nhập, và chọn *OK*

Hình 134: Cài đặt Visafe trên MacOS (3)

Bước 6: Công cụ Visafe sau khi cài đặt hoàn tất sẽ được bật, nhằm đảm bảo an toàn thông tin cho bạn trên mạng.



Hình 135: Cài đặt Visafe trên MacOS (4)

3. Điện thoại sử dụng hệ điều hành Android

3.1. Hướng dẫn cài đặt thiết bị Android về cài đặt gốc

Thiết lập cài đặt gốc trên thiết bị sẽ xóa bỏ tất cả dữ liệu cá nhân của bạn trên thiết bị, và đưa thiết bị về trạng thái ban đầu khi chưa qua sử dụng. Việc này cũng sẽ hữu ích trong trường hợp điện thoại của bạn có dấu hiệu bị lây nhiễm mã độc nhưng không có chuyên gia hỗ trợ.

Các bước thực hiện:

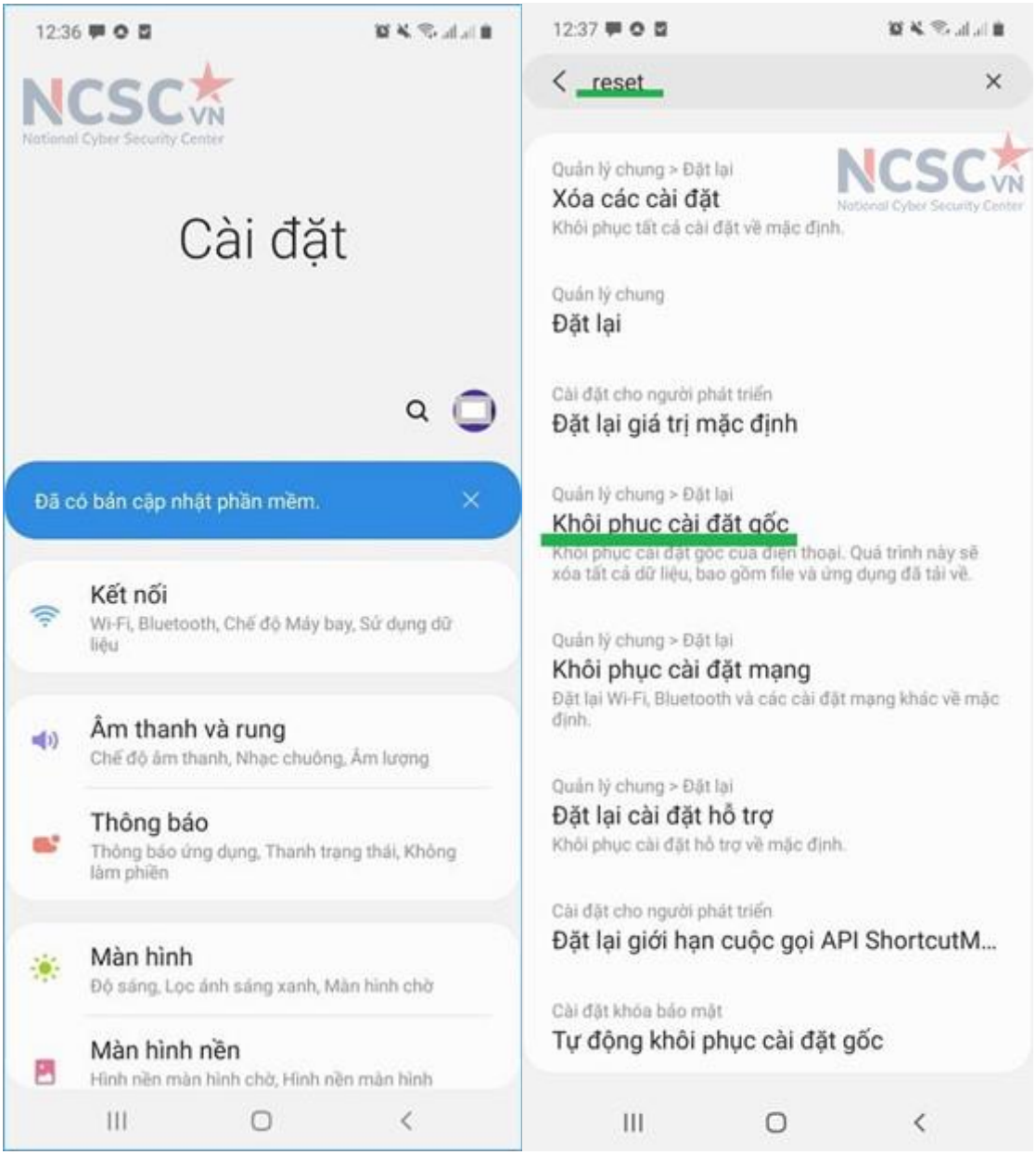
Bước 1: Chọn mục Cài đặt trong thiết bị và gõ vào ô tìm kiếm từ khóa “reset”, giao diện sẽ hiển thị các loại cài đặt reset thiết bị

Bước 2: Chọn Khôi phục cài đặt gốc > Đặt lại

Bước 3: Nhập mật khẩu trên thiết bị (nếu được yêu cầu) để xác thực quá trình cài đặt

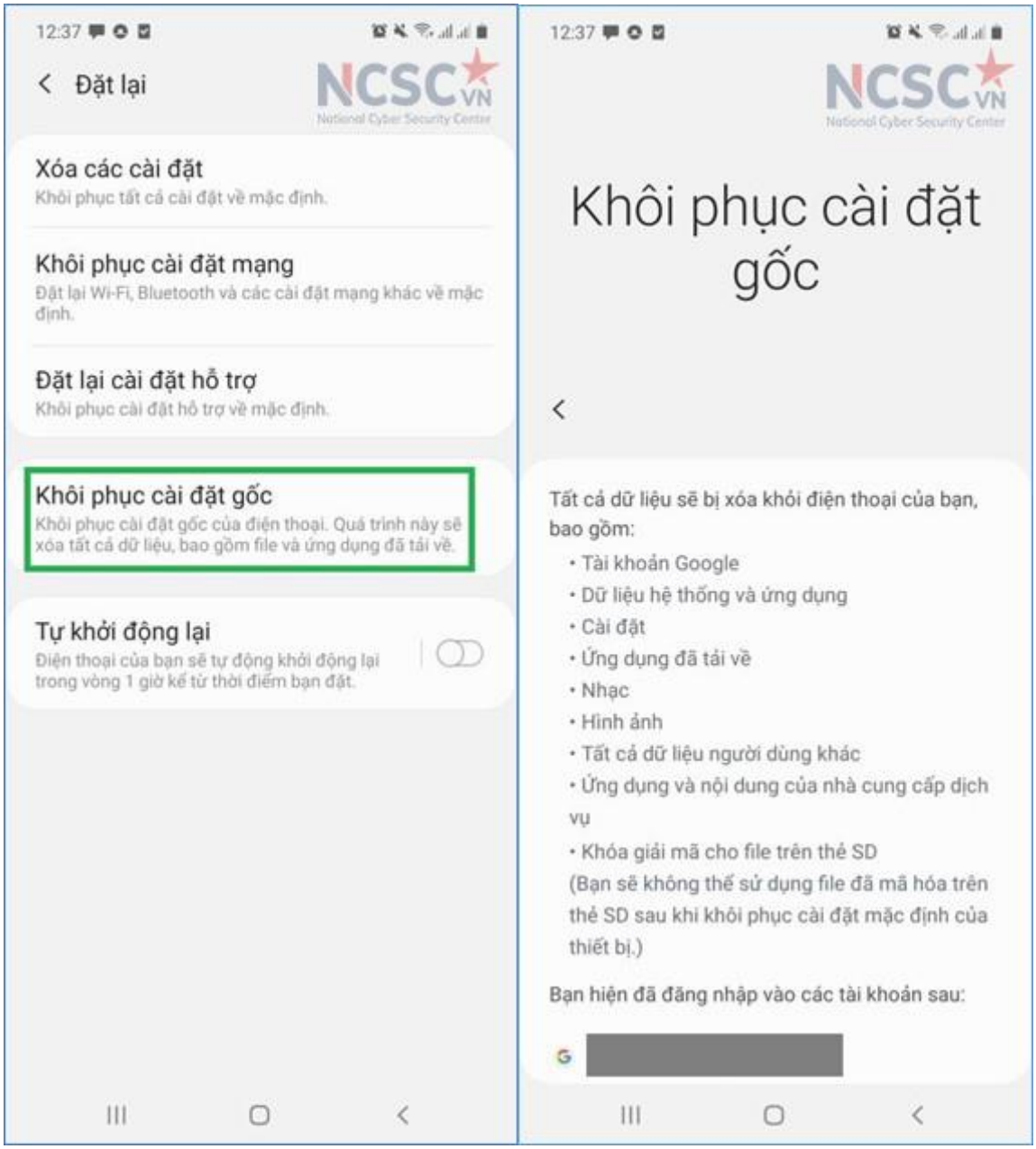
Bước 4: Chọn Xóa hết và đợi cho quá trình cài đặt lại hoàn tất.

Hình ảnh minh họa các bước cài đặt:



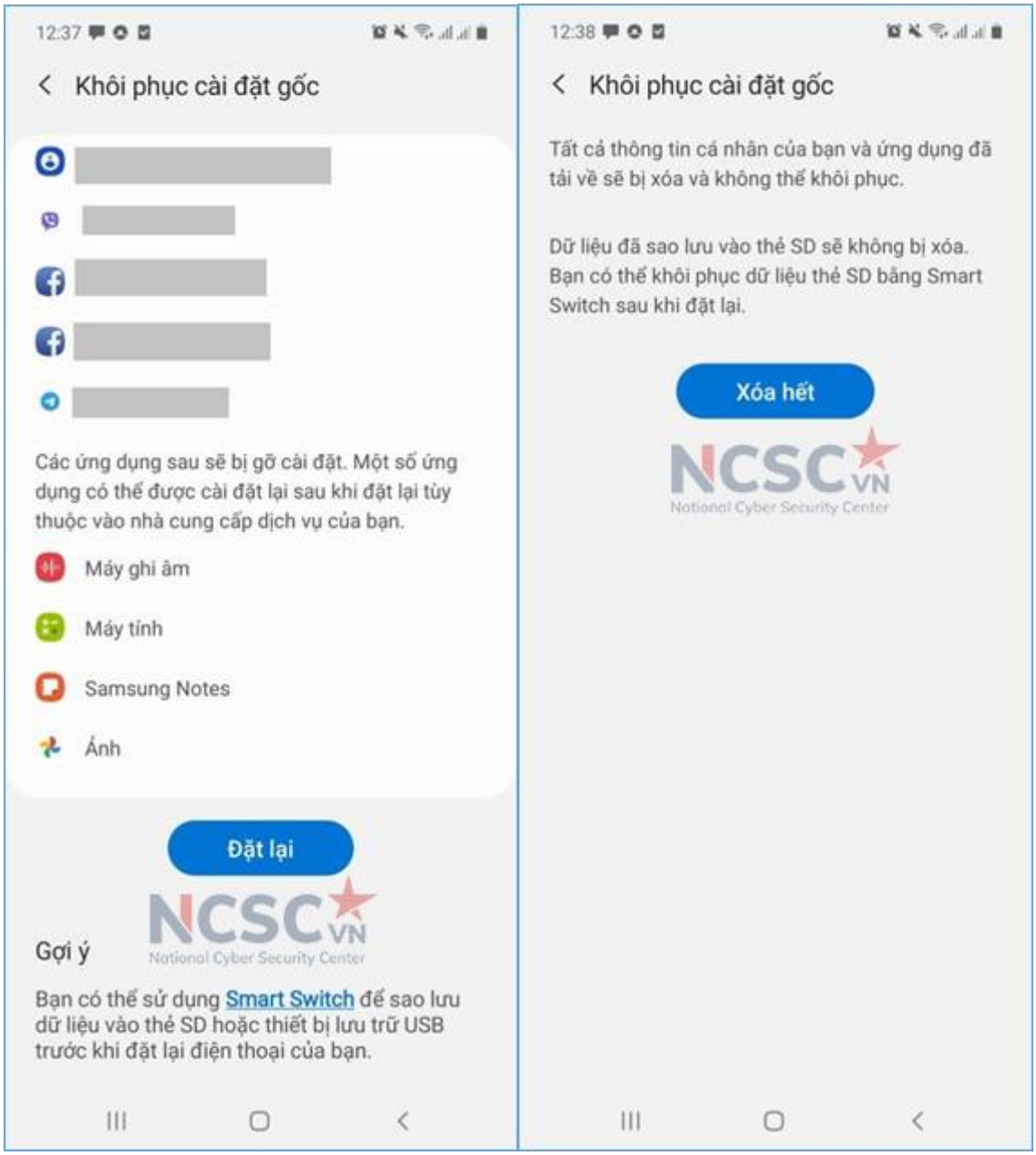
Hình 136: Đưa thiết bị Android về cài đặt gốc (1)

Chọn mục Cài đặt và tìm kiếm từ khóa “reset”



Hình 137: Đưa thiết bị Android về cài đặt gốc (2)

Giao diện tương ứng khi chọn Khôi phục cài đặt gốc



Hình 138: Đưa thiết bị Android về cài đặt đốc (3)

Chọn Đặt lại và Xóa hết rồi chờ quá trình cài đặt lại hoàn tất

3.2. Cài đặt ban đầu cho thiết bị Android

Sau khi mua mới hoặc thiết lập cài đặt gốc trên thiết bị Android, bạn nên thực hiện một số cài đặt ban đầu cho thiết bị bao gồm:

3.2.1. Cài đặt mật khẩu cho thiết bị

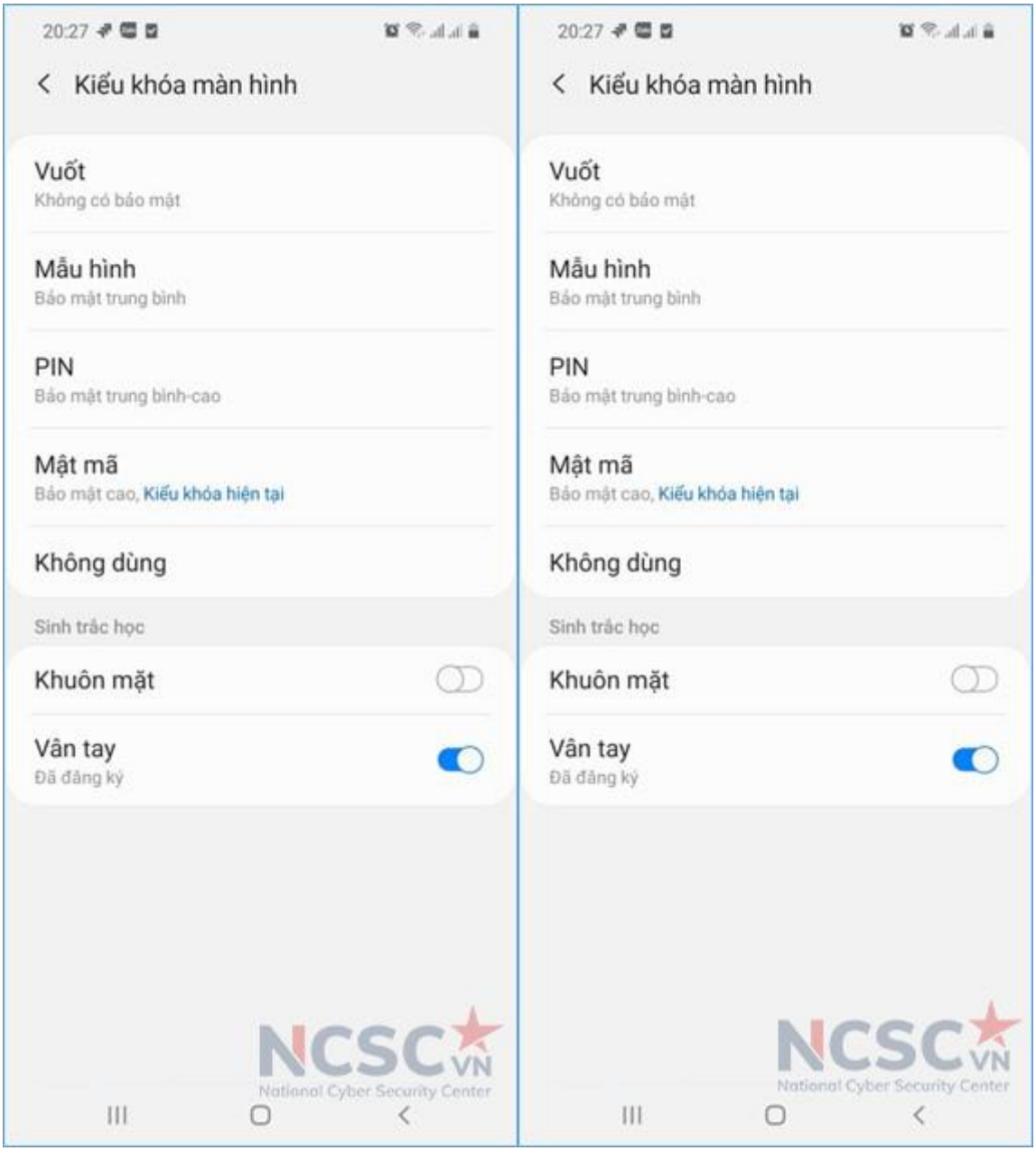
Bạn nên thiết lập mật khẩu để bảo vệ các thông tin cá nhân và thiết bị của mình.

Mật khẩu có thể sử dụng bằng đoạn kí tự, hình vẽ, sinh trắc học (dấu vân tay, khuôn mặt…)

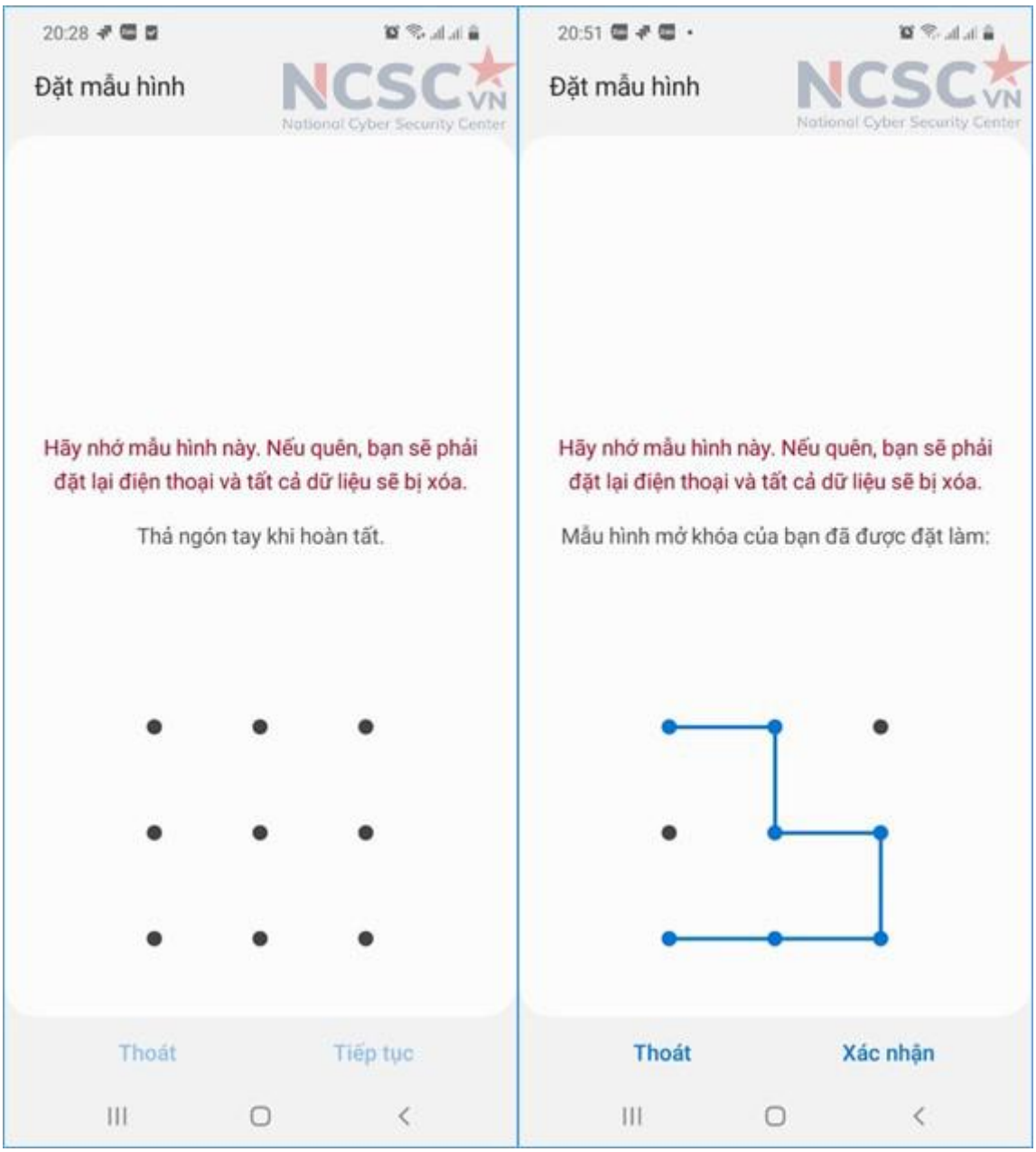
Để cài đặt bảo mật cho thiết bị, vào phần Cài đặt > Cài đặt màn hình khóa > Kiểu

khóa màn hình. Giao diện sẽ hiển thị các tùy chọn bảo mật mà bạn có thể chọn để khóa màn hình cho thiết bị. Bạn có thể chọn bất kỳ tùy chọn bảo mật nào và làm theo chỉ dẫn trên màn hình để hoàn tất thành cài đặt.

Dưới đây là hình minh họa một số cài đặt bảo mật cho thiết bị

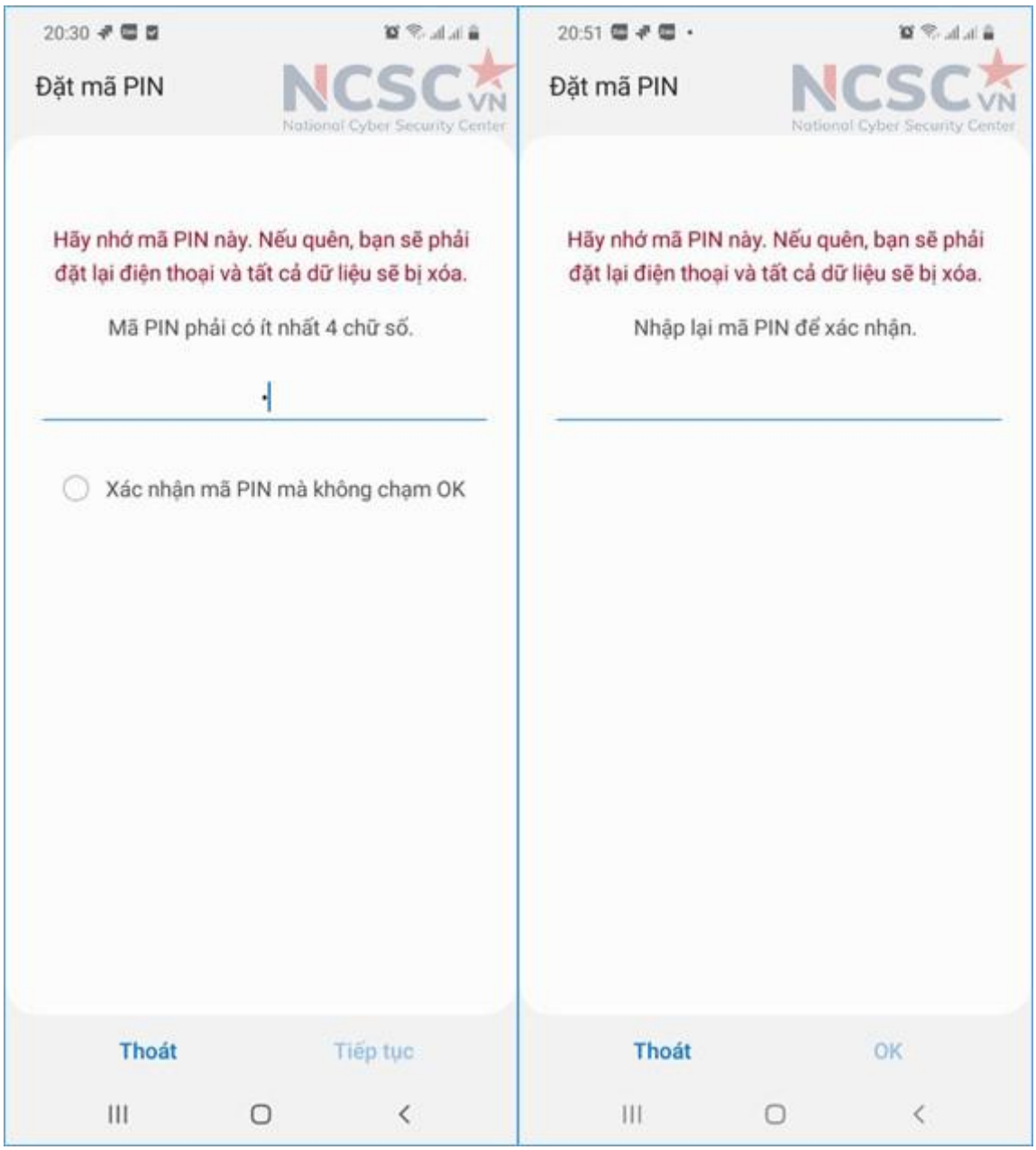


Hình 139: Các tùy chọn bảo mật cho thiết bị

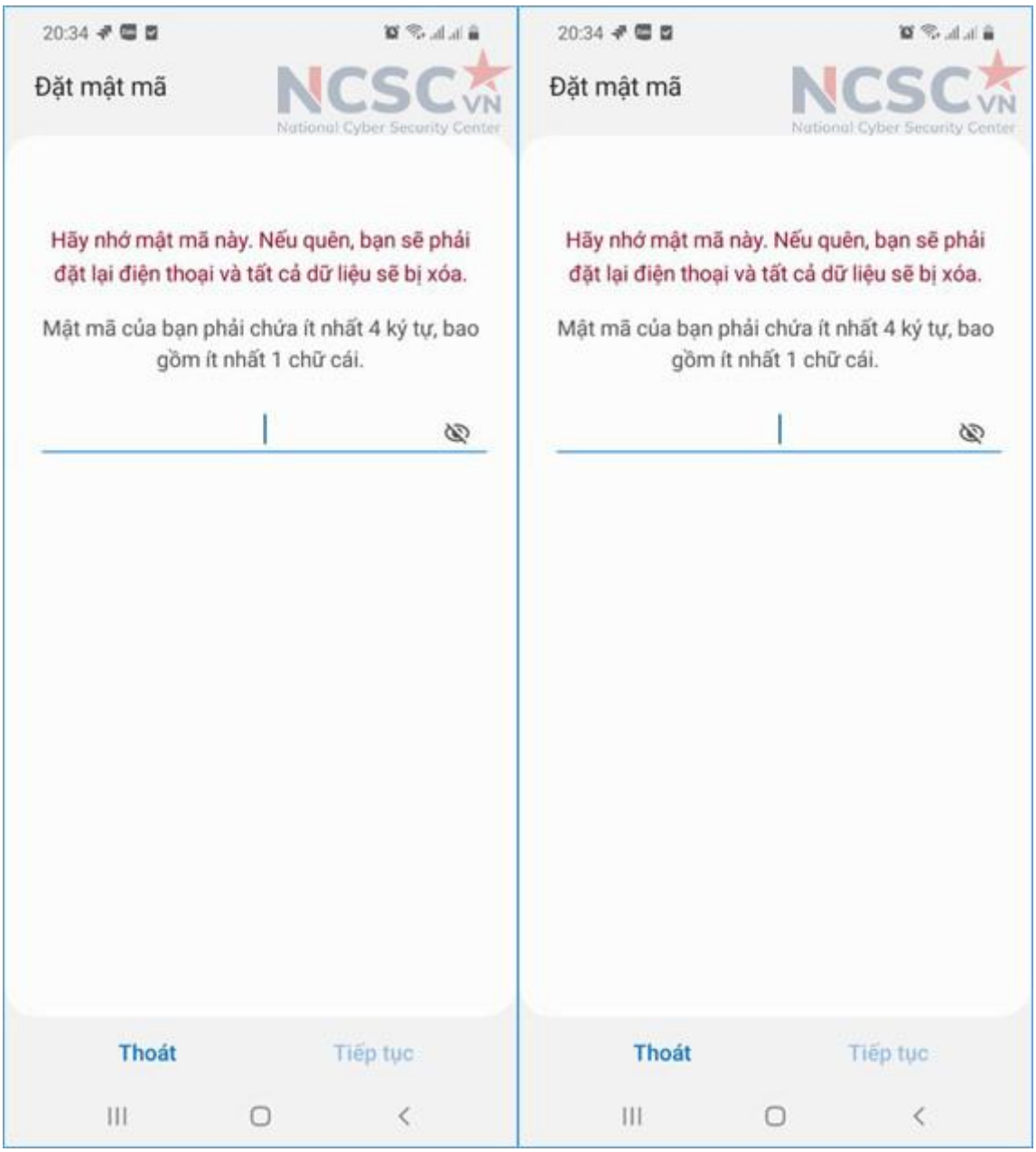


Hình 140: Cài đặt bảo mật bằng mẫu hình (Vẽ mẫu hình)

Hình 141: Cài đặt bảo mật bằng mẫu hình (Xác nhận lại mẫu hình)



Hình 142: Cài đặt bảo mật bằng mã PIN



Hình 143: Cài đặt bảo mật bằng mật khẩu

Hình 144: Cài đặt bảo mật bằng nhận diện khuôn mặt

3.2.2. Cài đặt tài khoản Google

Khi thiết bị ở trạng thái cài đặt gốc, nó sẽ yêu cầu bạn đăng nhập tài khoản Google (tài khoản Gmail) hoặc tạo mới nếu chưa có. Bước này giúp thiết bị đồng bộ với các dịch vụ Google của bạn như Email, lịch, bản đồ ...

