

# HƯỚNG DẪN SỬ DỤNG VINCSS FIDO2® FINGERPRINT CHO WINDOWS/macOS



**Ngày:** 27/04/2023

**Số hiệu:** CSS-PRD-PQMC-USG-230427-005

**Phiên bản:** 2.1

**Phân loại tài liệu:** Tài liệu công bố

**Thực hiện:** Trung tâm Sản phẩm, VinCSS

**CÔNG TY CỔ PHẦN DỊCH VỤ AN NINH MẠNG VINCSS**

Số 7 Đường Băng Lăng 1, Khu đô thị sinh thái Vinhomes Riverside, Phường  
Việt Hưng, Quận Long Biên, Thành phố Hà Nội.

## THEO DÕI PHIÊN BẢN

Phiên bản	Ngày	Người viết	Vị trí	Liên hệ	Nội dung
2.0	19/04/2023				Cập nhật nội dung phần xác thực không mật khẩu
2.1	27/04/2023				Cập nhật nội dung phần kết nối với máy tính trên nền tảng Windows



## MỤC LỤC

<b>THEO DÕI PHIÊN BẢN .....</b>	<b>2</b>
<b>MỤC LỤC .....</b>	<b>3</b>
<b>I. THÔNG TIN SẢN PHẨM .....</b>	<b>6</b>
I.1. Thông số kỹ thuật.....	6
I.2. Ý nghĩa của các đèn hiệu .....	7
<b>II. QUẢN LÝ MÃ PIN VÀ VÂN TAY.....</b>	<b>8</b>
II.1. Nền tảng Windows.....	8
II.1.1. Kết nối với máy tính.....	8
II.1.1.1 Sử dụng qua kết nối USB .....	9
II.1.1.2 Sử dụng qua kết nối NFC .....	9
II.1.1.3 Sử dụng qua kết nối Bluetooth .....	9
II.1.2. Tạo mã PIN mới .....	11
II.1.3. Thay đổi mã PIN.....	13
II.1.4. Thêm vân tay.....	15
II.1.5. Xóa vân tay.....	17
II.1.6. Thiết lập cài đặt gốc.....	19
II.2. Nền tảng macOS .....	23
II.2.1. Kết nối với máy tính.....	23
II.2.2. Tạo mới mã PIN .....	23
II.2.3. Thay đổi mã PIN.....	25
II.2.4. Thêm vân tay.....	26
II.2.5. Xóa vân tay.....	28
II.2.6. Quản lý dữ liệu đăng nhập.....	29
II.2.7. Thiết lập cài đặt gốc.....	31
<b>III. XÁC THỰC KHÔNG MẬT KHẨU VỚI VINCSS FIDO2® FINGERPRINT .....</b>	<b>32</b>
III.1. Đăng nhập với Window 10 .....	32
III.1.1. Cấu hình trên hệ thống Azure AD.....	32
III.1.1.1. Cấu hình Azure AD .....	32
III.1.1.2. Đăng nhập Windows 10 sử dụng FIDO2 với provisioning packages .....	33

III.1.1.3. Đăng ký khóa xác thực cho tài khoản Azure AD .....	34
<b><i>III.1.1.3.1. Sử dụng qua kết nối Bluetooth</i></b> .....	37
<b><i>III.1.1.3.2. Sử dụng qua kết nối USB</i></b> .....	39
<b><i>III.1.1.3.3. Sử dụng qua kết nối NFC</i></b> .....	40
III.1.1.4. Kết nối User vào Azure Work Account .....	42
<b><i>III.1.2. Đăng nhập Windows 10</i></b> .....	<b>46</b>
III.1.2.1. Sử dụng qua kết nối Bluetooth. ....	46
III.1.2.2. Sử dụng qua kết nối USB .....	47
III.1.2.3. Sử dụng qua kết nối NFC .....	47
<b><i>III.2. Xác thực không mật khẩu tài khoản Microsoft</i></b> .....	<b>48</b>
<b><i>III.2.1. Đăng ký khóa bảo mật</i></b> .....	<b>48</b>
<b><i>III.2.1.1. Sử dụng qua kết nối Bluetooth</i></b> .....	51
<b><i>III.2.1.2. Sử dụng qua kết nối USB</i></b> .....	53
<b><i>III.2.1.3. Sử dụng qua kết nối NFC</i></b> .....	54
<b><i>III.2.2. Xác thực không mật khẩu tài khoản Microsoft</i></b> .....	<b>56</b>
III.2.2.1. Sử dụng qua kết nối Bluetooth .....	57
III.2.2.2. Sử dụng qua kết nối USB .....	58
III.2.2.3. Sử dụng qua kết nối NFC .....	58
<b><i>III.3. VinCSS OVPN Client</i></b> .....	<b>59</b>
<b><i>III.3.1. Windows</i></b> .....	<b>59</b>
III.3.1.1. Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint .....	59
<b><i>III.3.1.1.1. Sử dụng qua kết nối Bluetooth</i></b> .....	60
<b><i>III.3.1.1.2. Sử dụng qua kết nối USB</i></b> .....	61
<b><i>III.3.1.1.3. Sử dụng qua kết nối NFC</i></b> .....	61
III.3.1.2. Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint.....	62
<b><i>III.3.1.2.1. Xác thực không mật khẩu</i></b> .....	65
<b><i>III.3.1.2.2. Xác thực không tên người dùng</i></b> .....	65
III.3.1.2.2.1. Sử dụng qua kết nối Bluetooth.....	66
III.3.1.2.2.2. Sử dụng qua kết nối USB.....	66
III.3.1.2.2.3. Sử dụng qua kết nối NFC .....	67
<b><i>III.3.2. macOS</i></b> .....	<b>68</b>
III.3.2.1. Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint ( <i>Chỉ hỗ trợ kết nối USB</i> )	68
III.3.2.2. Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint.....	69
<b><i>III.3.2.2.1. Xác thực không mật khẩu</i></b> .....	72

III.3.2.2.2. Xác thực không tên người dùng.....	72
III.3.2.2.2.1. Sử dụng qua kết nối Bluetooth.....	73
III.3.2.2.2.2. Sử dụng qua kết nối USB .....	74
III.3.2.2.2.3. Sử dụng qua kết nối NFC .....	74
<b>III.4. Xác thực 2 yếu tố tài khoản Facebook.....</b>	<b>75</b>
<b>III.4.1. Đăng ký khoá bảo mật.....</b>	<b>75</b>
III.4.1.1. Sử dụng qua kết nối Bluetooth .....	77
III.4.1.2. Sử dụng qua kết nối USB .....	78
III.4.1.3. Sử dụng qua kết nối NFC .....	78
<b>III.4.2. Xác thực 2 yếu tố với dịch vụ Facebook.....</b>	<b>79</b>
III.4.2.1. Sử dụng qua kết nối Bluetooth .....	80
III.4.2.2. Sử dụng qua kết nối USB .....	80
III.4.2.3. Sử dụng qua kết nối NFC .....	81
<b>III.5. Xác thực 2 yếu tố với Twitter .....</b>	<b>81</b>
<b>III.5.1. Đăng ký khoá bảo mật.....</b>	<b>81</b>
III.5.1.1. Sử dụng qua kết nối Bluetooth .....	83
III.5.1.2. Sử dụng qua kết nối USB .....	83
III.5.1.3. Sử dụng qua kết nối NFC .....	84
<b>III.5.2. Xác thực 2 yếu tố với dịch vụ Twitter .....</b>	<b>85</b>
III.5.2.1. Sử dụng qua kết nối Bluetooth .....	85
III.5.2.2. Sử dụng qua kết nối USB .....	86
III.5.2.3. Sử dụng qua kết nối NFC .....	86
<b>III.6. Xác thực 2 yếu tố với Google.....</b>	<b>86</b>
<b>III.6.1. Đăng ký khoá bảo mật.....</b>	<b>86</b>
III.6.1.1. Sử dụng qua kết nối Bluetooth .....	92
III.6.1.2. Sử dụng qua kết nối USB .....	93
III.6.1.3. Sử dụng qua kết nối NFC .....	93
<b>III.6.2. Xác thực 2 yếu tố với dịch vụ Google .....</b>	<b>95</b>
III.6.2.1. Sử dụng qua kết nối Bluetooth .....	95
III.6.2.2. Sử dụng qua kết nối USB .....	96
III.6.2.3. Sử dụng qua kết nối NFC .....	96
<b>THAM KHẢO.....</b>	<b>98</b>

## I. THÔNG TIN SẢN PHẨM

### I.1. Thông số kỹ thuật



Hình ảnh VinCSS FIDO2® Fingerprint

Thông tin	Chi tiết
Tên sản phẩm	VinCSS FIDO2® Fingerprint
USB	USB Type-C
Bluetooth	Bluetooth Low Energy 5.0
NFC	ISO7816/ISO14443
Hệ điều hành hỗ trợ	Windows, MacOS, Linux, Android, iOS
Tiêu chuẩn xác thực	Xác thực không mật khẩu, xác thực 2 yếu tố, xác thực đa yếu tố
Chứng chỉ	FIDO2 Certified
Giao thức hỗ trợ	WebAuthn, FIDO2 CTAP1, FIDO2 CTAP2, Xác thực 2 yếu tố (U2F)
Trình duyệt hỗ trợ	Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Microsoft Edge Chromium
Thuật toán mã hóa	ECC p256

Thông tin	Chi tiết
Kiến trúc CPU	32-bit ARM® Cortex™-M4
Số lượng tài khoản có thể lưu	50
Số lượng vân tay có thể lưu	5
Đèn LED báo hiệu	Đèn RGB
Độ phân giải cảm biến	508 dpi
Tỉ lệ chấp nhận sai FAR	<0.0002%
Thời gian xác thực vân tay	< 1s
Cân nặng	20gr
Kích thước sản phẩm	43,5 mm x 38 mm x 8 mm
Dung lượng/Loại pin	25mAh, Pin Lithium-ion
Thời lượng pin	5-7 ngày (12 lần xác thực/ngày)
Thời gian chờ	2 năm
Thời gian sạc đầy	2 giờ 30 phút
Nguồn điện sử dụng	5V/1A
Vật liệu sử dụng	Nhựa Polycarbonate cao cấp chịu lực, đảm bảo độ bền cho sản phẩm
Nhiệt độ hoạt động	-10°C ~ 60°C
Màu sắc	Đen, trắng, xanh
Phụ kiện đi kèm	Cáp USB type-C, móc khoá, giá đỡ
Xuất xứ	Việt Nam

## I.2. Ý nghĩa của các đèn hiệu

Đèn hiệu của VinCSS FIDO2® Fingerprint sẽ cho người dùng biết trạng thái hiện tại của pin, trạng thái đang sạc pin, hoặc chế độ hoạt động.

Tín hiệu	Ý nghĩa	Trạng thái
Nháy đèn đỏ ba lần liên tiếp	Sắp hết pin, cần sạc	Đang sử dụng Bluetooth hoặc NFC
Đèn bật màu hổ phách	Khoá đang được sạc	Đang kết nối với USB
Đèn bật màu xanh lá cây	Khoá đã sạc đầy	Đang kết nối với USB
Đèn bật màu xanh nước biển	Bật chế độ Bluetooth, và khoá đã được kết nối với một thiết bị Bluetooth	Đang sử dụng Bluetooth
Đèn nháy sáng màu xanh nước biển	Khoá bảo mật vào chế độ ghép nối	Đang sử dụng Bluetooth
Đèn bật màu tím	Đã kích hoạt NFC	Đang sử dụng NFC
Nhấp nháy nhanh với đèn màu trắng	Khoá bảo mật đang trong quá trình xử lý và yêu cầu người dùng tương tác.	Yêu cầu người dùng xác nhận bằng cách chạm vào cảm biến vân tay

## II. QUẢN LÝ MÃ PIN VÀ VÂN TAY

Việc đặt mã PIN cho VinCSS FIDO2® Fingerprint là yêu cầu bắt buộc để có thể thêm/xóa vân tay, nhằm đảm bảo an toàn cho thiết bị, tránh trường hợp thêm vân tay trái phép, thử vân tay quá nhiều lần hoặc xóa vân tay từ người lạ.

Trường hợp người dùng cần tạo mới, thay đổi mã PIN/vân tay hoặc reset thiết bị VinCSS FIDO2® Fingerprint thì có thể thực hiện theo các bước dưới đây.

### II.1. Nền tảng Windows

#### II.1.1. Kết nối với máy tính

**Lưu ý:** Pin sẽ được set ở chế độ nghỉ để duy trì thời gian chờ của pin được lâu hơn, vì vậy trước khi sử dụng key, người dùng cần phải “Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB type C để kích hoạt khoá cho lần đầu tiên sử dụng”.

### II.1.1.1 Sử dụng qua kết nối USB

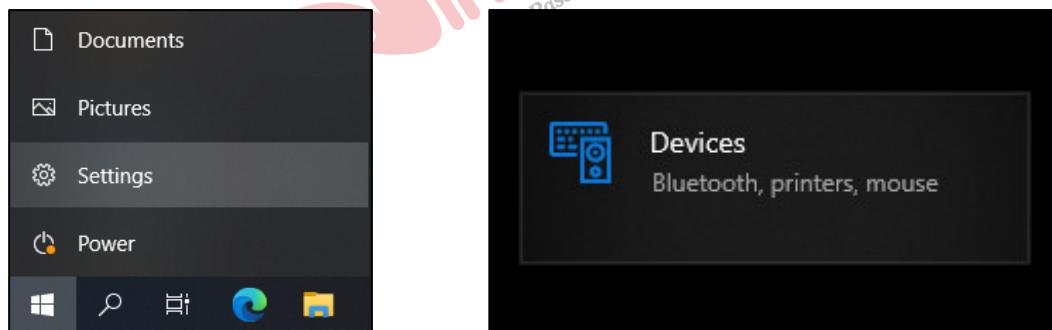
Tiến hành kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB, đảm bảo rằng khoá bảo mật đang **không** trong chế độ Bluetooth hoặc NFC. Nếu đèn LED nháy đỏ 3 lần liên tiếp cho biết mức pin đang ở dưới 20%, đèn LED màu hổ phách cho biết khoá bảo mật đang được sạc, đèn LED màu xanh lá cây cho biết pin đã được sạc đầy. Khoá bảo mật VinCSS FIDO2® Fingerprint có thể được sử dụng khi đang sạc.

### II.1.1.2 Sử dụng qua kết nối NFC

Tiến hành đặt khoá bảo mật VinCSS FIDO2® Fingerprint lên đầu đọc NFC. Khi đèn LED màu tím, có thể sử dụng tính năng NFC.

### II.1.1.3 Sử dụng qua kết nối Bluetooth

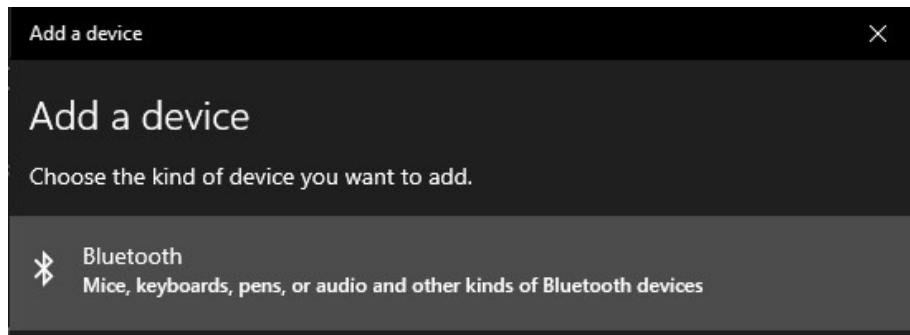
- Tại trạng thái tắt (*không có đèn sáng*), chuyển khoá bảo mật VinCSS FIDO2® Fingerprint vào chế độ kết nối Bluetooth bằng cách giữ cảm biến vân tay trong 5 giây. Khi đèn LED chuyển sang màu xanh lam, có thể sử dụng tính năng Bluetooth.
- Nếu đèn LED xanh lam không nhấp nháy, thực hiện giữ cảm biến vân tay trong vòng 5 giây để chuyển sang chế độ ghép đôi.
- Truy cập Windows > Settings > Devices.



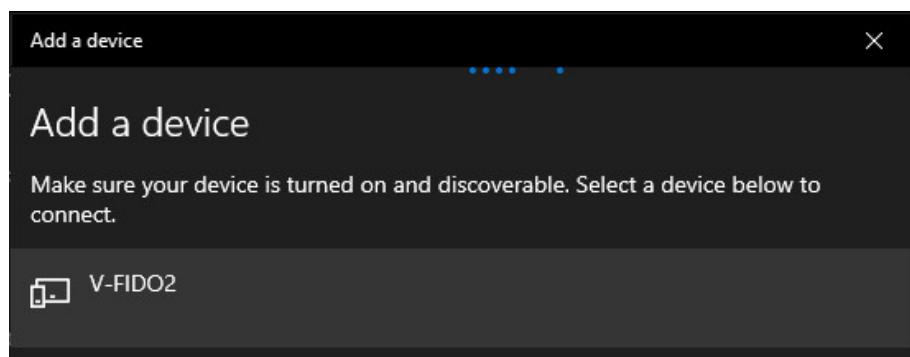
- Tại mục **Bluetooth** chọn **On**, sau đó chọn **Add Bluetooth or other device**.



- Tại mục Add a device, chọn Bluetooth.

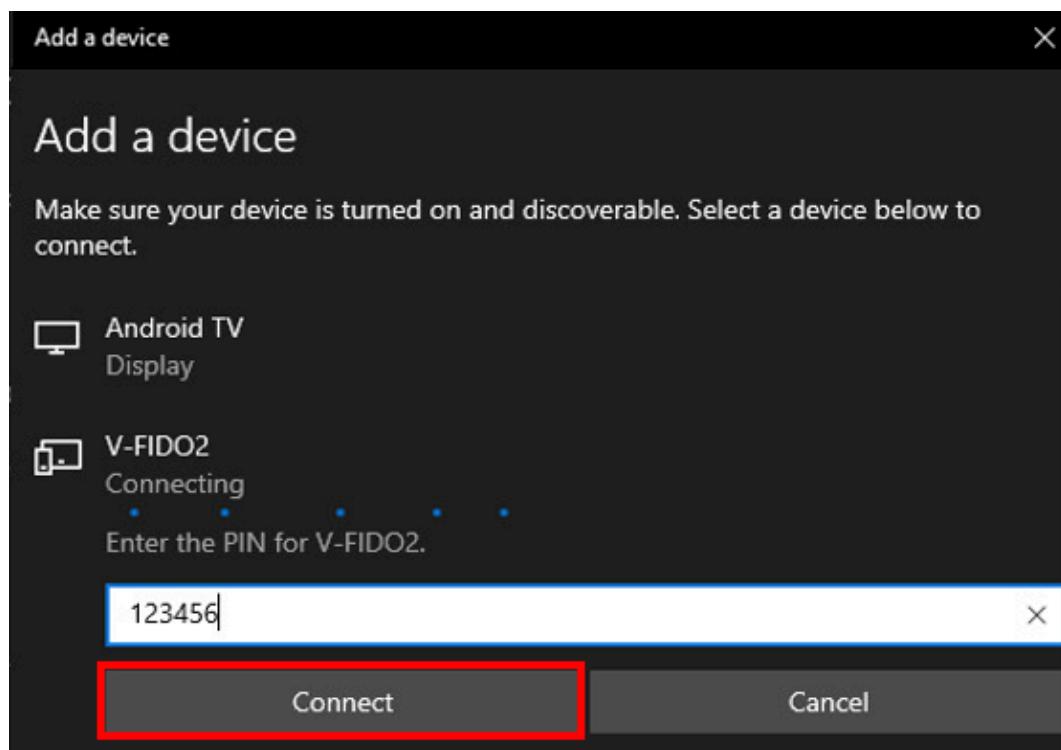


- Chọn thiết bị có tên V-FIDO2.

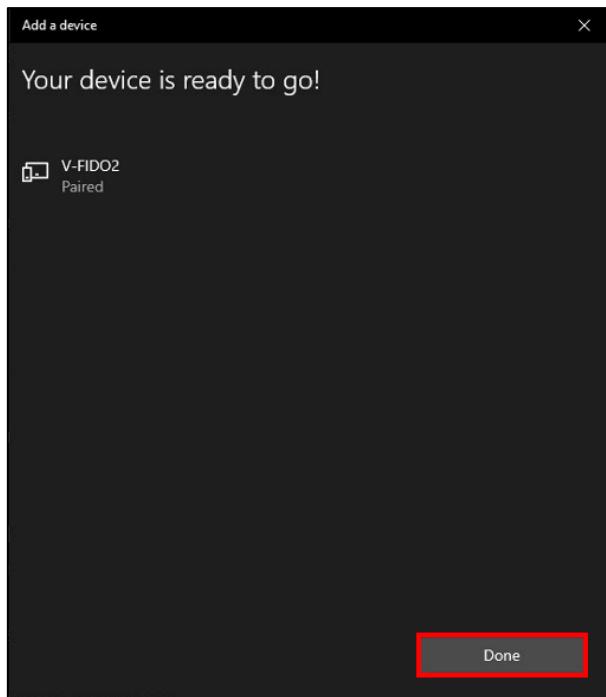


- Nhập mã ghép đôi để kết nối. Sau đó nhấn Connect.

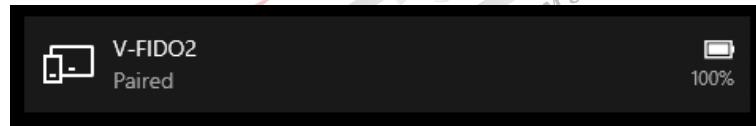
**Note:** Thiết bị sẽ có 1 mã serial bao gồm chữ và số (Ví dụ: XXX12345 hoặc XXX123456) được hiển thị ở mặt sau của khoá bảo mật. Mã ghép đôi là dãy số cuối của mã serial.



- Kết nối thành công. Nhấn **Done** để kết thúc.



- Sau khi kết nối thành công, trong danh sách thiết bị sẽ hiển thị khóa bảo mật VinCSS FIDO2® Fingerprint và dung lượng pin còn lại của khóa.

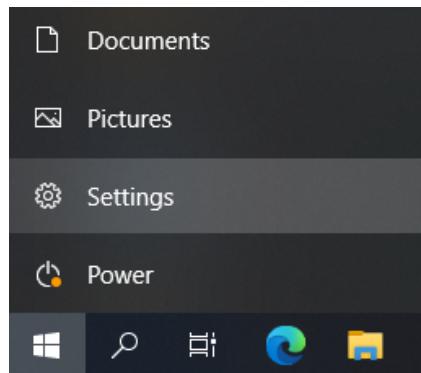


#### Lưu ý:

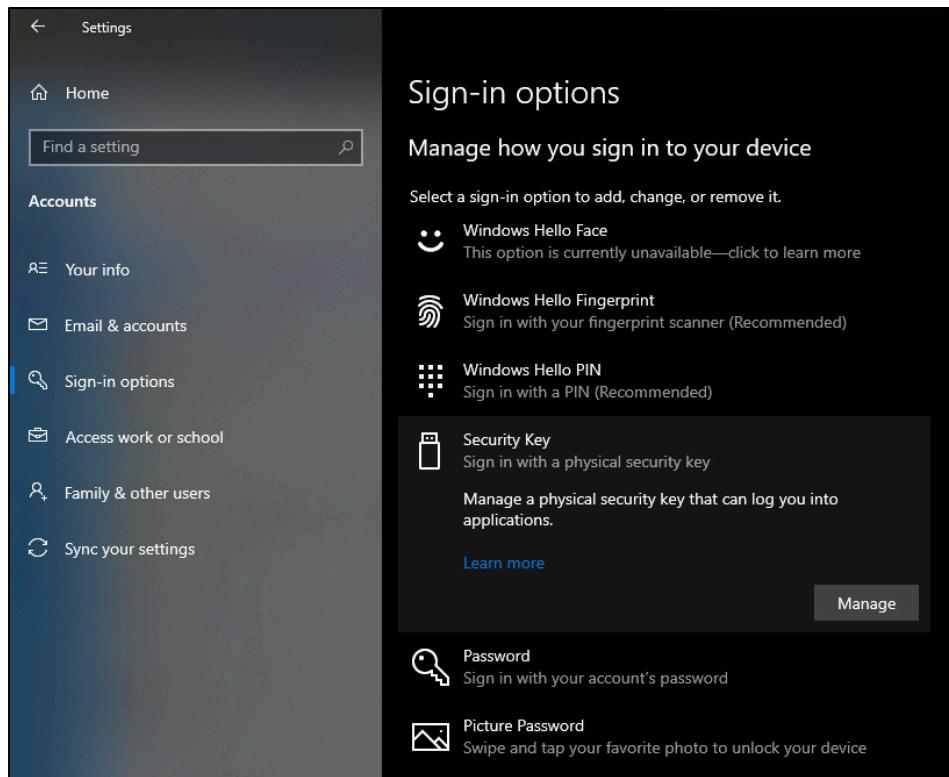
- Trong trường hợp muốn ghép nối với thiết bị mới, thực hiện nhấn giữ cảm biến vân tay trong vòng 5 giây khi khóa xác thực đang được bật.
- Nếu không có hoạt động xác thực trong 90 giây, đèn LED sẽ tắt, khóa tự chuyển vào chế độ Sleep.

#### II.1.2. Tạo mã PIN mới

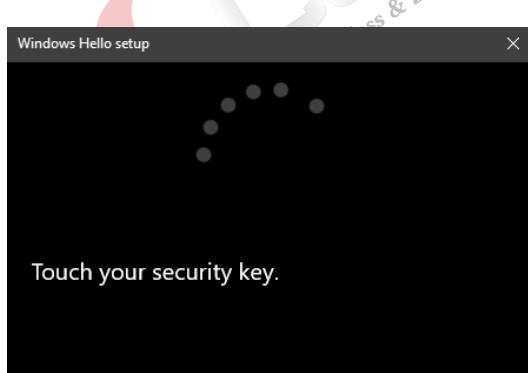
- Truy cập Start > Settings.



- Chọn Account > Sign-in options > Security Key, sau đó nhấn Manage.