Các bước thực hiện:

Bước 1: Mở ứng dụng Cài đặt trên điện thoại.

Bước 2: Nhấn vào mục Tài khoản. Nếu bạn không nhìn thấy mục "Tài khoản", hãy nhấn vào Người dùng và tài khoản.

Bước 3: Ở dưới cùng, hãy nhấn vào Thêm tài khoản.

Bước 4: Chọn Google

Bước 5: Thiết bị có thể yêu cầu xác nhận để tiếp tục quá trình cài đặt

Bước 6: Đăng nhập bằng Tài khoản Google hoặc Tạo tài khoản nếu chưa có.

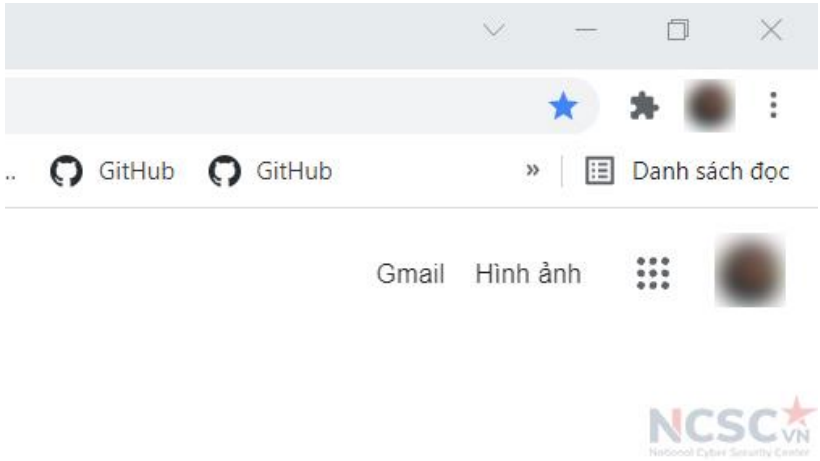
Bước 7: Làm theo hướng dẫn trên màn hình để hoàn tất quá trình cài đặt.

Lưu ý đối với tài khoản Google, cần thiết lập xác thực 2 bước để đảm bảo an toàn cho tài khoản.

Để thiết lập xác thực 2 bước cho tài khoản Google thực hiện như sau:

Bước 1: Vào phần quản lý tài khoản Google

Mở Tài khoản Google bằng cách truy cập https://www.google.com/account/about/?hl=en-US hoặc nhấp vào biểu tượng đại diện tài khoản ở góc bên phải trình duyệt.

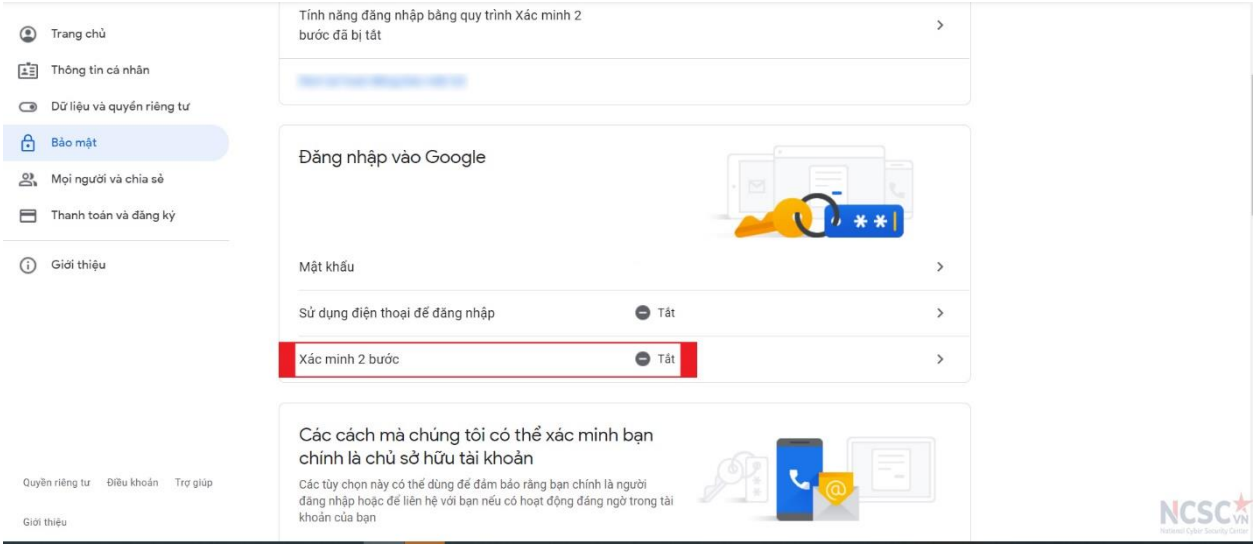


Hình 145: Thiết lập xác thực 2 bước cho tài khoản Google (1)

Sau đó, bấm chọn Quản lý Tài khoản Google của bạn.

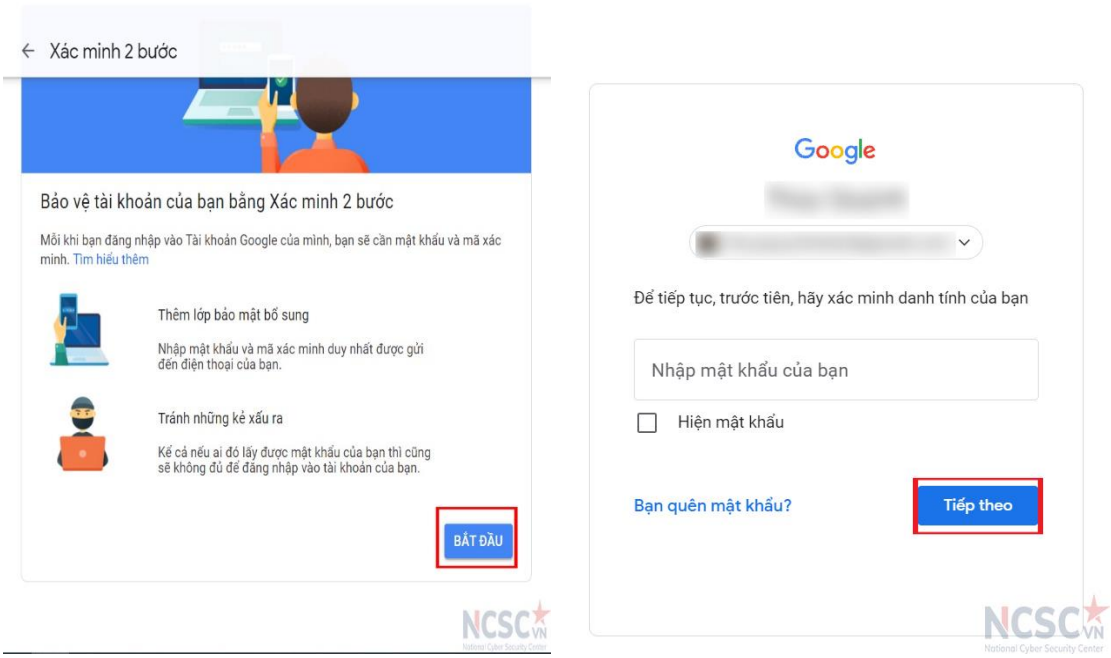
Hình 146: Thiết lập xác thực 2 bước cho tài khoản Google (2)

Bước 2: Chọn mục Bảo mật, tìm đến mục **Xác minh 2 bước** > Chọn **Đang tắt**.



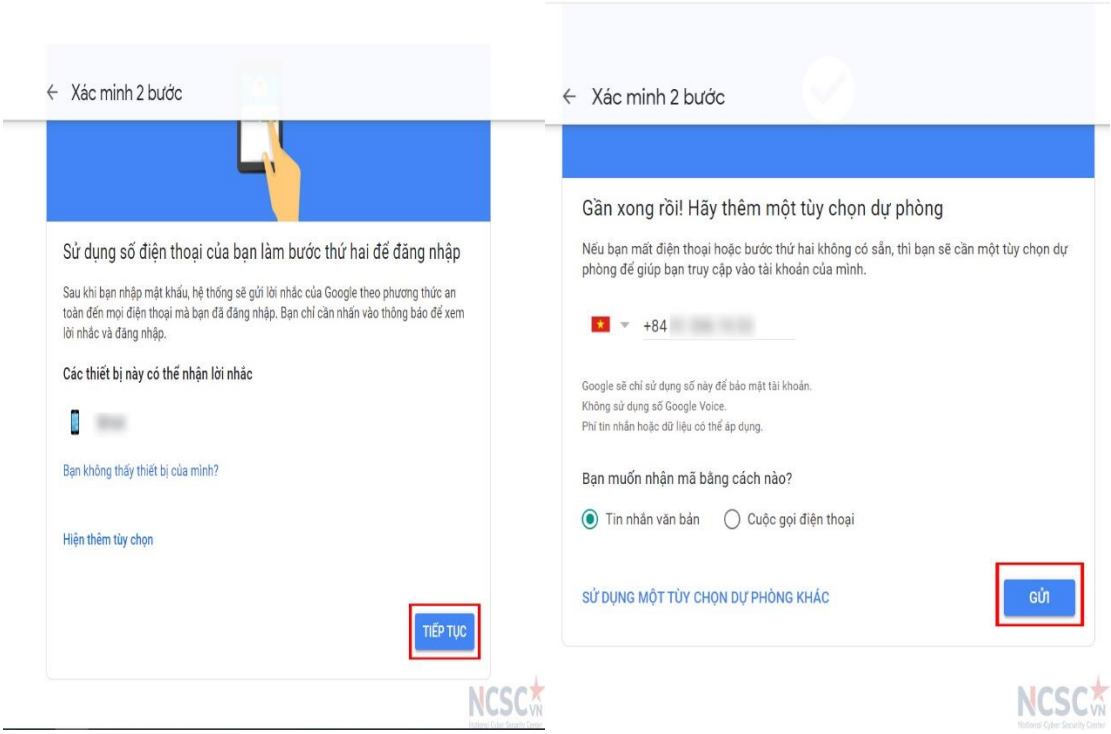
Hình 147: Thiết lập xác thực 2 bước cho tài khoản Google (3)

Bước 3: Chọn **Bắt đầu** > Nhập mật khẩu của bạn > Chọn **Tiếp theo**.



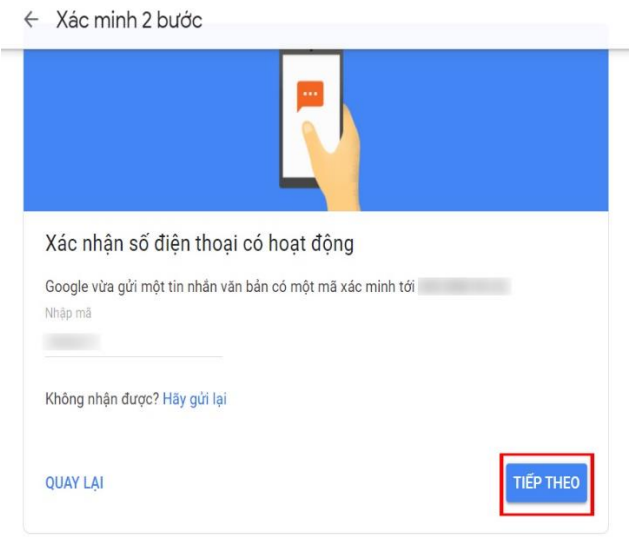
Hình 148: Thiết lập xác thực 2 bước cho tài khoản Google (4)

Bước 4: Chọn **Tiếp tục** > **Bạn muốn nhận mã bằng cách nào?** bạn có thể chọn 1 trong 2 cách nhận mã xác minh bằng **Tin nhắn văn bản** hoặc **Cuộc gọi điện thoại** > Nhấn **Gửi**.



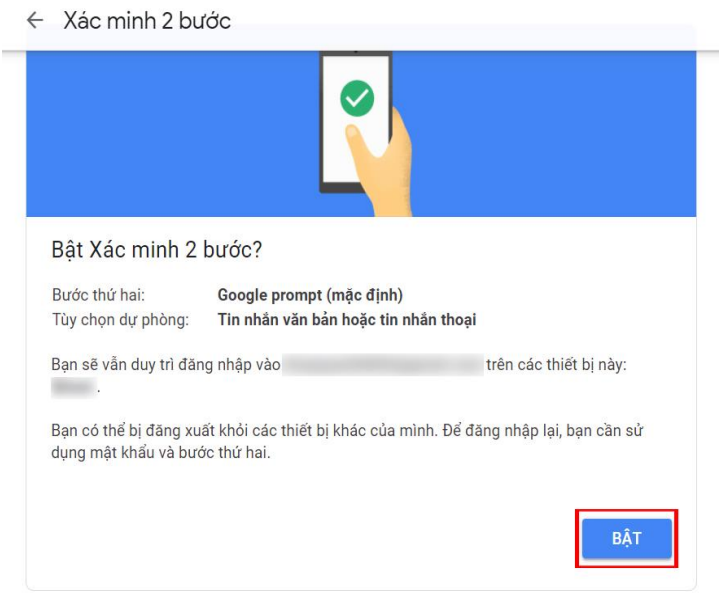
Hình 149: Thiết lập xác thực 2 bước cho tài khoản Google (5)

Bước 5: Nhập mã xác nhận vừa được gửi về điện thoại > Chọn **Tiếp Theo**.



Hình 150: Thiết lập xác thực 2 bước cho tài khoản Google (6)

Bước 6: Nhấn **Bật** để hoàn tất quá trình thiết lập.



Hình 151: Thiết lập xác thực 2 bước cho tài khoản Google (7)

2.2.3. Cài đặt một số ứng dụng cần thiết

Để cài đặt thêm các ứng dụng trên thiết bị, bạn có thể thực hiện theo các bước sau:

Bước 1: Mở chức năng Cửa hàng Google Play (CH Play)

Bước 2: Gõ tên ứng dụng muốn tìm tại thanh tìm kiếm của ứng dụng

Bước 3: Ứng dụng cần tìm sẽ hiện ra (nếu có)

Bước 4: Nhấn Cài đặt để thực hiện và chờ cho đến khi quá trình cài đặt hoàn tất.

Bước 5: Sau khi ứng dụng được cài đặt, bạn có thể mở nó và thiết lập các cài đặt cho ứng dụng.

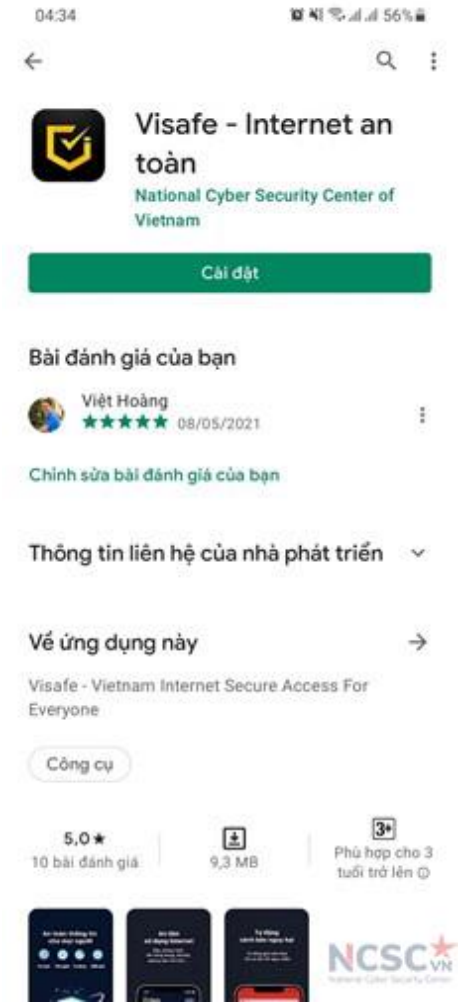
3.3. Sử dụng ứng dụng Internet an toàn trên hệ điều hành Android

Ứng dụng Internet an toàn (Visafe) là ứng dụng miễn phí dành cho người dùng Internet Việt Nam để tự bảo vệ mình trên không gian mạng trước các trang web lừa đảo, trang web có chứa mã độc, các quảng cáo và đường dẫn nguy hiểm, độc hại. Ngoài ra khi sử dụng Visafe, người dùng có thể sử dụng chức năng bảo vệ trẻ em để hạn chế các trang web không lành mạnh, các quảng cáo, đường link nguy hiểm không phù hợp với lứa tuổi.

Visafe do Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) xây dựng, vận hành và triển khai miễn phí hướng đến cảnh báo và bảo vệ mọi người dân trên không gian mạng trước các nguy cơ, trang web độc hại đã phát hiện ra.

Để sử dụng Visafe trên thiết bị chạy hệ điều hành Android thực hiện theo các bước sau:

Bước 1: Truy cập **Google Play** và tìm kiếm **Visafe.** Sau đó cài đặt ứng dụng **Visafe - Internet an toàn**



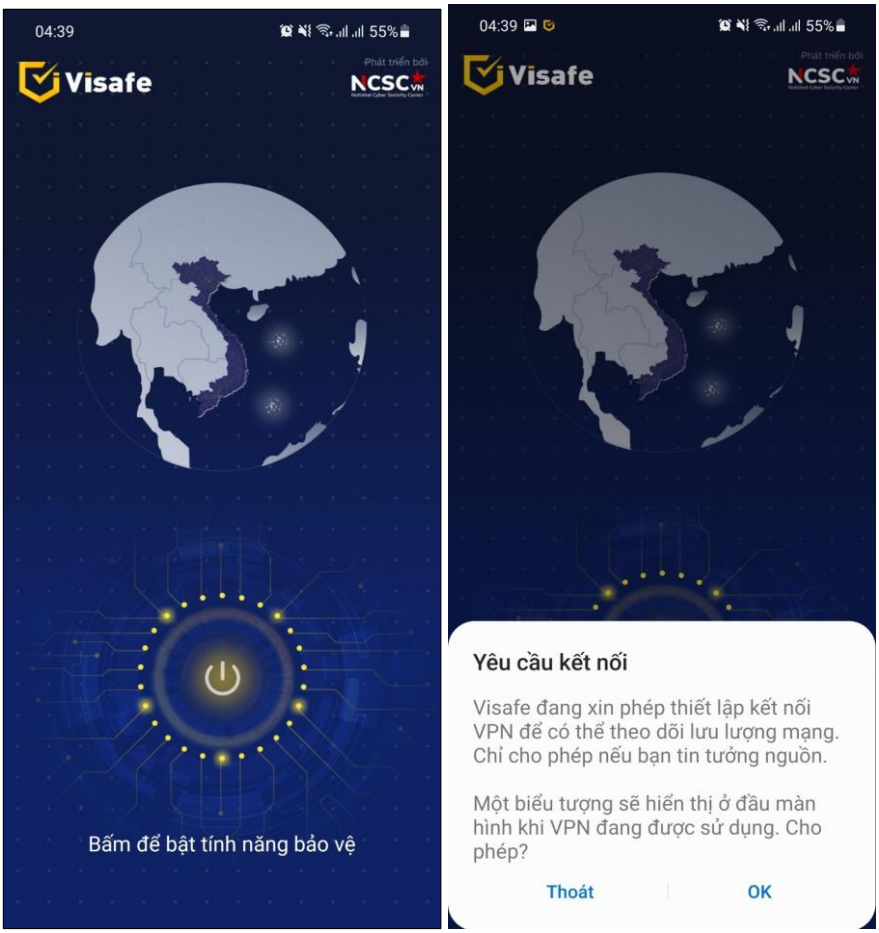
Hình 152: Cài đặt ứng dụng Visafe trên Android (1)

Bước 2: Truy cập ứng dụng Visafe để hoàn tất quá trình kích hoạt và sử dụng Visafe theo hướng dẫn dưới đây.

- Mở ứng dụng Visafe đã được cài đặt trên thiết bị. Bấm chọn "BẮT ĐẦU NGAY" để truy cập vào màn hình chính.

Hình 153: Cài đặt ứng dụng Visafe trên Android (2)

- Giao diện chính của ứng dụng như hình dưới đây:



Hình 154: Cài đặt ứng dụng Visafe trên Android (3)

"Bật tính năng bảo vệ" để kích hoạt **Visafe**. Ở lần đầu tiên **bật,** chọn "OK" để đồng ý tạo **VPN Visafe** trên thiết bị.

Sau khi kích hoạt thành công màn hình thiết bị sẽ hiển thị như sau:

Hình 155: Cài đặt ứng dụng Visafe trên Android (4)

4. Điện thoại sử dụng Hệ điều hành iOS

4.1. Tắt các dịch vụ, tính năng không cần thiết

Để giảm thiểu rủi ro cho thiết bị và dữ liệu trên thiết bị bạn nên vô hiệu hoá các dịch vụ tuỳ chọn không sử dụng đến, vì các dịch vụ này có thể bị lợi dụng để gửi, nhận dữ liệu độc hại.

4.1.1. Tắt Airdrop

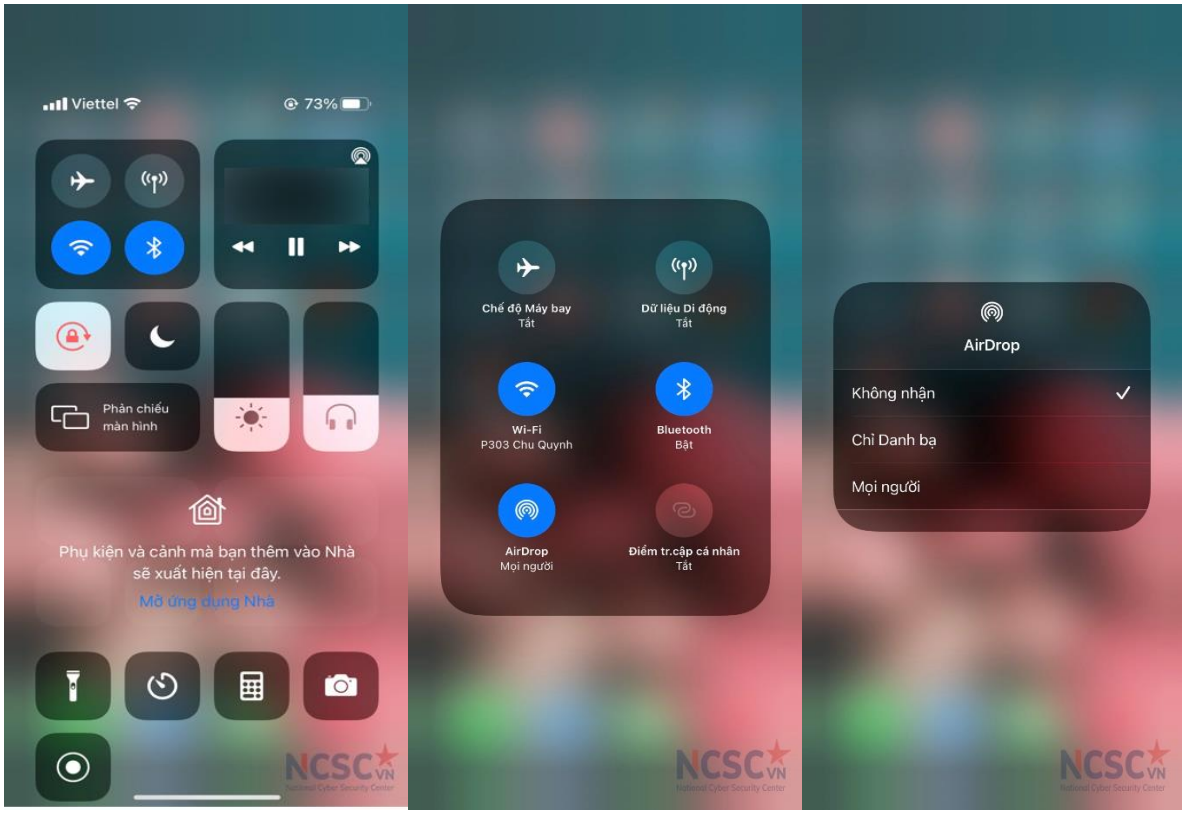
Airdrop cho phép gửi và nhận các hình ảnh, video, số liên lạc và các tập tin khác từ mọi người trong vùng lân cận. Trước đây, Airdrop có xu hướng dễ bị khai thác từ xa và xâm nhập.

Để tắt Airdrop thực hiện theo các bước sau:

Bước 1: Kéo xuống từ phía góc trên bên phải của màn hình để mở Trung tâm điều khiển.

Bước 2: Nhấn giữ hoặc chạm và giữ thẻ cài đặt mạng ở phía góc bên trái, sau đó nhấn Airdrop.

Bước 3: Sau đó chọn **Không nhận** để tắt Airdrop



Hình 156: Tắt Airdrop

4.1.2. Tắt Bluetooth

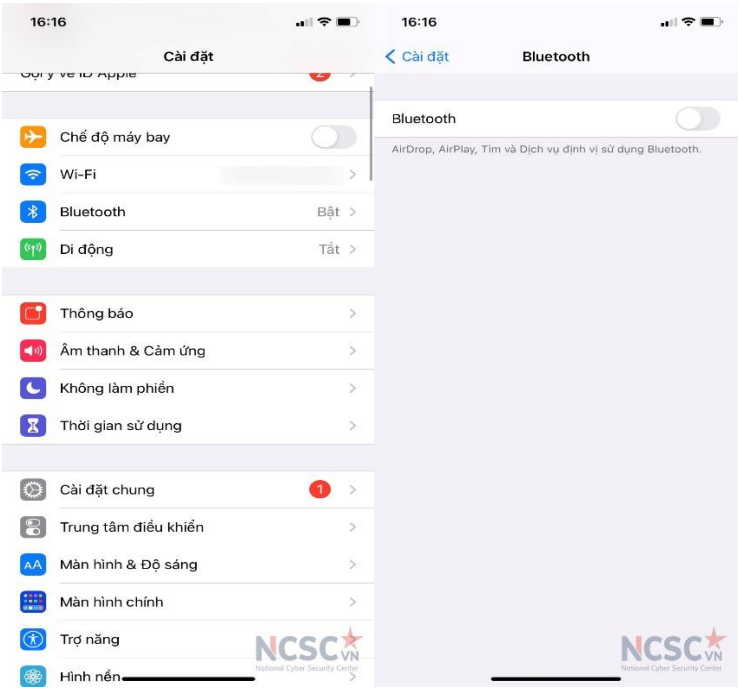
Việc luôn bật Bluetooth có thể tăng khả năng bị tấn công. Nếu bạn không thường xuyên sử dụng Bluetooth thì nên tắt đi. Để tắt Bluetooth thực hiện như sau:

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Chọn Bluetooth

Bước 3: Gạt nút sang vị trí Tắt để tắt hoàn toàn Bluetooth.

Lưu ý: Việt bật tắt Bluetooth trong Trung tâm điều khiển chỉ tạm thời ngắt kết nối thiết bị, nó không tắt hoàn toàn Bluetooth.