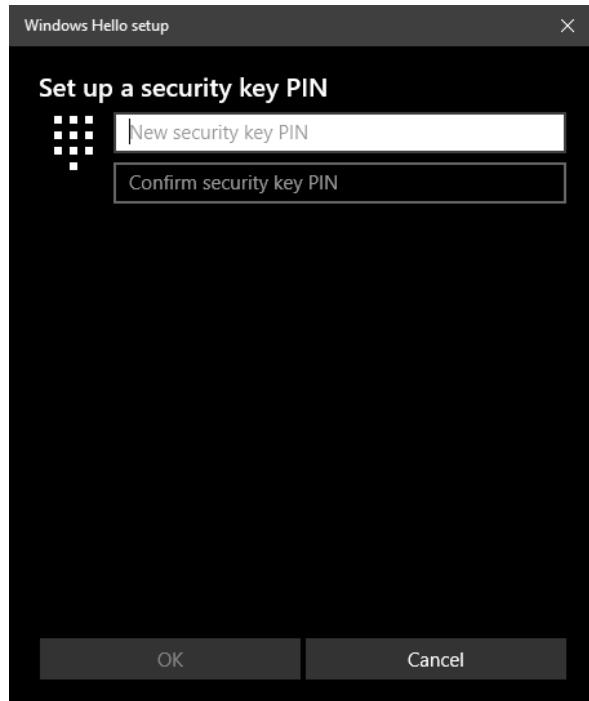
- **Chạm** vào cảm biến vân tay trên khóa bảo mật VinCSS FIDO2® Fingerprint.



- Mặc định ban đầu, khóa bảo mật VinCSS FIDO2® Fingerprint mới sẽ không có mã PIN. Hoặc trong trường hợp sau khi thiết lập cài đặt gốc, người dùng sẽ phải tạo mới mã PIN. Để tạo mới mã PIN, tại mục **Security Key PIN**, nhấn vào Add.

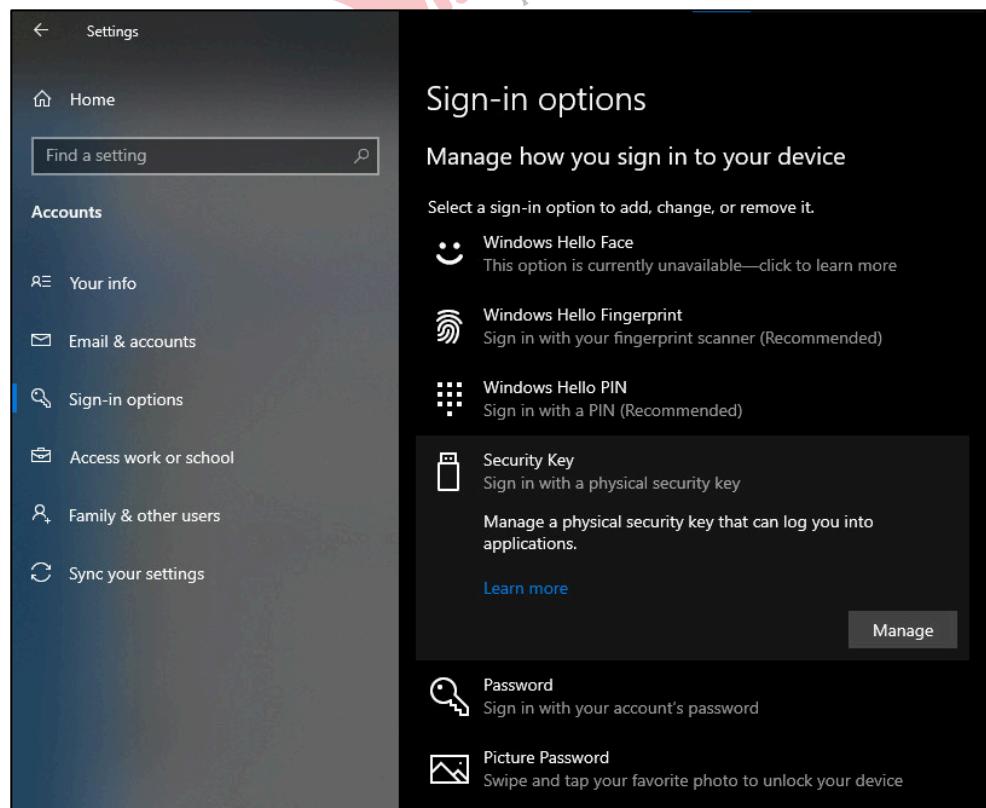


- Điền vào thông tin mã PIN mới (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*), sau đó chọn **OK**.

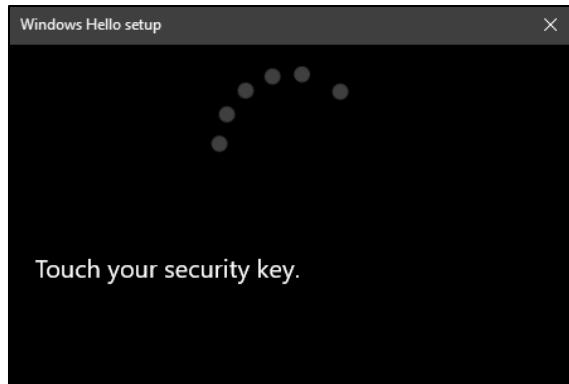


### II.1.3. Thay đổi mã PIN

- Truy cập Start > Settings > Account > Sign-in options > Security Key. Sau đó chọn **Manage**.



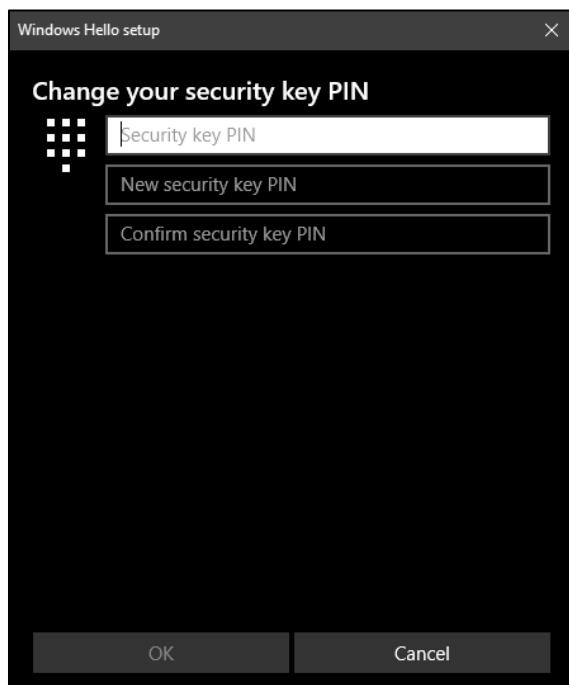
- **Chạm vào cảm biến vân tay trên khóa bảo mật.**



- Tại mục **Security Key PIN**, nhấn **Change** để thay đổi mã PIN của khóa bảo mật.



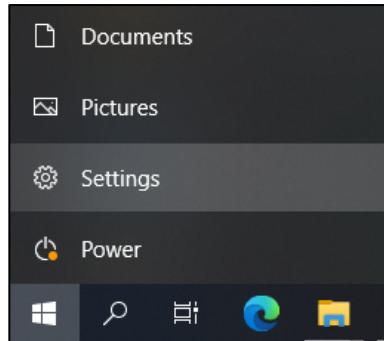
- Điền các thông tin theo thứ tự: mã PIN cũ, mã PIN mới, xác nhận mã PIN mới (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*). Sau đó nhấn **OK**.



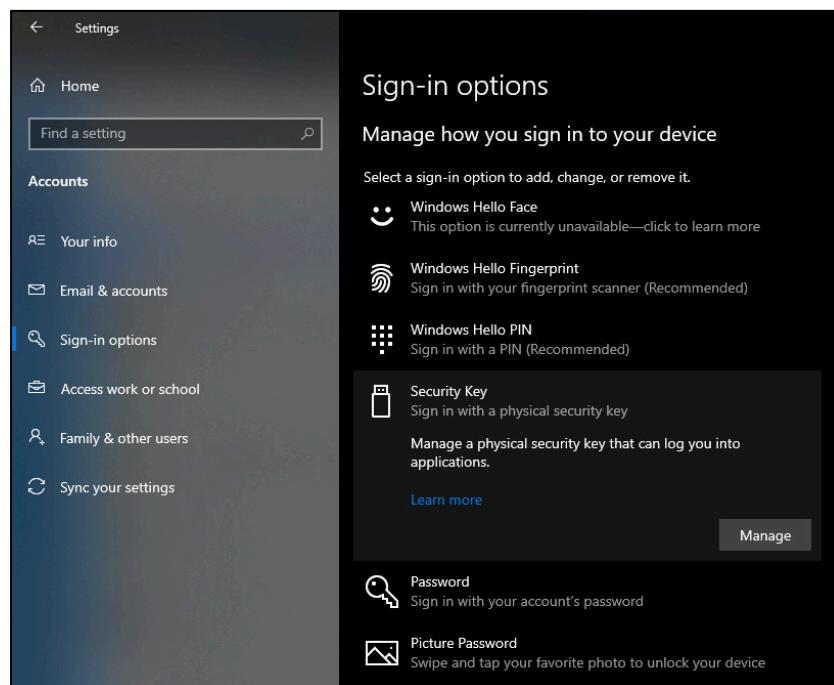
## II.1.4. Thêm vân tay

Sau khi tạo mã PIN cho VinCSS FIDO2® Fingerprint thành công, người dùng có thể thêm vân tay cho thiết bị (*tối đa 5 vân tay*). Thực hiện các bước sau:

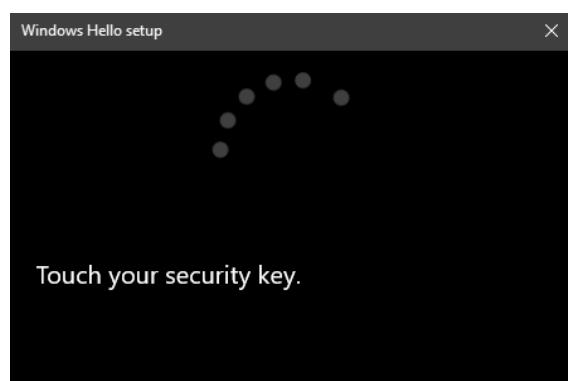
- Truy cập Start > Settings.



- Chọn Account > Sign-in options > Security Key. Sau đó chọn Manage.



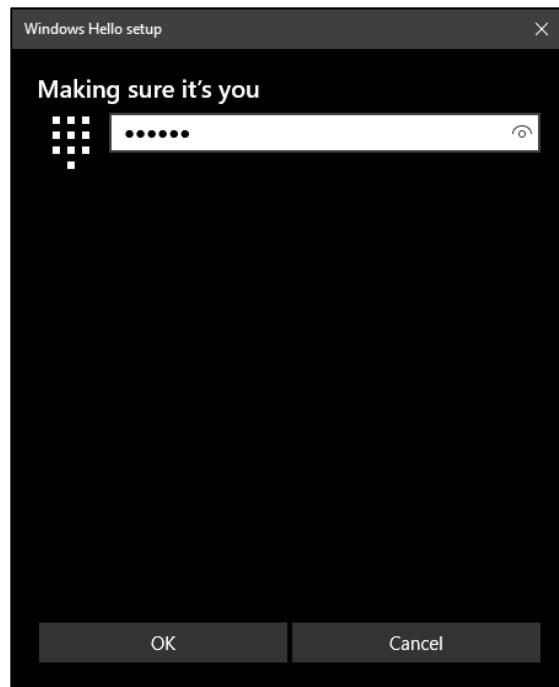
- Chạm vào cảm biến vân tay trên khóa bảo mật.



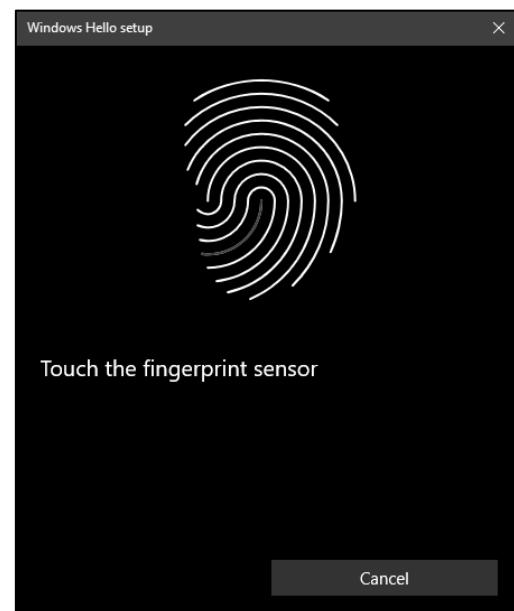
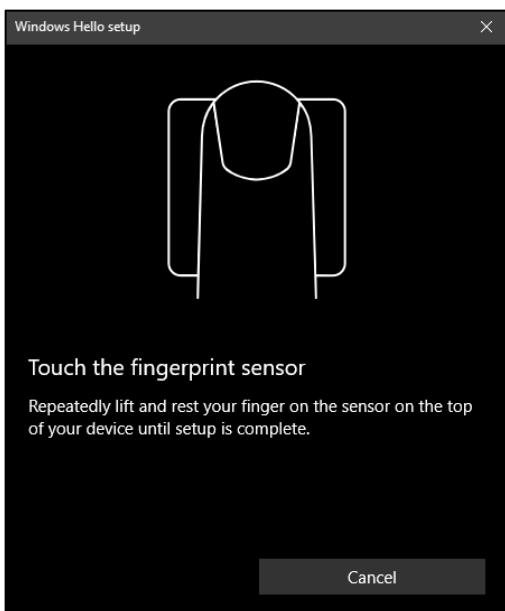
- Tại mục **Security Key Fingerprint**, nhấn **Set up**.



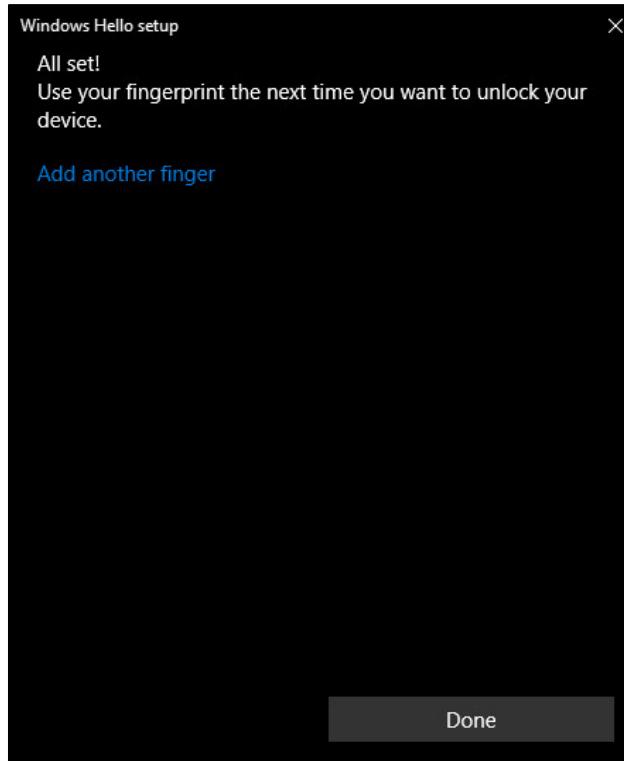
- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **OK**.



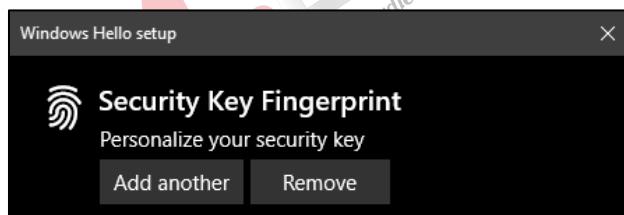
- Quét vân tay bằng cách chạm ngón tay vào vùng cảm biến vân tay của khoá bảo mật cho đến khi đèn hiển thị màu xanh lá, sau đó nhấc tay ra khỏi vùng cảm biến (*thực hiện 5 lần*).



- Sau khi quét xong vân tay, nhấn **Done** để kết thúc.



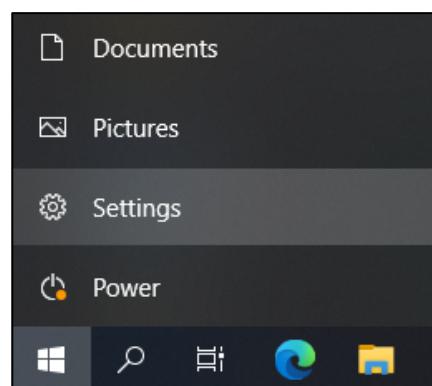
- Để thêm vân tay khác, tại mục **Security Key Fingerprint**, chọn **Add another**, sau đó thực hiện các bước tương tự như trên.



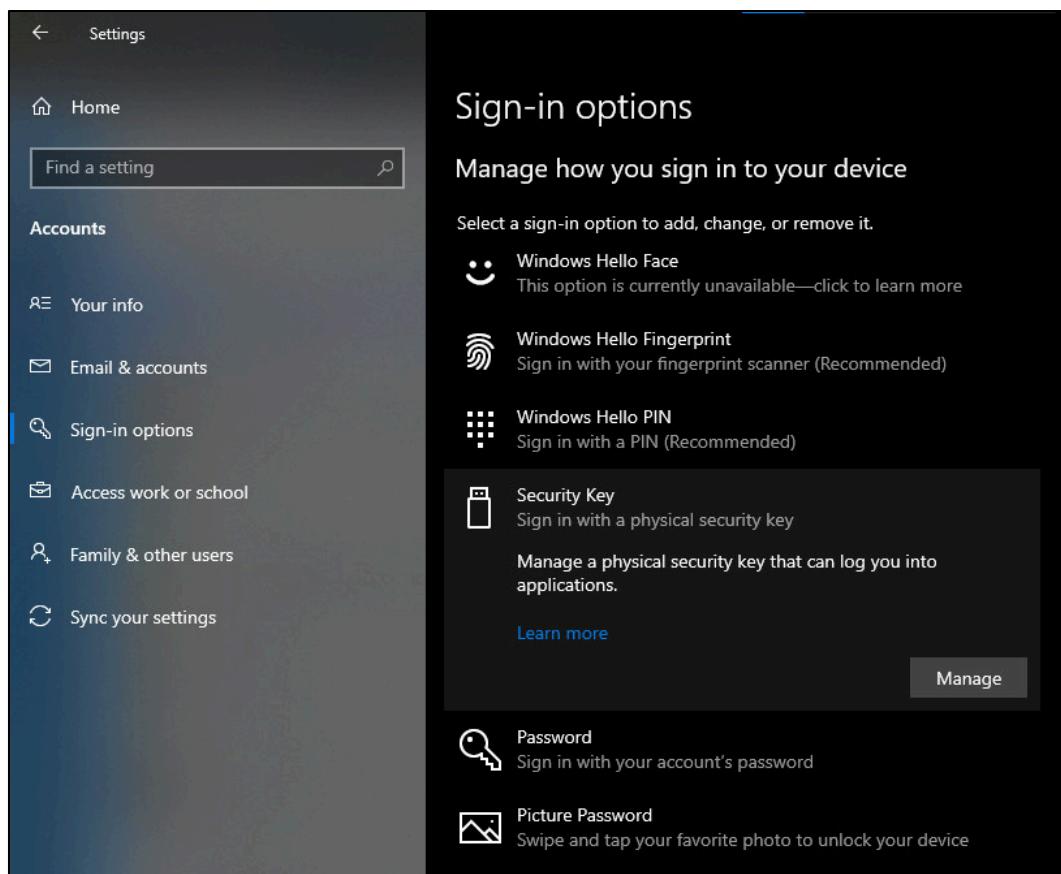
### II.1.5. Xóa vân tay

Hiện hệ điều hành Windows chưa hỗ trợ xóa từng dấu vân tay trên khóa bảo mật, chỉ có thể xóa toàn bộ dấu vân tay. Các bước thực hiện như sau:

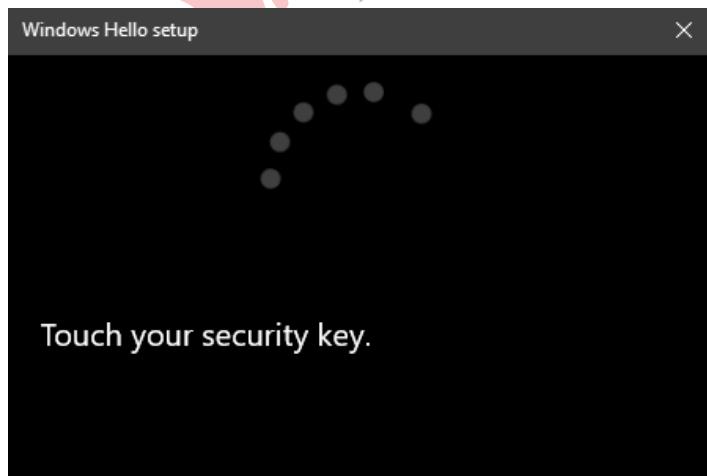
- Truy cập Start > Settings.



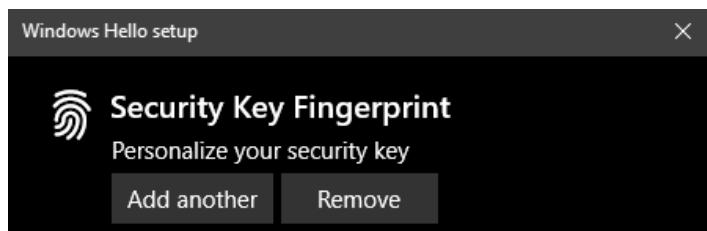
- Chọn Account > Sign-in options > Security Key, sau đó chọn Manage.



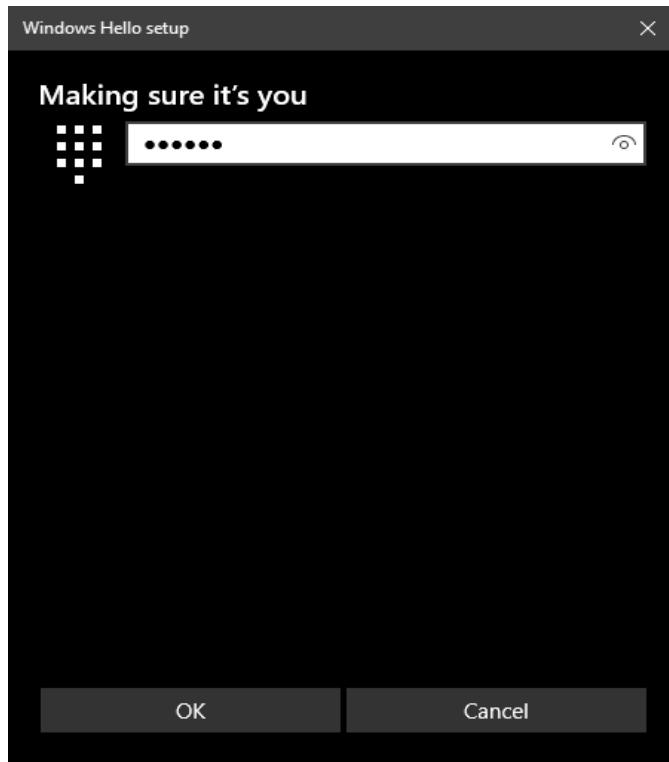
- Chạm vào cảm biến vân tay trên khóa bảo mật.



- Tại mục Security Key Fingerprint, chọn Remove.



- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **OK**.

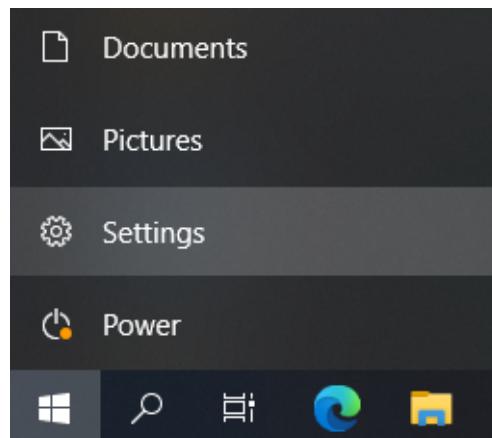


### II.1.6. Thiết lập cài đặt gốc

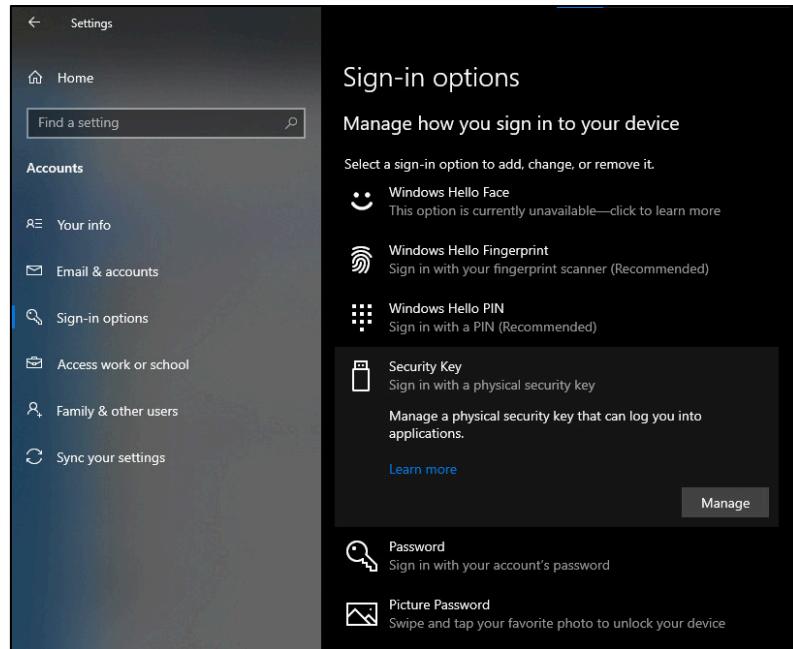
Trong trường hợp quên mã PIN của VinCSS FIDO2® Fingerprint, người dùng có thể reset thiết bị, tuy nhiên điều này sẽ khiến các dịch vụ đã đăng ký trước đó không thể xác thực được. Sau khi reset, thiết bị trở thành khóa bảo mật mới, vì vậy cần đăng ký lại các dịch vụ để có thể xác thực. Trong trường hợp nhập sai mã PIN nhiều lần (*trên 8 lần*) thì thiết bị sẽ bị khóa vĩnh viễn, người dùng bắt buộc phải reset để có thể sử dụng lại khóa bảo mật VinCSS FIDO2® Fingerprint như một thiết bị mới.