Hình 157: Tắt Bluetooth

4.1.3. Tắt Điểm truy cập cá nhân

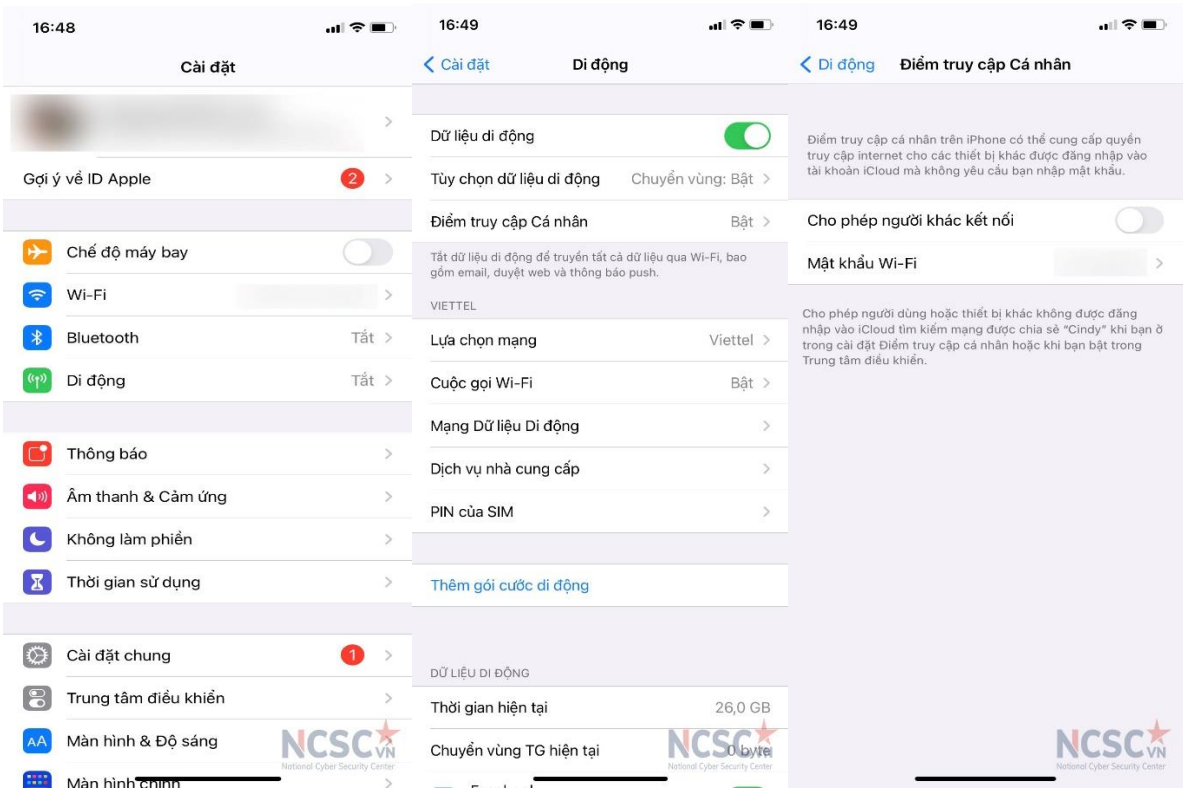
Điểm truy cập cá nhân cho phép các thiết bị khác chia sẻ kết nối dữ liệu di động của bạn. Sử dụng tính năng này cho phép thiết bị của bạn trở thành Điểm Truy Cập Wifi mà các thiết bị khác có thể kết nối vào và truy cập Internet. Tắt Điểm truy cập cá nhân để hạn chế việc tiếp xúc của các thành phần với các thiết bị không đáng tin cậy.

Bước 1: Mở Cài đặt

Bước 2: Chọn Dữ liệu di động hoặc Di động

Bước 3: Chọn Điểm truy cập cá nhân

Bước 4: Nhấn vào thanh trượt để tắt



Hình 158: Tắt Điểm truy cập cá nhân

4.1.4. Tắt chuyển tiếp cuộc gọi trên các thiết bị khác

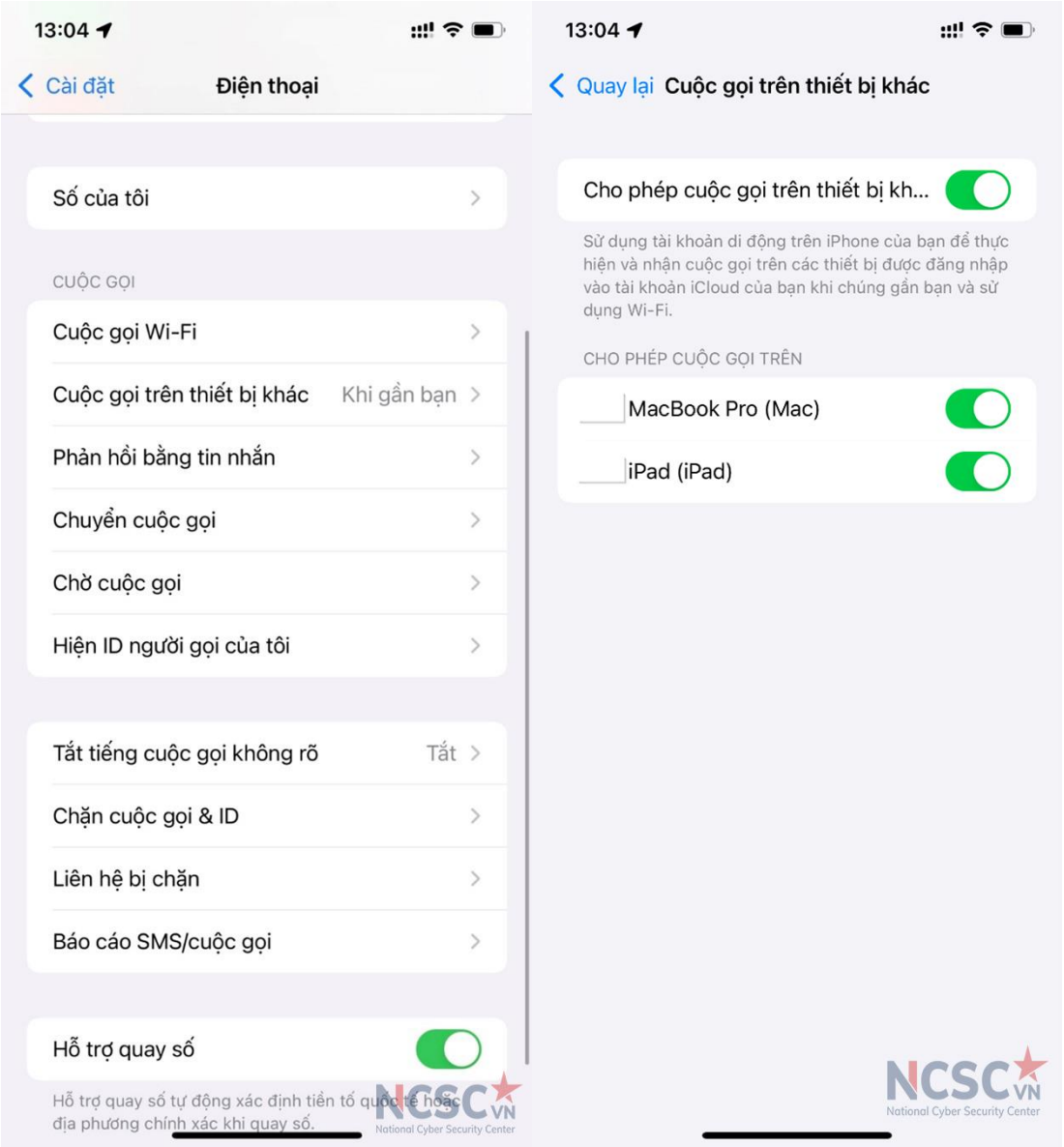
Các thiết bị iOS có thể được cấu hình để chuyển tiếp các cuộc gọi đến các thiết bị Apple khác (như MacBooks và iPads). Để tắt chuyển tiếp cuộc gọi đến thiết bị khác thực hiện như sau:

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Chọn Điện thoại

Bước 3: Chọn Cuộc gọi trên thiết bị khác

Bước 4: Tắt tùy chọn Cho phép cuộc gọi trên thiết bị khác. Các cuộc gọi của bạn sẽ không được chia sẻ truy cập với các thiết bị Apple khác.



Hình 159: Tắt chuyển tiếp cuộc gọi trên thiết bị khác

4.1.5. Tắt chuyển tiếp tin nhắn văn bản

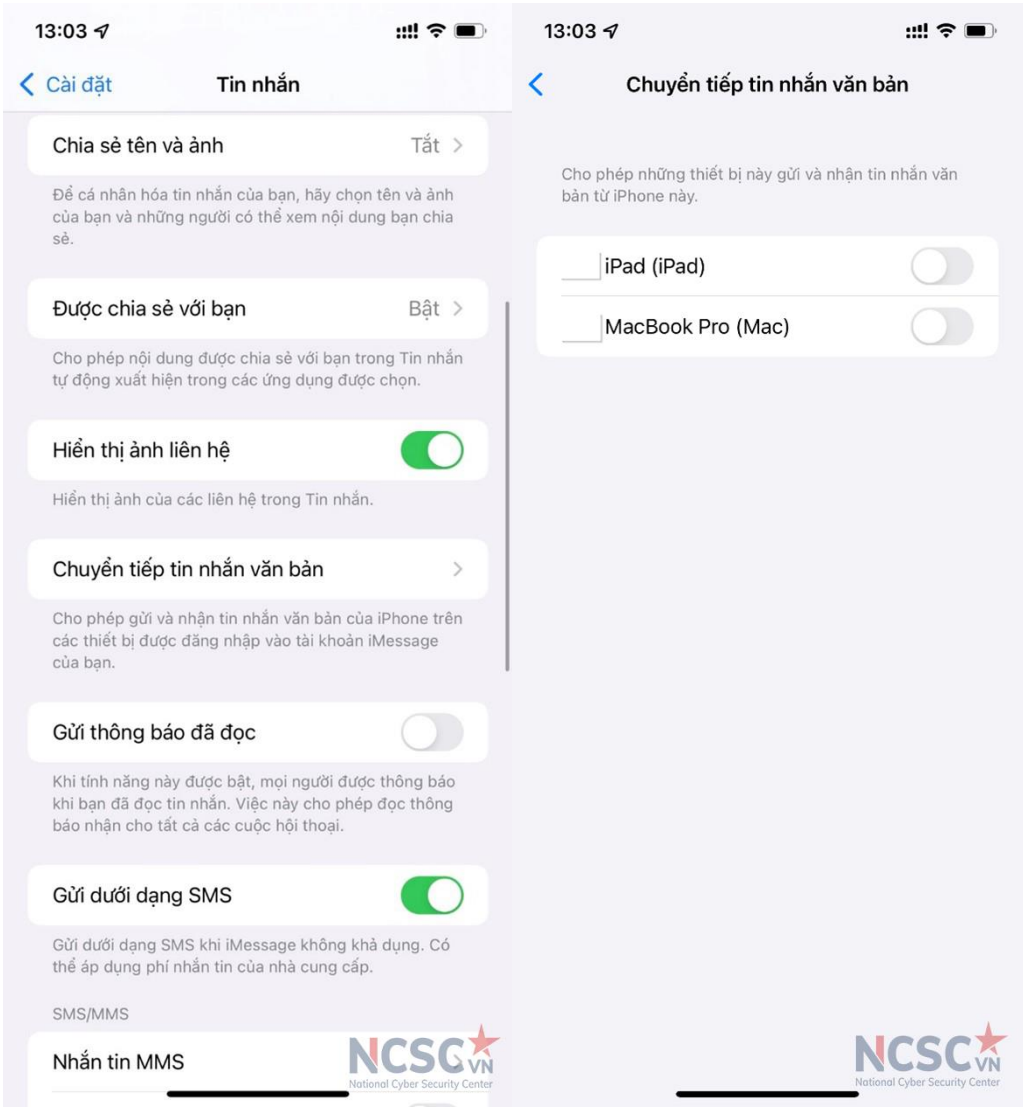
Khi tính năng Chuyển tiếp tin nhắn văn bản (Text Message Forwarding) được bật, tin nhắn SMS/MMS mới trên iPhone có thể xuất hiện trên thiết bị khác khi trong cùng mạng Wi-Fi. Nó có thể được sử dụng để theo dõi trái phép cũng như đánh cắp dữ liệu nhạy cảm (Ví dụ lấy mã OTP).

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Chọn Tin nhắn

Bước 3: Chọn Chuyển tiếp tin nhắn văn bản

Bước 4: Xem xét danh sách thiết bị và vô hiệu hóa thiết bị không thích hợp



Hình 160: Tắt chuyển tiếp tin nhắn văn bản

4.1.6. Tắt theo dõi qua ứng dụng

Việc theo dõi truy cập được sử dụng bởi hầu hết các nhà bán lẻ để theo dõi sở thích và các lần mua sắm của bạn qua web. Họ thường sử dụng mọi kỹ thuật có sẵn để theo dõi bạn, bao gồm cookies, tracking pixels, các URL tuỳ chỉnh và hơn thế nữa.

Apple cung cấp tính năng theo dõi cho các ứng dụng và chúng ta có thể tắt nó.

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Đi đến Quyền riêng tư

Bước 3: Chọn Theo dõi

Bước 4: Chọn tắt ở Cho phép ứng dụng yêu cầu theo dõi

4.1.7. Tắt tính năng tải hình ảnh email từ xa

Theo mặc định, ứng dụng Mail sẽ tải và hiển thị những hình ảnh từ xa. Tắt các hình ảnh từ xa sẽ ngăn ngừa các email spam và quảng cáo biết bạn đang mở thư của họ. Để tắt tính năng này có thể thực hiện theo các bước sau:

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Kéo xuống dưới và chọn Mail

Bước 3: Chọn tắt ở Tải hình ảnh từ xa

Hình 161: Tắt tính năng tải hình ảnh email từ xa

4.1.8. Tắt quảng cáo dựa trên vị trí

Iphone của bạn gửi vị trí, bao gồm cả tốc độ và hướng di chuyển đến Apple để cung cấp cho bạn quảng cáo trên Apple News và trên App Store liên quan đến vị trí địa lý. Vô hiệu hóa dịch vụ Apple Ads dựa trên vị trí.

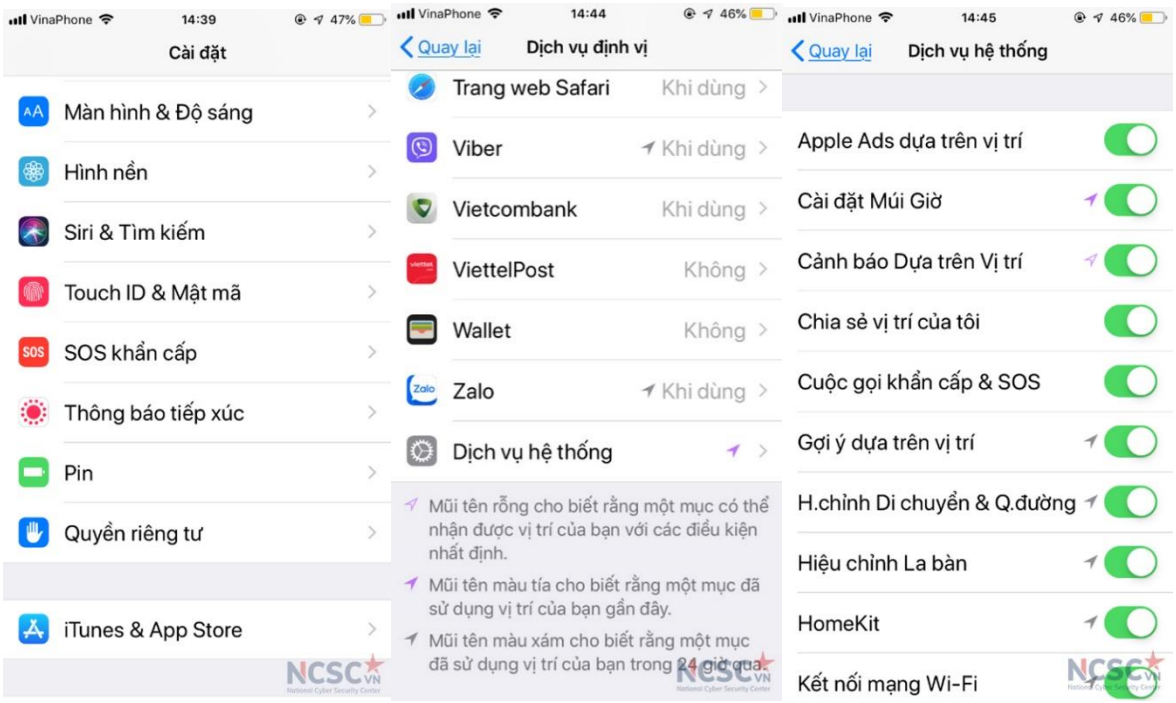
Bước 1: Mở ứng dụng Cài đặt

Bước 2: Chọn Quyền riêng tư

Bước 3: Chọn Dịch vụ định vị. Tại bước này nếu Dịch vụ định vị đang tắt thì tất cả các tùy chọn dưới cũng đã tắt hết.

Bước 4: Cuộn xuống dưới cùng và chọn Dịch vụ hệ thống

Bước 5: Tắt Apple Ads dựa trên vị trí



Hình 162: Tắt quảng cáo dựa trên vị trí

4.1.9. Tắt chia sẻ dữ liệu Siri

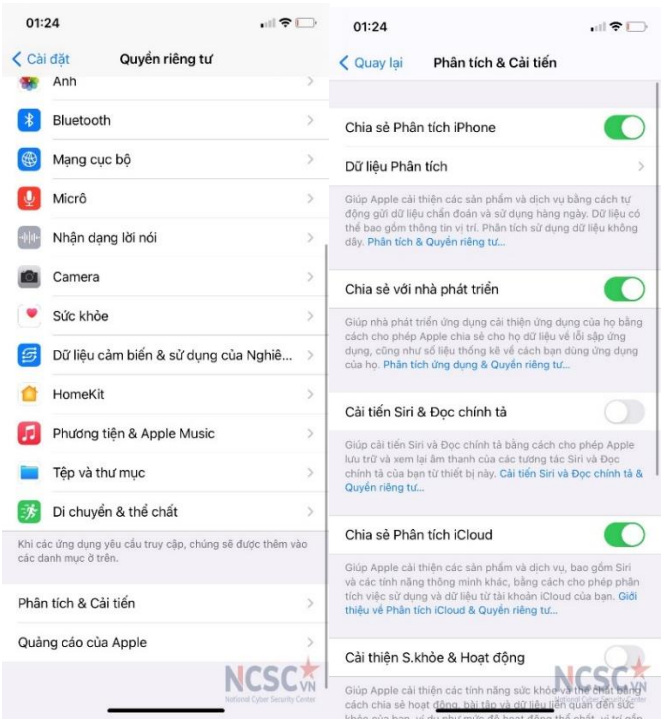
Apple sử dụng một lượng nhỏ các bản ghi Siri ẩn danh để cải thiện tính chính xác và đáng tin cậy. Điều này có thể dẫn đến việc tiết lộ những thông tin bí mật, thông tin định danh của người dùng. Apple cho phép người dùng có thể tắt tính năng thu thập các bản ghi của Siri và Đọc chính tả, và xoá lịch sử. Để tắt chia sẻ dữ liệu Siri thực hiện các bước sau:

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Chọn Quyền riêng tư

Bước 3: Kéo xuống dưới cùng và chọn Phân tích và cải tiến

Bước 4: Tắt Cải tiến Siri và Đọc chính tả



Hình 163: Tắt chia sẻ dữ liệu Siri (1)

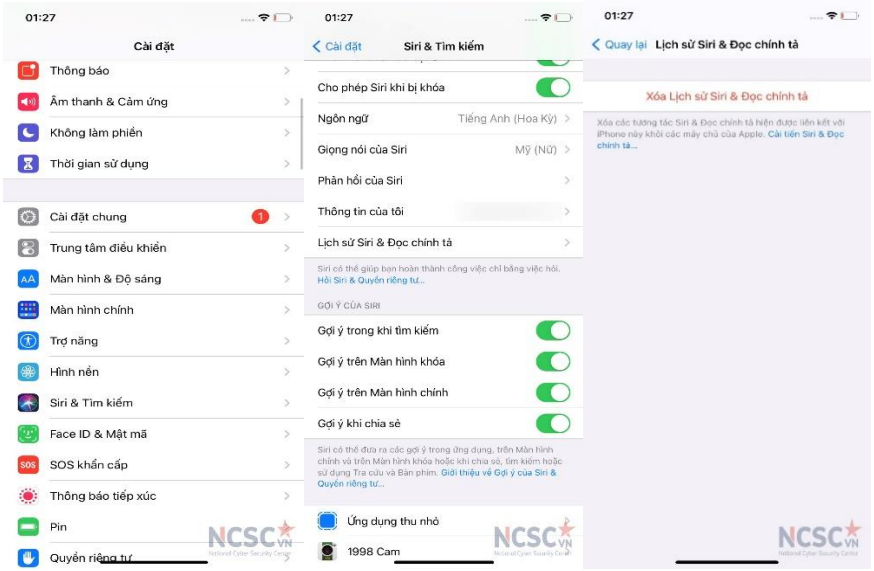
Để xoá lịch sử, chọn Xoá Lịch sử Siri & Đọc chính tả. Việc làm như thế này không ảnh hưởng đến độ chính xác của Siri

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Chọn Siri & Tìm kiếm

Bước 3: Chọn Lịch sử Siri & Đọc chính tả

Bước 4: Chọn Xoá Lịch sử Siri & Đọc chính tả



Hình 164: Tắt chia sẻ dữ liệu Siri (2)

4.2. Sử dụng các tính năng hữu ích

4.2.1. Vô hiệu hóa Trung tâm điều khiển khi khóa điện thoại

Mặc định, Trung tâm điều khiển có thể được truy cập trên màn hình khoá và có thể dẫn đến rủi ro về an toàn thông tin như thay đổi trái phép cài đặt trên thiết bị. Để vô hiệu hóa Trung tâm điều khiển khi khóa thiết bị, thực hiện như sau:

Bước 1: Mở Cài đặt

Bước 2: Chọn

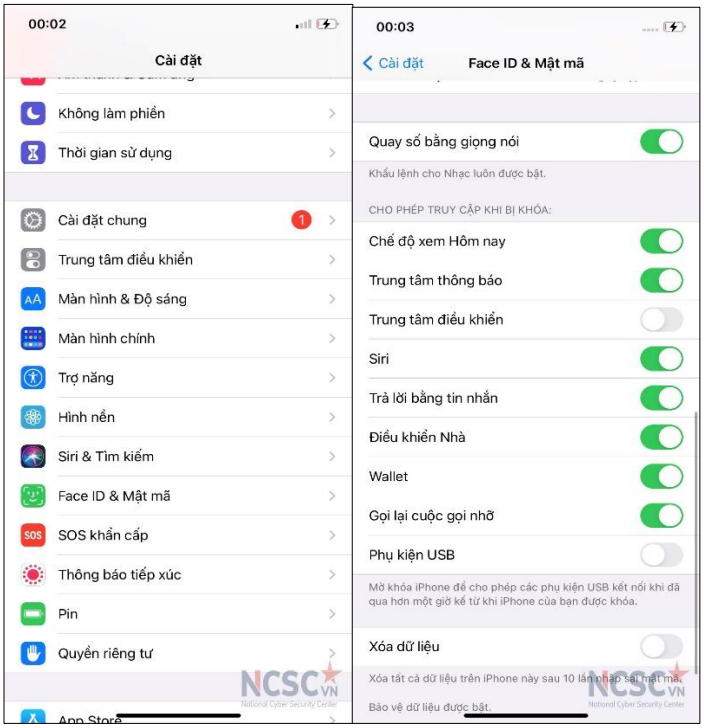
- Touch ID&Mật mã nếu Touch ID được cấu hình
- Face ID& Mật mã nếu Face ID được cấu hình

Bước 3: Nhập mật mã của bạn

Bước 4: Kéo xuống đến mục Cho phép truy cập khi bị khóa

Bước 5: Bỏ chọn Trung tâm điều khiển

Bỏ chọn cả các phần khác nếu không sử dụng



Hình 165: Vô hiệu hóa Trung tâm điều khiển khi khóa thiết bị

4.2.2. Ẩn bản xem trước thông báo khi đang khóa điện thoại

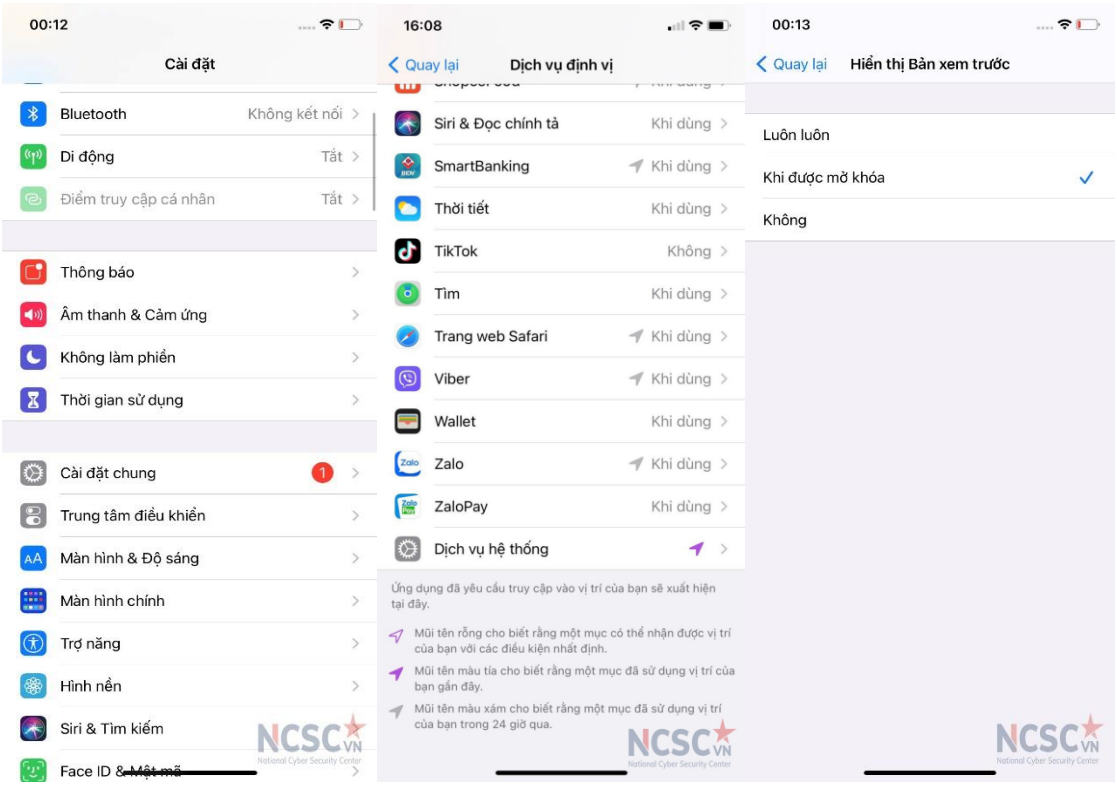
Bạn có thể xem nhanh các thông báo gần đây từ màn hình khoá khi cầm thiết bị. Mặc dù thuận tiện nhưng nó cũng cho phép người lân cận cũng có thể thấy thông báo, bao gồm tin nhắn văn bản, các mã dùng một lần hoặc các tin nhắn nhạy cảm. Bạn có thể tắt tính năng để ẩn việc hiển thị các tin nhắn khi đang khóa máy này như sau:

Bước 1: Mở ứng dụng Cài đặt

Bước 2: Chọn Thông báo

Bước 3: Chọn Hiển thị bản xem trước

Bước 4: Chọn Khi được mở khóa



Hình 166: Ẩn bản xem trước thông báo khi đang khóa máy

4.2.3. Sử dụng chế độ Hạn chế USB

Chế độ Hạn chế USB ngăn các phụ kiện USB cắm vào cổng Lightning để thực hiện kết nối dữ liệu với iPhone, iPad hoặc iPod Touch nếu thiết bị iOS bị khoá hơn một giờ. Sự thay đổi này gây khó khăn cho đối tượng xấu khi muốn đột nhập hơn vào thiết bị.

Các bước thực hiện để bật chế độ cho phép hạn chế USB:

Bước 1: Mở ứng dụng **Cài đặt**

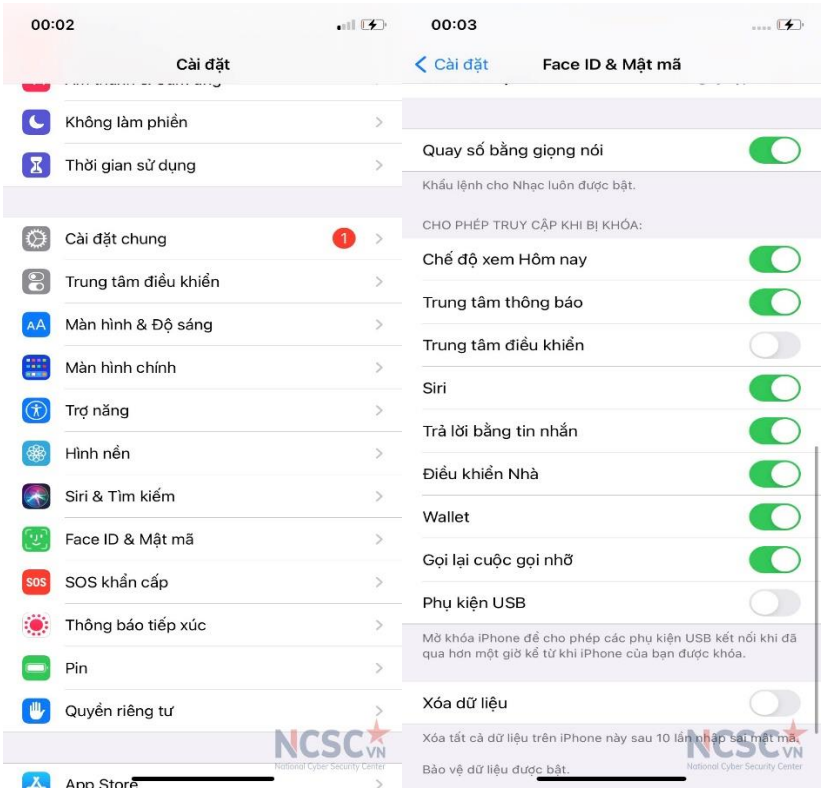
Bước 2: Chọn **Face ID&Mật mã**

Bước 3: Nhập mật mã hiện tại của bạn

Bước 4: Kéo xuống phần **Cho phép truy cập khi bị khóa**

Bước 5: Bỏ chọn **Phụ kiện USB**

Cũng nên bỏ chọn các phần khác mà bạn không sử dụng.



Hình 167: Bật chế độ hạn chế USB

4.2.4. Sử dụng tính năng SOS khẩn cấp

SOS khẩn cấp vô hiệu hoá Touch ID và Face ID cho đến khi nhập mật khẩu đã cài đặt. Tuỳ trường hợp, nó có thể gọi dịch vụ khẩn cấp một cách tự động.

Mặc định, màn hình Khẩn cấp xuất hiện sau khi bạn nhấn và giữ nút nguồn và có thể là nút âm lượng trong 3 giây. Bạn có thể thiết lập cho phép cài đặt Gọi bằng nút sườn. Khi Gọi bằng nút sườn được thiết lập, **nhấn nút sườn 5** lần sẽ kích hoạt tính năng SOS khẩn cấp. Ngoài ra có thể thiết lập chế độ Tự động gọi, thiết bị sẽ tự động liên hệ 911 hay số điện thoại dịch vụ khẩn cấp của địa phương khi SOS khẩn cấp được sử dụng.

Bước 1: Mở **Cài đặt**

Bước 2: Chọn **SOS khẩn cấp**

Bước 3: Cho phép **Gọi bằng nút sườn**

Bước 4: Có thể chọn **Tự động gọi**

Bên cạnh đó, bạn có thể cho phép SOS khẩn cấp hiển thị số điện thoại dịch vụ khẩn cấp bằng cách chọn Tạo liên hệ khẩn cấp trong Sức khoẻ.

Hình 168: Cấu hình tính năng sử dụng SOS khẩn cấp

4.2.5. Sử dụng tính năng cho phép Tìm

Tính năng này sẽ hữu ích khi thiết bị bị mất hoặc trộm cắp. Một chiếc Iphone bị khoá không thể sử dụng mà không có thông tin đăng nhập Apple ID – ngay cả khi điện thoại bị xoá và đã được cài đặt lại phần mềm.

Các bước thiết lập tính năng **Tìm**:

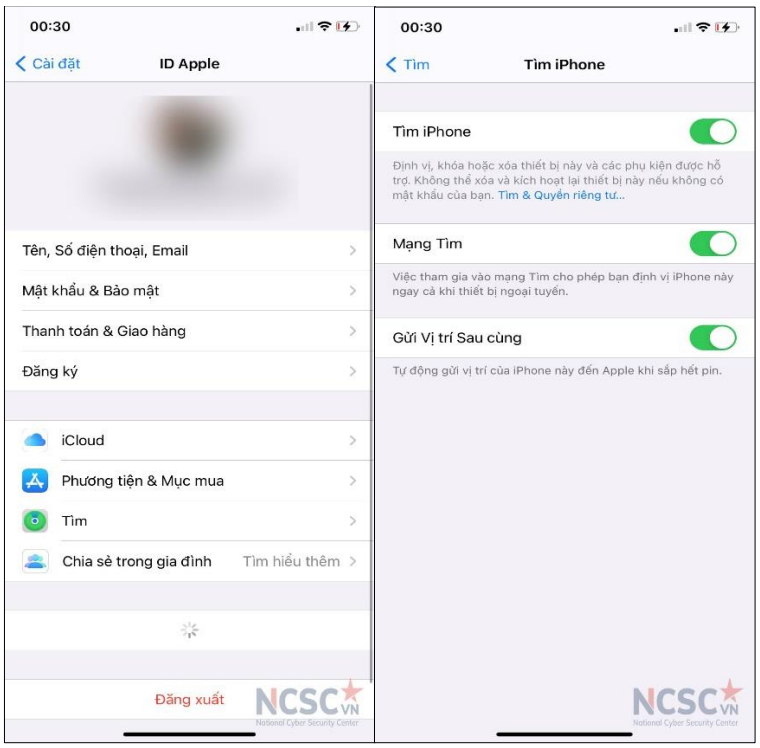
Bước 1: Mở ứng dụng **Cài đặt**

Bước 2: Chọn **Tên của bạn**

Bước 3: Chọn **Tìm**

Bước 4: Cho phép **Tìm iPhone** và **Gửi Vị trí Sau cùng**

Nếu bạn được yêu cầu đăng nhập, nhập thông tin đăng nhập Apple ID của bạn. Khi bạn thiết lập Tìm, các ứng dụng ghép kết nối như Apple Watch hay AirPods cũng được thiết lập tương tự.



Hình 169: Bật tính năng cho phép Tìm kiếm

4.2.6. Bật tính năng tự động cập nhật

Tự động cập nhật bảo đảm rằng thiết bị luôn sử dụng phiên bản iOS mới nhất và an toàn nhất. Sử dụng phiên bản iOS lỗi thời khiến thiết bị dễ bị tấn công hơn.

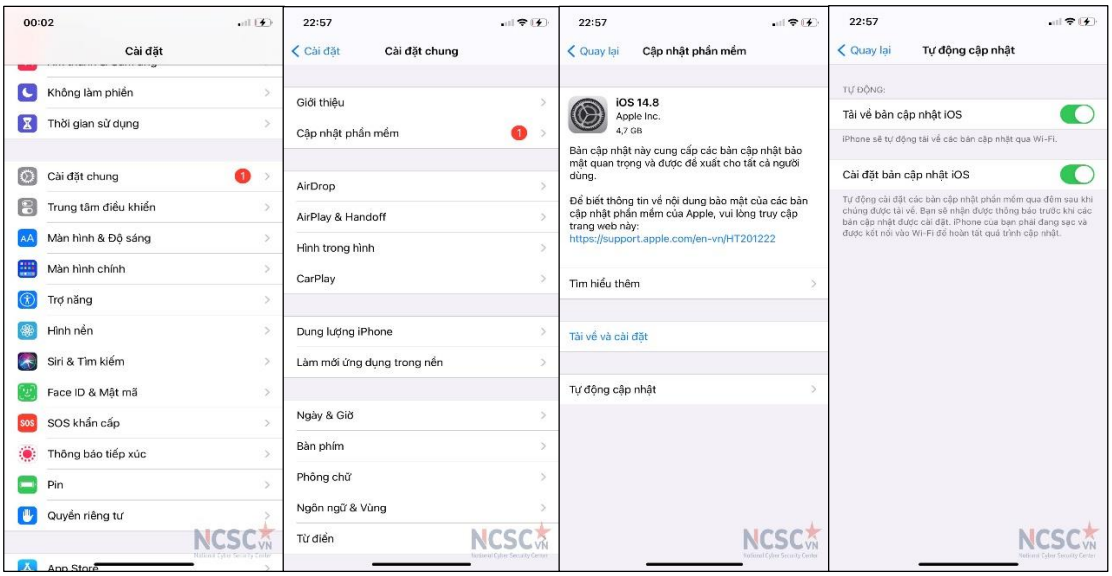
Bước 1: Mở ứng dụng **Cài đặt**

Bước 2: Vào **Cài đặt chung**

Bước 3: Chọn **Cập nhật phần mềm**

Bước 4: Chọn **Tự động cập nhật**

Bước 5: Cho phép Tải về bản cập nhật iOS và Cài đặt bản cập nhật iOS



Hình 170: Cài đặt tính năng tự động cập nhật iOS

4.2.7. Khởi động lại thiết bị định kỳ

Định kì khởi động lại thiết bị có thể bảo vệ bạn khỏi các khai thác từ xa bằng cách làm cho kẻ tấn công khó duy trì quyền kiểm soát thiết bị, khi bạn khởi động lại điện thoại kẻ tấn công sẽ phải tấn công bạn lại từ đầu. Ngoài ra việc định kỳ khởi động lại thiết bị cũng có thể giúp điện thoại chạy nhanh, ổn định hơn.

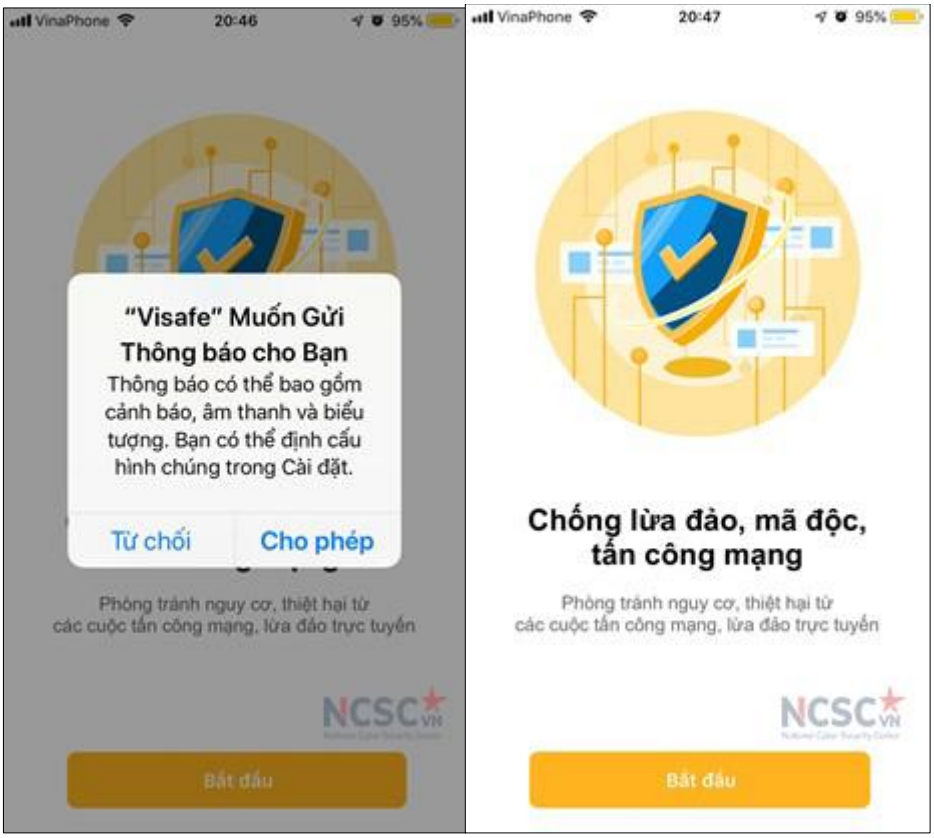
4.3. Sử dụng ứng dụng Internet an toàn trên điện thoại Iphone

Bước 1: Truy cập vào **App Store** trên thiết bị, và tìm kiếm **Visafe Internet an toàn.** Sau đó cài đặt ứng dụng **Visafe - Internet an toàn**

Hình 171: Cài đặt ứng dụng Visafe trên iOS

Bước 2: Truy cập ứng dụng **Visafe** để hoàn tất quá trình kích hoạt và sử dụng **Visafe** theo hướng dẫn dưới đây.

- Mở ứng dụng **Visafe** đã được cài đặt trên thiết bị. Lần lượt chọn “Cho phép” để nhận được thông báo từ Visafe, và “Bắt đầu” để truy cập vào màn hình chính.

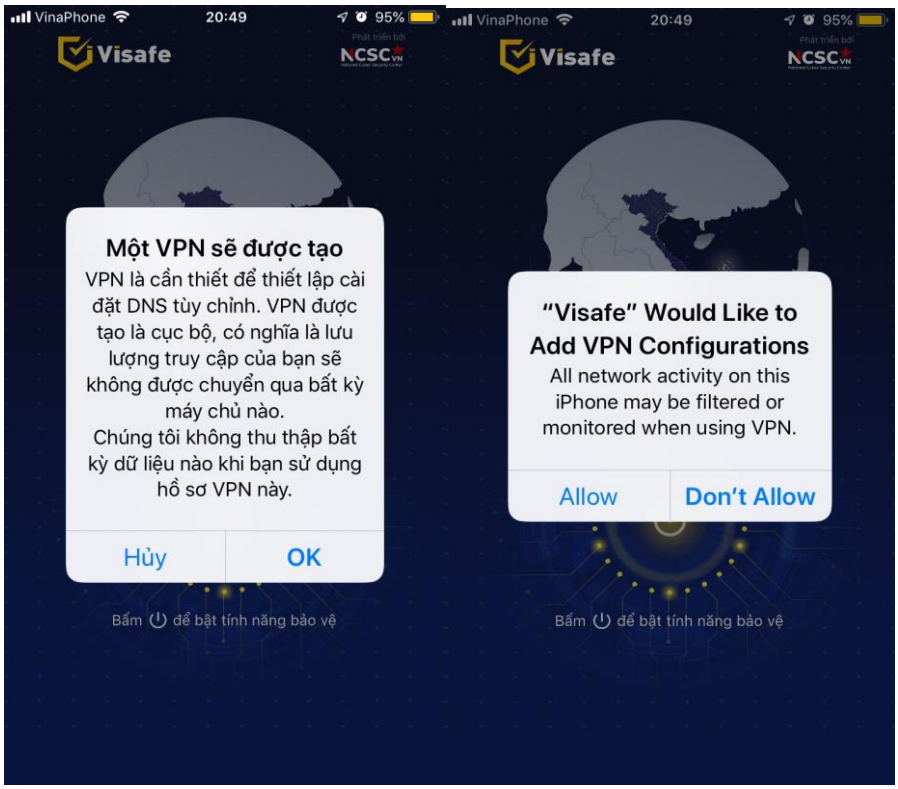


Hình 172: Sử dụng ứng dụng Visafe trên iOS (1)

- Giao diện chính của ứng dụng như hình dưới đây

Hình 173: Sử dụng ứng dụng Visafe trên iOS (2)

- “Bật tính năng bảo vệ” để kích hoạt **Visafe**. Ở lần đầu tiên **bật,** làm theo hướng dẫn trên ứng dụng để tạo **VPN Visafe** trên thiết bị. Lần lượt chọn “OK” -> “Allow”, để đồng ý tạo **VPN Visafe**.



Hình 174: Sử dụng ứng dụng Visafe trên iOS (3)

Màn hình thiết bị sẽ chuyển sang màn **VPN** của **Cài đặt.** Thêm **VPN** bằng cách sử dụng các phương thức xác thực theo hướng dẫn. Ví dụ như dưới đây là xác thực bằng vân tay.

Hình 175: Sử dụng ứng dụng Visafe trên iOS (4)

- Sau khi kích hoạt thành công màn hình thiết bị sẽ hiển thị như sau:

Hình 176: Sử dụng ứng dụng Visafe trên iOS (5)

CHƯƠNG 3: HƯỚNG DẪN SỬ DỤNG AN TOÀN CÁC PHẦN MỀM

1. Hướng dẫn cho giáo viên

1.1. Lưu ý chung để bảo đảm an toàn khi dạy học trực tuyến

Đối với giáo viên, sau khi đã biết cách bảo đảm an toàn cho thiết bị sử dụng để giảng dạy, giáo viên cần lưu ý thêm việc sử dụng những tính năng an toàn của phần mềm đang sử dụng để giảng dạy trực tuyến.

- Chỉ tải và cài đặt phần mềm từ địa chỉ tin cậy (thông qua kho ứng dụng hoặc trang chủ của nhà phát triển)
- Luôn đặt mật khẩu cho lớp học nếu phần mềm có tính năng đặt mật khẩu.
- Gửi thông tin để truy cập lớp học trực tuyến (như đường dẫn để truy cập lớp học, ID, mật khẩu để vào lớp học s…) cho các em học sinh/cha mẹ họ*c* sinh qua các kênh riêng như nhóm trao đổi giữa giáo viên và học sinh, cha mẹ học sinh.
- Sử dụng tính năng phòng chờ và xác thực, phê duyệt học viên khi vào lớp học nếu phần mềm có hỗ trợ các tính năng đó.
- Khóa phòng học khi đã đầy đủ học sinh.
- Thiết lập mặc định để tắt Mic và chia sẻ màn hình của các thành viên. Khi nào học sinh cần sử dụng đến mới mở.
- Dành thời gian để kiểm tra và cập nhật phần mềm dạy học trực tuyến khi có phiên bản mới. Đối với trường hợp sử dụng trình duyệt web trên máy tính hoặc điện thoại để tham gia lớp học, cần lưu ý cập nhật phiên bản trình duyệt web. Đối với phần mềm cài trên điện thoại di động việc cập nhật phiên bản phần mềm có thể thực hiện thông qua App Store (Iphone), CH Play (Android). Khi có phiên bản phần mềm mới, người dùng sẽ được thông báo để cập nhật. Đối với máy tính, thông thường các phần mềm cũng sẽ báo khi có phiên bản mới, có thể cập nhật ngay hoặc để sau. Tham khảo cập nhật phần mềm trong mục "Kiểm tra và cập nhật phần mềm" tại mục 2 của chương này.

Ngoài ra có thể kết hợp sử dụng 6 nền tảng dạy và học trực tuyến Việt Nam gồm: VNEdu, ViettelStudy, MobiEdu, Onluyen, Hocmai, Misa EMIS.

1.2. Dạy học an toàn trên phần mềm Zoom

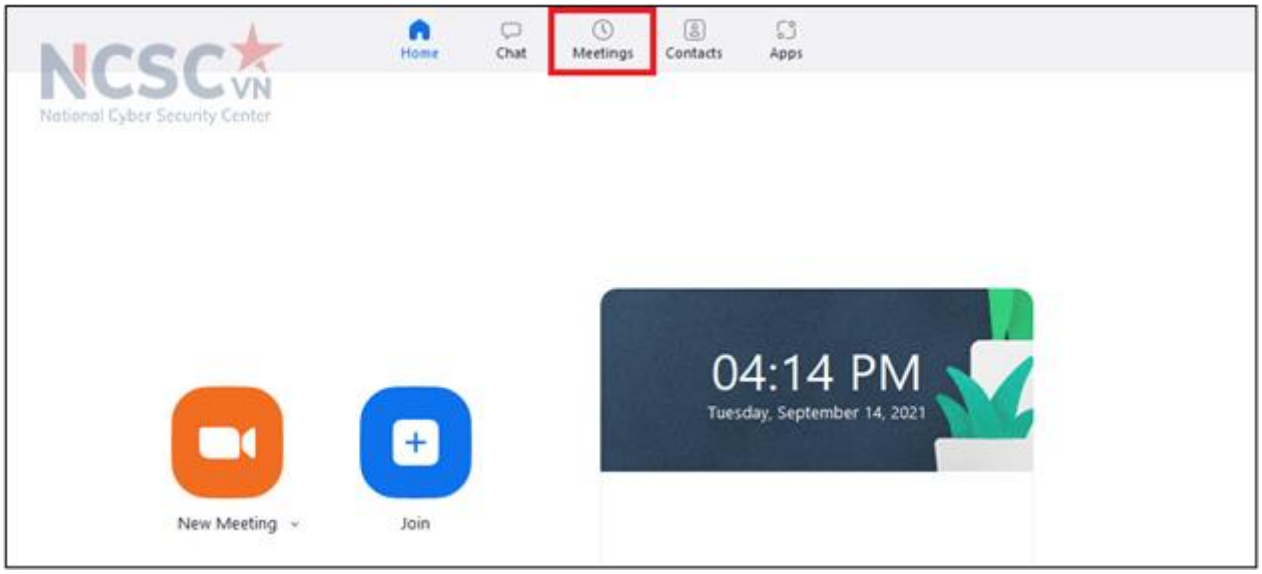
1.2.1. Đặt mật khẩu cho lớp học

Tính năng mật khẩu cho lớp học giúp bảo đảm an toàn 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 lớp học và buổi học trực tuyến.

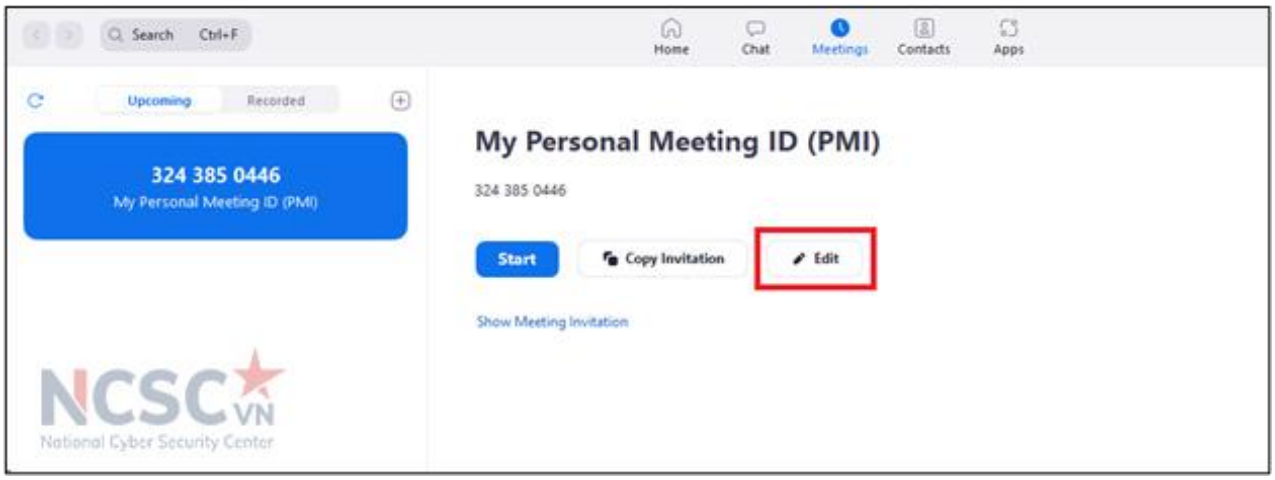
Các bước thực hiện:

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



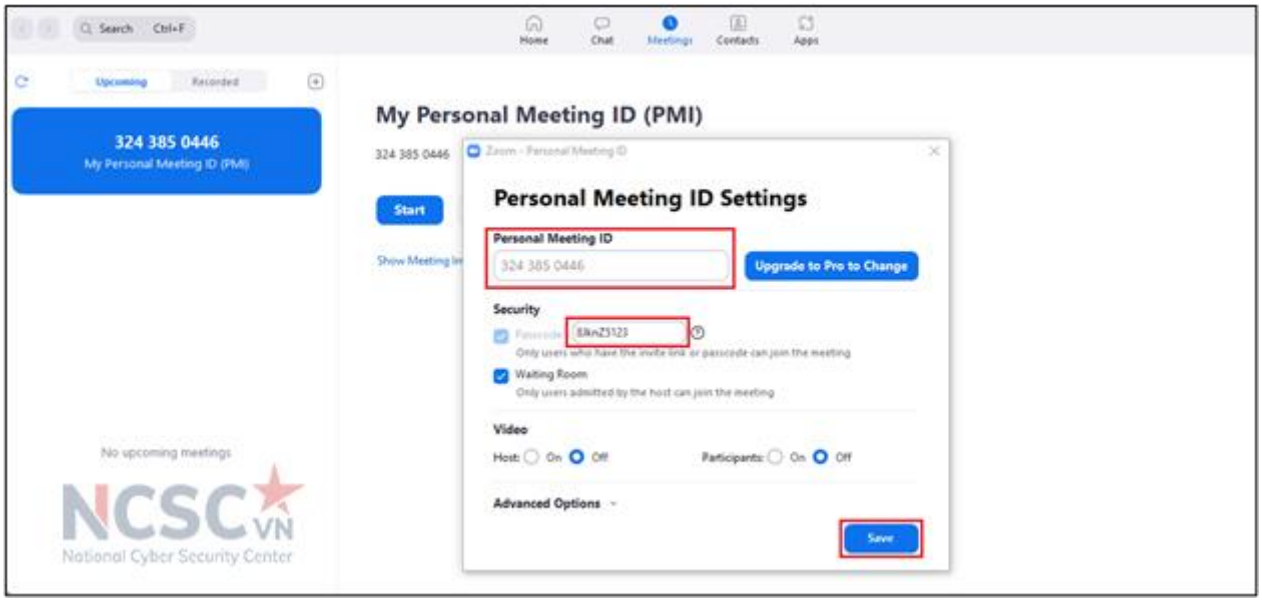
Hình 177: Đặt mật khẩu cho lớp học (1)

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



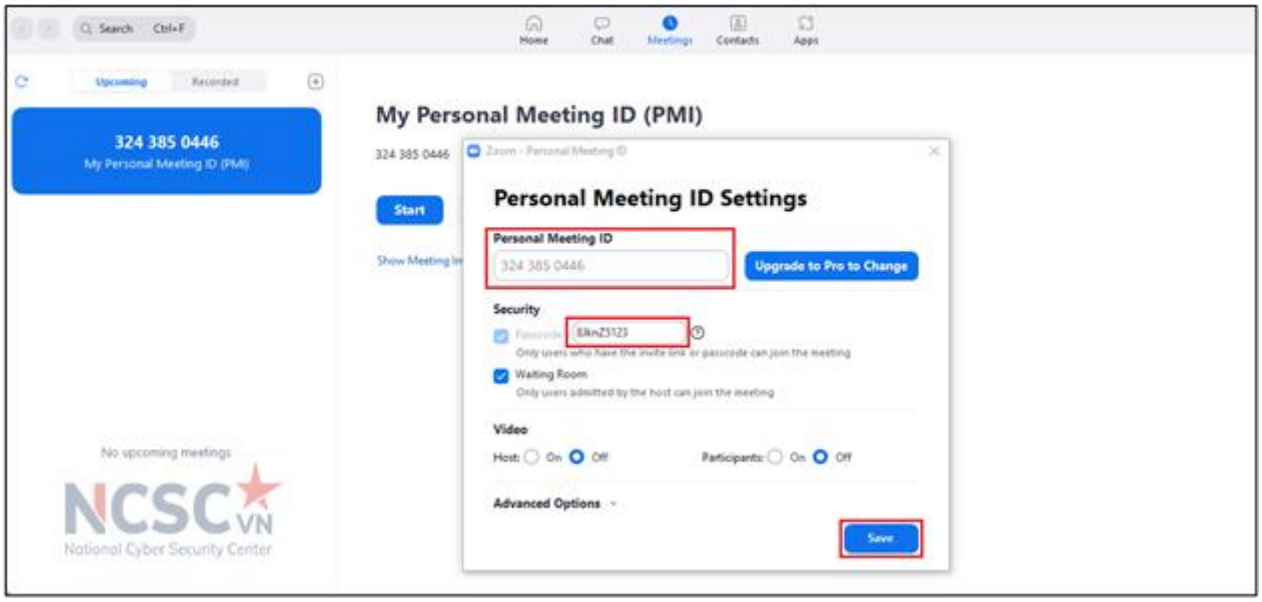
Hình 178: Đặt mật khẩu cho lớp học (2)

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.



Hình 179: Đặt mật khẩu cho lớp học (3)

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



Hình 180: Đặt mật khẩu cho lớp học (4)

1.2.2. Xác thực học sinh tham gia vào lớp học

Bước 1: Đăng nhập Zoom.