Để reset VinCSS FIDO2® Fingerprint, người dùng thực hiện các bước sau:

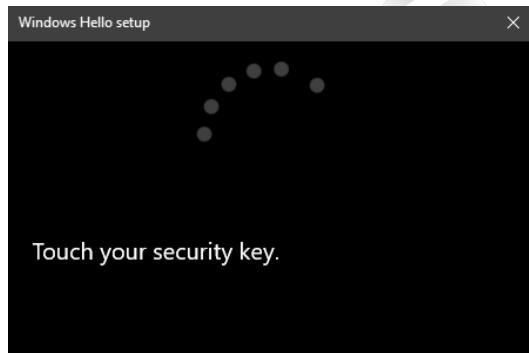
- Truy cập Start > Settings.



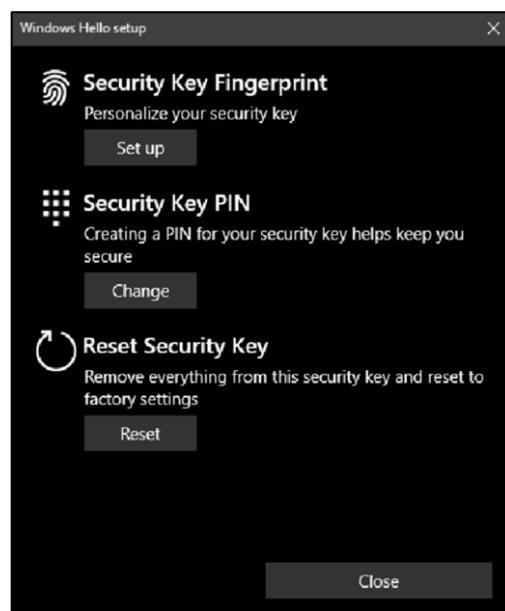
- Chọn Account > Sign-in options > Security Key. Sau đó nhấn Manage.



- Chạm vào cảm biến vân tay trên khóa bảo mật.



- Tại mục Reset Security Key, nhấn Reset.



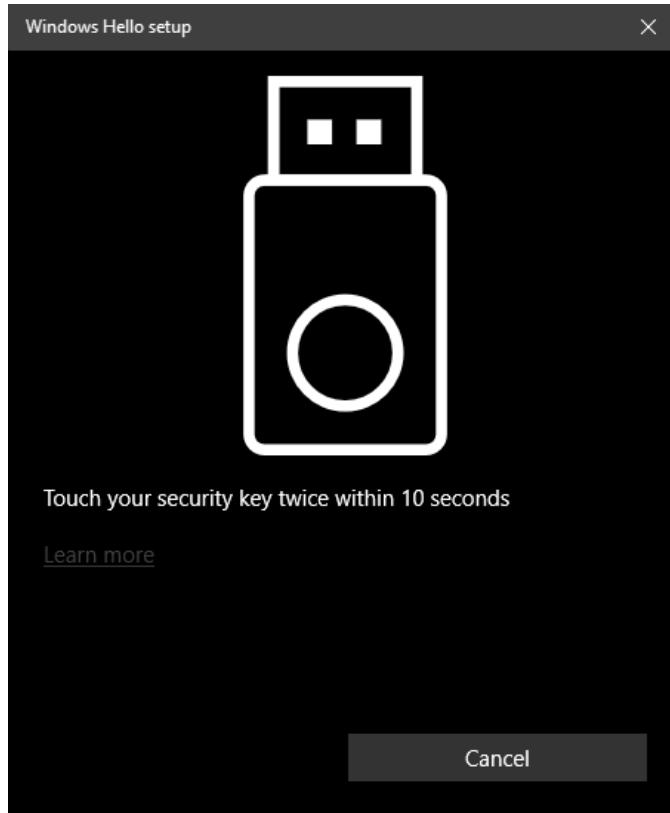
- Nhấn **Proceed** để tiến hành Reset khóa bảo mật VinCSS FIDO2® Fingerprint.



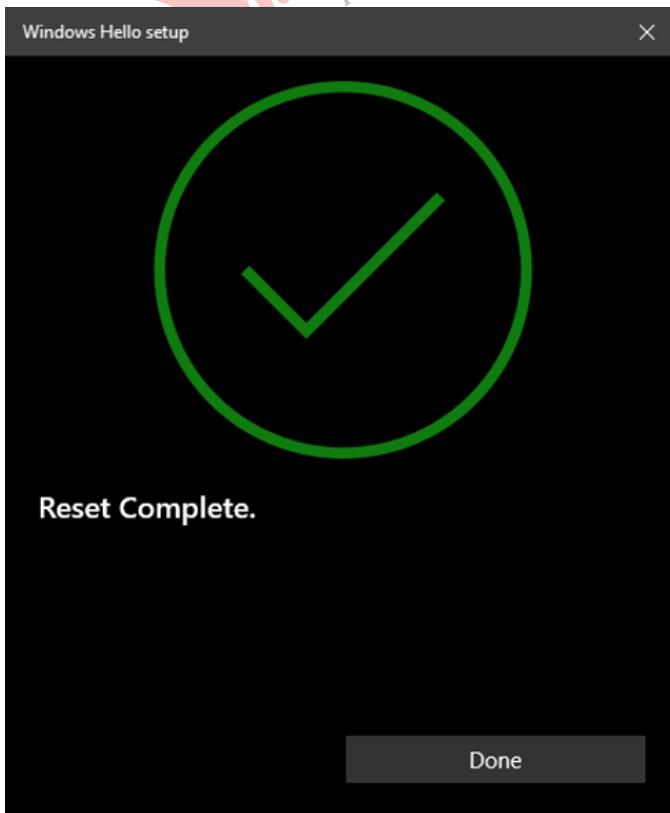
- Rút khóa bảo mật VinCSS FIDO2® Fingerprint ra khỏi máy tính, sau đó cắm lại.



- Khi hiện đèn màu trắng tay trên khóa bảo mật VinCSS FIDO2® Fingerprint, chạm 2 lần vào cảm biến vân tay trong 10s.



- Reset khóa bảo mật thành công, chọn **Done** để hoàn tất.



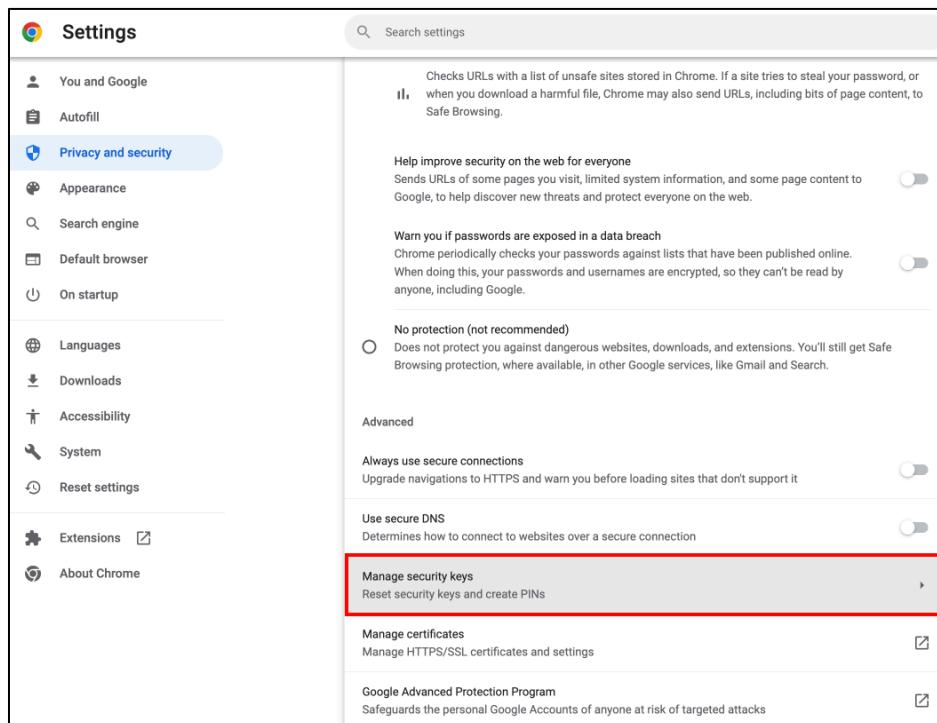
## II.2. Nền tảng macOS

### II.2.1. Kết nối với máy tính

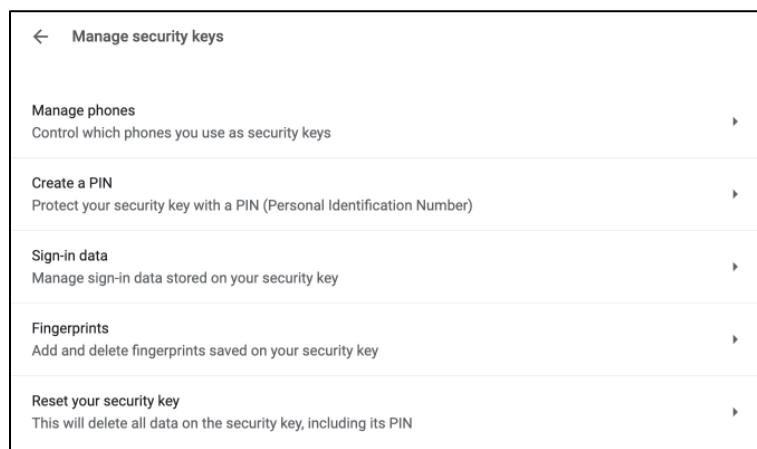
Tiến hành kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB. Nếu đèn LED nháy đỏ 3 lần liên tiếp cho biết mức pin đang ở dưới 20%, đèn LED màu hổ phách cho biết khoá bảo mật đang được sạc, đèn LED màu xanh lá cây cho biết pin đã được sạc đầy. Khoá bảo mật VinCSS FIDO2® Fingerprint có thể được sử dụng khi đang sạc.

### II.2.2. Tạo mới mã PIN

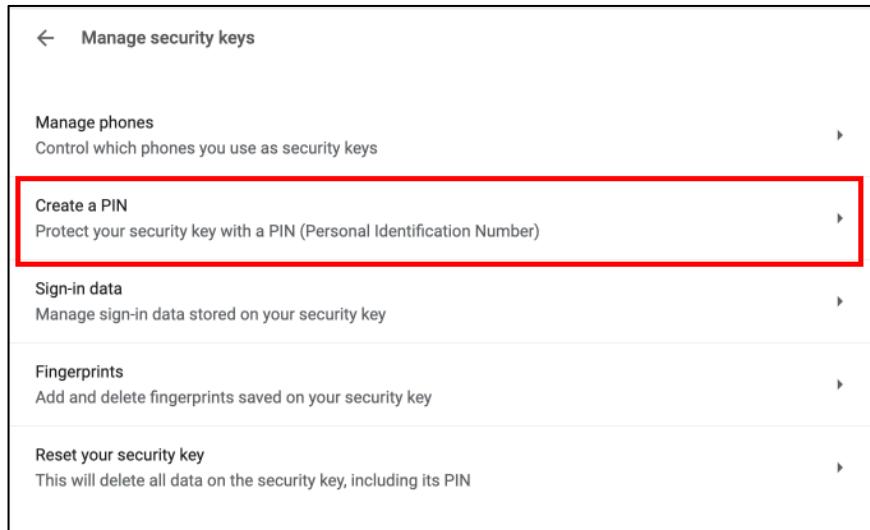
- Mở trình duyệt Chrome, chọn **Setting > Privacy and security > Security > Manage security keys.**



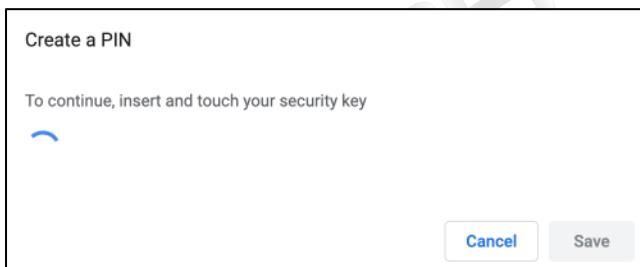
- Giao diện **Manage security keys** được mở lên.



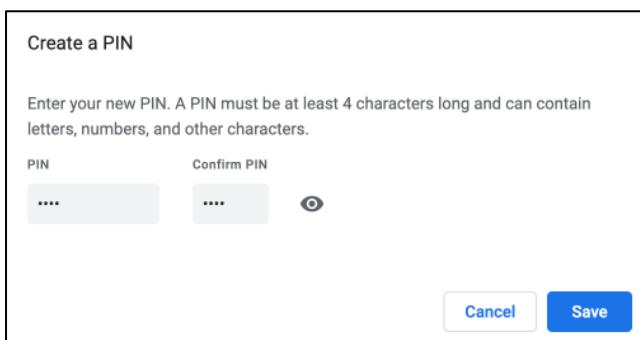
- Mặc định ban đầu, khóa bảo mật VinCSS FIDO2® Fingerprint không có mã PIN. Hoặc trong trường hợp sau khi thiết lập cài đặt gốc, người dùng sẽ phải tạo mới mã PIN. Để tạo mới mã PIN, trên giao diện **Manage security keys**, chọn **Create a PIN**.



- Chạm vào cảm biến vân tay trên VinCSS FIDO2® Fingerprint để xác nhận.



- Nhập mã PIN (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*) và xác nhận lại rồi nhấn **Save** để tạo mã PIN.

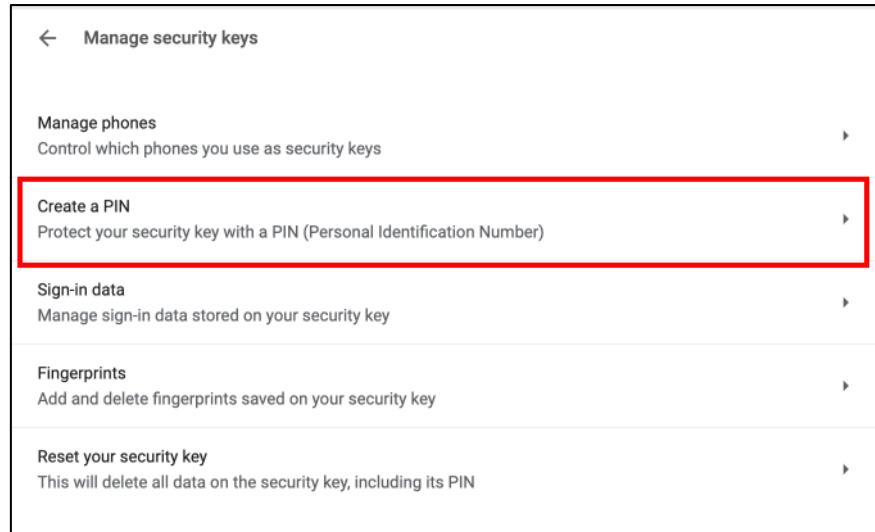


- Nhấn **OK** để hoàn thành việc tạo mã PIN cho khoá bảo mật.

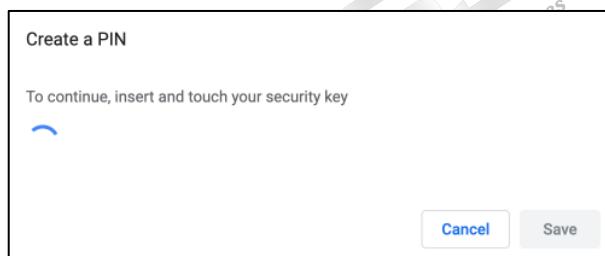


### II.2.3. Thay đổi mã PIN

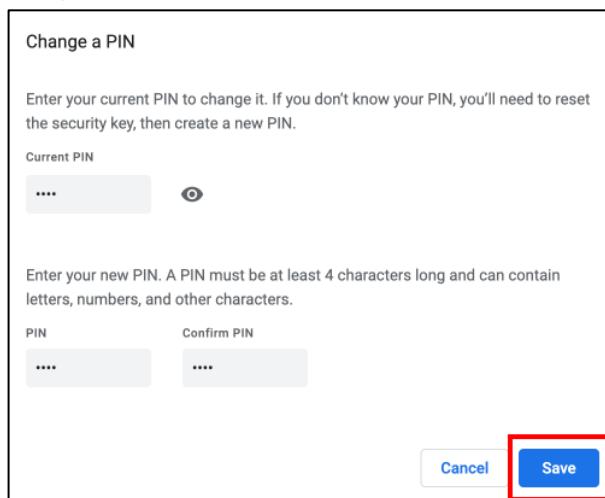
- Để thay đổi mã PIN cho VinCSS FIDO2® Fingerprint, trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Create a PIN**.



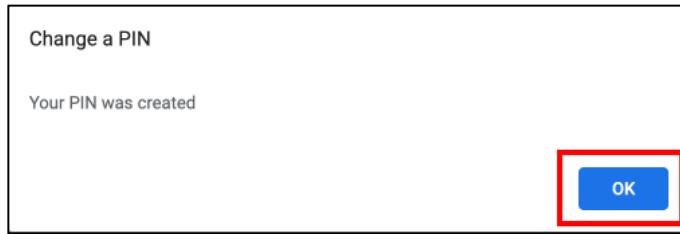
- Chạm vào cảm biến vân tay trên thiết bị để xác nhận.



- Tại cửa sổ **Change a PIN** nhập mã PIN hiện tại đang sử dụng, ở phía dưới nhập mã PIN mới cần thay đổi và xác nhận lại (*Tối thiểu 4 ký tự, tối đa 63 ký tự; bao gồm chữ (chữ thường, chữ hoa), số và ký tự đặc biệt*), sau đó chọn **Save** để thay đổi.



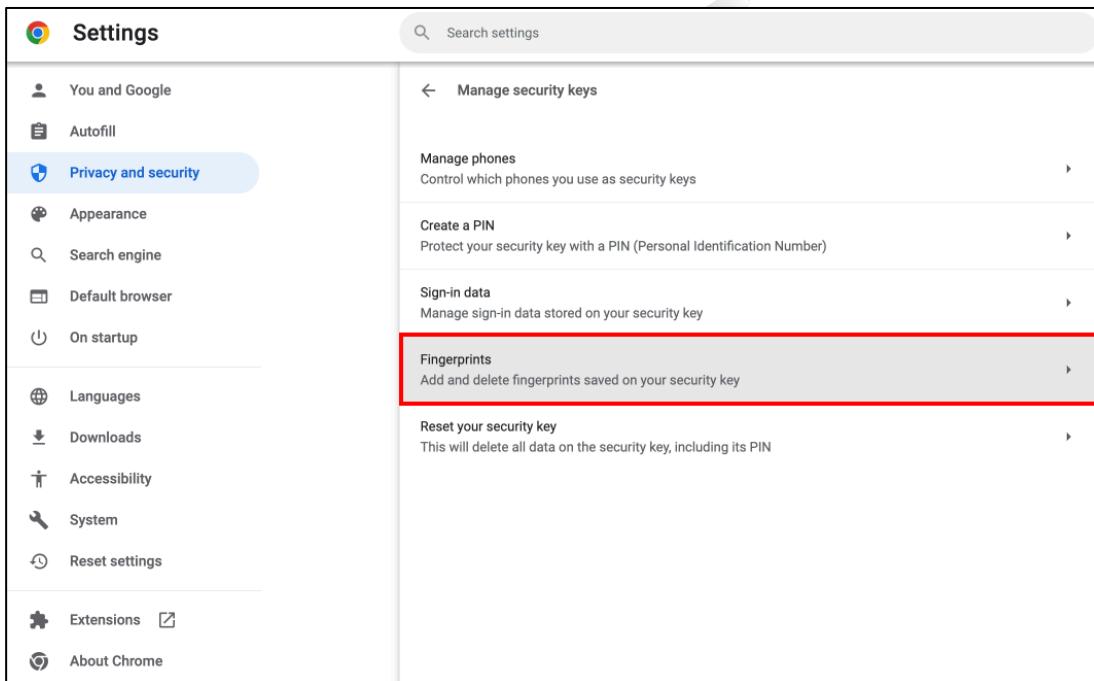
- Nhấn **OK** để hoàn thành việc thay đổi mã PIN cho VinCSS FIDO2® Fingerprint.



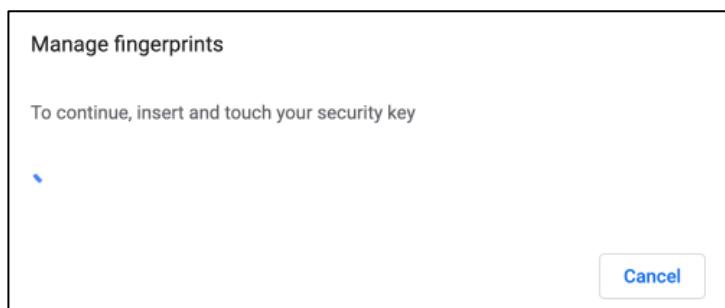
#### II.2.4. Thêm vân tay

Sau khi tạo mã PIN cho VinCSS FIDO2® Fingerprint thành công, người dùng có thể thêm vân tay cho thiết bị (*tối đa 5 vân tay*). Thực hiện các bước sau:

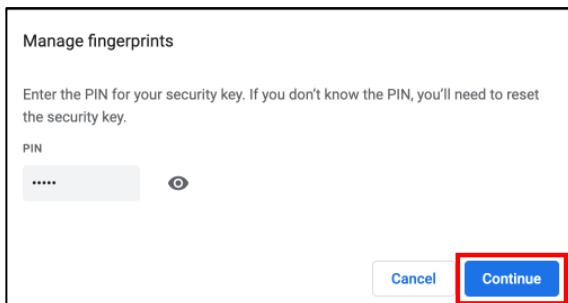
- Trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Fingerprints**.



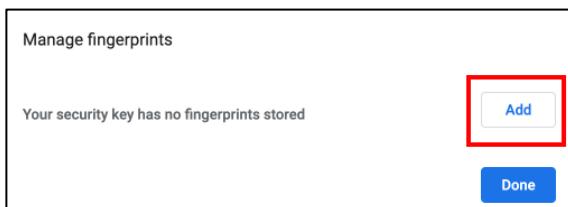
- Chạm vào cảm biến vân tay trên khóa bảo mật.



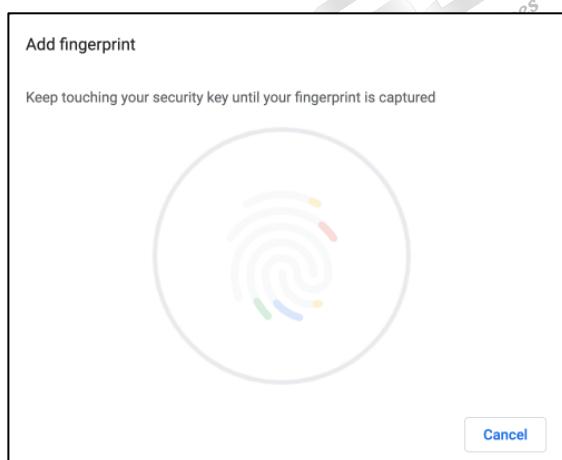
- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **Continue** để tiếp tục.



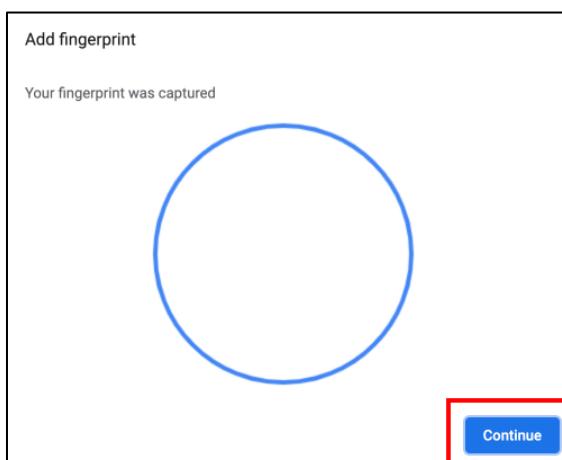
- Để thêm vân tay cho khóa bảo mật, nhấn **Add**.



- Khi thiết bị nháy đèn trắng, tiến hành quét vân tay bằng cách chạm ngón tay vào cảm biến vân tay cho đến khi đèn hiển thị màu xanh lá, sau đó nhấc tay ra khỏi cảm biến (*thực hiện 5 lần*).



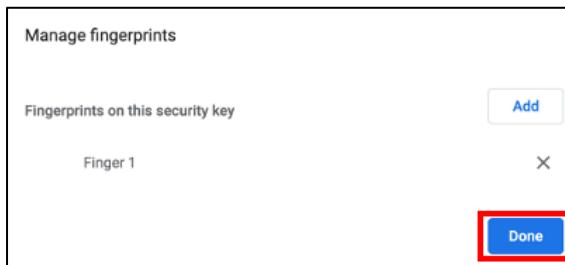
- Sau khi quét xong vân tay, nhấn **Continue** để tiếp tục.



- Đặt tên cho vân tay (*tối đa 30 ký tự không dấu*), sau đó nhấn **Continue** để tiếp tục.

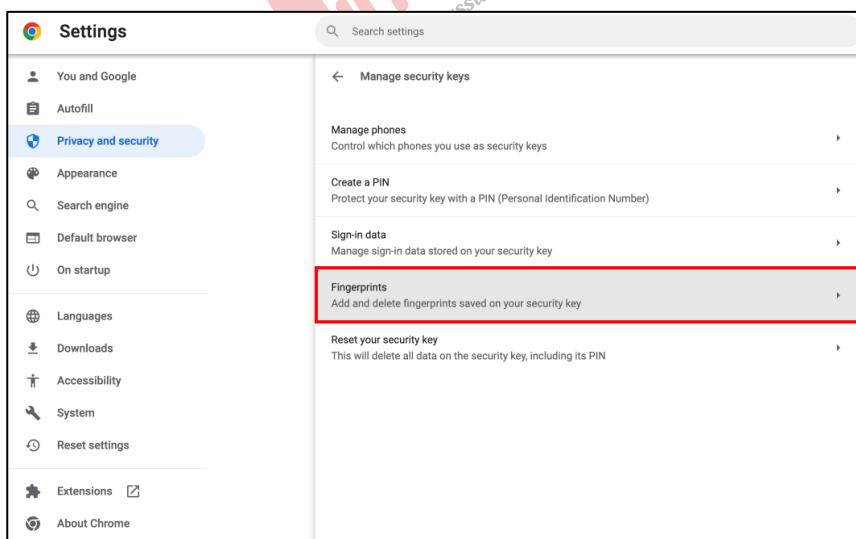


- Nhấn **Add** để tiếp tục thêm vân tay, hoặc nhấn **Done** để kết thúc.