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

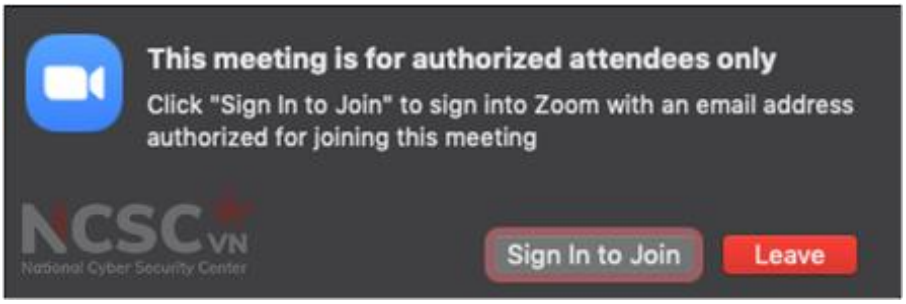
Bước 3: Trong phần Security, xác minh "Only authenticated users can join meetings"

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

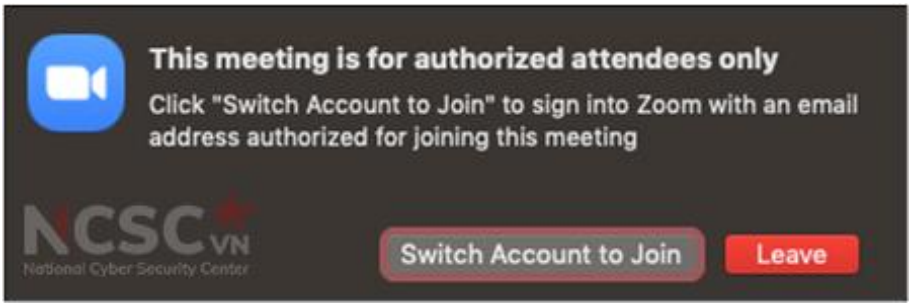
cấp tài khoản. Bạn cần liên hệ với quản trị viên Zoom.

Nếu chưa đăng nhập vào Zoom, sẽ hiển thị:



Hình 181: Xác thực học sinh tham gia vào lớp học (1)

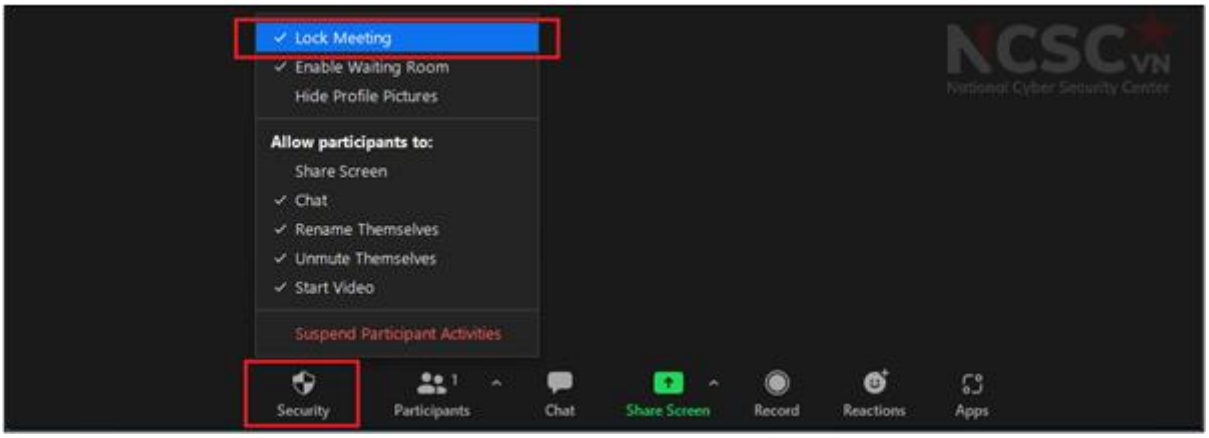
Nếu đăng nhập email không hợp lệ:



Hình 182: Xác thực học sinh tham gia vào lớp học (2)

1.2.3. Khóa lớp học

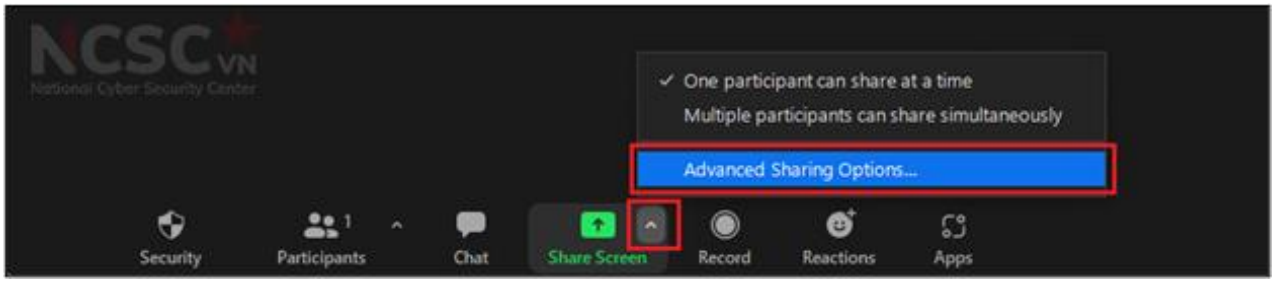
Khi lớp học đã bắt đầu, hãy chuyển đến tab "Security" và chọn "Lock Meeting" lớp học sau khi tất cả mọi người tham gia đã vào. Điều này sẽ ngăn những người khác tham gia kể cả khi thông tin ID lớp học hoặc thông tin truy cập bị rò rỉ.



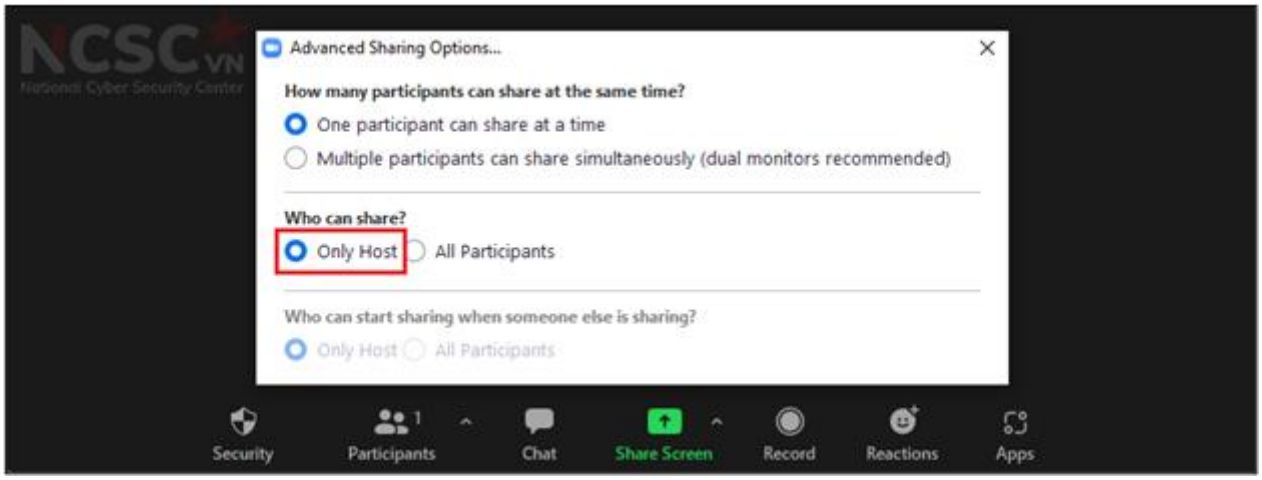
Hình 183: Khóa lớp học

1.2.4. Tắt chia sẻ màn hình của học sinh

Để ngăn học sinh chia sẻ màn hình trong quá trình giảng dạy, nhấp vào mũi tên bên cạnh "Share Screen" > "Advanced Sharing Options" > "Who can share?" chọn "Only Host" và đóng cửa sổ.



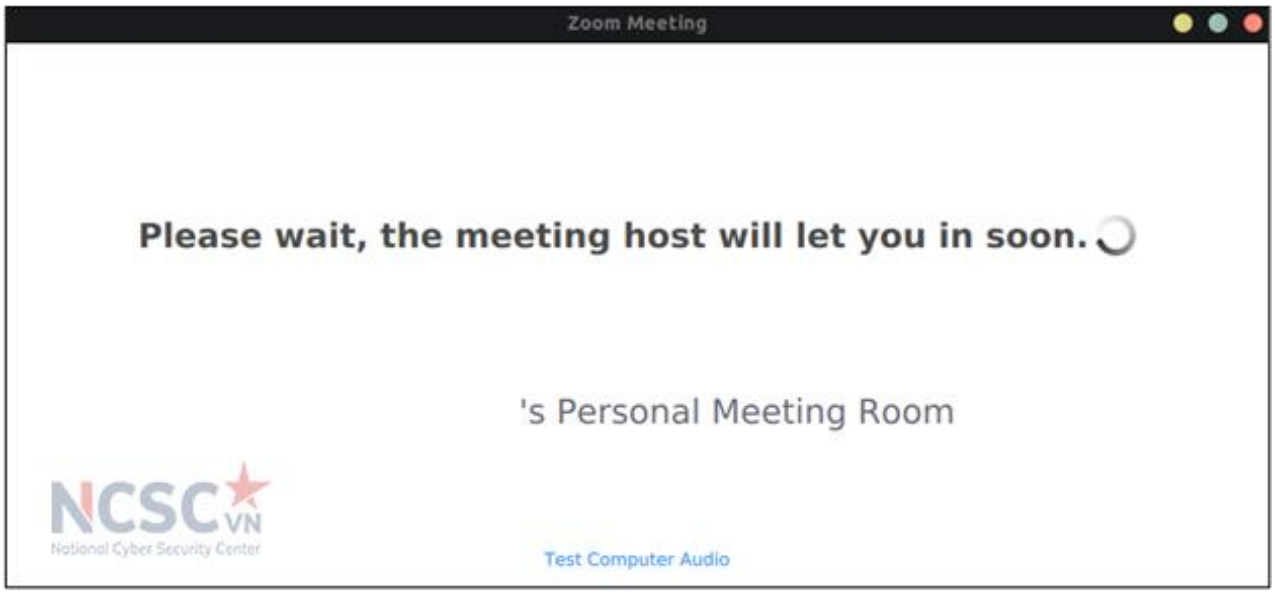
Hình 184: Tắt chia sẻ màn hình của học sinh (1)



Hình 185: Tắt chia sẻ màn hình của học sinh (2)

1.2.5. Sử dụng phòng chờ

Tính năng Phòng chờ (Waiting Room) là một cách để lọc những thành viên không phải của lớp. Điều này cũng cho phép giáo viên kiểm soát tốt hơn các vấn đề trong phiên họp.



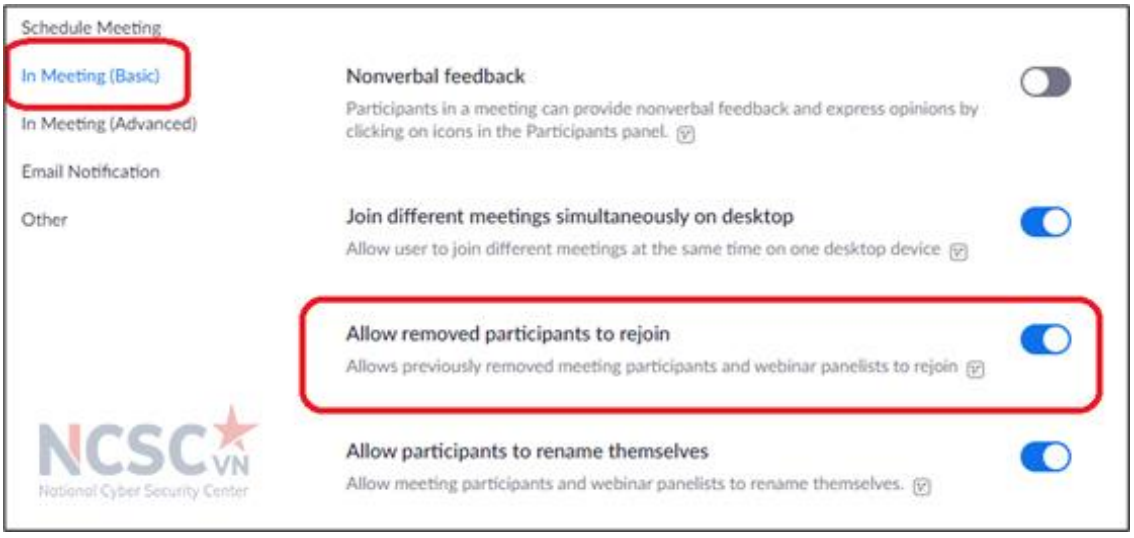
Hình 186: Sử dụng phòng chờ

1.2.6. Loại bỏ người không phải học sinh của lớp

Nếu nhận thấy ai đó đang làm gián đoạn lớp học, giáo viên có thể loại ra khỏi lớp Participants > chọn người muốn loại khỏi lớp > "More" > Remove.

Hình 187: Loại bỏ người không phải học sinh của lớp

Giáo viên có thể không cho phép người này tham gia lớp học lại:
Settings: Meetings – Basic > Allow Removed Participants to Rejoin

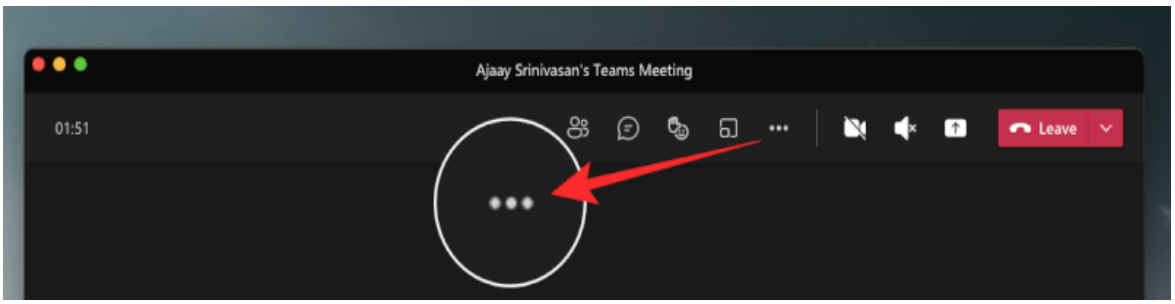


Hình 188: Loại bỏ người không phải học sinh của lớp

1.3. Dạy học an toàn trên phần mềm Microsoft Teams

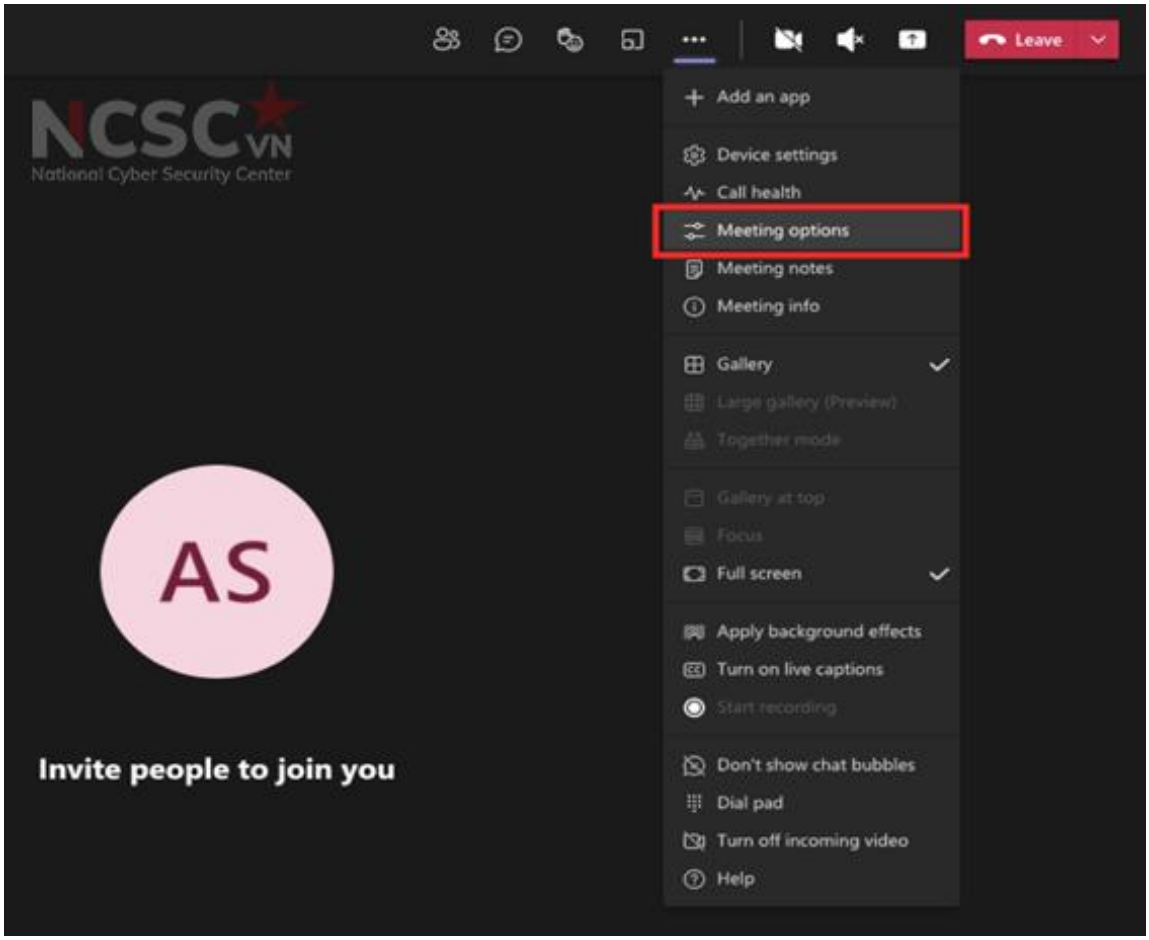
1.3.1. Sử dụng phòng chờ

Để thiết lập phòng chờ trên Microsoft Teams thực hiện các bước sau:
Bước 1: Sau khi tham gia vào lớp học, vào biểu tượng "..."



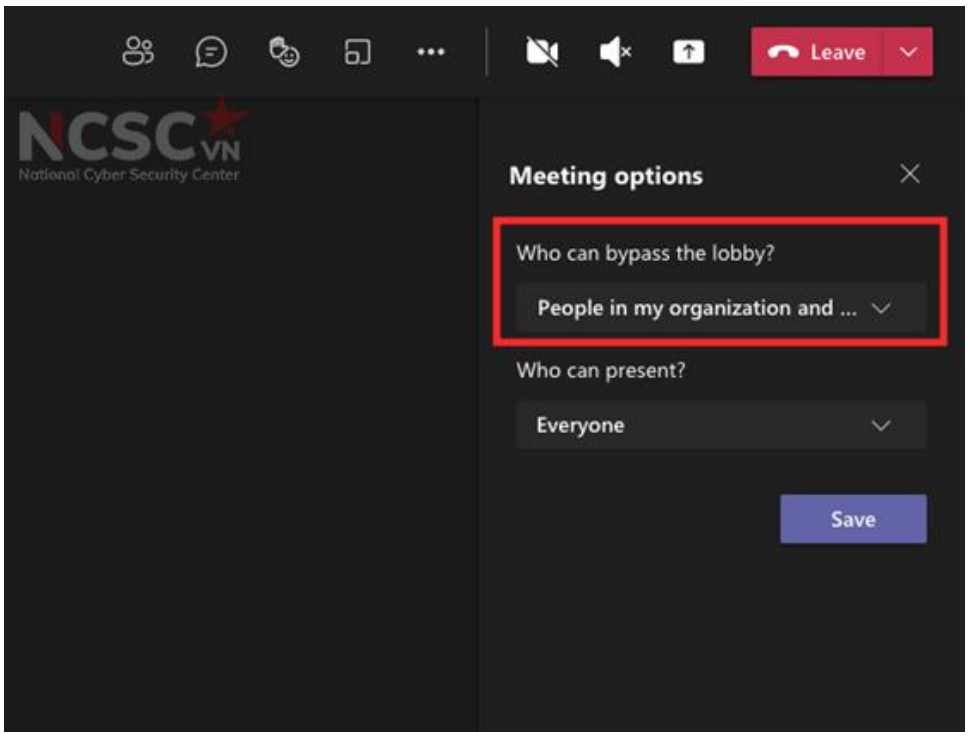
Hình 189: Cấu hình phòng chờ (1)

Bước 2: Chọn Meeting options



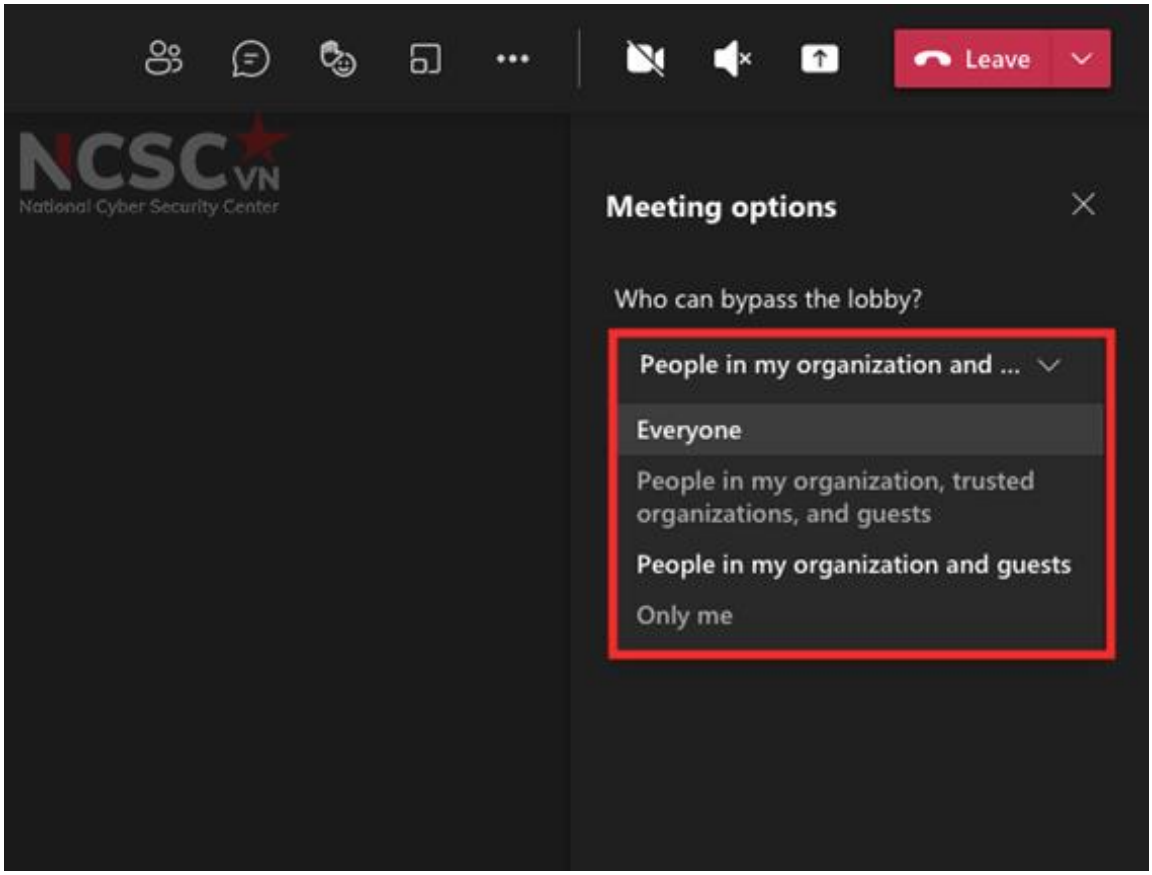
Hình 190: Cấu hình phòng chờ (2)

Bước 3: Vào “Who can bypass the lobby” để xem thêm các tùy chọn



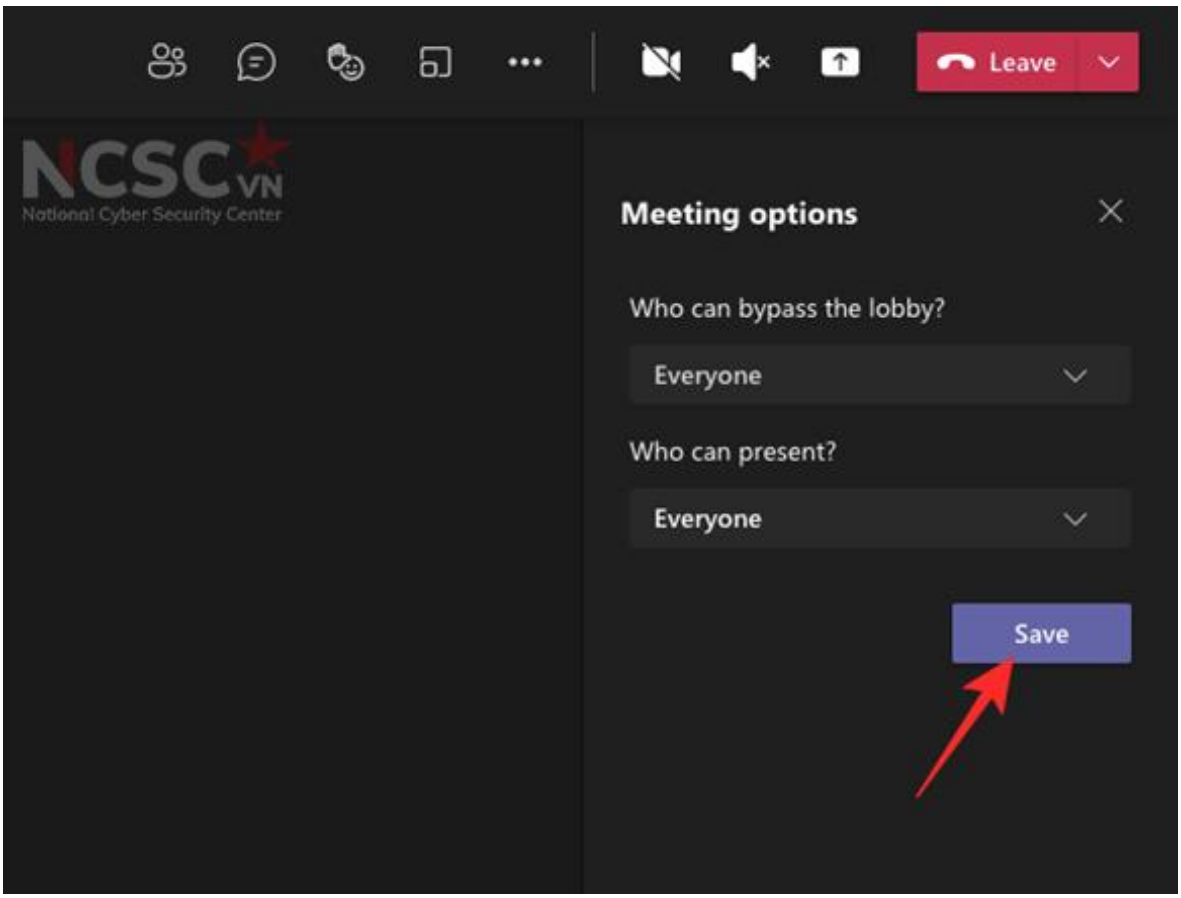
Hình 191: Cấu hình phòng chờ (3)

Bước 4: Lựa chọn cài đặt mặc định cho phòng chờ. Các tùy chọn này sẽ bị giới hạn dựa trên loại tài khoản của giáo viên.



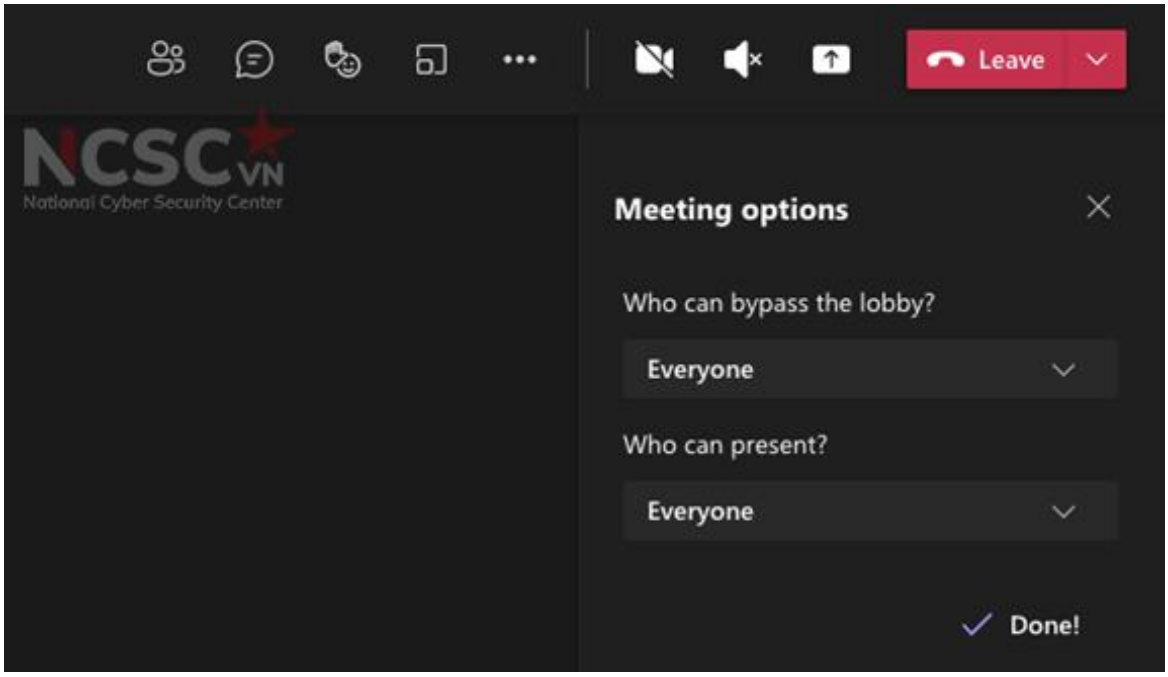
Hình 192: Cấu hình phòng chờ (4)

Bước 5. Nhấp vào nút ‘Save’ (Lưu) bên dưới để xác nhận các thay đổi.