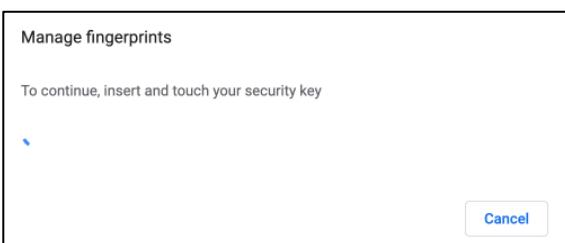


## II.2.5. Xóa vân tay

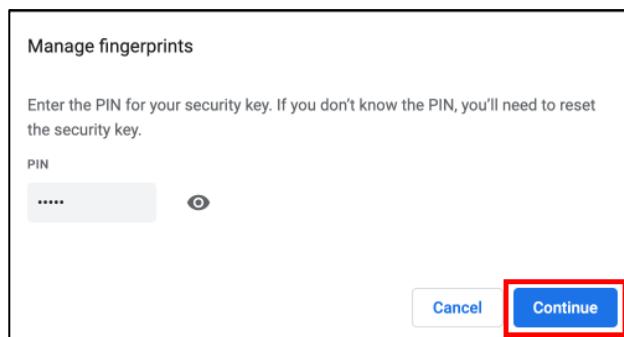
- Trên giao diện **Manage security keys** (mở trình duyệt Chrome, chọn **Setting > Privacy and security > Security > Manage security keys**), chọn **Fingerprints**.



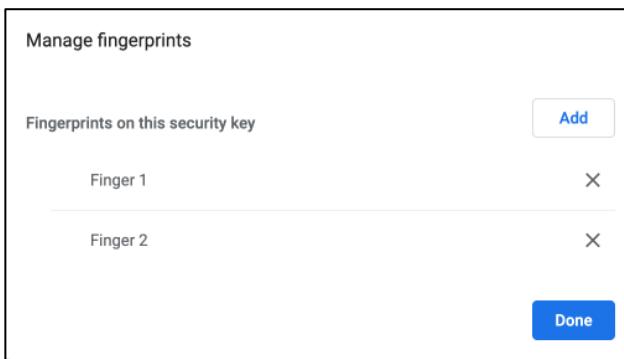
- Chạm vào cảm biến vân tay trên khóa xác thực.



- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **Continue** để tiếp tục.

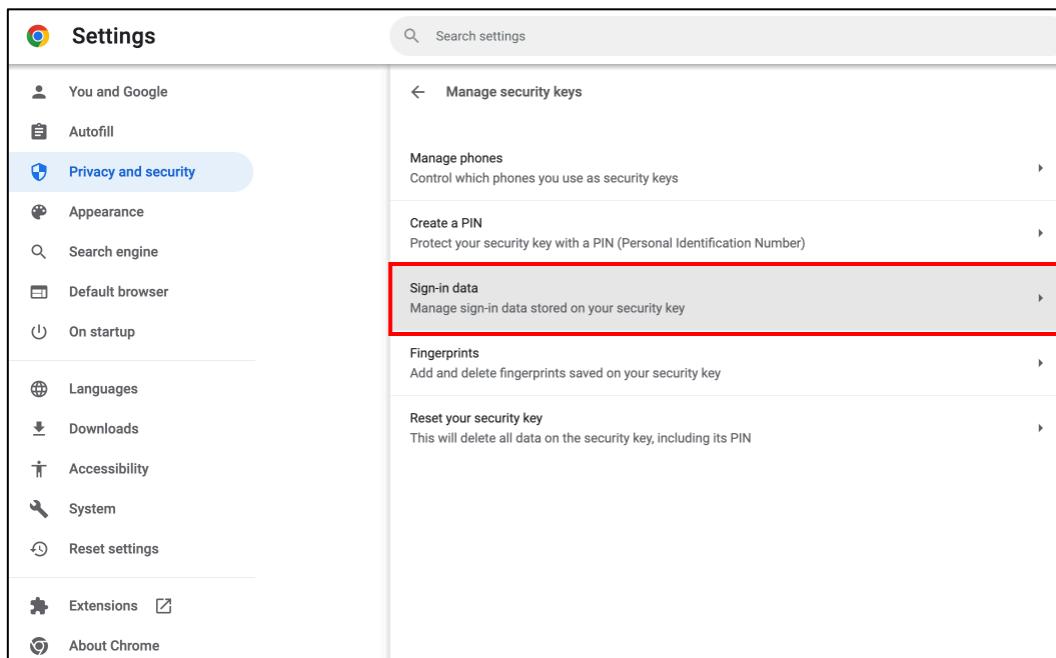


- Trên màn hình sẽ hiển thị danh sách vân tay đã được đăng ký trên khóa bảo mật. Nhấn vào biểu tượng chữ “X” tại mỗi vân tay tương ứng để xóa vân tay đã đăng ký.

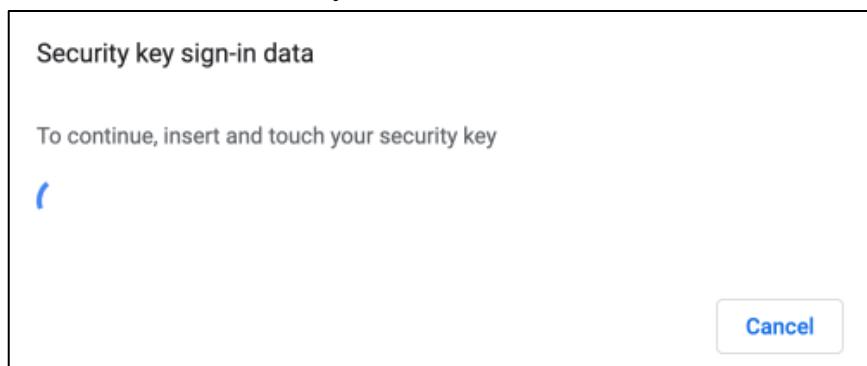


## II.2.6. Quản lý dữ liệu đăng nhập

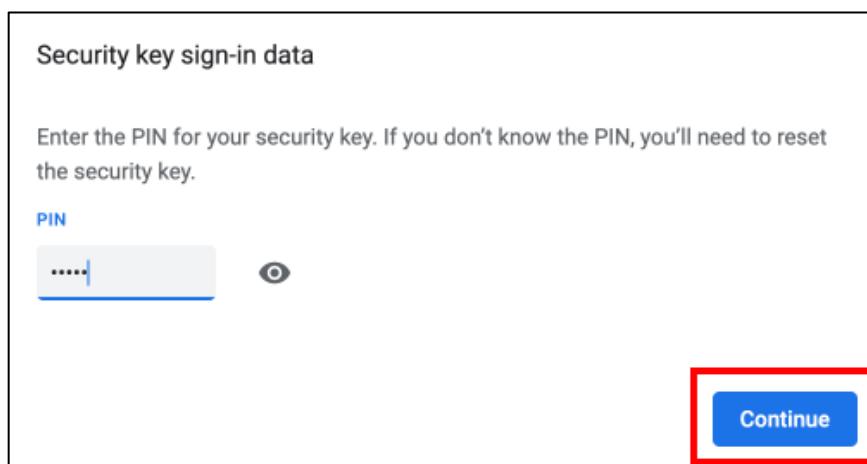
- Trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Sign-in data**.



- Chạm vào cảm biến vân tay trên khóa xác thực.



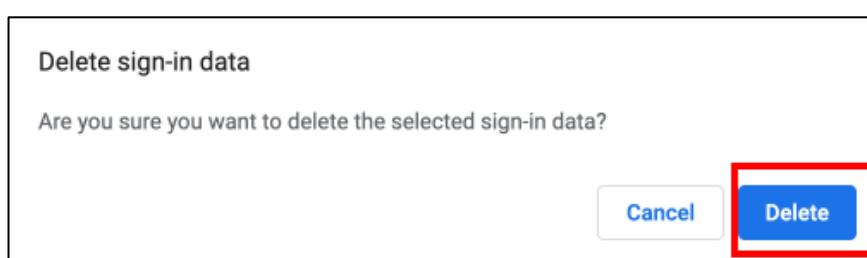
- Điền mã PIN (*đã tạo ở bước trên*), sau đó nhấn **Continue** để tiếp tục.



- Trên màn hình sẽ hiển thị danh sách dữ liệu đăng nhập, bao gồm tên website và tên đăng nhập.



- Để xóa dữ liệu đăng nhập, nhấn chọn vào biểu tượng  ở cuối mỗi dòng. Hộp thoại **Delete sign-in data** hiện ra. Nhấn **Delete**.



- Hoàn thành quá trình xoá dữ liệu đăng nhập. Quay trở lại hộp thoại **Security key sign-in data**. Nhấn **Done** để kết thúc.

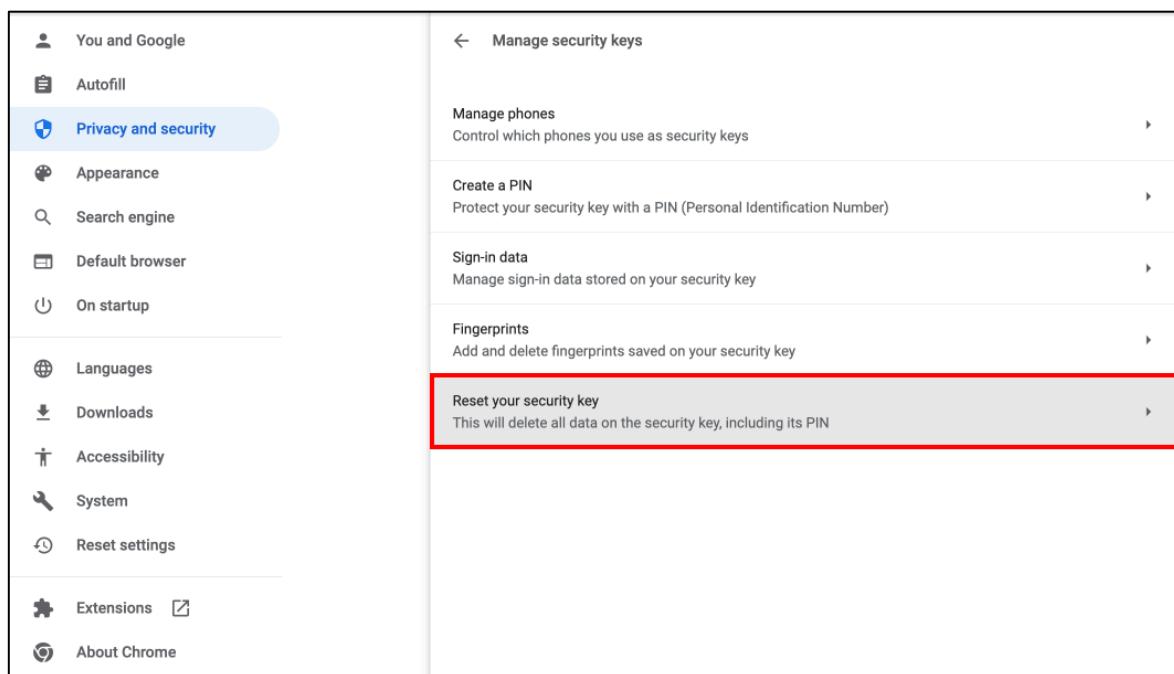


## II.2.7. Thiết lập cài đặt gốc

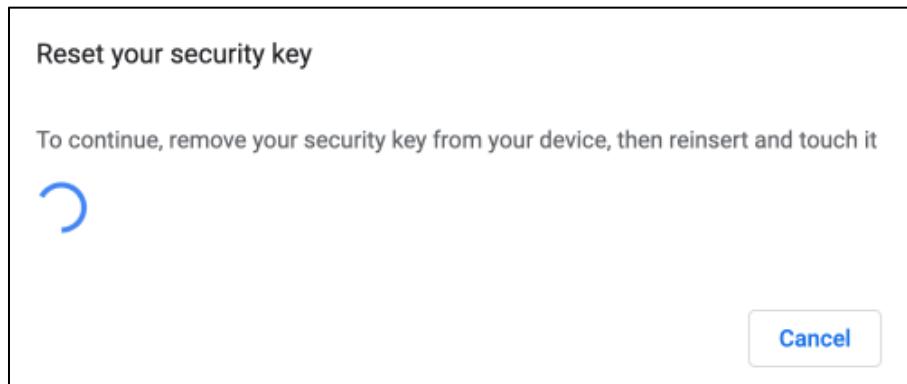
Trong trường hợp quên mã PIN của VinCSS FIDO2® Fingerprint, người dùng có thể reset thiết bị, tuy nhiên điều này sẽ khiến các dịch vụ đã đăng ký trước đó không thể xác thực được nữa. Sau khi reset, thiết bị trở thành khóa bảo mật mới, vì vậy cần đăng ký lại các dịch vụ để có thể xác thực. Trong trường hợp nhập sai mã PIN nhiều lần (*trên 8 lần*) thì thiết bị sẽ bị khóa vĩnh viễn, người dùng bắt buộc phải reset để có thể sử dụng lại khóa bảo mật VinCSS FIDO2® Fingerprint như một thiết bị mới.

Để reset VinCSS FIDO2® Fingerprint, thực hiện các bước sau:

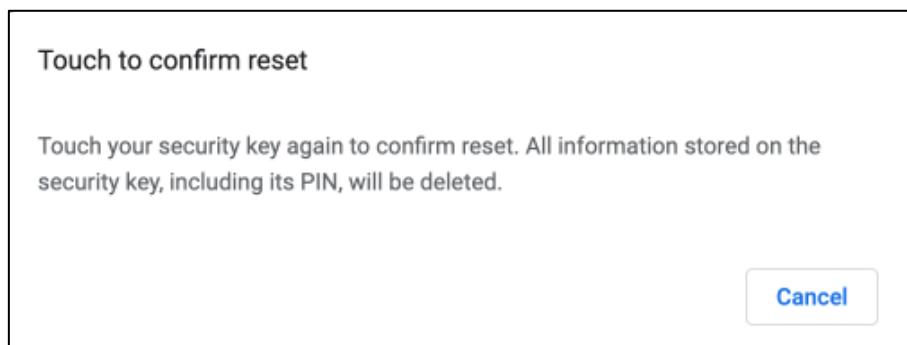
- Trên giao diện **Manage security keys** (*mở trình duyệt Chrome, chọn Setting > Privacy and security > Security > Manage security keys*), chọn **Reset your security key**.



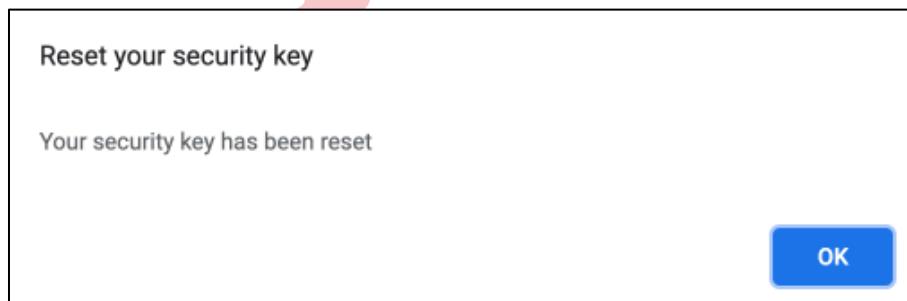
- Rút khoá bảo mật VinCSS FIDO2® Fingerprint ra khỏi máy tính và cắm lại. Chạm vào cảm biến vân tay trên khoá bảo mật để xác nhận.



- Chạm tiếp vào cảm biến vân tay trên VinCSS FIDO2® Fingerprint lần nữa để xác nhận việc reset VinCSS FIDO2® Fingerprint.



- Quá trình reset thành công. Nhấn OK để kết thúc.



### **III. XÁC THỰC KHÔNG MẬT KHẨU VỚI VINCSS FIDO2® FINGERPRINT**

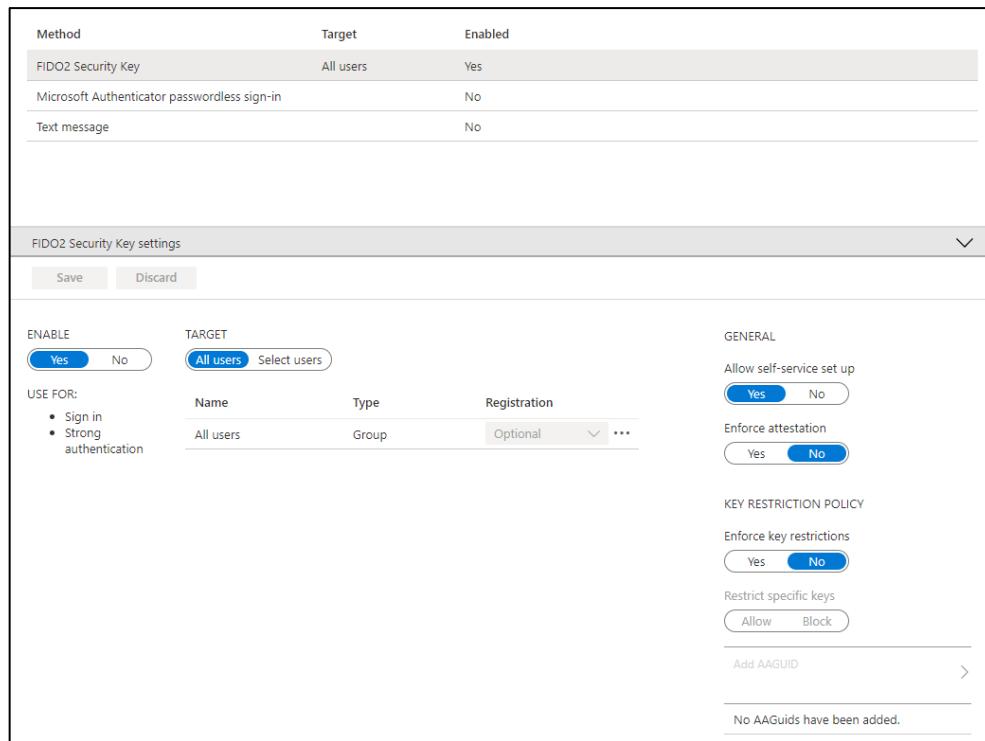
#### **III.1. Đăng nhập với Window 10**

##### **III.1.1. Cấu hình trên hệ thống Azure AD**

###### **III.1.1.1. Cấu hình Azure AD**

- Truy cập vào đường link sau: [https://portal.azure.com/-blade/Microsoft\\_AAD\\_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods](https://portal.azure.com/-blade/Microsoft_AAD_IAM/AuthenticationMethodsMenuBlade/AdminAuthMethods)

- Chọn Method FIDO2 Security Key, sau đó chọn các cấu hình như sau:

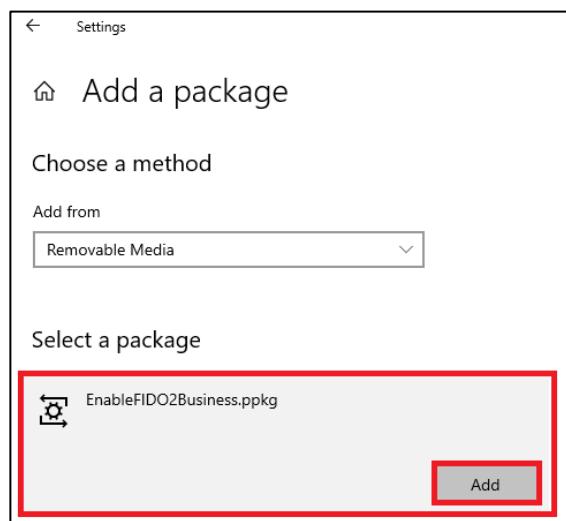


The screenshot shows the 'FIDO2 Security Key settings' page. At the top, there's a table with columns: Method, Target, and Enabled. The 'FIDO2 Security Key' row is selected, showing 'All users' as the target and 'Yes' as enabled. Below the table, there are sections for 'ENABLE' (set to 'Yes'), 'TARGET' (set to 'All users'), 'GENERAL' (allow self-service set up, Yes), 'KEY RESTRICTION POLICY' (enforce key restrictions, No), and 'Restrict specific keys' (Allow). A note at the bottom says 'No AAGuids have been added.'

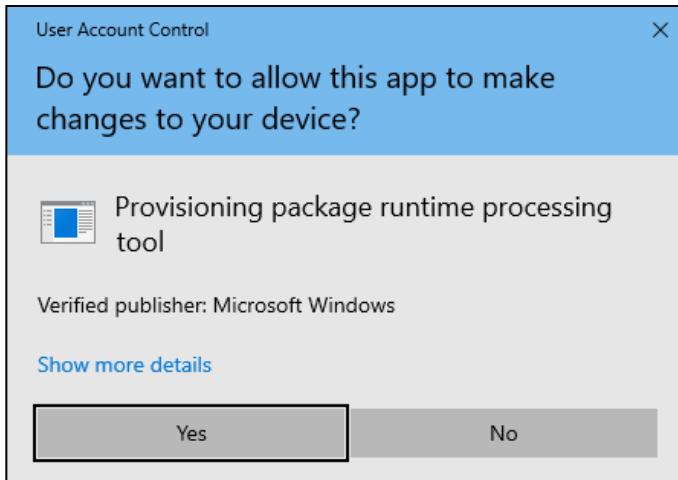
- Nhấn Save để lưu lại cấu hình.

### III.1.1.2. Đăng nhập Windows 10 sử dụng FIDO2 với provisioning packages

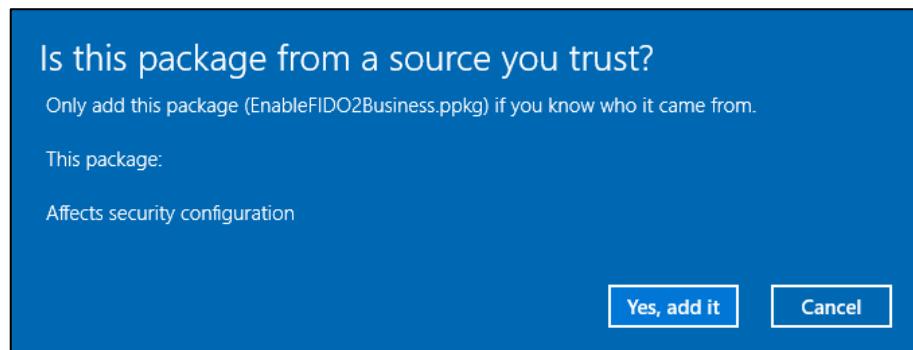
- Chuyển tải 2 file **EnableFIDO2Business.cat** và **EnableFIDO2Business.ppkg** được VinCSS cung cấp vào thiết bị lưu trữ.
- Kết nối thiết bị lưu trữ đó với máy tính cần kích hoạt tính năng FIDO2, sau đó truy cập vào **Settings > Accounts > Access work or school > Add or remove a provisioning package > Add a package**, chọn vào gói và nhấn **Add**.



- Chọn Yes.

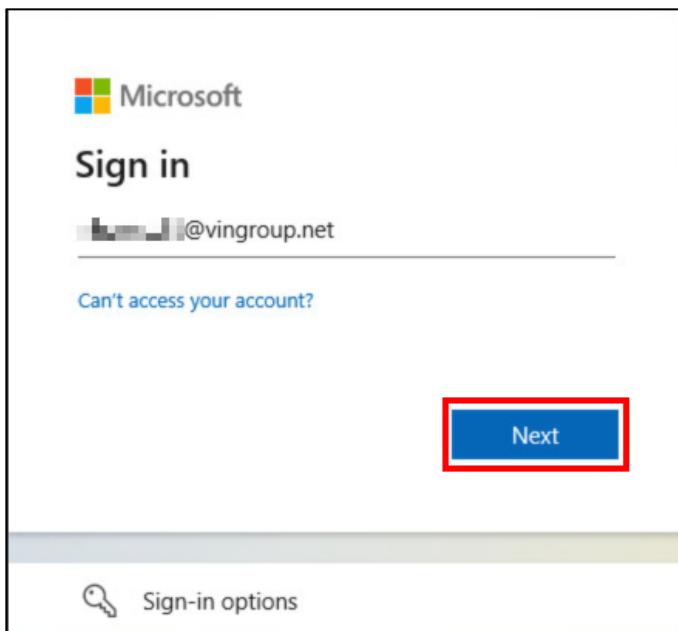


- Chọn Yes, add it.

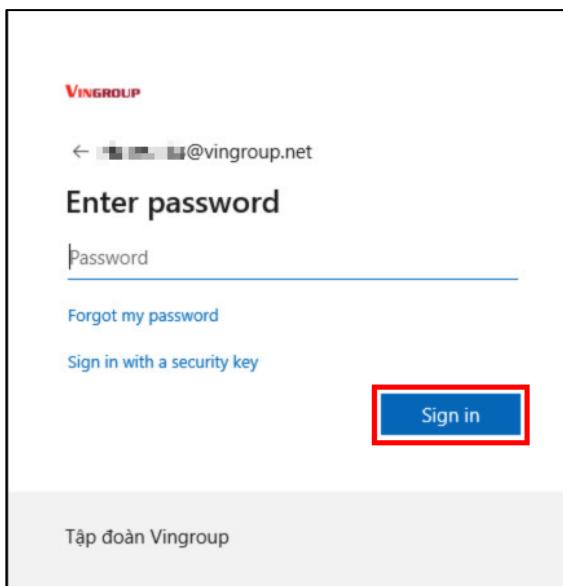


### III.1.1.3. Đăng ký khóa xác thực cho tài khoản Azure AD

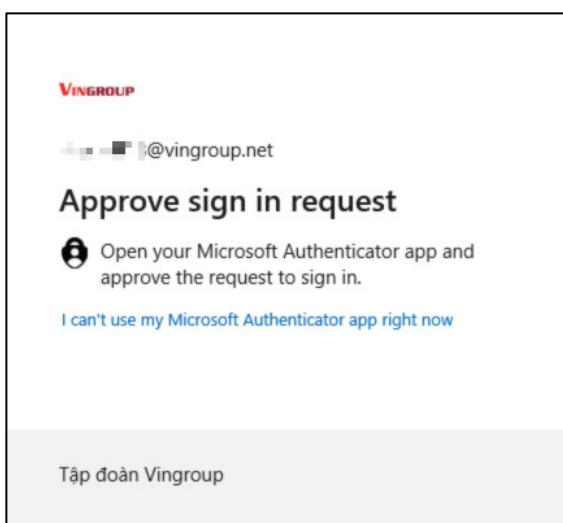
- Truy cập <https://myaccount.microsoft.com>, nhập thông tin tài khoản AD, sau đó nhấn Next.