Hình 193: Cấu hình phòng chờ (5)

Bước 6: Khi các thay đổi được lưu, người dùng sẽ thấy thông báo ‘Done’ (Hoàn tất) bên trong thanh Meeting options.

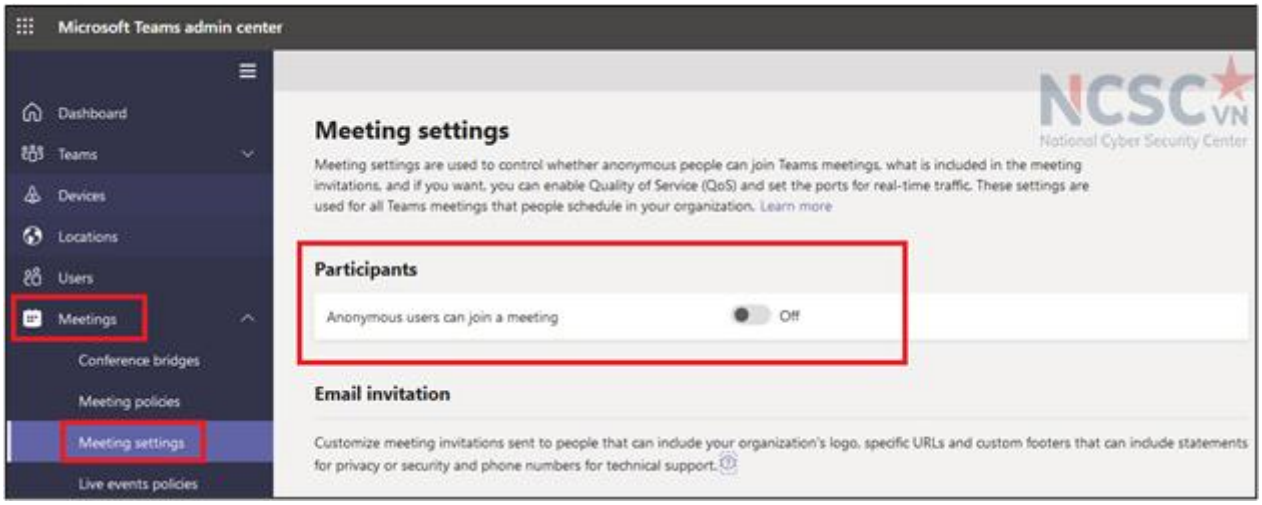


Hình 194: Cấu hình phòng chờ (6)

1.3.2. Hạn chế người dùng ẩn danh tham gia lớp học

Giáo viên có thể hạn chế người dùng ẩn danh tham gia lớp học như sau:

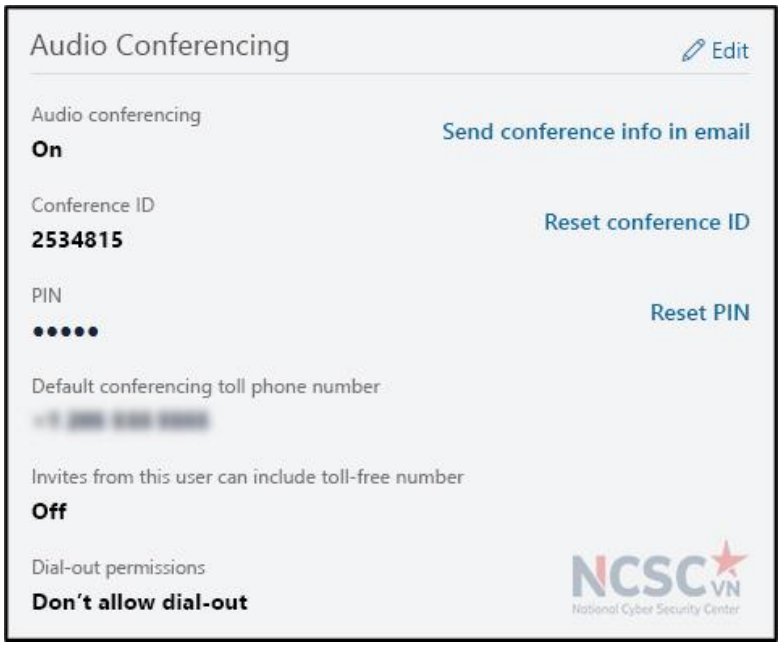
Tắt chức năng "Anonymous users can join a meeting"



Hình 195: Hạn chế người dùng ẩn danh tham gia lớp học

1.3.3. Sử dụng các ID và link khác nhau cho các lớp

Để bảo vệ lớp học trên Teams, giáo viên nên đảm bảo mỗi lớp học sẽ được tạo một với ID với mật khẩu (PIN) riêng.



Hình 196: Sử dụng các ID và link khác nhau cho các lớp

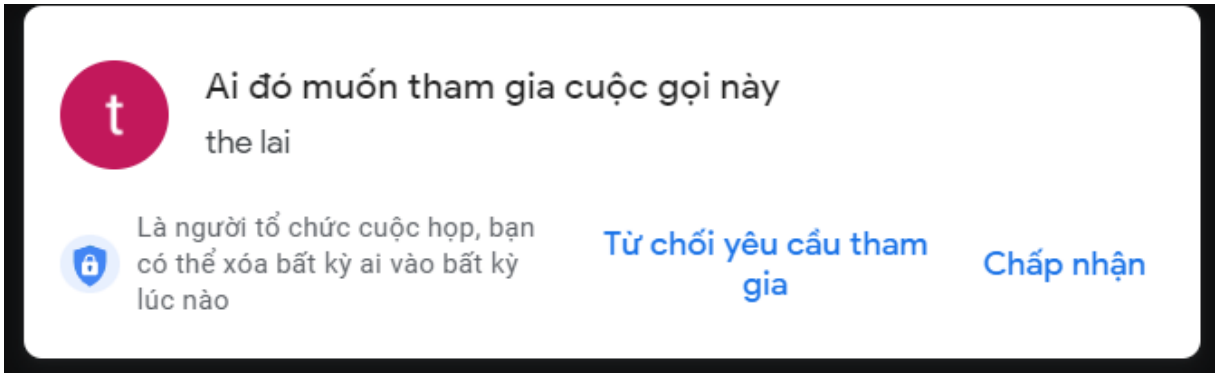
1.4. Dạy học an toàn trên phần mềm Google Meet

1.4.1. Sử dụng phòng chờ

Khi sử dụng Google Meet, giáo viên (người tạo lớp học) luôn luôn phải xác thực người truy cập vào.

Khi đã xác thực được giáo viên có thể Chấp nhận hoặc từ chối học sinh tham gia

Bước 1: Nhấp vào **Chấp nhận** hoặc **Từ chối yêu cầu tham gia** khi nội dung yêu cầu tham gia cuộc gọi video xuất hiện trong cửa sổ.



Hình 197: Sử dụng phòng chờ (1)

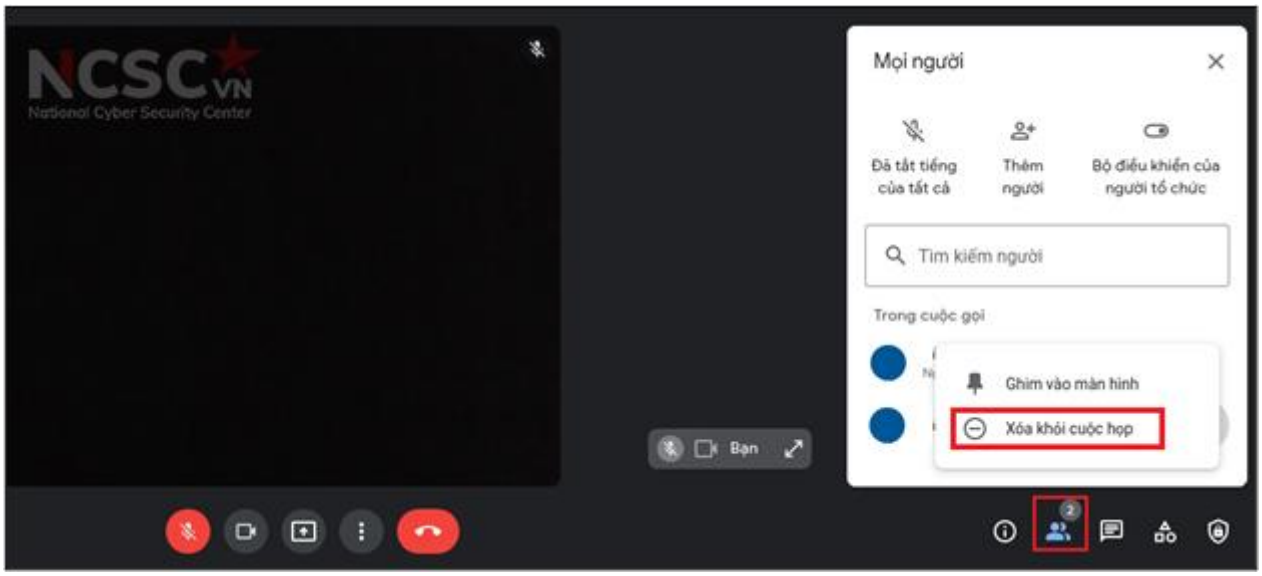
Bước 2: Nhấp vào **Xem tất cả** khi có nhiều người đang chờ tham gia. Giáo viên có thể chấp nhận từng người hoặc chấp nhận tất cả những thành viên đang chờ.

Chấp nhận/từ chối từng người: Bên cạnh tên, hãy nhấp vào **Chấp nhận** hoặc **Từ chối** để cho phép hoặc từ chối lần lượt từng người tham gia.

Chấp nhận/từ chối tất cả: Nhấp vào **Chấp nhận tất cả** hoặc **Từ chối tất cả** để cho phép hoặc từ chối tất cả người tham gia cùng lúc

1.4.2. Loại bỏ người không phải học sinh của lớp

Để loại bỏ một người khỏi lớp học: Chọn biểu tượng Thao tác khác, dấu ba chấm ngay tên người muốn xóa)



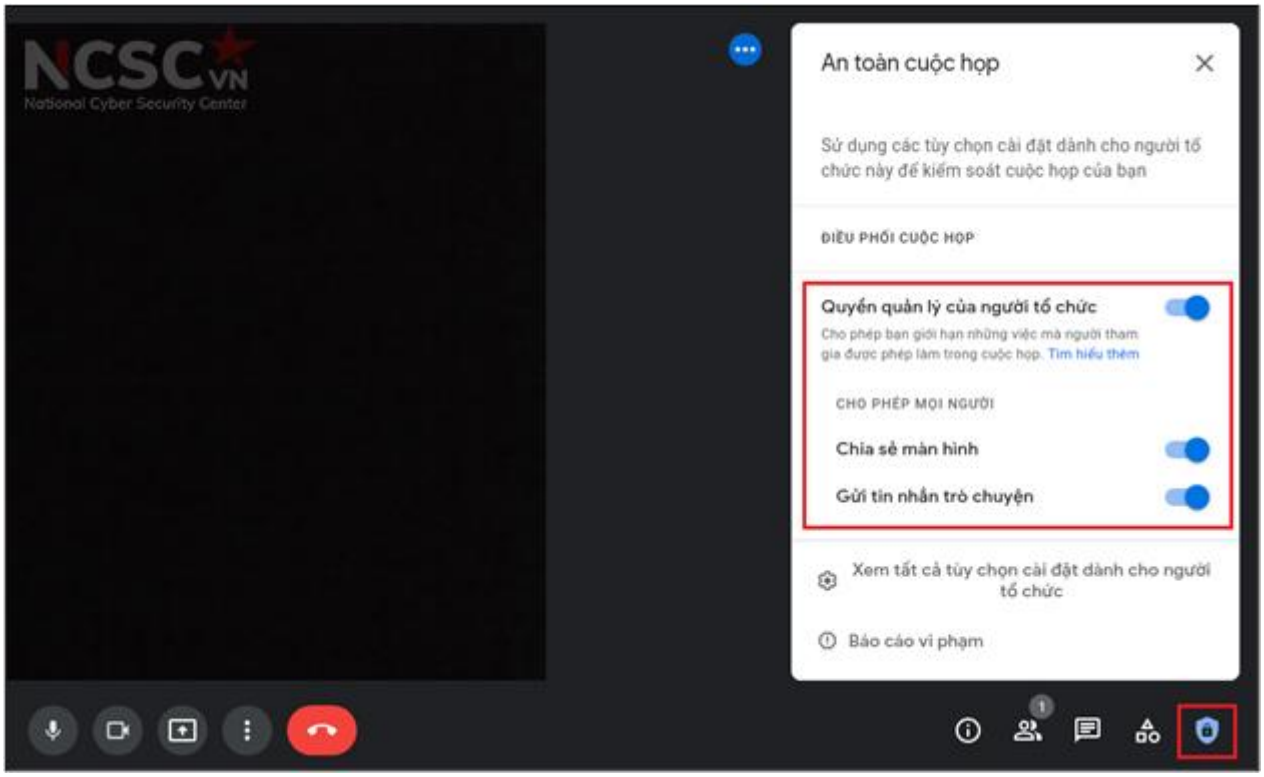
Hình 198: Loại bỏ người không phải học sinh của lớp

1.4.5. Thiết lập bảo mật cho lớp học

Khi giáo viên tổ chức/khởi tạo buổi học, giáo viên có thể điều khiển các tính năng bảo mật để đảm bảo buổi học được an toàn và tránh bị làm phiền, thực hiện bằng cách:

Bước 1: Chọn nút **Bộ điều khiển của người tổ chức** sau đó tùy tình huống có thể:

tắt **Chia sẻ màn hình** (không cho người tham gia chia sẻ màn hình trừ **Người tổ chức**) và tắt **Gửi tin nhắn trò truyện**.

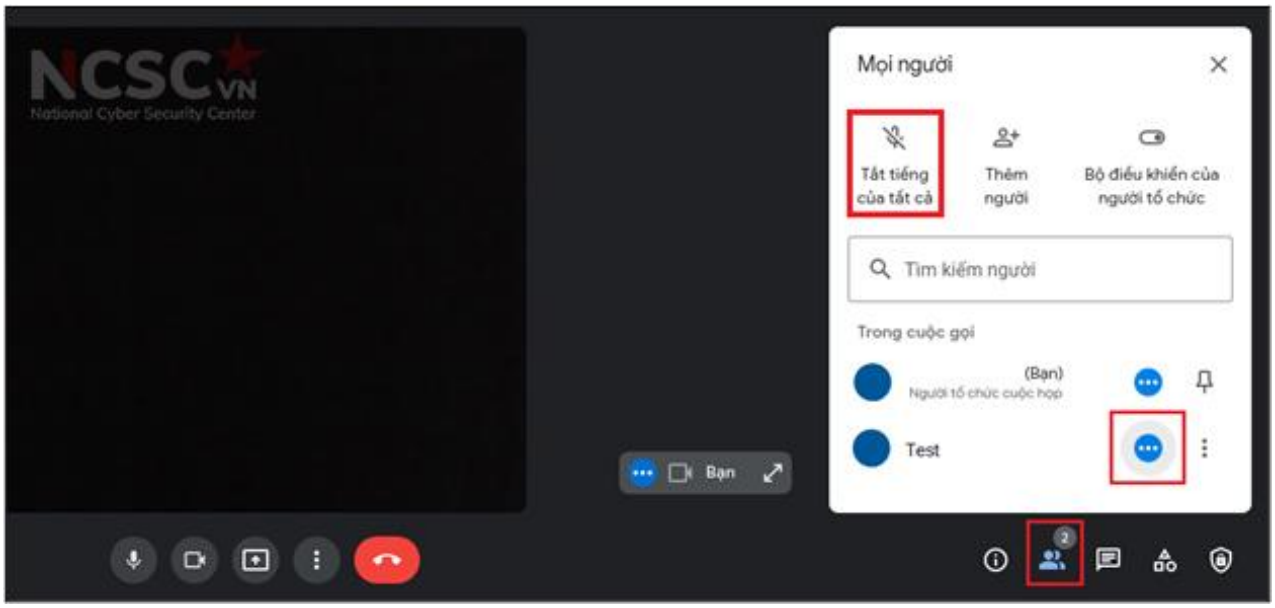


Hình 199: Thiết lập bảo mật khác cho lớp học

1.4.3. Tắt tiếng của tất cả học sinh

Giáo viên có thể tắt tiếng của tất cả học sinh tham gia vào lớp học để bắt đầu giảng bài.

Chọn nút **Hiển thị tất cả mọi người** sau đó tùy tình huống có thể: **Tắt tiếng của tất cả** hoặc **Tắt tiếng của một người cụ thể nào đó**



Hình 200: Tắt tiếng của tất cả học sinh trong lớp

1.5. Dạy học an toàn trên phần mềm Trans

1.5.1. Cài đặt cho lớp học

Đối với phần mềm Trans, giáo viên có thể cài đặt cấu hình phòng học để duyệt thành viên tham gia phòng học

Giáo viên chọn Tiện ích -> Cài đặt phòng -> Chọn yêu cầu xác thực với người dùng

Hình 201: Dạy học an toàn trên phần mềm Trans (1)

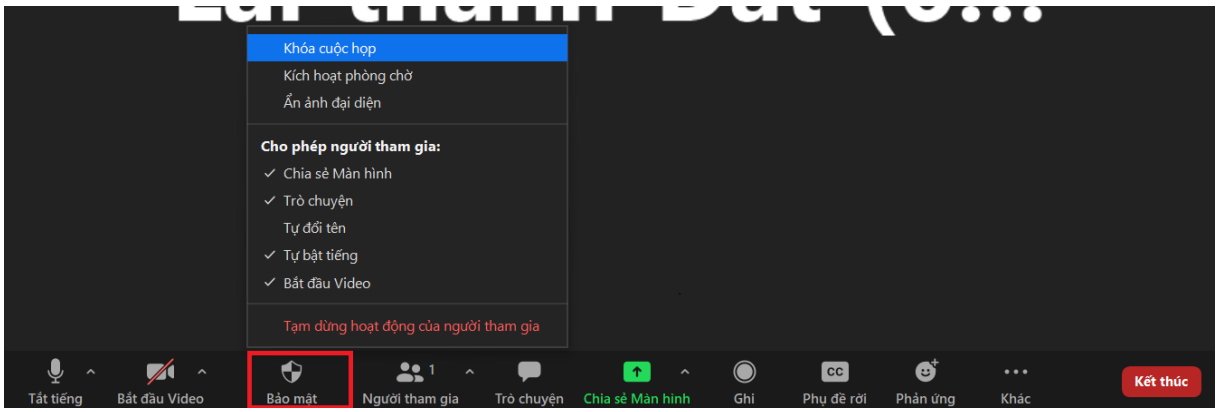
+ Vào tự do: Người dùng chỉ cần nhập ID của phòng là có thể tham dự

+ Phải đăng nhập: Người dùng phải có tài khoản TranS mới có thể tham dự

+ Phải đăng ký trước: Người dùng phải có tài khoản TranS và phải được phê duyệt mới có thể tham dự

1.5.1. Khóa lớp học

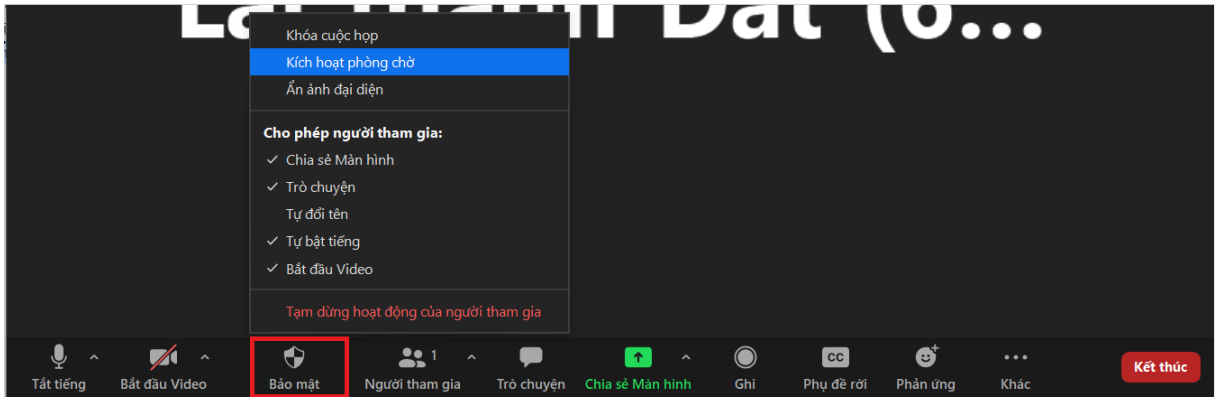
Giáo viên chọn nút **Bảo mật** -> Chọn **Khóa cuộc họp**, kể từ lúc này không ai có thể tham gia vào được lớp.



Hình 202: Dạy học an toàn trên phần mềm Trans (2)

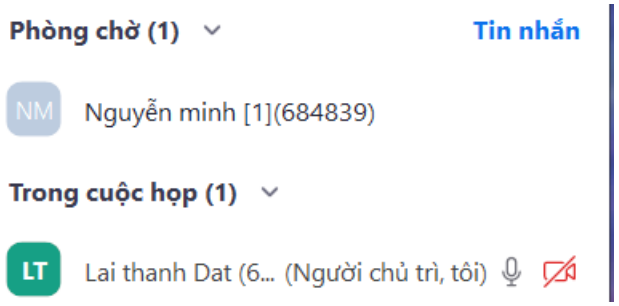
1.5.2. Sử dụng phòng chờ

Bấm vào nút **Bảo mật (**hình khiên như trong hình) -> **Kích hoạt phòng chờ**



Hình 203: Dạy học an toàn trên phần mềm Trans (3)

Những ai vào sau thời điểm bật thì sẽ không được vào thẳng phòng mà sẽ được TranS đưa vào phòng chờ và chờ giáo viên phê duyệt mới vào được phòng. Sau khi bật chế độ này thì khi có người vào giáo viên sẽ thấy cửa sổ thông báo như sau:



Hình 204: Dạy học an toàn trên phần mềm Trans (4)

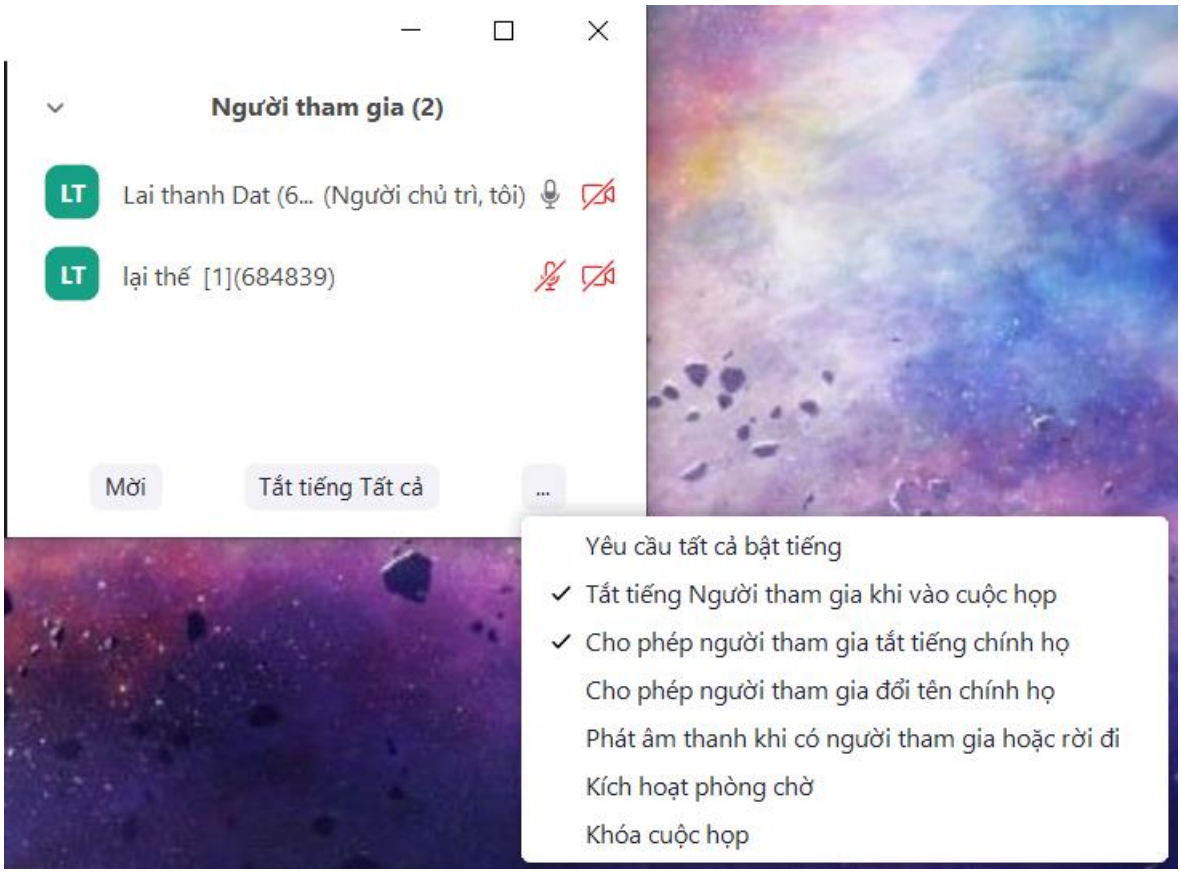
Giáo viên có thể bấm nút "**Admit**" để người đó vào được phòng hoặc bấm nút "**Remove**" xoá người dùng khỏi phòng họp.

1.5.3. Quản lý học sinh tham gia vào lớp học

Việc này hỗ trợ giáo viên xem danh sách sinh viên/học sinh đang tham gia trong

lớp học, ngắt/mở webcam của người tham gia học, đẩy người tham gia ra khỏi lớp,…

Nhấn vào mục **Quản lý người tham gia (Manager Participants)** và thao tác các bước như hình dưới đây.