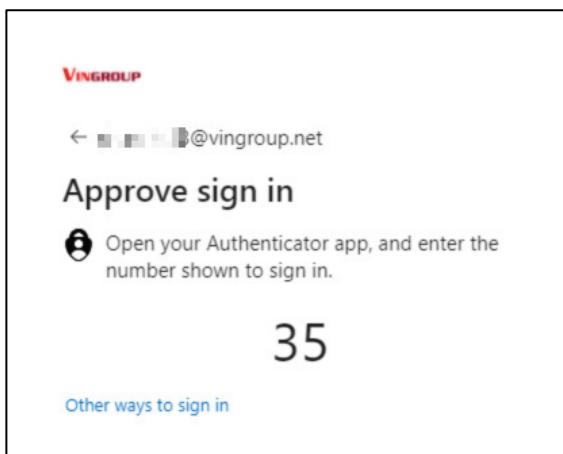
- Nhập mật khẩu của tài khoản AD rồi chọn **Sign in**.



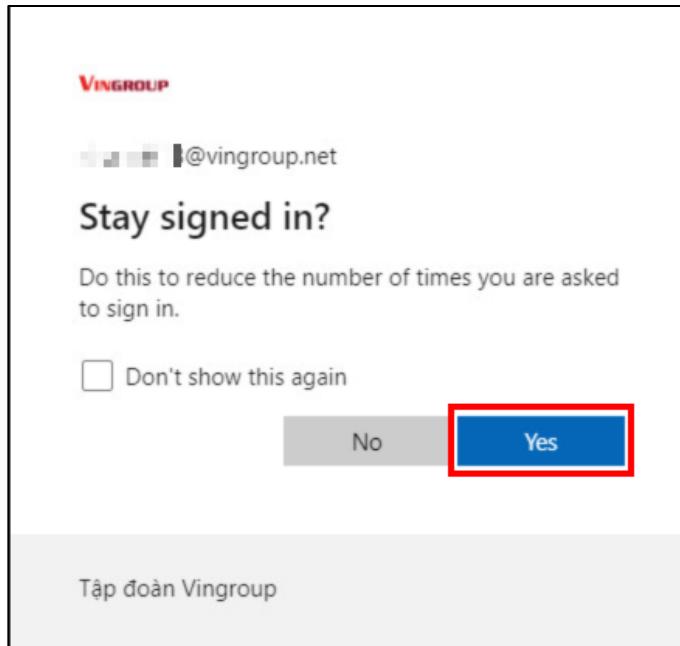
- Xác thực bằng ứng dụng Microsoft Authenticator trên điện thoại.



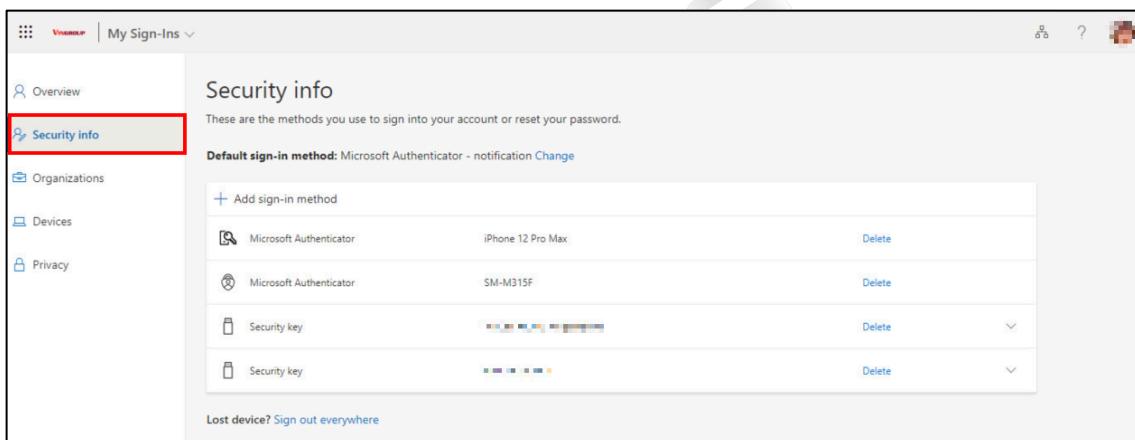
- Trên ứng dụng Authenticator, nhập vào điện thoại chữ số đã được hiển thị trên màn hình máy tính.



- Nhấn Yes để tiếp tục đăng nhập.

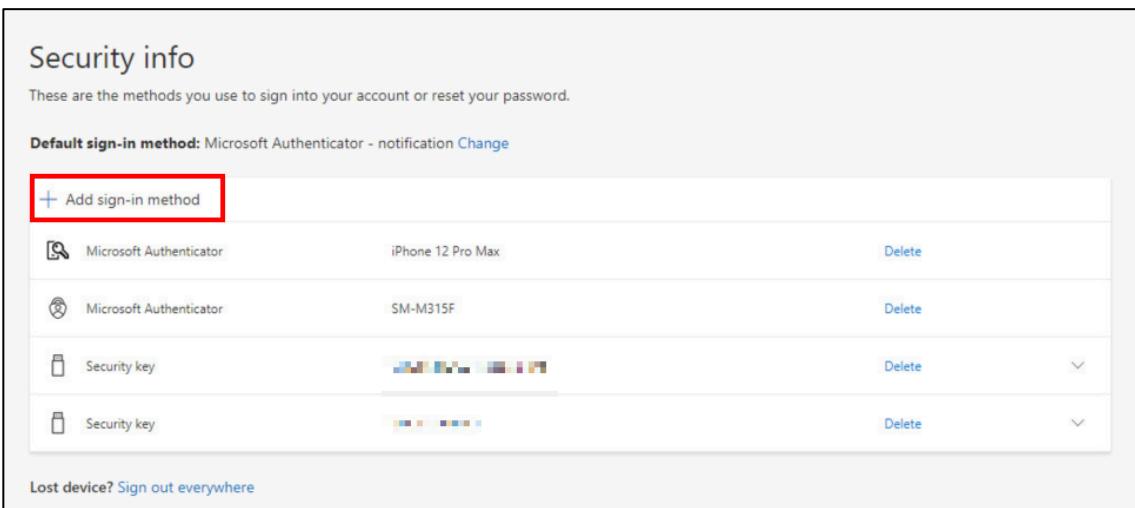


- Sau khi đăng nhập thành công, chọn My sign-ins > Security info.



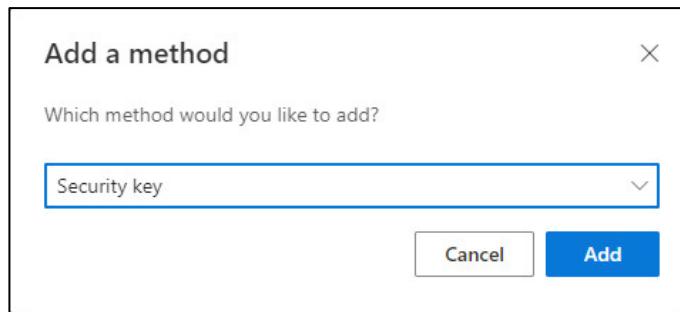
Type	Device	Action
Microsoft Authenticator	iPhone 12 Pro Max	Delete
Microsoft Authenticator	SM-M315F	Delete
Security key	[QR code]	Delete
Security key	[QR code]	Delete

- Chọn Add sign-in method để thêm phương thức bảo mật.



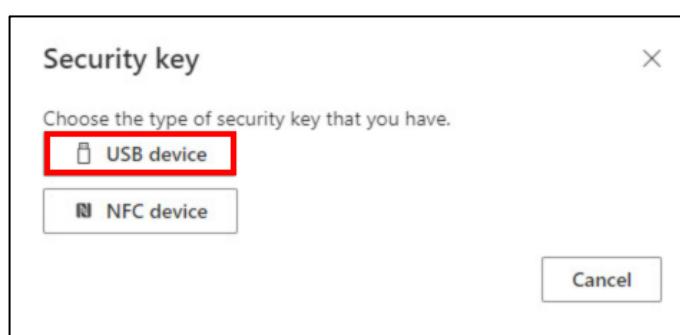
Type	Device	Action
Microsoft Authenticator	iPhone 12 Pro Max	Delete
Microsoft Authenticator	SM-M315F	Delete
Security key	[QR code]	Delete
Security key	[QR code]	Delete

- Hộp thoại **Add a method** hiện ra, chọn **Security key** rồi nhấn **Add**.

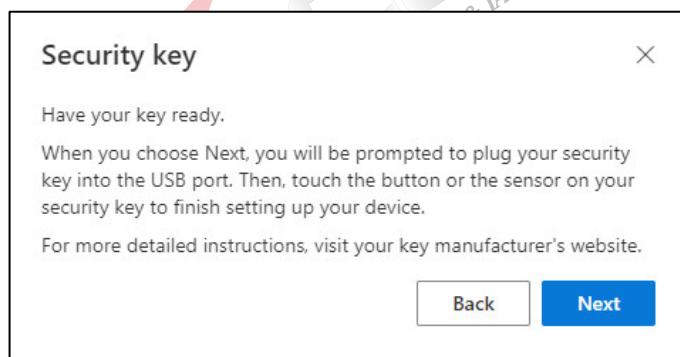


### III.1.1.3.1. Sử dụng qua kết nối Bluetooth

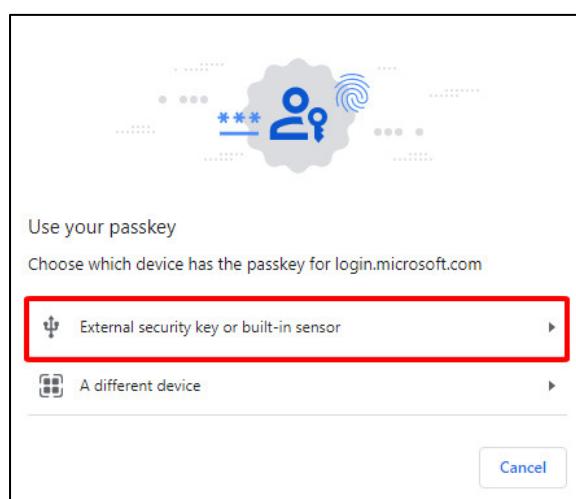
- Chọn **USB device**.



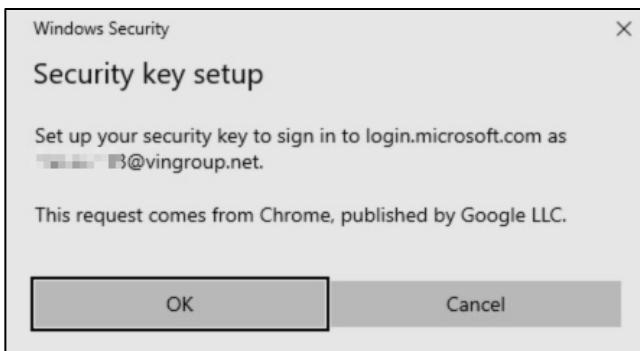
- Nhấn **Next** để tiếp tục.



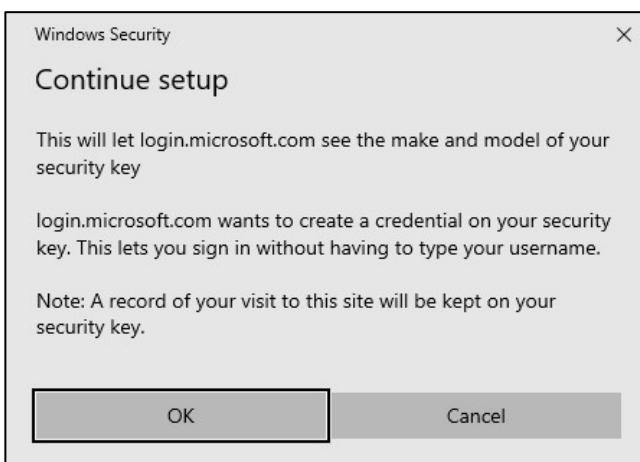
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



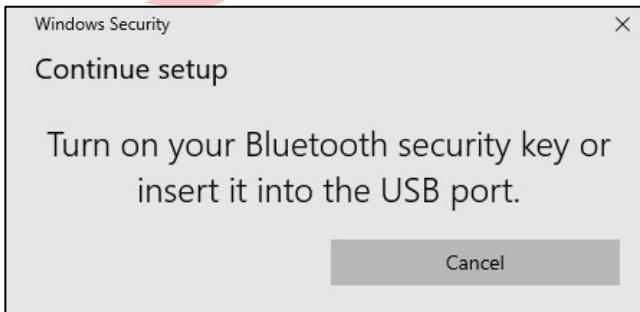
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



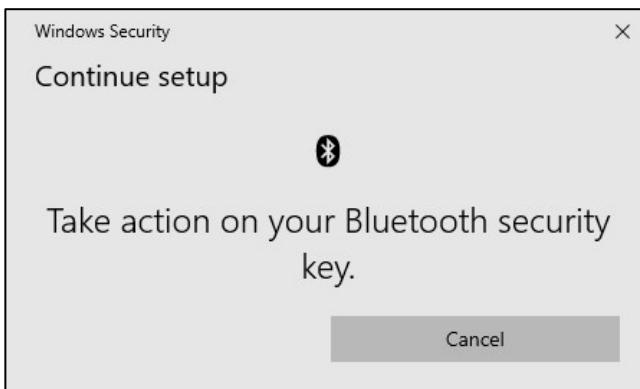
- Nhấn **OK** để tiếp tục.



- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

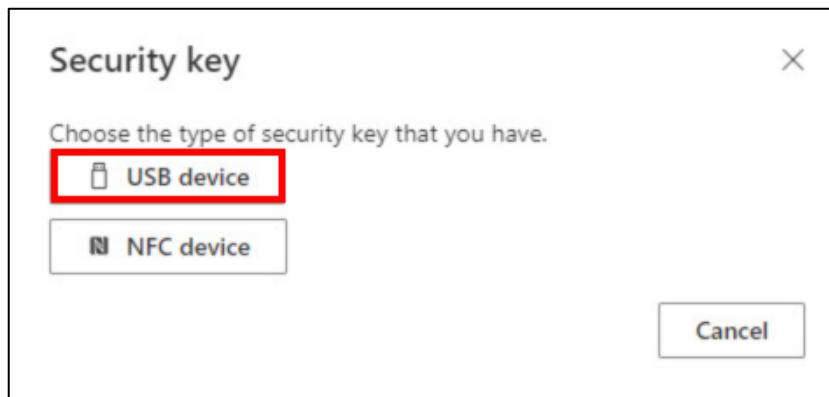


- Quét dấu vân tay khi nhận được thông báo.

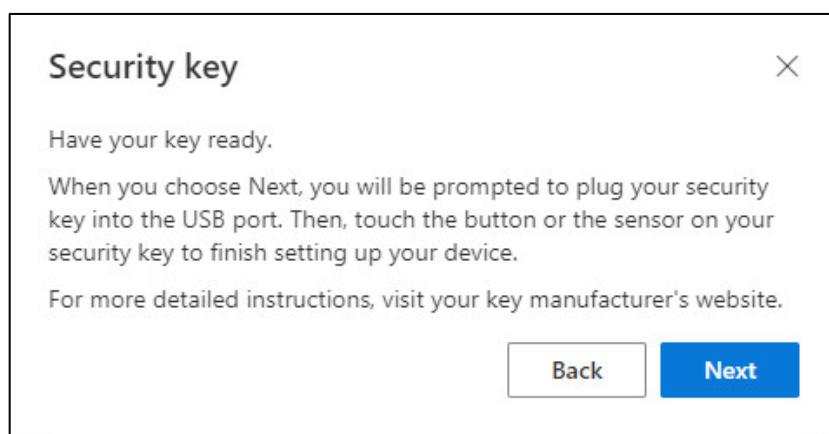


### III.1.1.3.2. Sử dụng qua kết nối USB

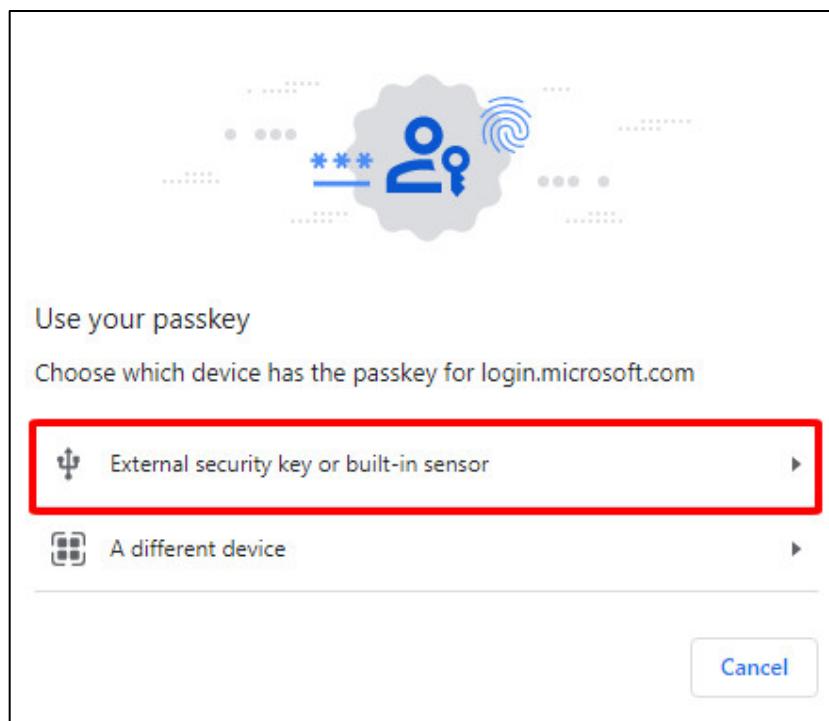
- Chọn **USB device**.



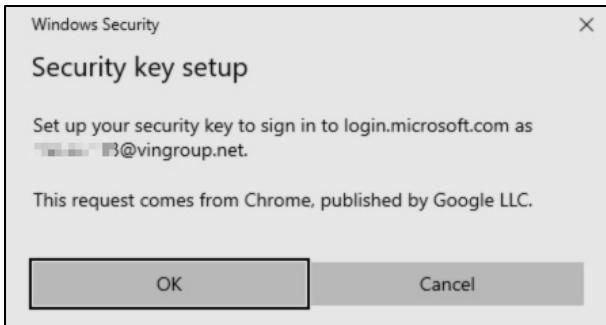
- Nhấn **Next** để tiếp tục.



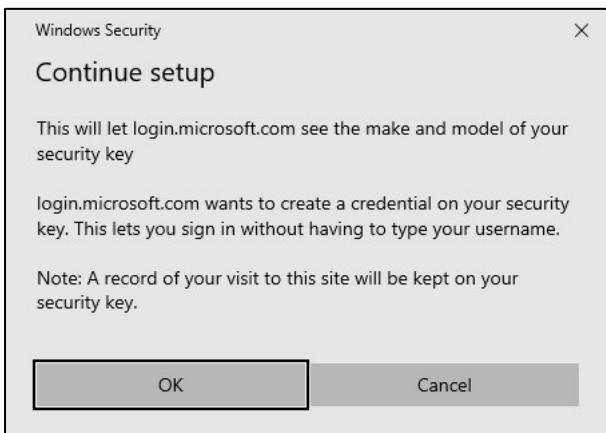
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



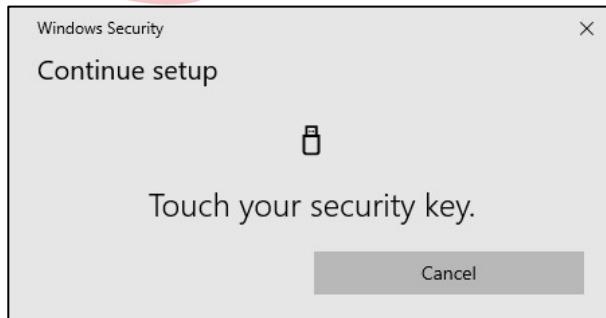
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



- Nhấn **OK** để tiếp tục.



- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

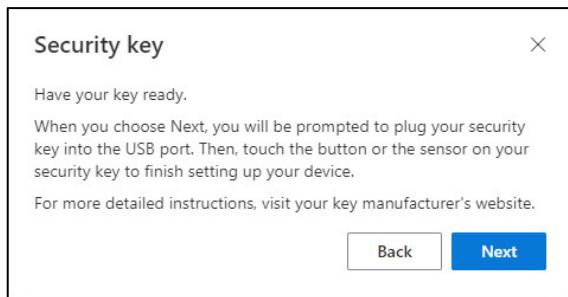


### III.1.1.3.3. Sử dụng qua kết nối NFC

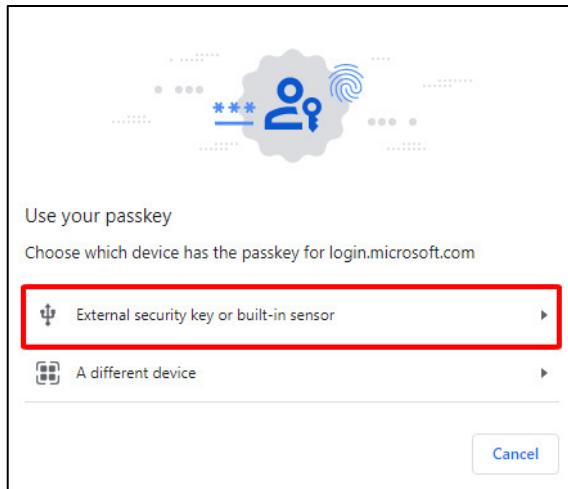
- Chọn **NFC device**.



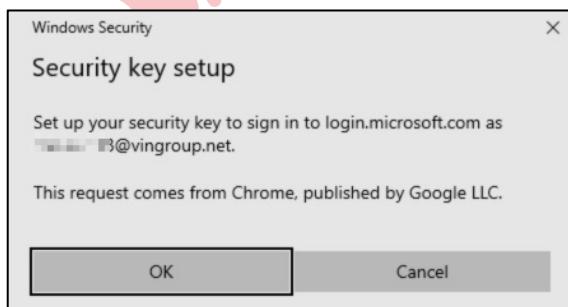
- Nhấn **Next** để tiếp tục.



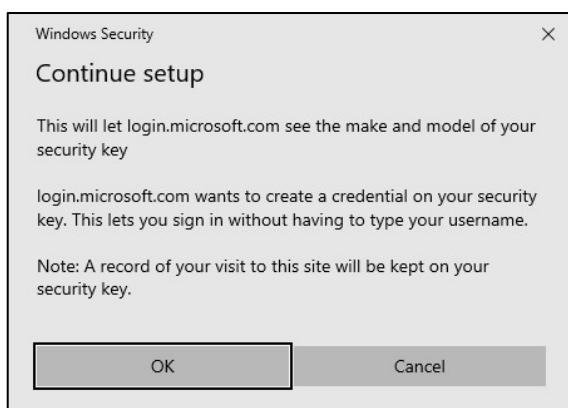
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



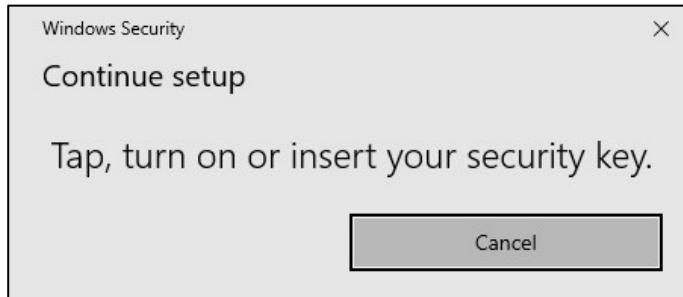
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



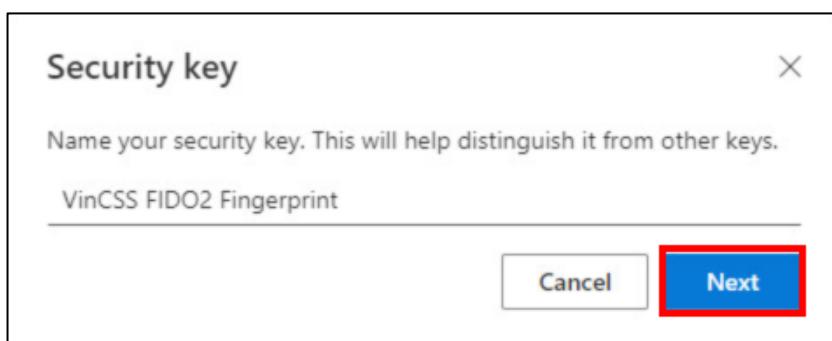
- Nhấn **OK** để tiếp tục.



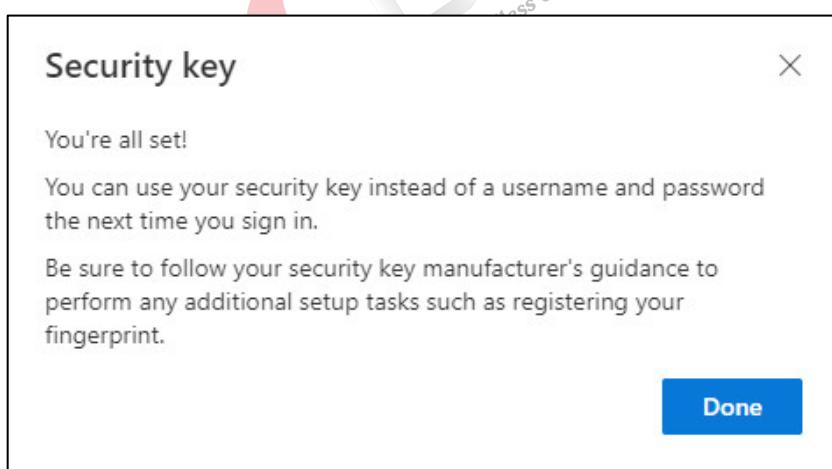
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật (*Tối đa 30 ký tự*) để phân biệt giữa các khoá rồi nhấn **Next**.

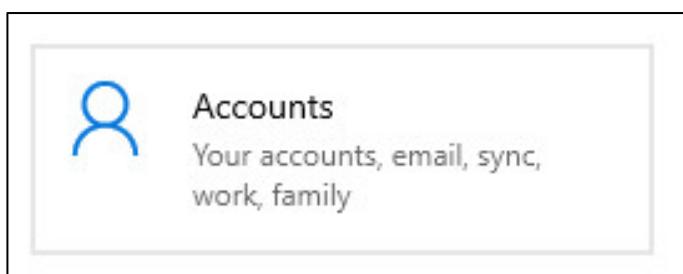


- Nhấn **Done** để hoàn tất đăng ký khoá bảo mật.

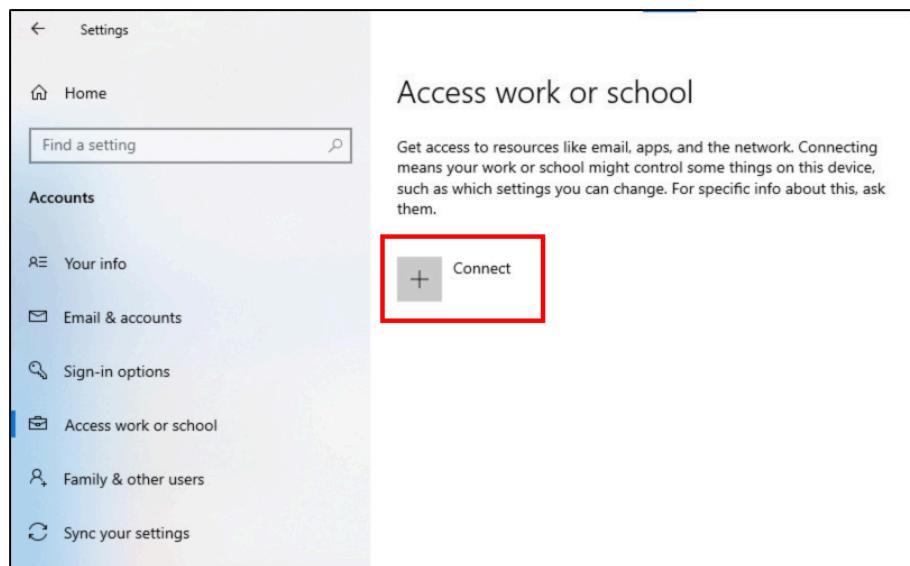


### III.1.1.4. Kết nối User vào Azure Work Account

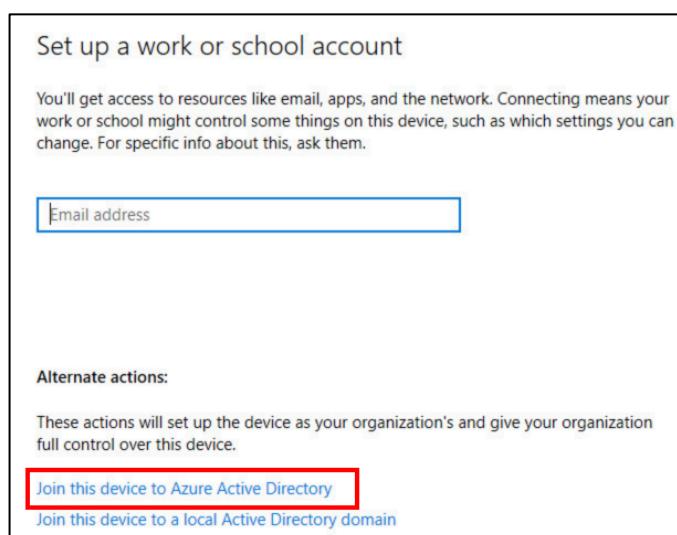
- Trên máy tính Windows, chọn **Settings > Account**.



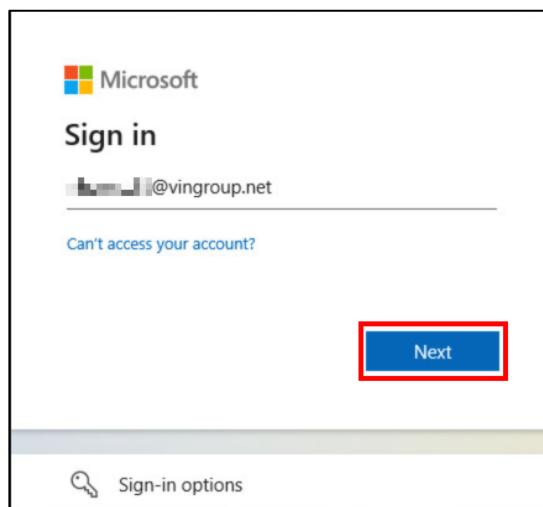
- Chọn Access work or school > Connect.



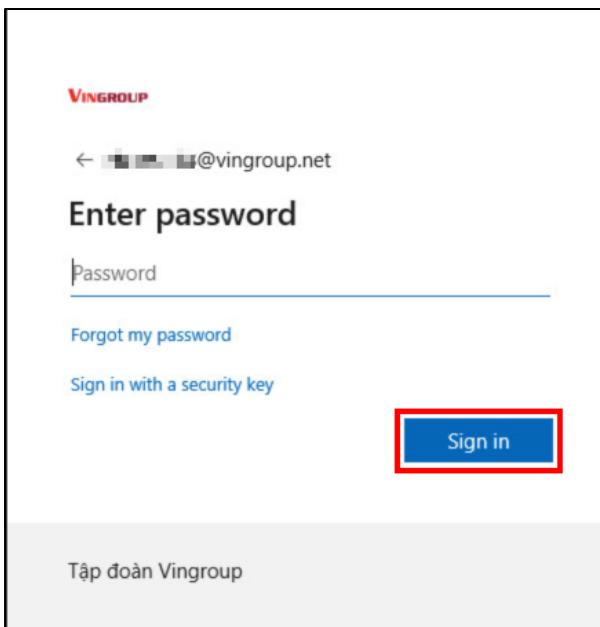
- Chọn Join this device to Azure Active Directory.



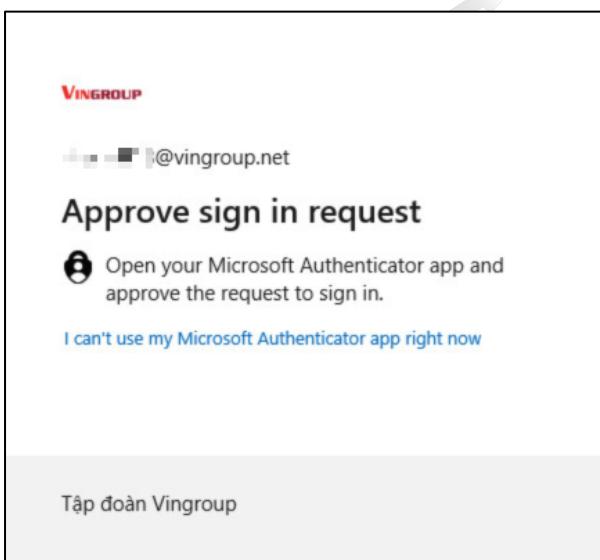
- Nhập thông tin tài khoản AD, sau đó nhấn Next.



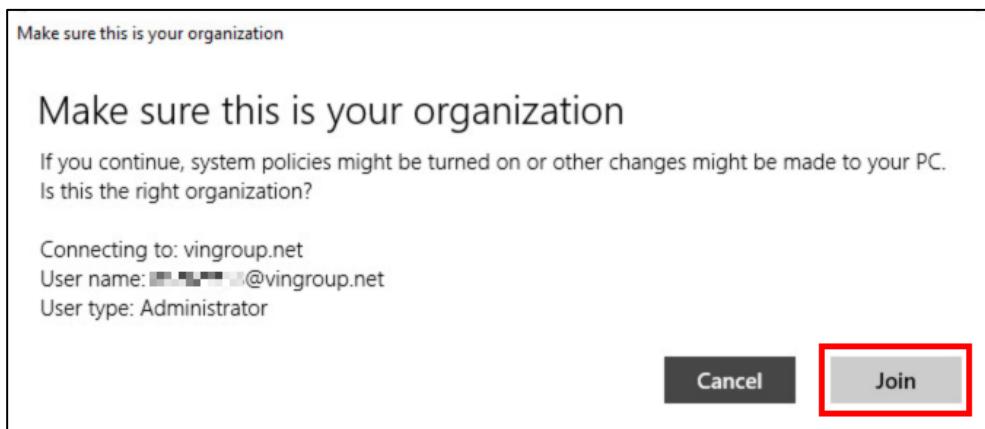
- Nhập mật khẩu của tài khoản AD rồi chọn **Sign in**.



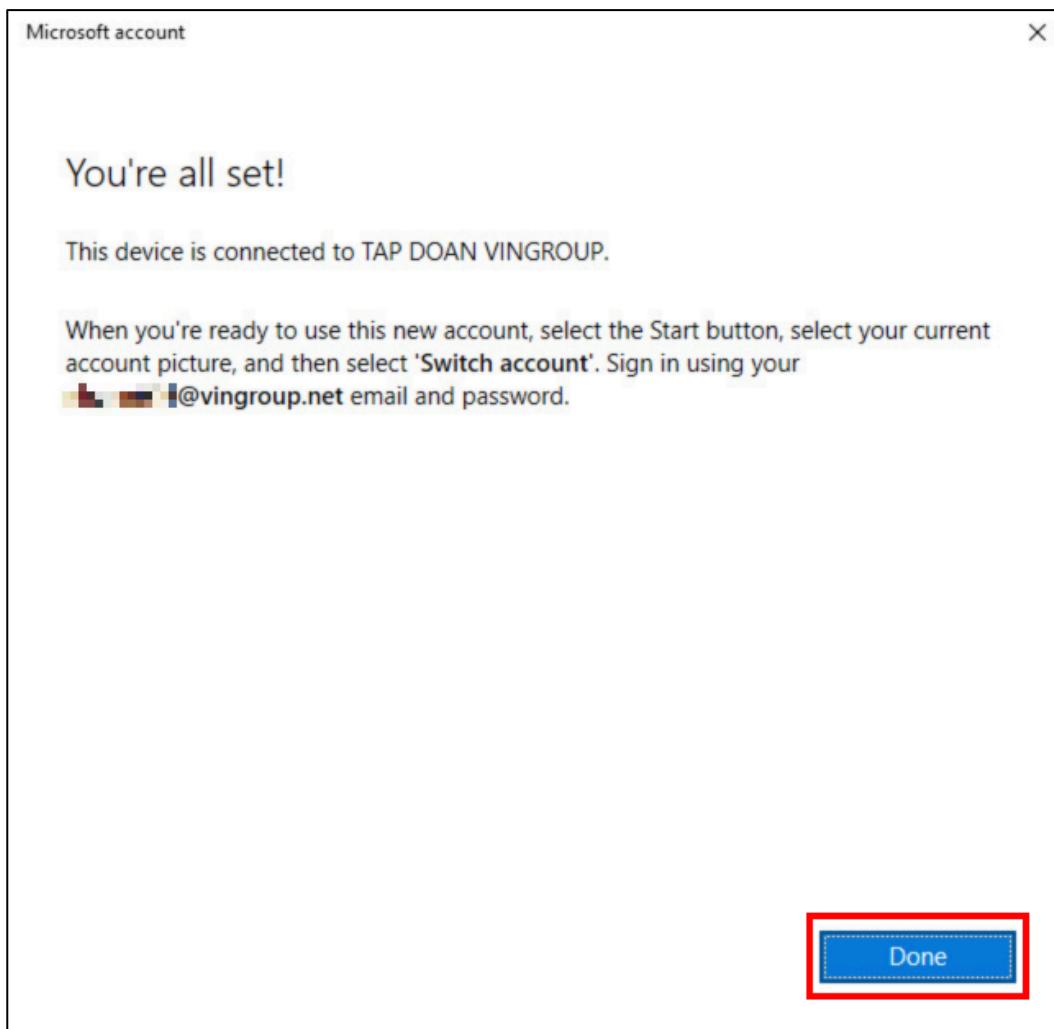
- Xác thực bằng ứng dụng Microsoft Authenticator trên điện thoại.



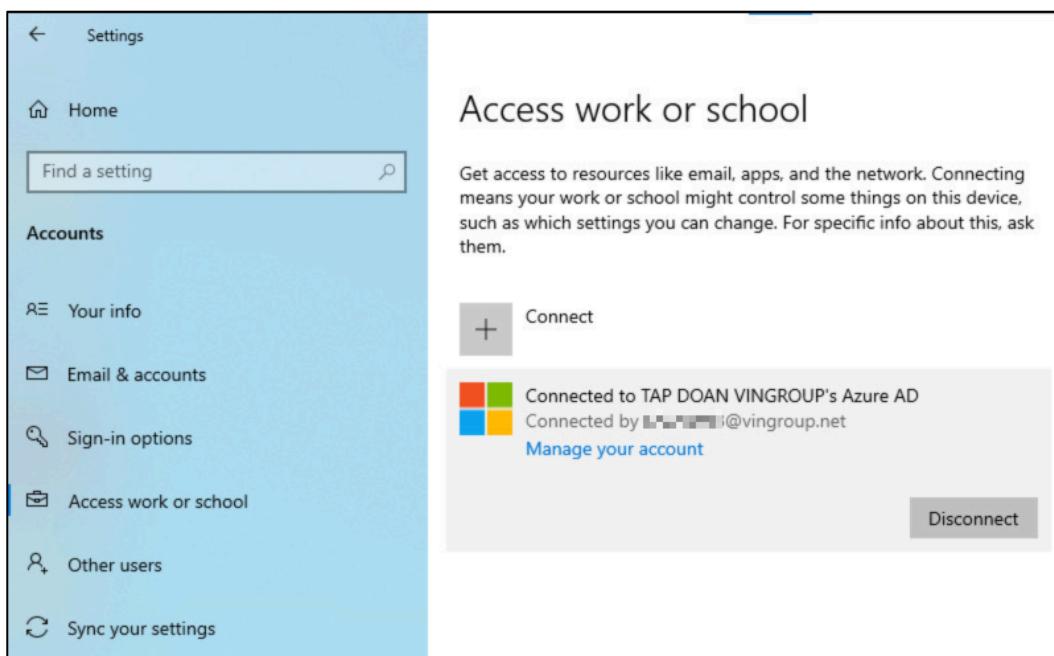
- Kiểm tra thông tin, sau đó nhấn **Join**.



- Nhấn **Done** để kết thúc.

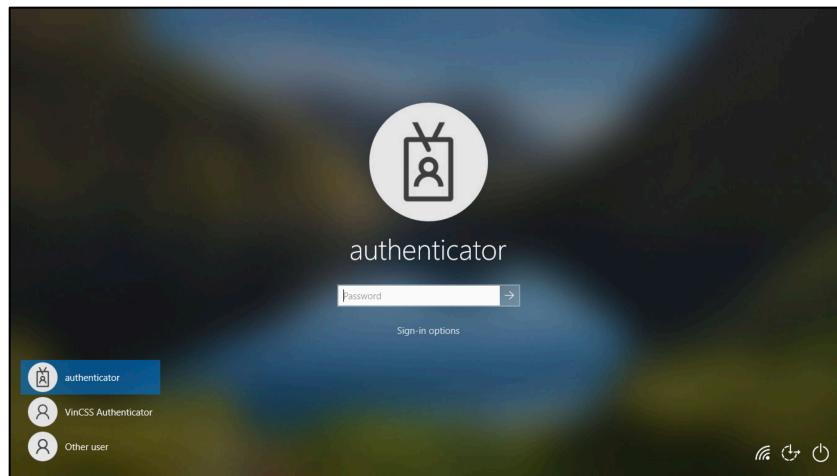


- Kết nối thành công, màn hình hiển thị như hình dưới.

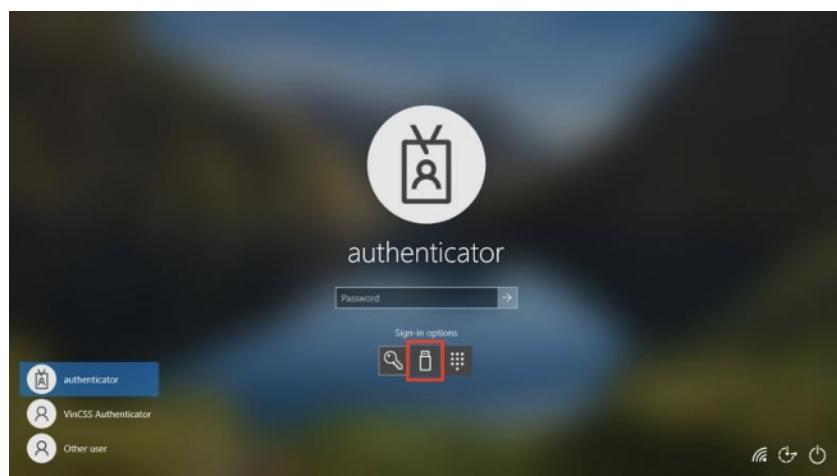


### III.1.2. Đăng nhập Windows 10

- Trên giao diện đăng nhập vào Windows 10, chọn **Sign-in options**.

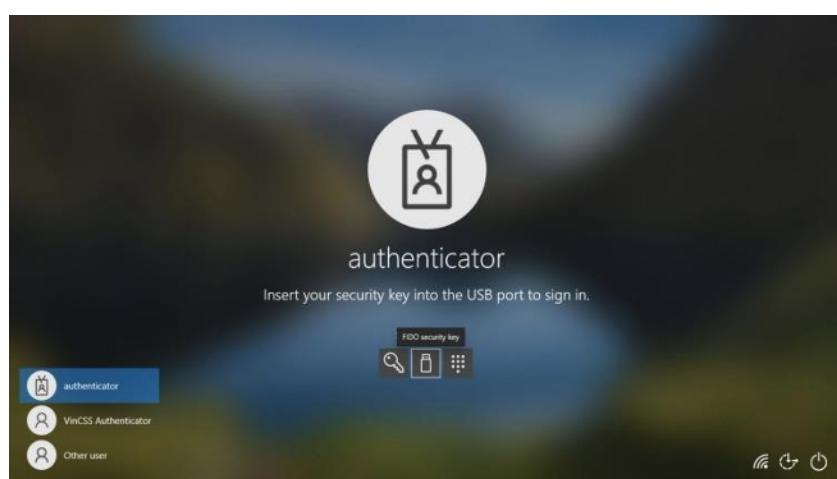


- Để lựa chọn đăng nhập Windows 10 với khoá bảo mật VinCSS FIDO2® Fingerprint thông qua kết nối Bluetooth.



#### III.1.2.1. Sử dụng qua kết nối Bluetooth.

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.



- Quét vân tay khi nhận được thông báo.



### III.1.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



### III.1.2.3. Sử dụng qua kết nối NFC

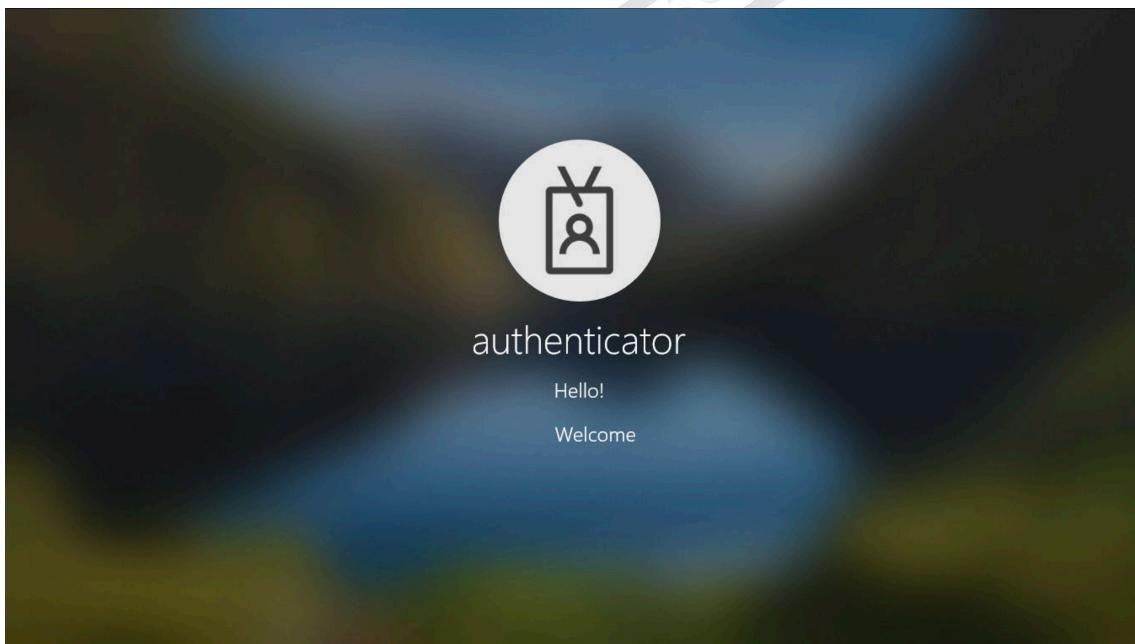
- Để lựa chọn đăng nhập Windows 10 với khoá bảo mật VinCSS FIDO2® Fingerprint thông qua kết nối NFC, chọn biểu tượng smart card.



- Kết nối khoá bảo mật với máy tính thông qua kết nối NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đăng nhập thành công.



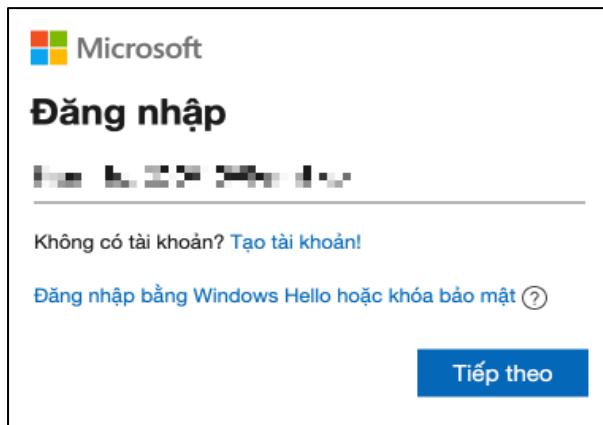
### III.2. Xác thực không mật khẩu tài khoản Microsoft

#### III.2.1. Đăng ký khóa bảo mật

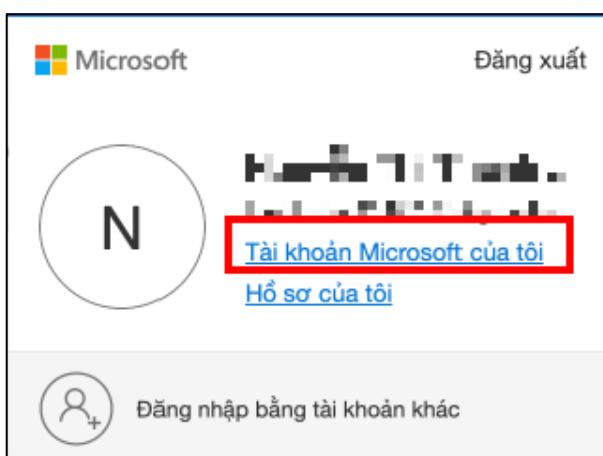
- Truy cập <https://microsoft.com>, chọn **Đăng nhập**.



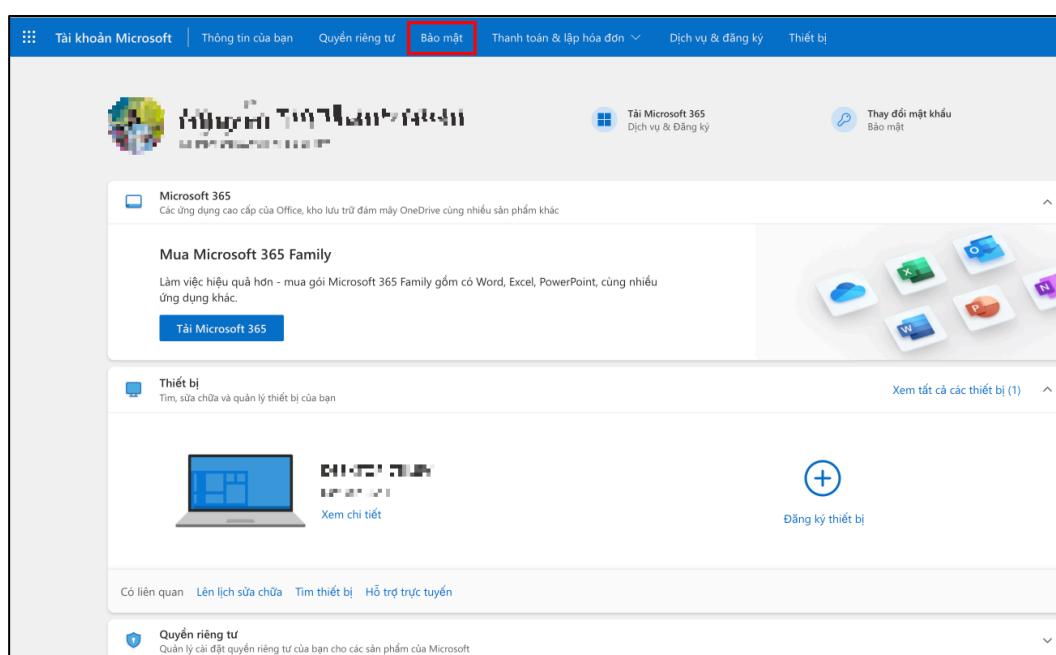
- Nhập thông tin tài khoản/mật khẩu rồi nhấn **Tiếp theo** để đăng nhập.