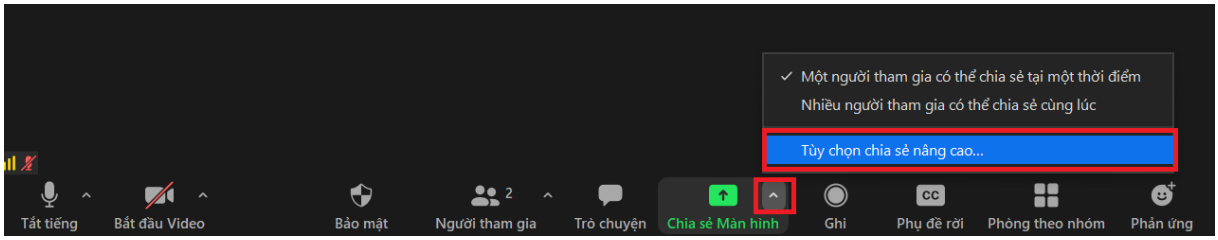


Hình 205: Quản lý học sinh tham gia lớp học

1.5.4. Tắt chia sẻ màn hình của học sinh

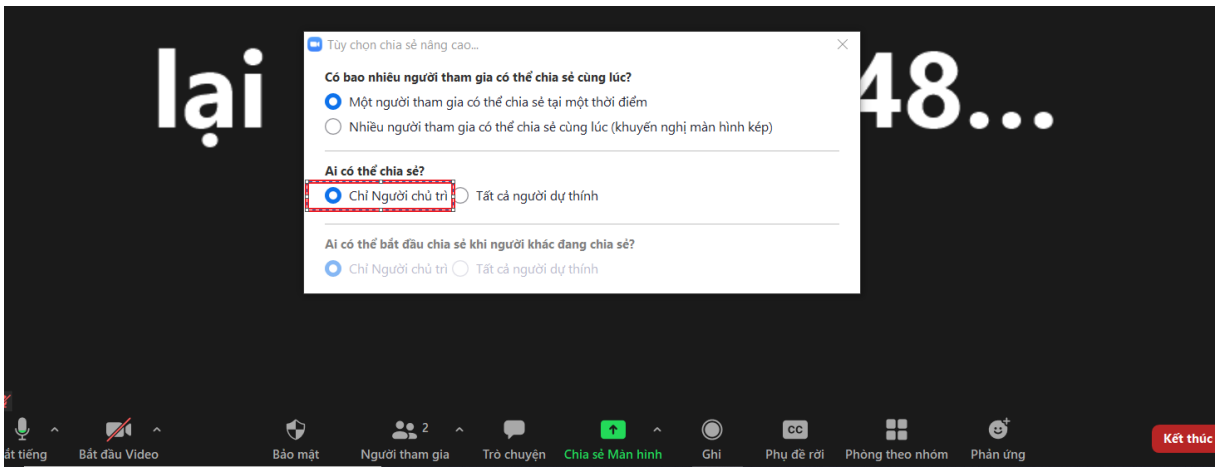
Để tắt chức năng chia sẻ màn hình của học sinh, chỉ có giáo viên mới được phép chia sẻ màn hình và trình chiếu slide thực hiện các bước sau:

Bước 1: Vào phần mở rộng tại mục **Chia sẻ màn hình** (nút mũi tên bên cạnh biểu tượng Share), chọn "**Tùy chọn chia sẻ nâng cao…**"



Hình 206: Tắt màn hình chia sẻ của học sinh

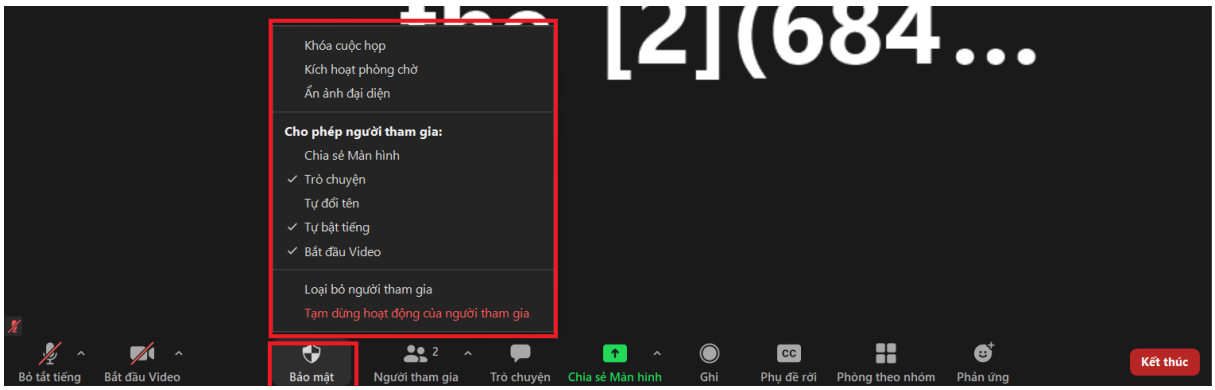
Bước 2: Tại cửa sổ hiển thị, tích chọn **Only Host**



Hình 207: Tắt màn hình chia sẻ của học sinh

1.5.5. Một số chức năng bảo mật khác khi tổ chức lớp học

Khi vào phòng với vai trò giáo viên hoặc chủ tọa sẽ có thêm nút Security như hình dưới đây:



Hình 208: Chức năng bảo mặt khác của Trans

Khi bấm vào nút này sẽ có các menu lệnh gồm:

+ Rename Themselves: Nếu tích chọn nghĩa là cho phép người dùng tự đổi tên (khuyến nghị không tích để người dùng không tự sửa được tên)

+ Chat: Cho phép sử dụng tính năng chat hoặc không cho chat (tích là cho phép)

+ Share Screen: Cho phép người dự chia sẻ màn hình (tích là cho phép)

+ Lock Meeting: Khóa phòng -> Nếu chọn tích thì từ thời điểm này thì không ai có thể vào phòng. Giáo viên lưu ý nên chọn sau khi đã bắt đầu giờ học 15 phút và sau đó chọn tiếp "Enable waiting room"

+ Enable waiting room: Bật chế độ những ai vào sau thời điểm bật thì sẽ không được vào thẳng phòng mà sẽ được TranS đưa vào phòng đợi (Waiting room) và chờ GV hoặc chủ tọa phê duyệt với vào được phòng. Sau khi bật chế độ này thì khi có người vào GV/Chủ tọa sẽ thấy cửa sổ thông báo hiển thị.

Giáo viên/chủ tọa có thể bấm nút "Admin" để người đó vào được phòng hoặc bấm nút "See waiting room" để mở cửa sổ danh sách các tài khoản đang đợi như sau:

Bấm Admin để cho vào phòng hoặc Remove để đẩy ra ngoài. (Trong khi đợi người

chờ sẽ nhận được thông báo vui lòng đợi để được phê duyệt vào phòng).

1.5.6. Kết thúc lớp học

Giáo viên/quản lý lớp học cần chú ý đóng lớp học khi ca học kết thúc để tránh bị chiếm dụng trên hệ thống Trans làm người khác không truy cập được.

Để kết thúc lớp học: Nhấn vào biểu tượng End meeting ở góc dưới bên phải của giao diện phần mềm > Cửa số thông báo hiển thị, nhấn chọn vào End meeting for all.

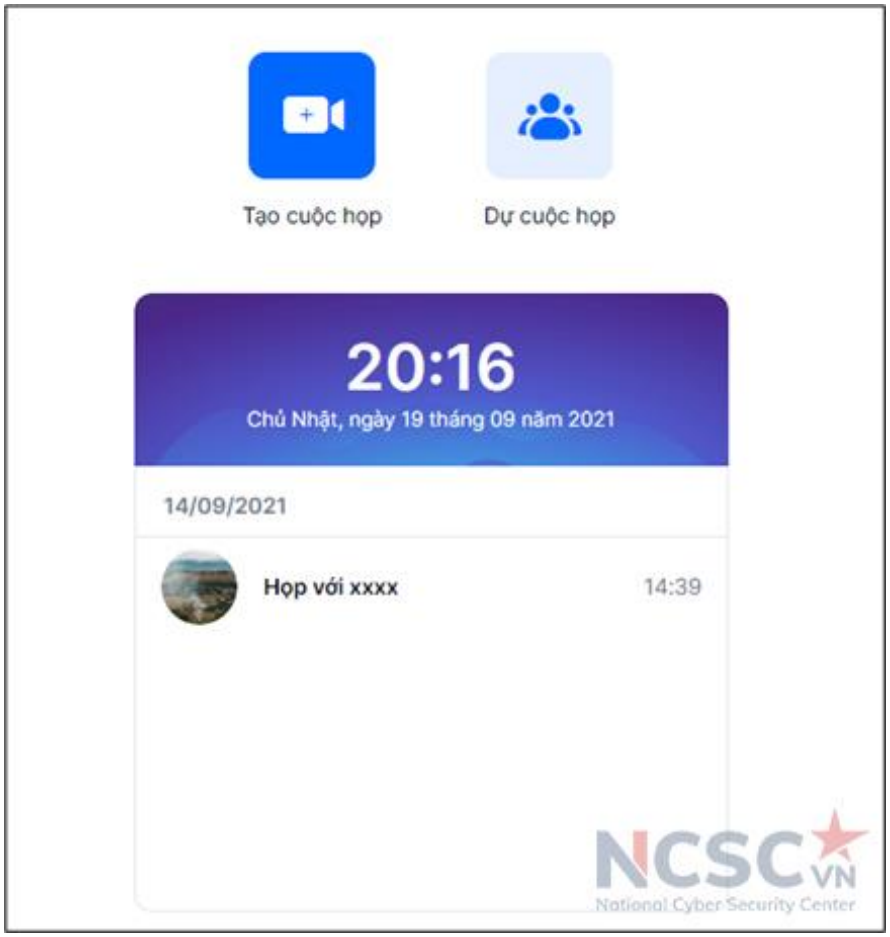
1.6. Dạy học an toàn trên phần mềm Zavi

1.6.1. Đặt mật khẩu cho lớp học

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

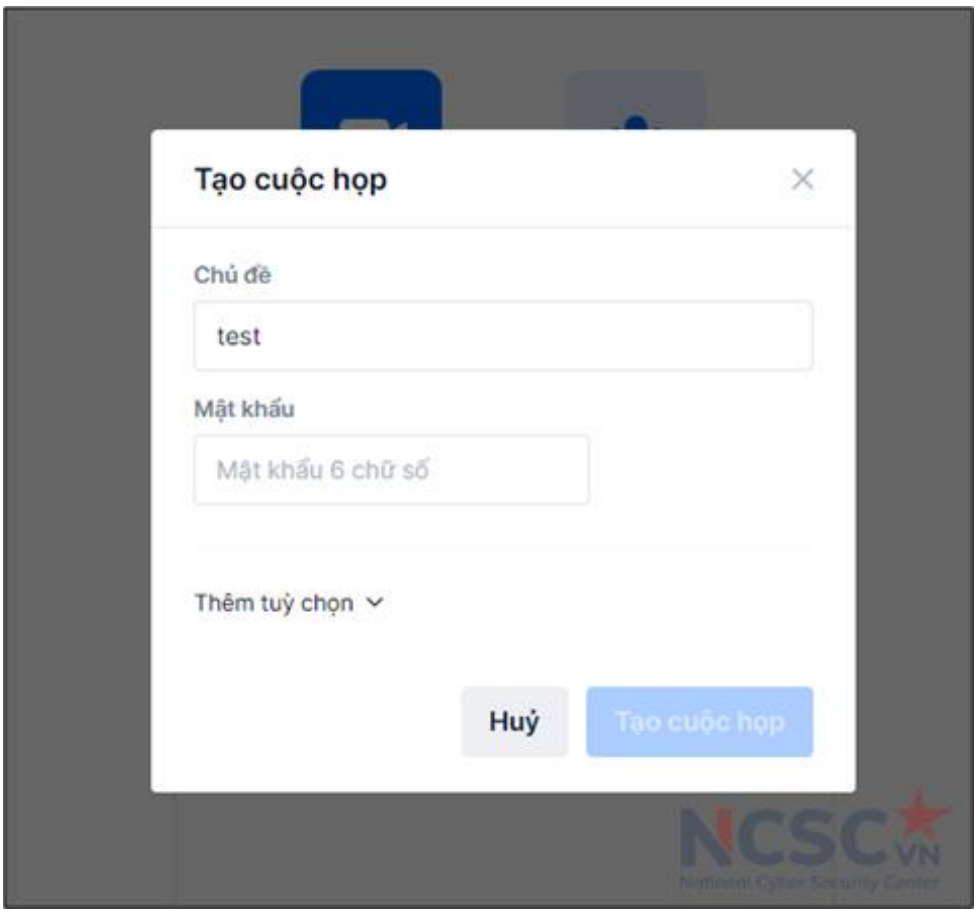
Các bước thực hiện như sau:

Bước 1: Tại giao diện chính của phần mềm, Chọn "Tạo cuộc họp".



Hình 209: Dạy học an toàn trên phần mềm Zavi (1)

Bước 2: Tại giao diện, mặc định Zavi sẽ tự động đặt mật khẩu cho bạn. Nếu muốn thay đổi mật khẩu, hãy tích chọn và nhập mật khẩu muốn cài đặt.



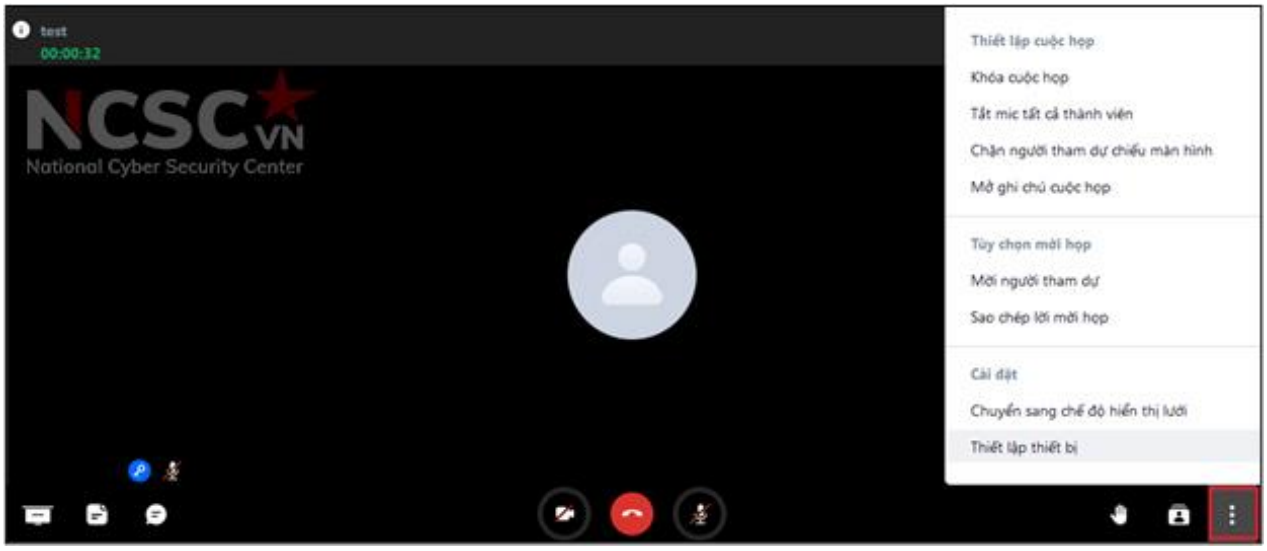
Hình 210: Dạy học an toàn trên phần mềm Zavi (2)

Bước 3: Nhấn vào "Tạo cuộc họp" để lưu lại thông tin mật khẩu.

1.6.2. Khóa lớp học

Khi số lượng người tham gia học đã đầy đủ, bạn có thể sử dụng tính năng **Khóa cuộc họp** để giới hạn người tham gia. Khi bạn kích hoạt tính năng này cho lớp học trực tuyến trên Zavi, người khác sẽ không thể tham gia lớp học dù đã có thông tin lớp học.

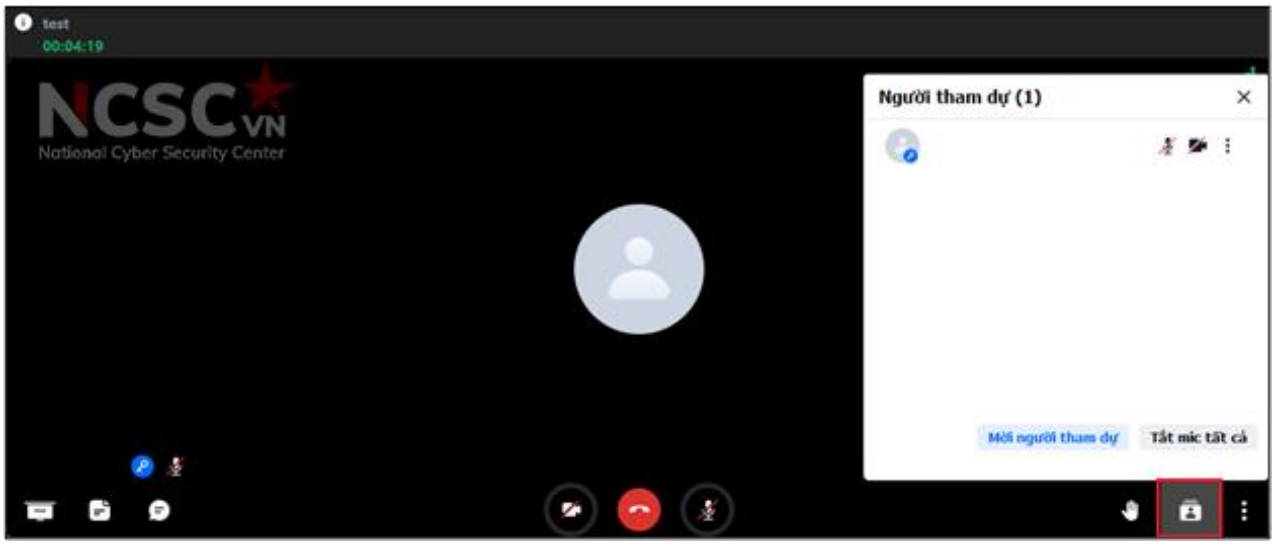
Để khóa lớp học, bạn nhấn chọn vào biểu tượng "**Thêm**" hình ba chấm trên góc phải màn hình, chọn "**Khóa cuộc họp**".



Hình 211: Khóa lớp học trên Zavi

1.6.3. Loại bỏ người không phải học sinh của lớp

Bấm vào biểu tượng "**Thành viên**" ở góc phải màn hình để xem danh sách thành viên đang tham gia, để kiểm soát và lọc những người lạ có thể truy cập vào lớp học online.



Hình 212: Loại bỏ người không phải học sinh của lớp trên Zavi

Để mời một thành viên ra khỏi lớp học, trong danh sách thành viên, bấm vào biểu tượng "**Thêm**" bên cạnh tên thành viên đó > Chọn "**Mời ra khỏi phòng**".

1.7. Dạy học an toàn trên phần mềm Jitsi

1.7.1. Đặt mật khẩu cho lớp học

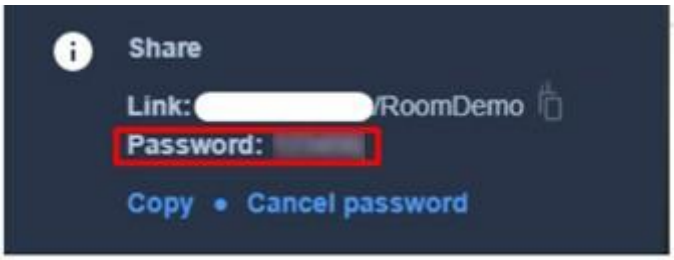
Bước 1. Trên giao diện lớp học, chọn biểu tượng **Share** -> **Add password**

Hình 213: Đặt mật khẩu cho lớp học (1)

Bước 2. Nhập mật khẩu, rồi gõ phím **Enter**

Hình 214: Đặt mật khẩu cho lớp học (2)

Bước 3. Sau khi tạo thành công, giáo viên sẽ thấy như sau



Hình 215: Đặt mật khẩu cho lớp học (3)

Khi đó, người nào truy cập lớp học đều phải nhập mật khẩu mà giáo viên đã tạo.

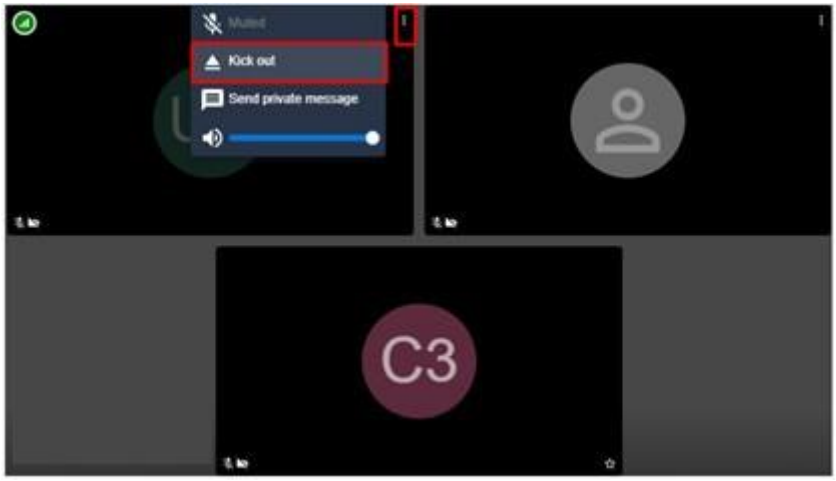
Chú ý: Giáo viên có thể thay đổi hay xóa mật khẩu bất cứ lúc nào bằng cách chỉnh sửa mật khẩu hoặc chọn **Remove password** để xóa bỏ mật khẩu.

1.7.2. Loại bỏ người không phải là học sinh của lớp

Để xóa một người dùng ra khỏi lớp học, giáo viên có thể làm như sau:

Bước 1: Chọn dấu 3 chấm bên góc của hình đại diện người dùng

Bước 2: Chọn Rời phòng họp



Hình 216: Xóa người dùng ra khỏi lớp học

2. Hướng dẫn cho học sinh và cha mẹ

2.1. Lưu ý chung đối với cha mẹ và học sinh

- Chỉ tải và cài đặt phần mềm từ địa chỉ tin cậy (thông qua kho ứng dụng hoặc trang chủ của nhà phát triển)

- Đối với các em học sinh sử dụng chung máy tính để học tập, cha mẹ nên là người tạo riêng tài khoản cho từng bạn và cài đặt chỉ các phần mềm cần thiết, không cho phép cài đặt, sử dụng các phần mềm khác; (có thể thiết lập theo chương 2 của hướng dẫn này) để hạn chế việc các em làm lộ dữ liệu trên máy tính của cha mẹ.

- Đối với các em còn nhỏ tuổi, cha mẹ cần theo sát hướng dẫn của giáo viên và hỗ trợ các em sử dụng các phần mềm để tham gia vào lớp học trong những buổi học đầu tiên.

- Cha mẹ cũng như các em học sinh không chia sẻ thông tin về lớp học trên các kênh thông tin công khai.

- Khi tham gia vào lớp học cần đặt theo tên của học sinh, hoặc đặt theo hướng dẫn của giáo viên.

- Dành thời gian để kiểm tra, cập nhật ứng dụng đang sử dụng để học trực tuyến khi có phiên bản mới, tránh cập nhật trong giờ học của các em. Đối với trường hợp sử dụng trình duyệt web trên máy tính hoặc điện thoại để tham gia lớp học, cần lưu ý cập nhật phiên bản trình duyệt web. Đối với phần mềm cài trên điện thoại di động việc cập nhật phiên bản phần mềm có thể thực hiện thông qua App Store (Iphone), CH Play (Android). Khi có phiên bản phần mềm mới, người dùng sẽ được thông báo để cập nhật. Đối với máy tính, thông thường các phần mềm cũng sẽ báo khi có phiên bản mới, có thể cập nhật ngay hoặc để sau.

- Cảnh giác, không mở đường dẫn, và tập tin lạ khi xuất hiện trên lớp học mà không phải do giáo viên chia sẻ.

2.2. Học an toàn trên phần mềm Zoom

2.2.1. Sử dụng ID ngẫu nhiên

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

2.2.2. Tránh chia sẻ tệp tin

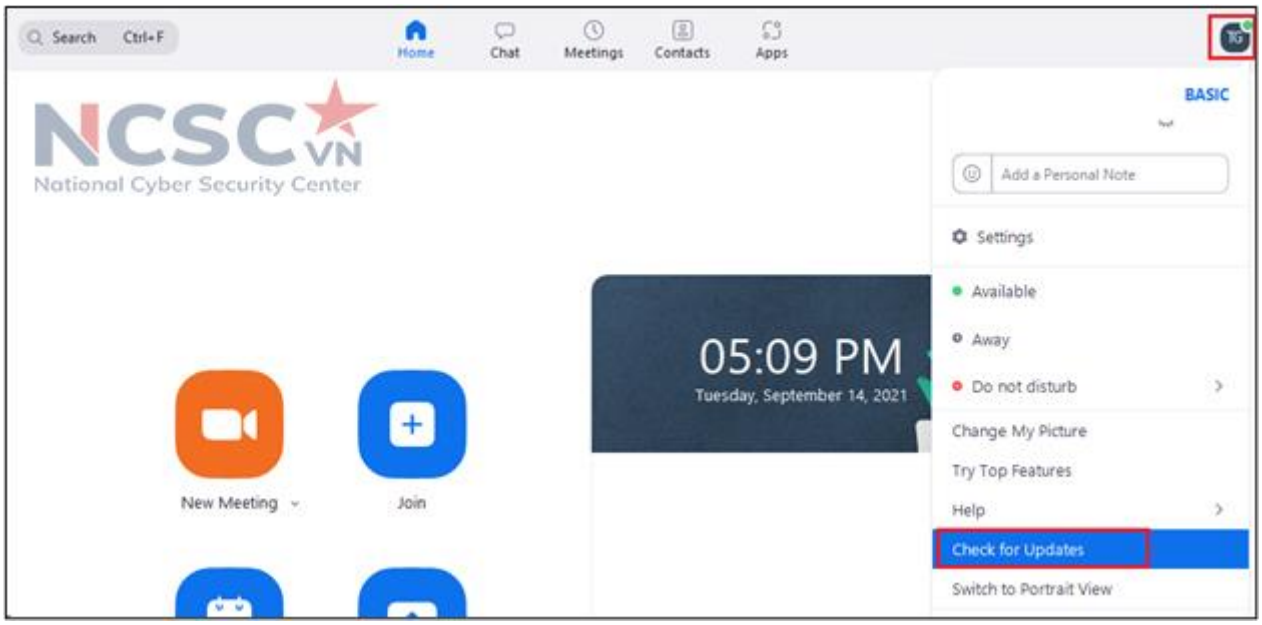
Cẩn thận với tính năng chia sẻ tệp của các lớp học, đặc biệt nếu người dùng không xác định đang gửi một tệp tin hoặc liên kết qua đó, những thứ này có thể chứa virus. Thay vào đó, hãy chia sẻ tài liệu thông qua các dịch vụ đáng tin cậy như Box hoặc Google Drive.

2.2.3. Kiểm tra và cập nhật phiên bản phần mềm

Để kiểm tra và cập nhật phần mềm Zoom thực hiện như sau:

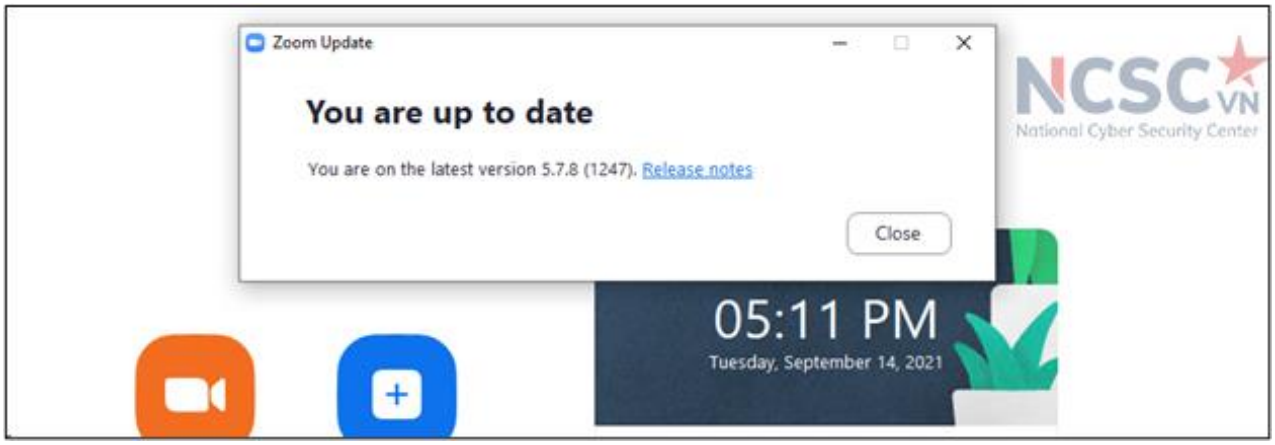
Bước 1: Kiểm tra phiên bản phần mềm

Mở ứng dụng dành cho máy tính để bàn, chọn profile ở trên cùng bên phải và chọn "Check for updates".