- Sau khi đăng nhập thành công, Chọn **Tài khoản Microsoft của tôi** để tiến hành cấu hình.



- Chọn mục **Bảo mật**.



The screenshot shows the Microsoft Security settings page. The top navigation bar has tabs for Tài khoản Microsoft, Thông tin của bạn, Quyền riêng tư, **Bảo mật** (highlighted with a red box), Thanh toán & lập hóa đơn, Dịch vụ & đăng ký, and Thiết bị. The main content area features sections for Microsoft 365 (with a 'Tải Microsoft 365' button), Mua Microsoft 365 Family (with a 'Tải Microsoft 365' button), Thiết bị (with a '+ Đăng ký thiết bị' button), and Quyền riêng tư (with a 'Quản lý các thiết bị của bạn' link). A sidebar on the left lists 'Có liên quan' items like Lịch sửa chữa, Tìm thiết bị, and Hỗ trợ trực tuyến.

- Chọn Các tùy chọn bảo mật nâng cao để thay đổi phương thức bảo mật.

Bảo mật

Thông tin cơ bản về bảo mật

Thay đổi mật khẩu

Lần cập nhật gần đây nhất: 23/12/2020

Hoạt động Đăng nhập

Bảo mật Mật khẩu

Các tùy chọn bảo mật nâng cao

Duy trì bảo mật với Windows 10

Xem hoạt động của tôi

Thay đổi mật khẩu của tôi

Bắt đầu

Kiểm tra bảo mật Windows

- Chọn Thêm cách mới để đăng nhập hoặc xác minh.

Tài khoản Microsoft | Thông tin của bạn | Quyền riêng tư | Bảo mật | Rewards | Thanh toán & lập hóa đơn | Dịch vụ & đăng ký | Thiết bị | ? | NV

Bảo mật

Thay đổi mật khẩu

Cập nhật gần nhất: 23/12/2020

Thay đổi >

Xác nhận hai bước

TẮT

Quản lý >

Cách để chứng minh bạn là ai

Nhập mật khẩu

Cập nhật

Thay đổi gần nhất

Được sử dụng cho: Đăng nhập tài khoản

Gửi mã qua email

@gmail.com

Cập nhật

+ Thêm cách mới để đăng nhập hoặc xác minh

- Chọn Sử dụng khóa bảo mật.

Chọn thêm một cách để xác minh hoặc đăng nhập

Sử dụng ứng dụng

Nhanh chóng chấp thuận thông báo đăng nhập trên điện thoại của bạn.

Gửi mã qua email

Nhận email và đăng nhập bằng mã.

Sử dụng PC chạy Windows của bạn

Đăng nhập bằng cách sử dụng khuôn mặt, dấu vân tay hoặc mã PIN.

Sử dụng khóa bảo mật

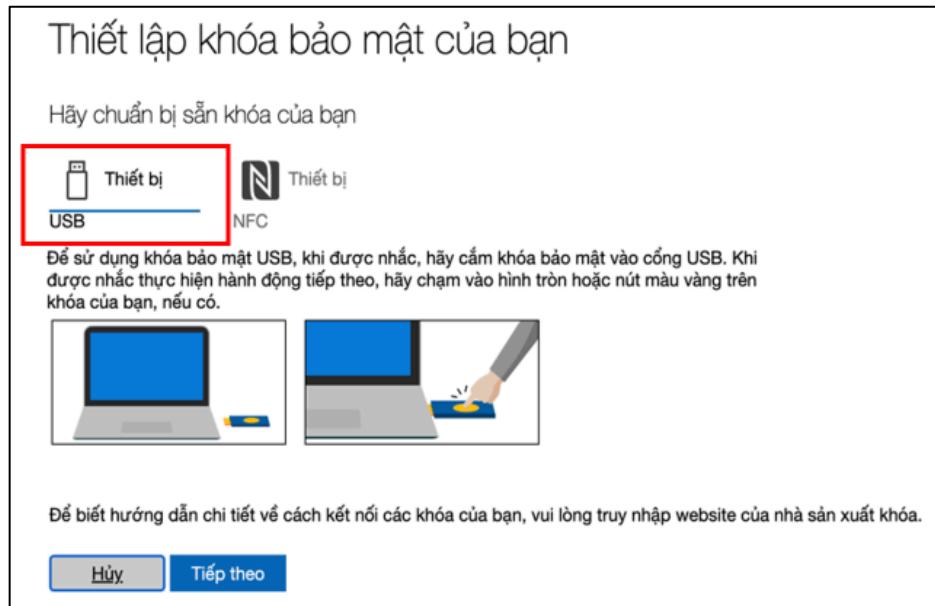
Đăng nhập bằng thiết bị USB, Bluetooth hoặc NFC.

Gửi mã qua tin nhắn văn bản

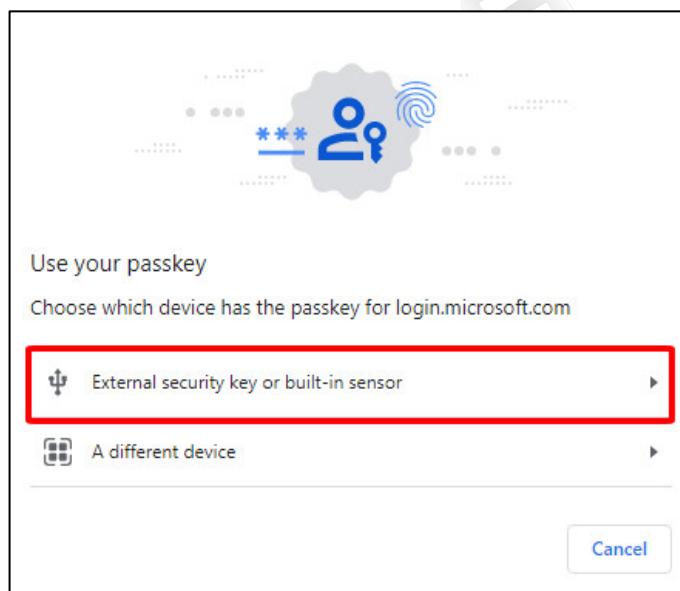
Nhận tin nhắn văn bản và đăng nhập bằng mã.

### III.2.1.1. Sử dụng qua kết nối Bluetooth

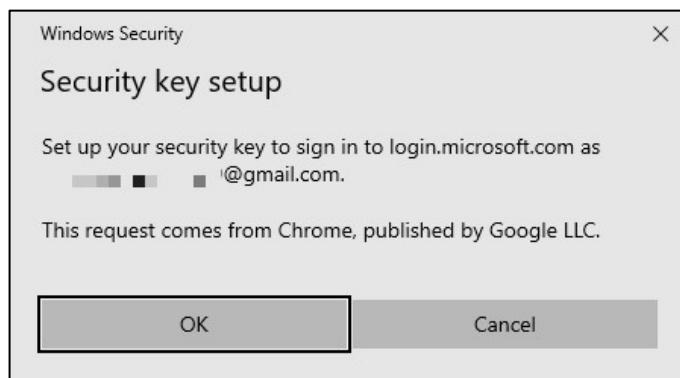
- Chọn **Thiết bị USB**, nhấn **Tiếp theo**.



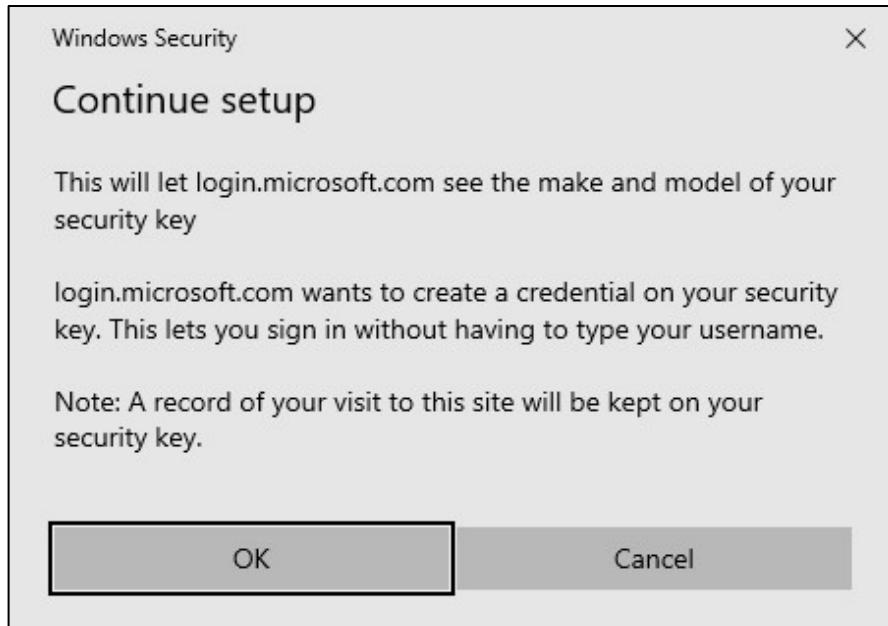
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



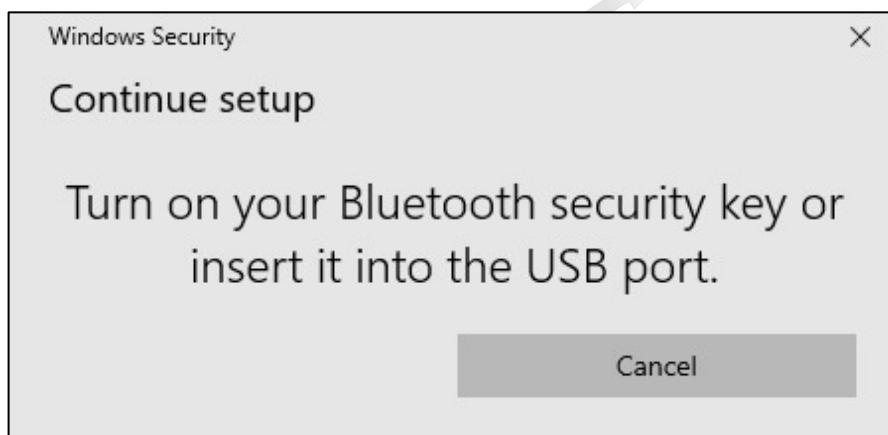
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



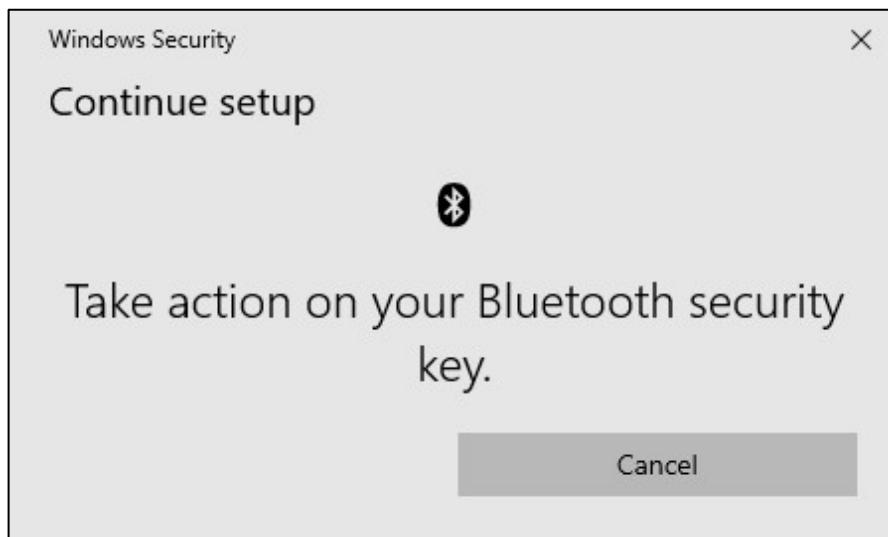
- Nhấn **OK** để tiếp tục.



- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

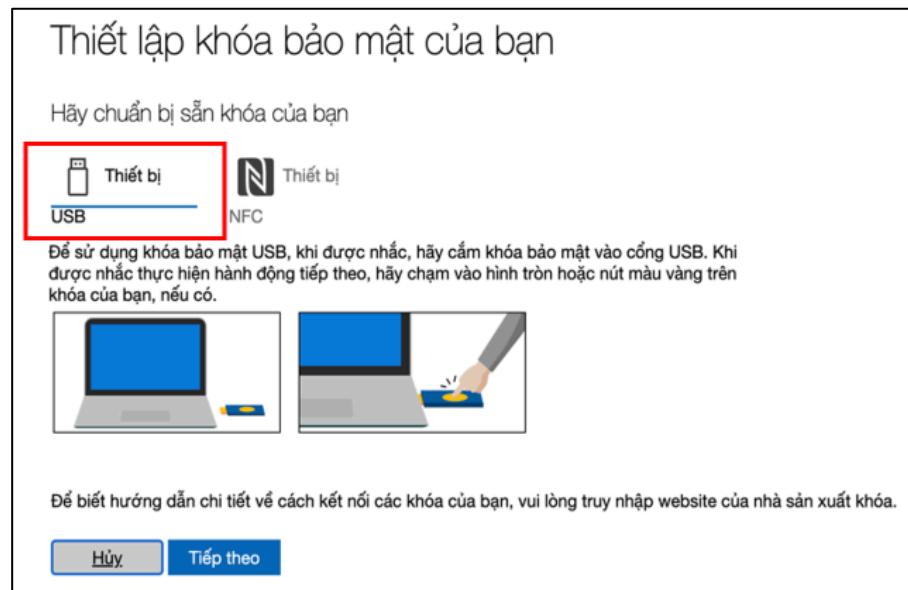


- Quét dấu vân tay khi nhận được thông báo.

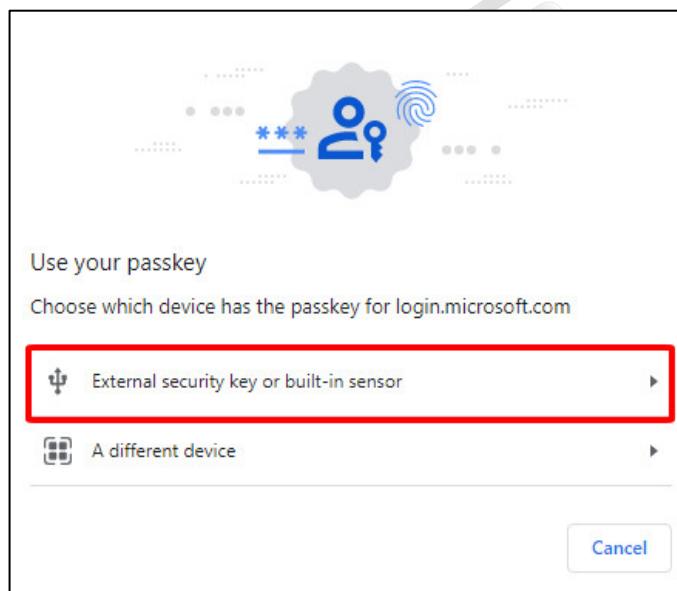


### III.2.1.2. Sử dụng qua kết nối USB

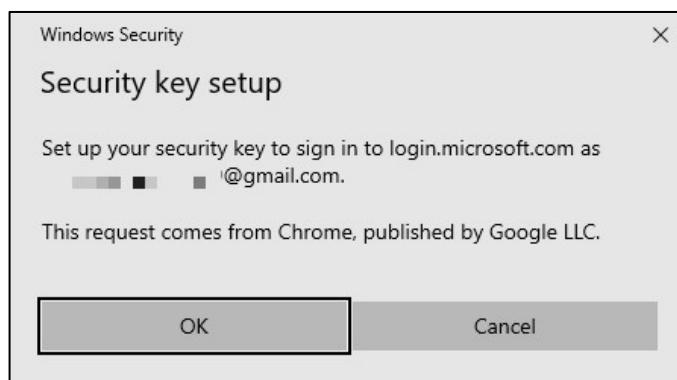
- Chọn Thiết bị USB, nhấn Tiếp theo.



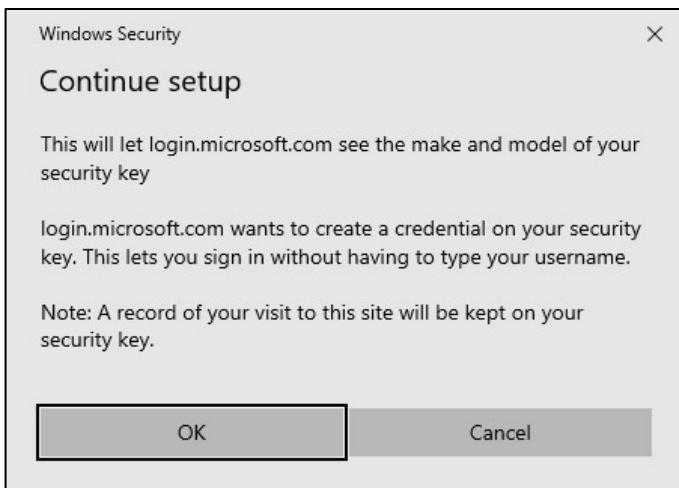
- Chọn External security key or built-in sensor để thiết lập khoá bảo mật.



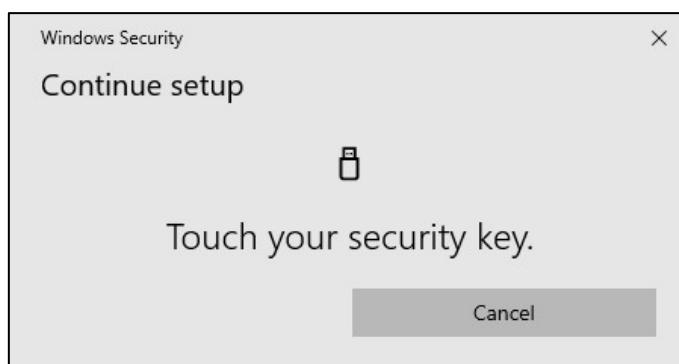
- Nhấn OK để tiếp tục thiết lập khoá bảo mật.



- Nhấn **OK** để tiếp tục.



- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

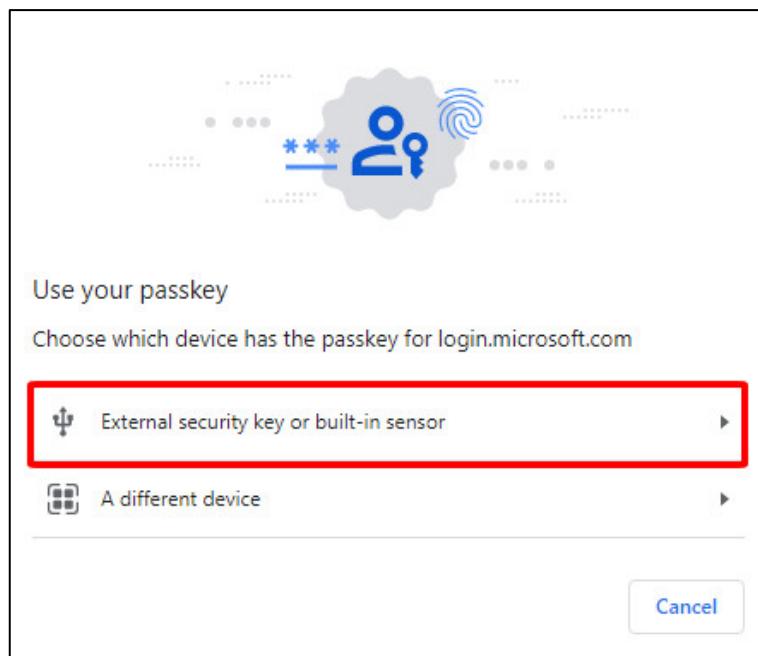


### III.2.1.3. Sử dụng qua kết nối NFC

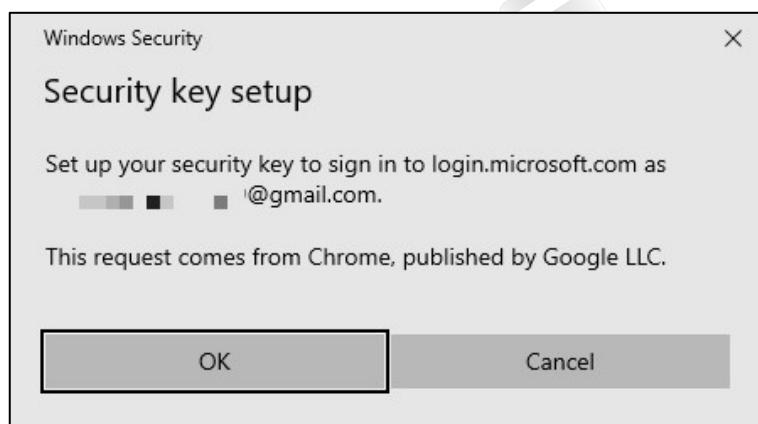
- Chọn **Thiết bị NFC**. nhấn **Tiếp theo**.



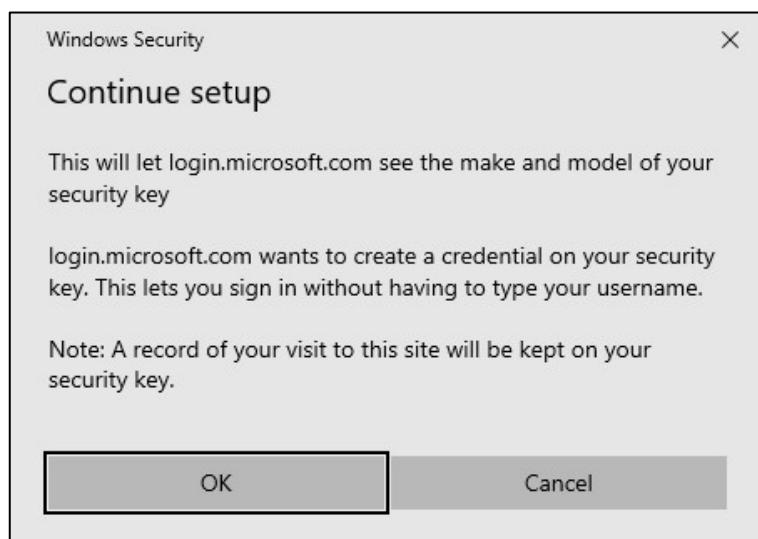
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



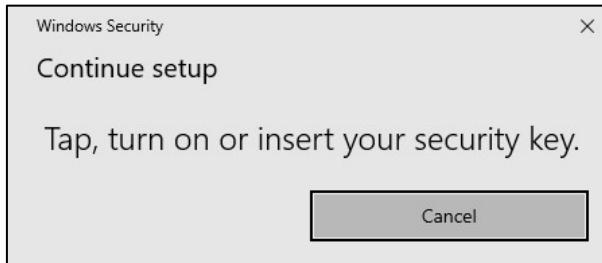
- Nhấn **OK** để tiếp tục thiết lập khoá bảo mật.



- Nhấn **OK** để tiếp tục.



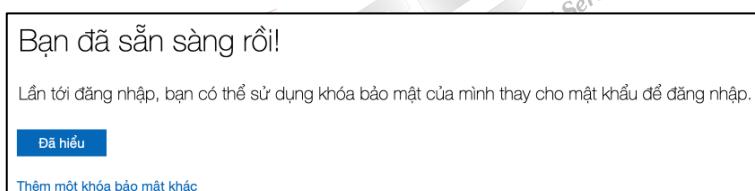
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật để phân biệt giữa các khoá rồi nhấn **Tiếp theo**.



- Nhấn **Đã hiểu** để hoàn tất đăng ký Security key.

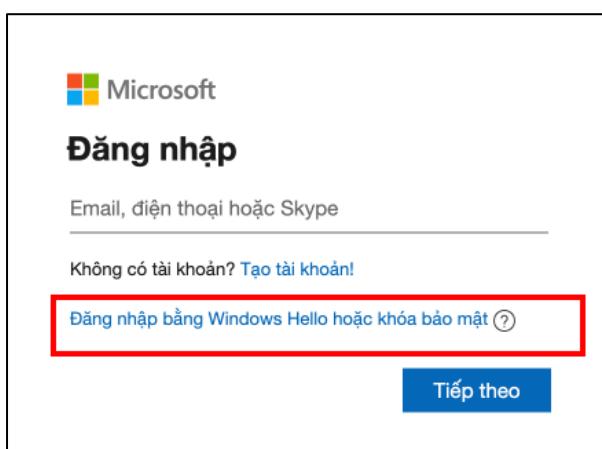


### III.2.2. Xác thực không mật khẩu tài khoản Microsoft

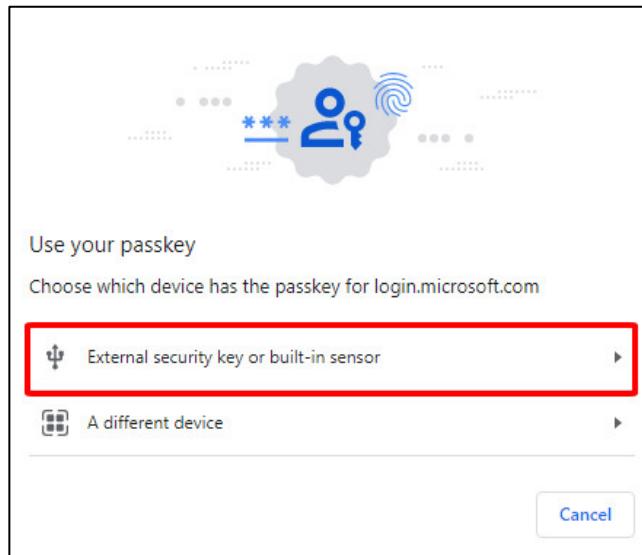
- Truy cập <https://www.microsoft.com/vi-vn/>, chọn **Đăng nhập**.



- Chọn **Đăng nhập bằng Windows Hello hoặc khóa bảo mật**.



- Chọn **External security key or built-in sensor** để đăng nhập bằng khoá bảo mật.