Hình 217: Kiểm tra và cập nhật phần mềm Zoom(1)

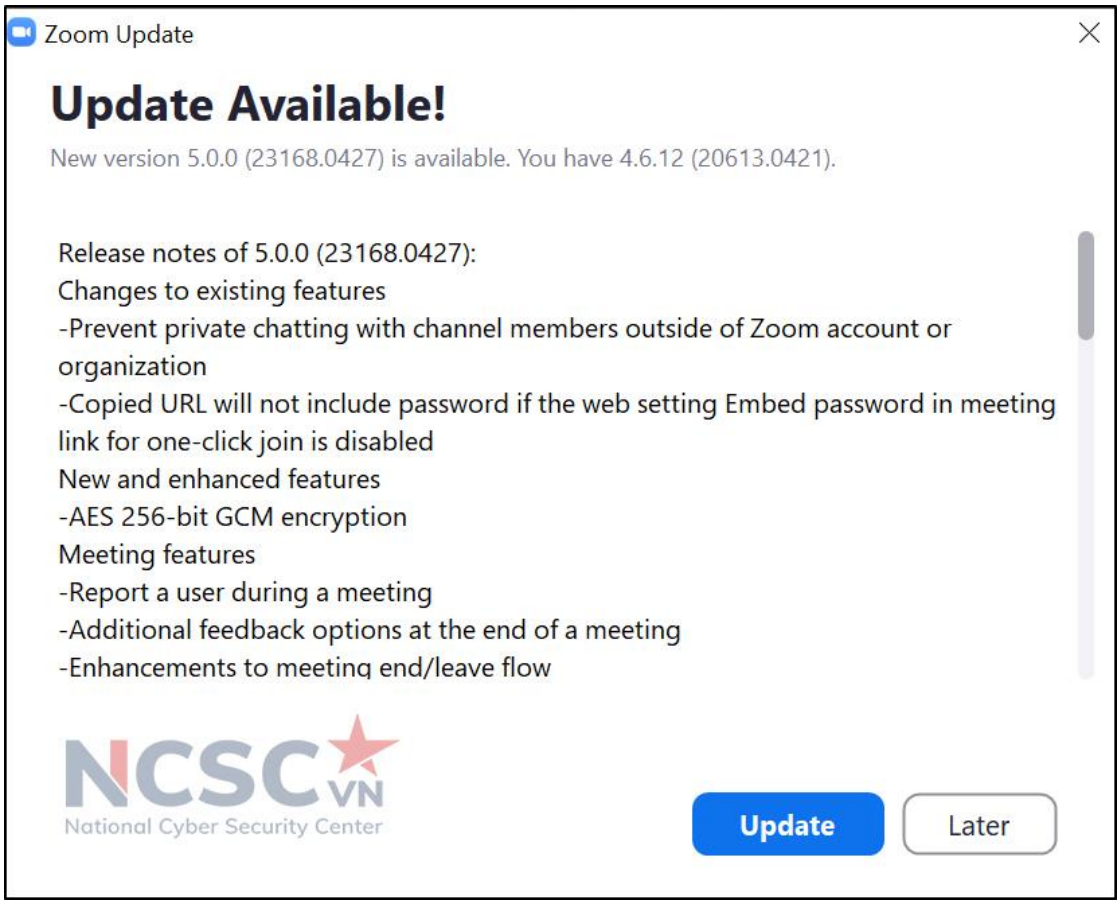
Nếu phiên bản là mới nhất chúng ta sẽ nhận được thông tin “You are up to date”



Hình 218: Kiểm tra và cập nhật phần mềm Zoom (2)

Bước 2: Cập nhật phần mềm

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.



Hình 219: Kiểm tra và cập nhật phần mềm Zoom (3)

2.3. Học an toàn trên phần mềm Microsoft Teams

2.3.1. Xác định đúng thông tin liên quan đến lớp học cần tham gia

Bạn cần xác định đúng thông tin liên quan để tham gia lớp học. Để tránh tình trạng các đối tượng tấn công có thể giả mạo gửi cho bạn 1 đường link độc hại để bạn truy cập

thông qua email hoặc zalo của bạn.

2.3.2. Cảnh giác với các đường link lạ và nội dung được chia sẻ

Bạn không nên chia sẻ thông tin liên quan đến lớp học của mình ra bên ngoài, đặc biệt với người lạ để tránh nguy cơ bị đánh cắp thông tin của lớp học. Đồng thời cảnh giác với các đường link hay nội dung lạ được chia sẻ trong lớp học, không tùy tiện nhấn vào nếu không có sự cho phép hay hướng dẫn và xác nhận của giáo viên/quản lý lớp học.

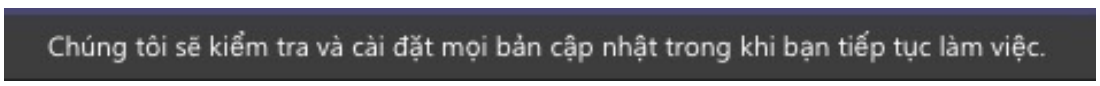
2.2.3. Kiểm tra và cập nhật phần mềm Microsoft Team

Để kiểm tra, cập nhật phần mềm Microsoft Team thực hiện như sau:

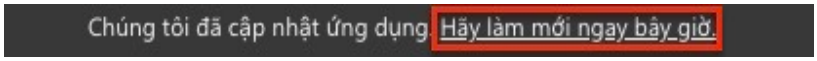
Truy cập vào menu Cài đặt > Kiểm tra bản cập nhật

Hình 220: Kiểm tra và cập nhật phần mềm Microsoft Team

Xuất hiện thông báo "Chúng tôi sẽ kiểm tra và cài đặt mọi bản cập nhật trong khi bạn tiếp tục làm việc" xuất hiện.



Thanh thông báo "Chúng tôi đã cập nhật ứng dụng. Hãy làm mới ngay bây giờ" > "Hãy làm mới ngay bây giờ" để ứng dụng tự khởi động lại. Người dùng chờ ứng dụng xuất hiện trở lại để hoàn tất quá trình sử cập nhật.



2.4. Học an toàn trên phần mềm Google Meet

2.4.1. Xác định đúng thông tin liên quan đến lớp học cần tham gia

Bạn cần xác định đúng thông tin của lớp học. Để tránh tình trạng các đối tượng tấn công có thể giả mạo gửi cho bạn 1 đường link độc hại để bạn truy cập và cài cắm mã độc hoặc thu thập thông tin cá nhân.

2.4.2. Cảnh giác với các đường link lạ và nội dung được chia sẻ

Không chia sẻ thông tin liên quan đến lớp học của mình ra bên ngoài, đặc biệt với người lạ để tránh nguy cơ bị đánh cắp thông tin của lớp học. Đồng thời cảnh giác với các đường link hay nội dung lạ được chia sẻ trong lớp học, không tùy tiện nhấn vào nếu không có sự cho phép hay hướng dẫn và xác nhận của giáo viên/quản lý lớp học.

2.4.3. Kiểm tra và cập nhật phần mềm Google Meet

Google Meet là ứng dụng chạy trên nền tảng web, do vậy bạn có thể cập nhật trình duyệt web bạn đang sử dụng.

2.5. Học an toàn trên phần mềm Trans

2.5.1. Xác định đúng thông tin liên quan đến lớp học cần tham gia

Bạn cần xác định đúng thông tin liên quan đến đường link tham gia lớp học, ID lớp học và mật khẩu được cung cấp. Để tránh tình trạng các đối tượng tấn công có thể giả mạo gửi cho bạn 1 đường link độc hại để bạn truy cập thông qua email hoặc zalo của bạn.

2.5.2. Cảnh giác với các đường link lạ và nội dung được chia sẻ

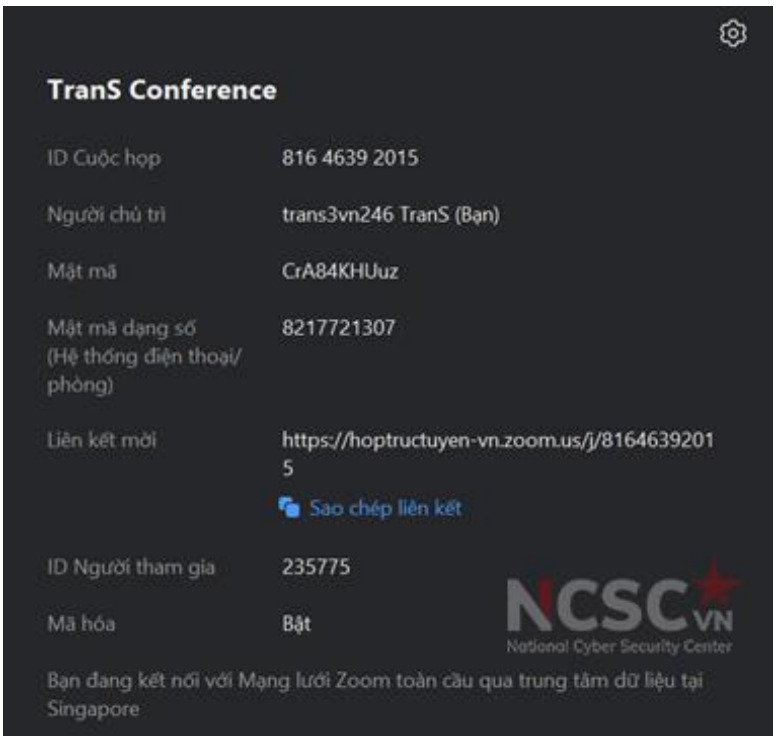
Bạn không nên chia sẻ thông tin liên quan đến lớp học của mình ra bên ngoài, đặc biệt với người lạ để tránh nguy cơ bị đánh cắp thông tin của lớp học. Đồng thời cảnh giác với các đường link hay nội dung lạ được chia sẻ trong lớp học, không tùy tiện nhấn vào nếu không có sự cho phép hay hướng dẫn và xác nhận của giáo viên/quản lý lớp học.

2.5.3. Kiểm tra và cập nhật phần mềm Trans

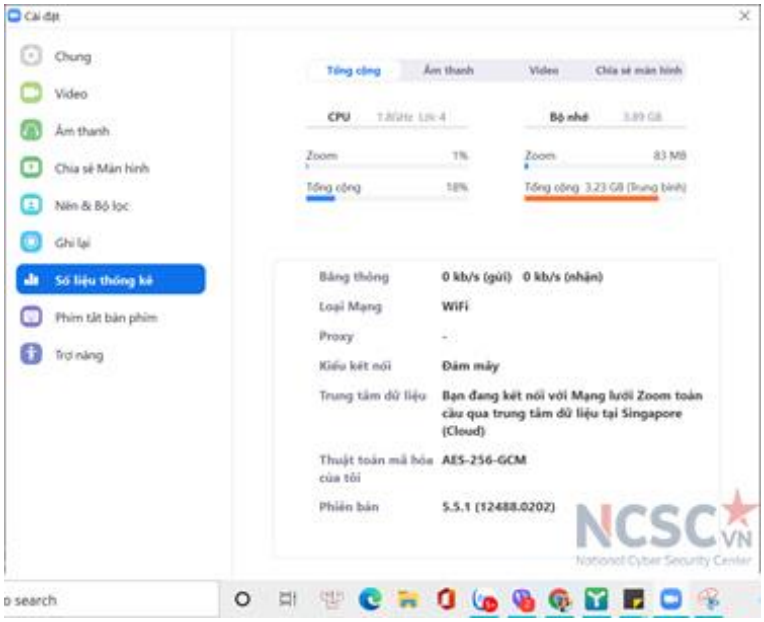
Các bước thực hiện để kiểm tra và cập nhật phần mềm như sau:

Bước 1: Kiểm tra phiên bản phần mềm đang sử dụng.

Chọn biểu tượng Cài đặt (hình răng cưa) ở phía góc bên phải ở cửa sổ hiện ra. Phiên bản hiện ở mục Số liệu thống kê.

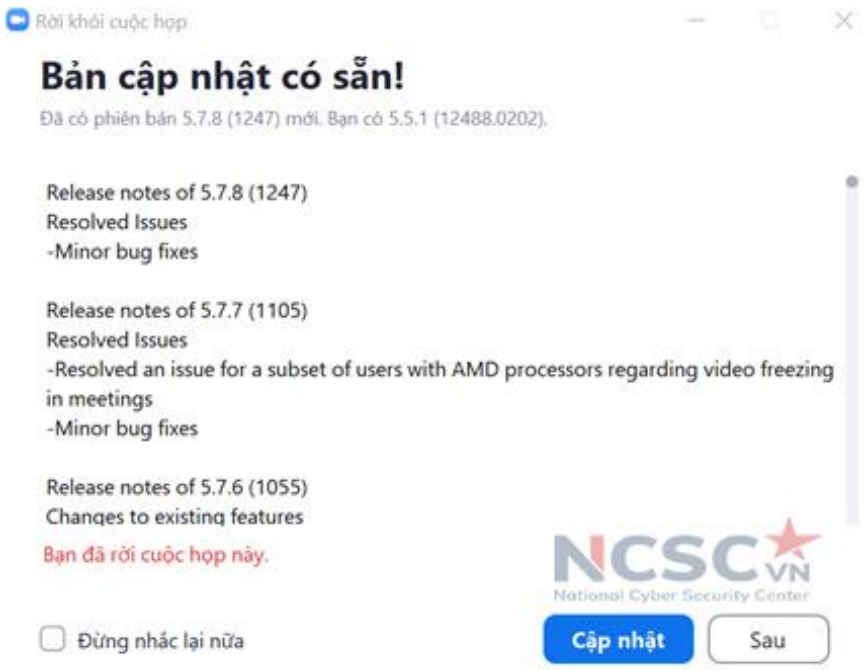


Hình 221: Kiểm tra và cập nhật phần mềm Trans (1)



Hình 222: Kiểm tra và cập nhật phần mềm Trans (2)

Bước 2: Để người dùng chủ động cập nhật phần mềm, Trans không có tính năng này mà hệ thống sẽ tự động hỏi có cập nhật phiên bản khi có phiên bản mới sau khi mình rời lớp học/cuộc họp hay không. Lúc này bạn có thể chọn cập nhật ngay hoặc để sau



Hình 223: Kiểm tra và cập nhật phần mềm Trans (3)

2.6. Học an toàn trên phần mềm Zavi

2.6.1. Xác định đúng thông tin liên quan đến lớp học cần tham gia

Bạn cần xác định đúng thông tin liên quan đến đường link tham gia lớp học, ID lớp học và mật khẩu được cung cấp. Để tránh tình trạng các đối tượng tấn công có thể giả mạo gửi cho bạn 1 đường link độc hại để bạn truy cập thông qua email hoặc zalo của bạn.

2.6.2. Cảnh giác với các đường link lạ và nội dung được chia sẻ

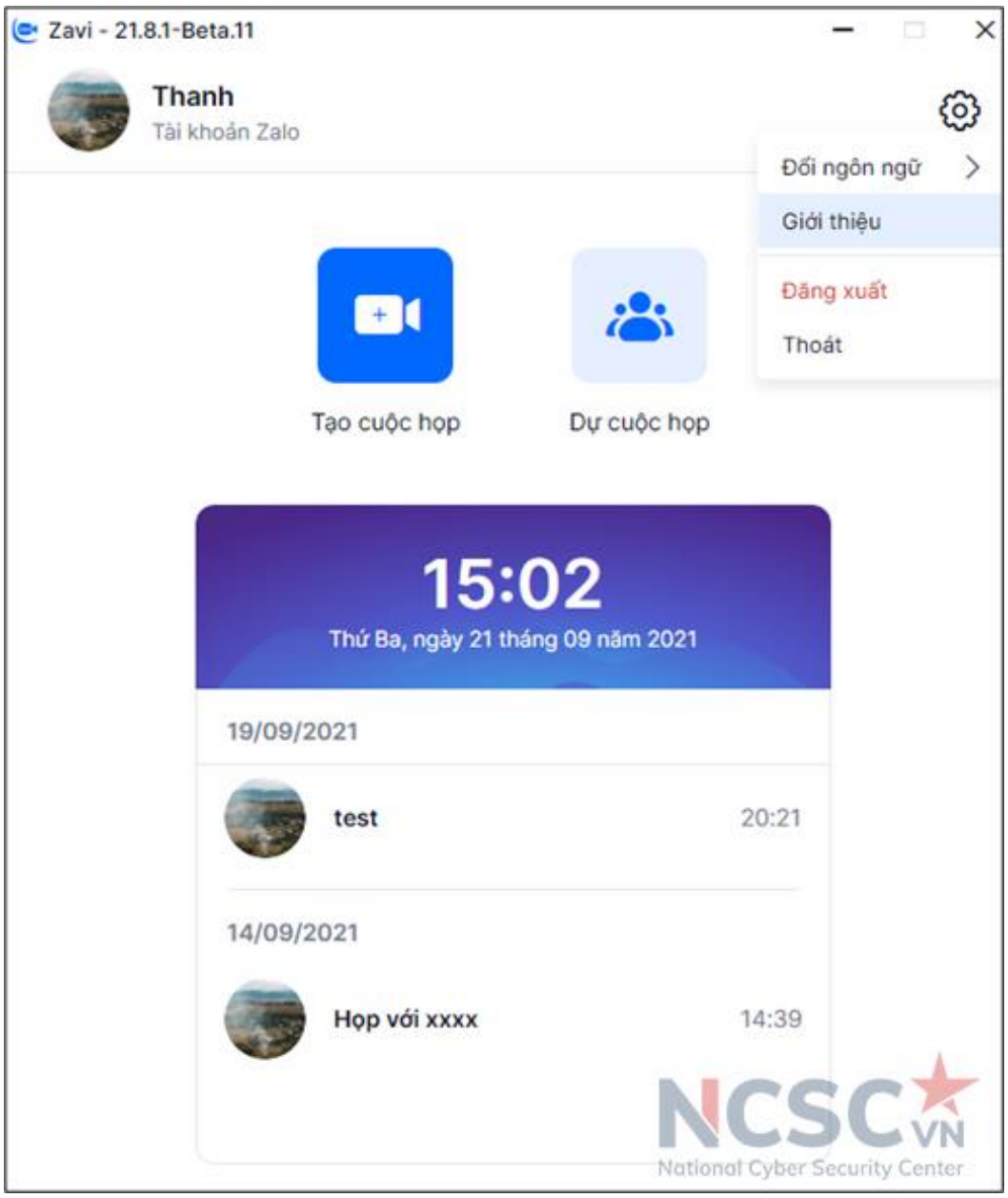
Không chia sẻ thông tin liên quan đến lớp học của mình ra bên ngoài, đặc biệt với người lạ để tránh nguy cơ bị đánh cắp thông tin của lớp học. Đồng thời cảnh giác với các đường link hay nội dung lạ được chia sẻ trong lớp học, không tùy tiện nhấn vào nếu không có sự cho phép hay hướng dẫn và xác nhận của giáo viên/quản lý lớp học.

2.6.3. Kiểm tra và cập nhật phần mềm Zavi

Các bước thực hiện để kiểm tra và cập nhật phần mềm như sau:

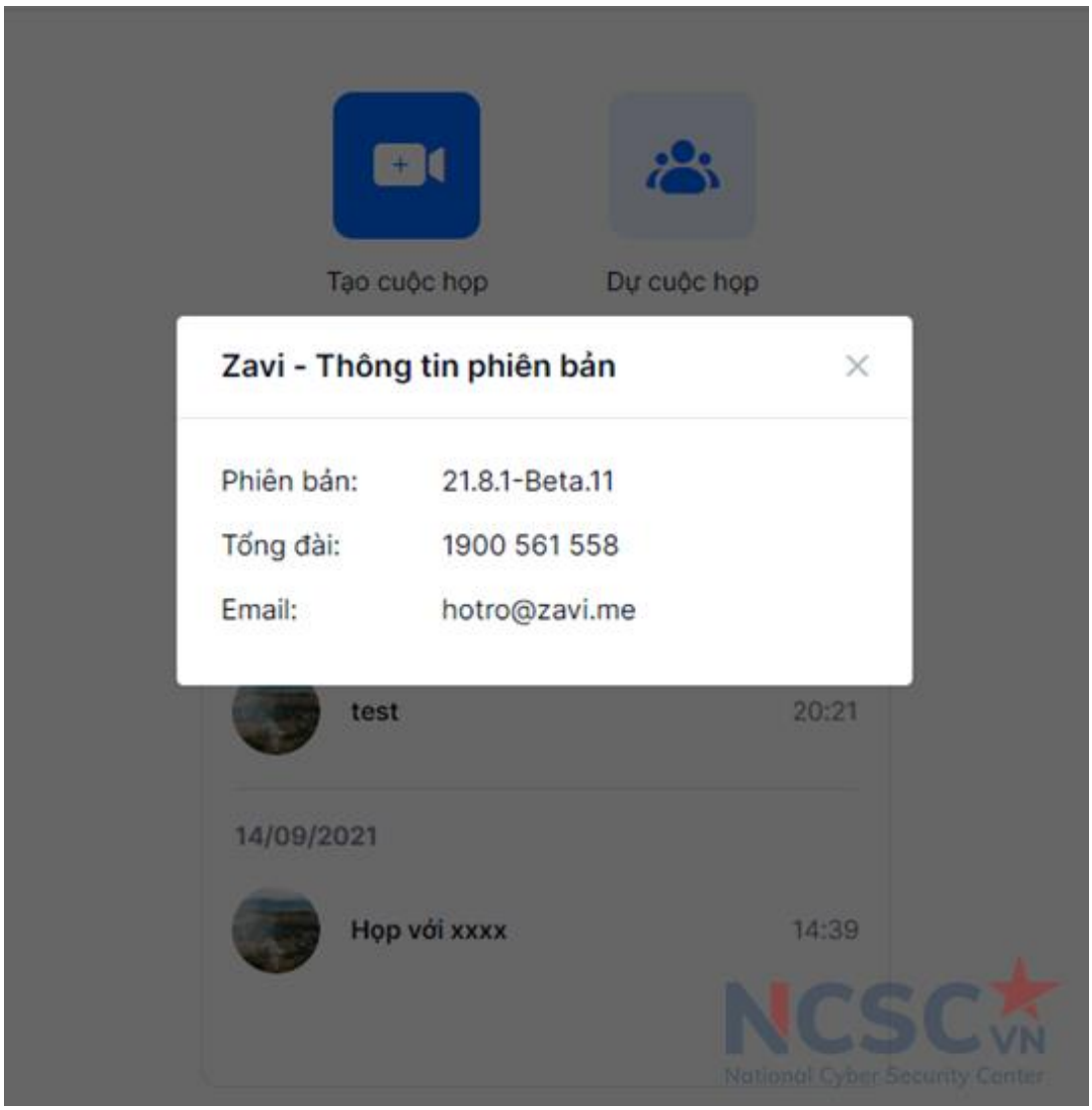
Bước 1: Kiểm tra phiên bản đang sử dụng

Tại giao diện chính của Zavi, Chọn vào hình bánh răng cưa ở góc trên cùng bên phải màn hình > Giới thiệu



Hình 224: Kiểm tra và cập nhật phần mềm Zavi (1)

Một cửa sổ sẽ xuất hiện và hiển thị các thông tin phiên bản ứng dụng mà bạn đang sử dụng.



Hình 225: Kiểm tra và cập nhật phần mềm Zavi (2)

Hoặc 1 cách đơn giản khác để kiểm tra phiên bản đang sử dụng là trên giao diện chính của Zavi, đã có hiện phiên bản bạn đang sử dụng ở góc trên cùng bên trái màn hình.

Bước 2: Cài đặt phiên bản mới (nếu có)

Để cập nhật phiên bản mới nhất của phần mềm Zavi, người dùng truy cập tại: https://zavi.me/?lang=vi#

2.7. Học an toàn trên phần mềm Jitsi

2.6.1. Xác định đúng thông tin liên quan đến lớp học cần tham gia

Bạn cần xác định đúng thông tin liên quan đến đường link tham gia lớp học, ID lớp học và mật khẩu được cung cấp. Để tránh tình trạng các đối tượng tấn công có thể giả mạo gửi cho bạn 1 đường link độc hại để bạn truy cập thông qua email hoặc zalo của bạn.

2.6.2. Cảnh giác với các đường link lạ và nội dung được chia sẻ

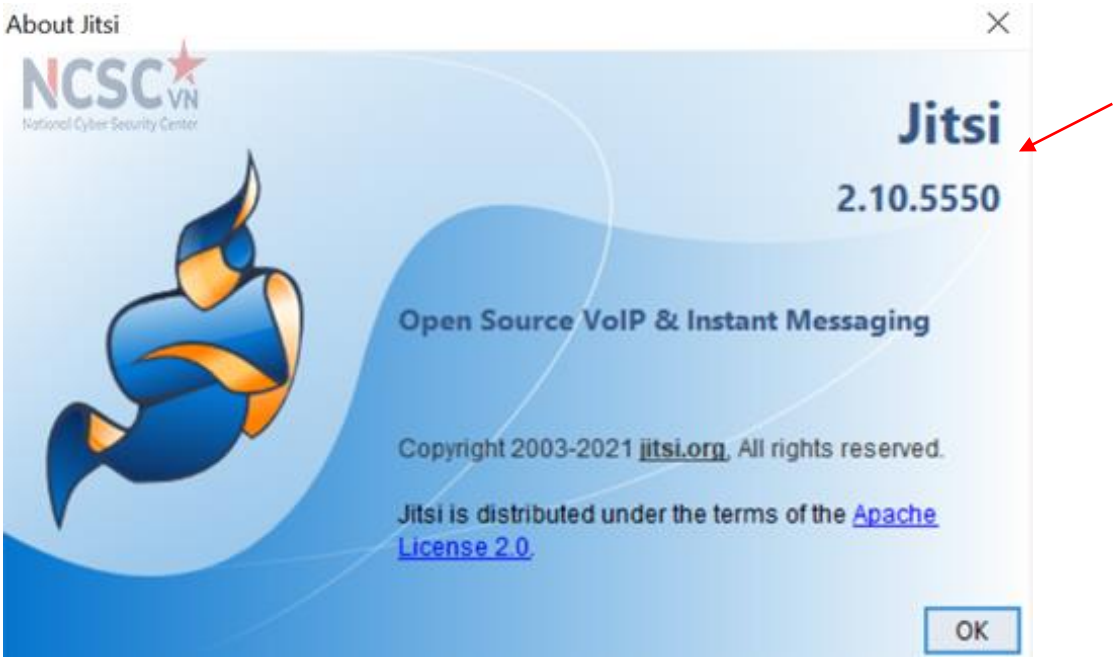
Không chia sẻ thông tin liên quan đến lớp học của mình ra bên ngoài, đặc biệt với người lạ để tránh nguy cơ bị đánh cắp thông tin của lớp học. Đồng thời cảnh giác với các đường link hay nội dung lạ được chia sẻ trong lớp học, không tùy tiện nhấn vào nếu không có sự cho phép hay hướng dẫn và xác nhận của giáo viên/quản lý lớp học.

2.6.3. Kiểm tra và cập nhật phần mềm Jitsi

Các bước thực hiện để kiểm tra và cập nhật phần mềm như sau:

Bước 1: Kiểm tra phiên bản đang sử dụng

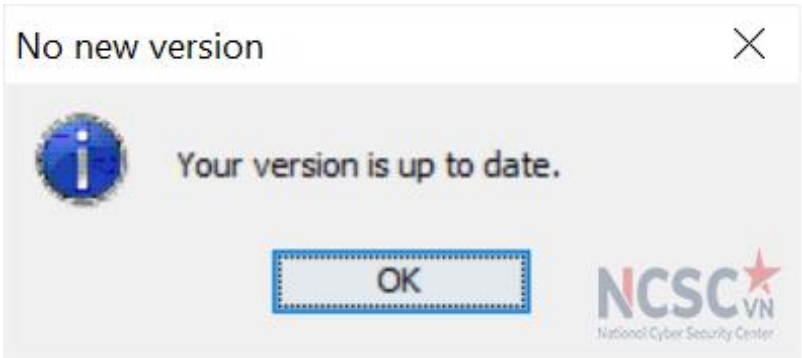
Vào mục Help phía bên trái góc giao diện > **About**. Thông tin về phiên bản sẽ hiện dưới phần tên phần mềm



Hình 226: Kiểm tra và cập nhật phần mềm Jitsi (1)

Bước 2: Cập nhật phiên bản

Để cập nhật phiên bản chọn Check for Updates. Nếu thấy thông báo Your version is up to date tức là phiên bản hiện tại đang là mới nhất.



Hình 227: Kiểm tra và cập nhật phần mềm Jitsi (2)

Phụ lục: Địa chỉ tin cậy để tải phần mềm

Tên phần mềm	Địa chỉ tải phần mềm
Ứng dụng Internet an toàn Visafe	- Kho ứng dụng: + App Store (Visafe) + CH Play (Visafe) - Trang chủ: https://visafe.vn
Zoom Cloud Meetings	- Kho ứng dụng: + App Store (Zoom Cloud Meetings) + CH Play (Zoom Cloud Meetings) - Trang chủ: https://zoom.us
Microsoft Teams	- Kho ứng dụng: + App Store (Microsoft Teams) + CH Play (Microsoft Teams) - Trang chủ: https://www.microsoft.com
Google Meet	- Kho ứng dụng: + App Store (Google Meet) + CH Play (Google Meet) - Trang chủ: https://meet.google.com
TranS	- Kho ứng dụng: + App Store (TranS Japan) + CH Play (TranS) - Trang chủ: https://hoptructuyen.vn
Zavi	- Kho ứng dụng: + App store (Zavi) + CH Play (Zavi) - Trang chủ: https://zavi.me
Jitsi	- Kho ứng dụng: + App Store (Jitsi Meet) + CH Play (Jitsi Meet) - Trang chủ: https://jitsi.org