### III.2.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

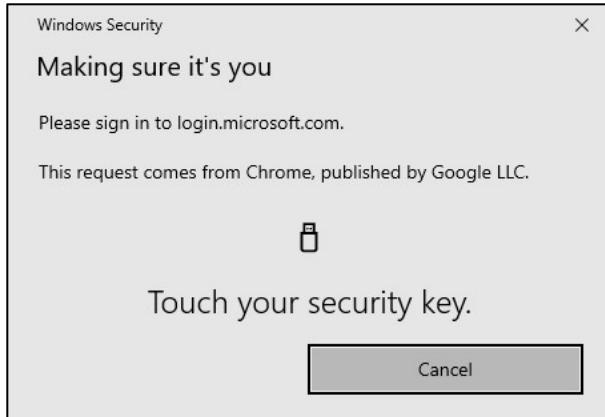


- Quét dấu vân tay khi nhận được thông báo.



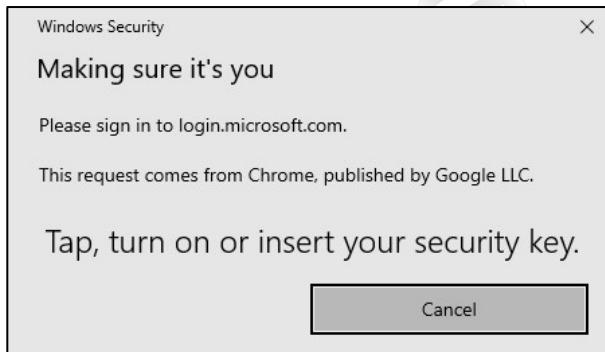
### III.2.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

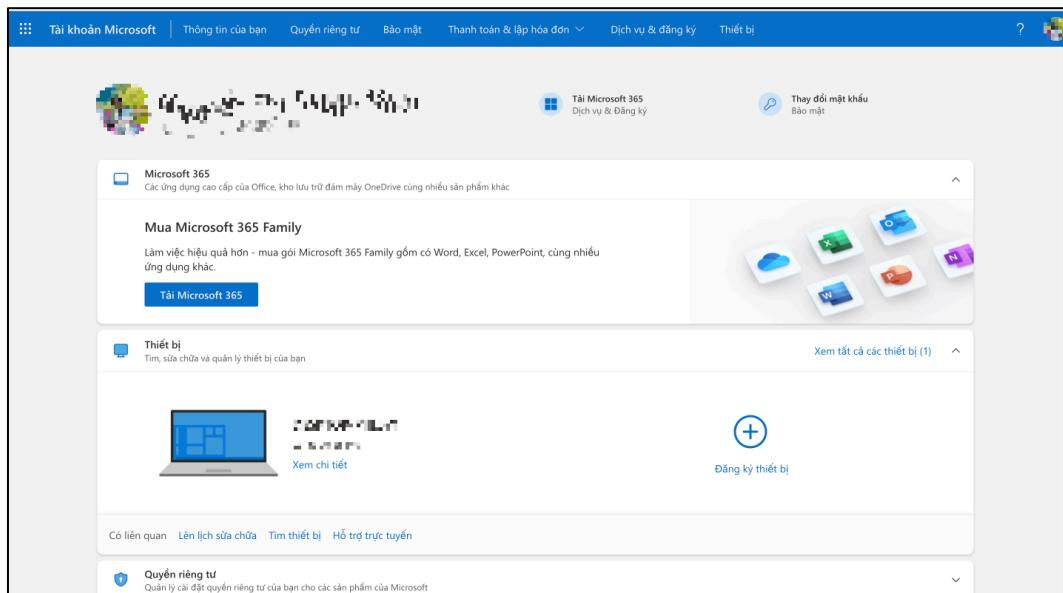


### III.2.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đăng nhập thành công.

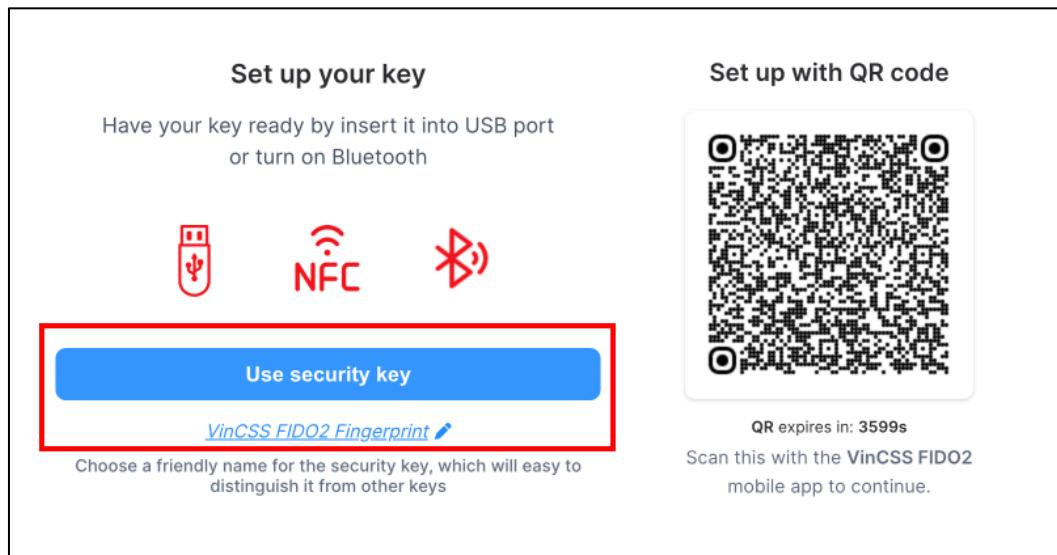


### III.3. VinCSS OVPN Client

#### III.3.1. Windows

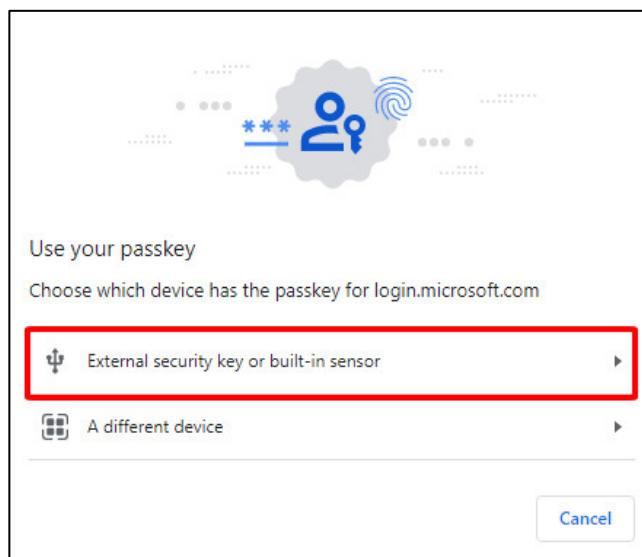
##### III.3.1.1. Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint

- Liên hệ người quản trị để lấy đường link đăng ký khoá được gửi cho người dùng qua email hoặc IM (*có hiệu lực trong 1 giờ*). Thay đổi tên khoá bảo mật và chọn **Use security key**.

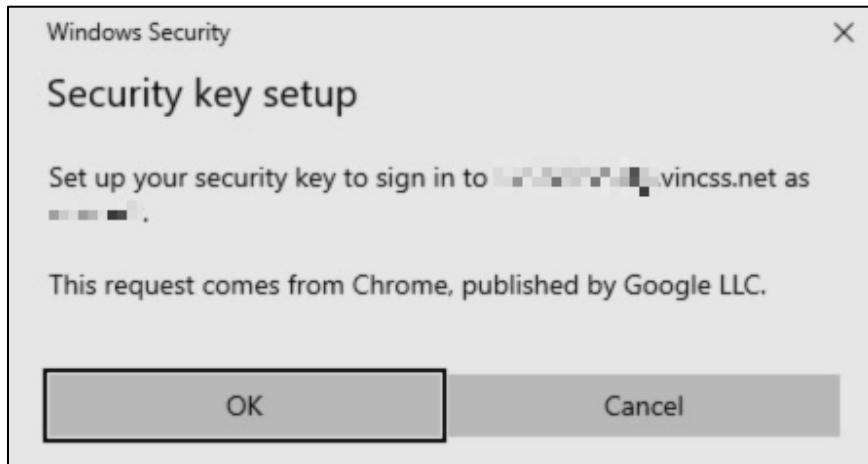


**Lưu ý:** Mặc định người quản trị sẽ gửi link đăng ký khoá bảo mật sử dụng được với tất cả các hình thức đăng nhập sau khi đăng ký khoá bảo mật thành công (Hình thức xác thực không mật khẩu (Tham khảo mục III.3.1.2.1.) và hình thức xác thực không tên người dùng (Tham khảo mục III.3.1.2.2.)).

- Chọn **External security key or built-in sensor** để đăng ký khoá bảo mật VinCSS FIDO2® Fingerprint.



- Chọn **OK** để tiếp tục quá trình đăng ký khóa bảo mật.

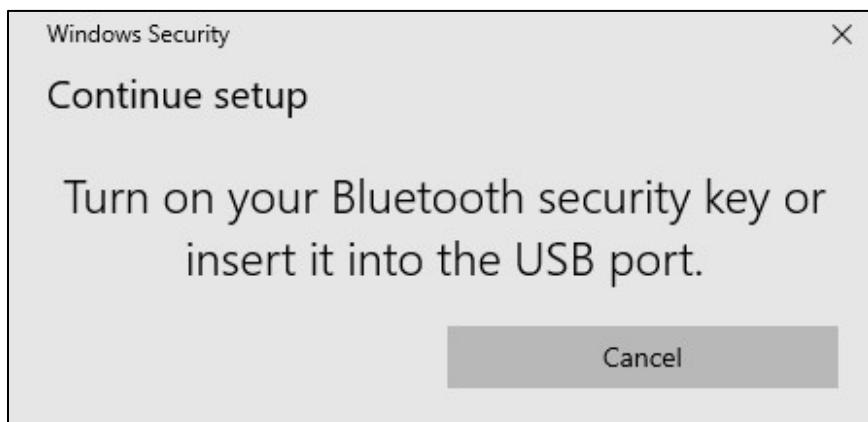


- Nhấn **OK** để tiếp tục.

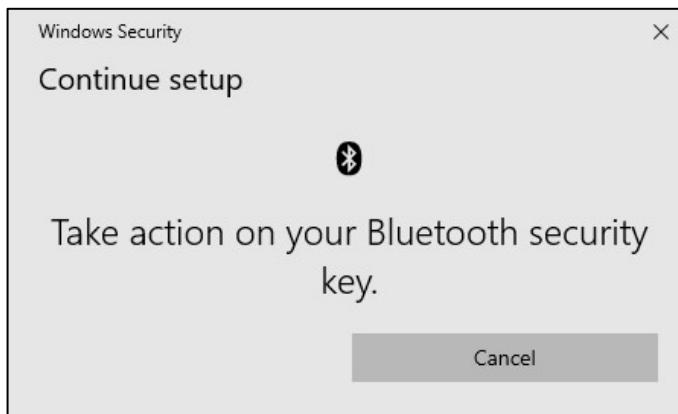


### III.3.1.1.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.

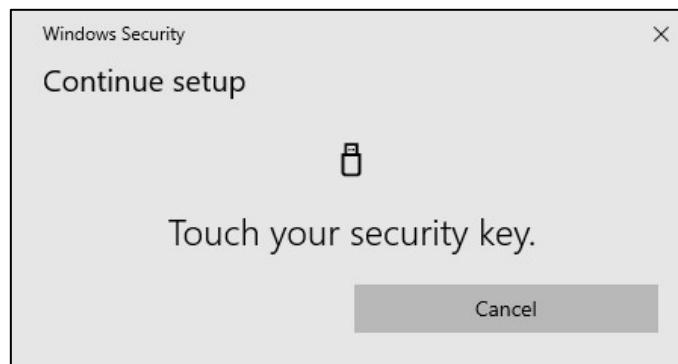


- Quét dấu vân tay khi nhận được thông báo.



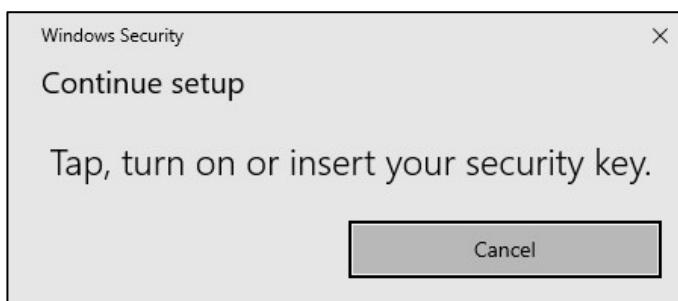
### III.3.1.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

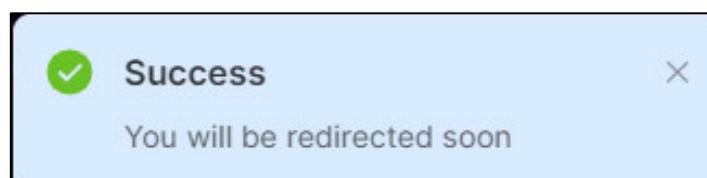


### III.3.1.1.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.

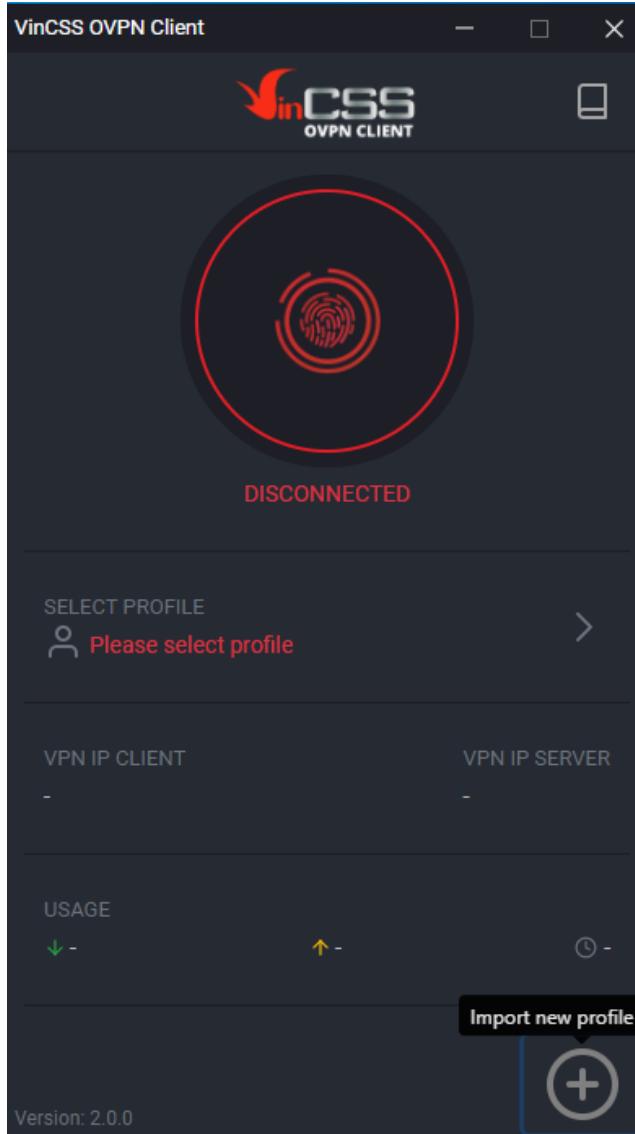


- Trên màn hình máy tính hiện thông báo người dùng đã đăng ký khoá bảo mật thành công.

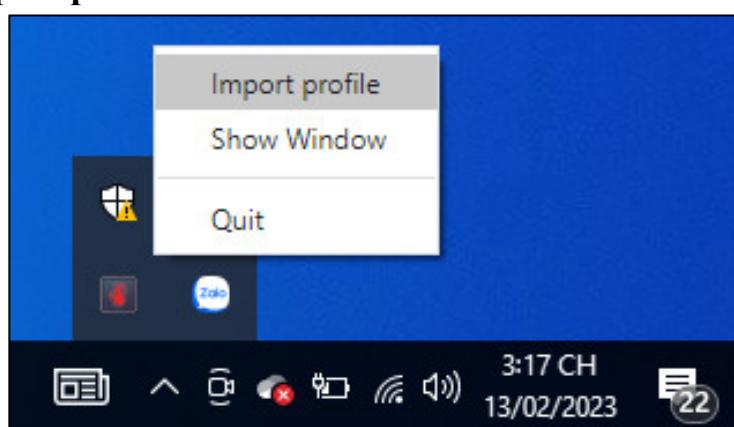


### III.3.1.2. Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint

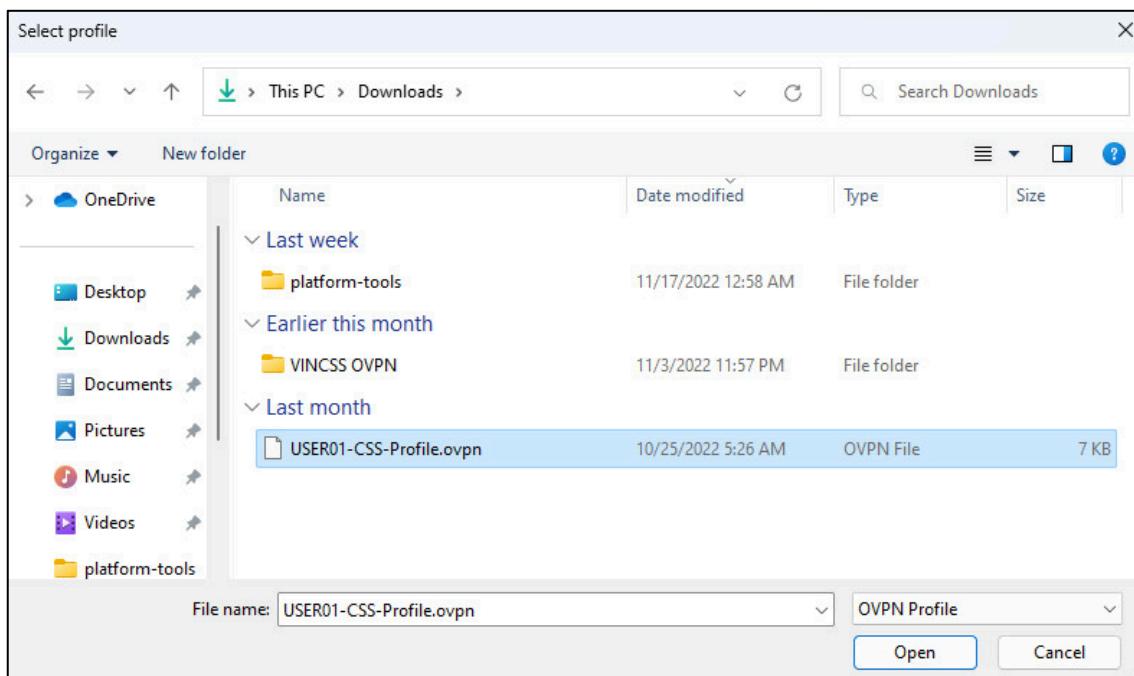
- Mở ứng dụng VinCSS OVPN Client, trên giao diện chọn **Import new profile**.



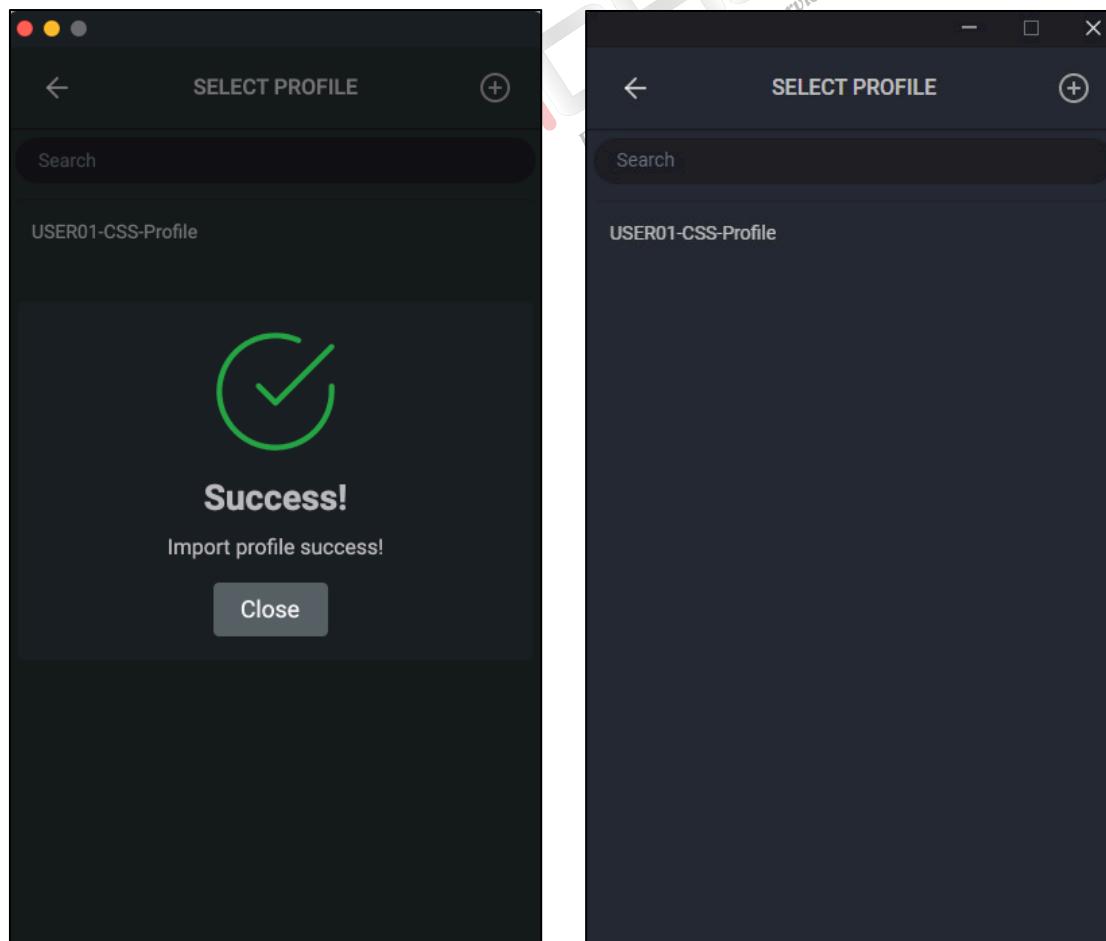
- Hoặc nhấn chuột phải vào biểu tượng VinCSS OVPN Client trên taskbar, chọn **Import profile**.



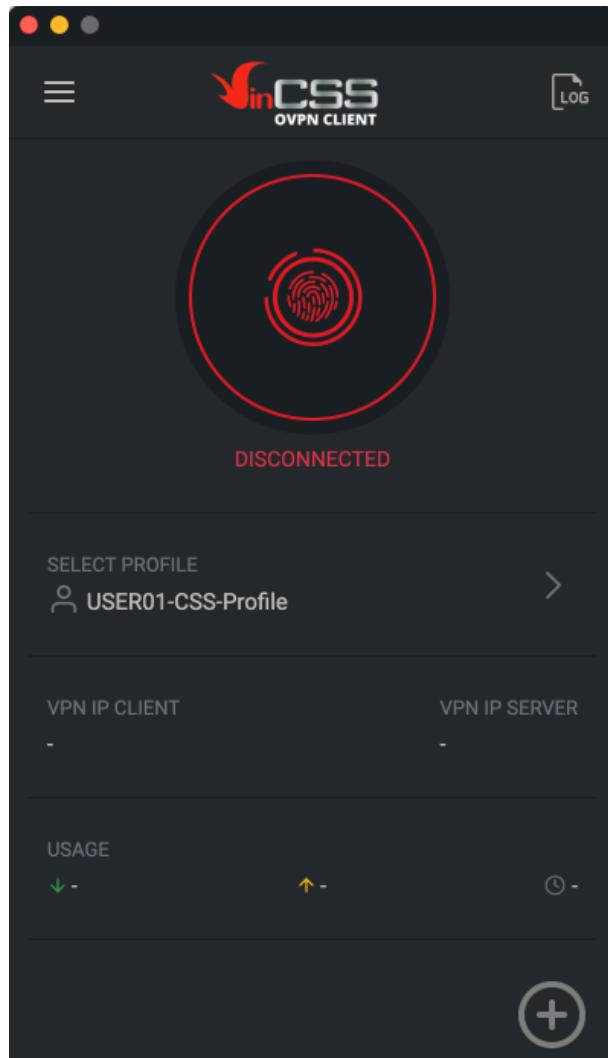
- Chọn profile được gửi bởi quản trị viên (*file .ovpn*) và chọn **Open**.



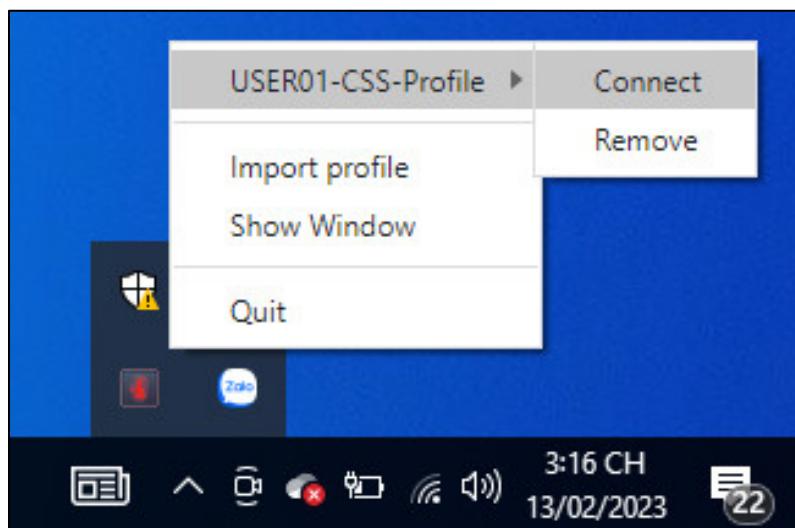
- Profile được thêm thành công. Nhấn **Close** để đóng cửa sổ thông báo. Màn hình hiển danh sách profile đã thêm.



- Nhấn vào biểu tượng vân tay màu đỏ trên giao diện ứng dụng để tiến hành kết nối VPN.

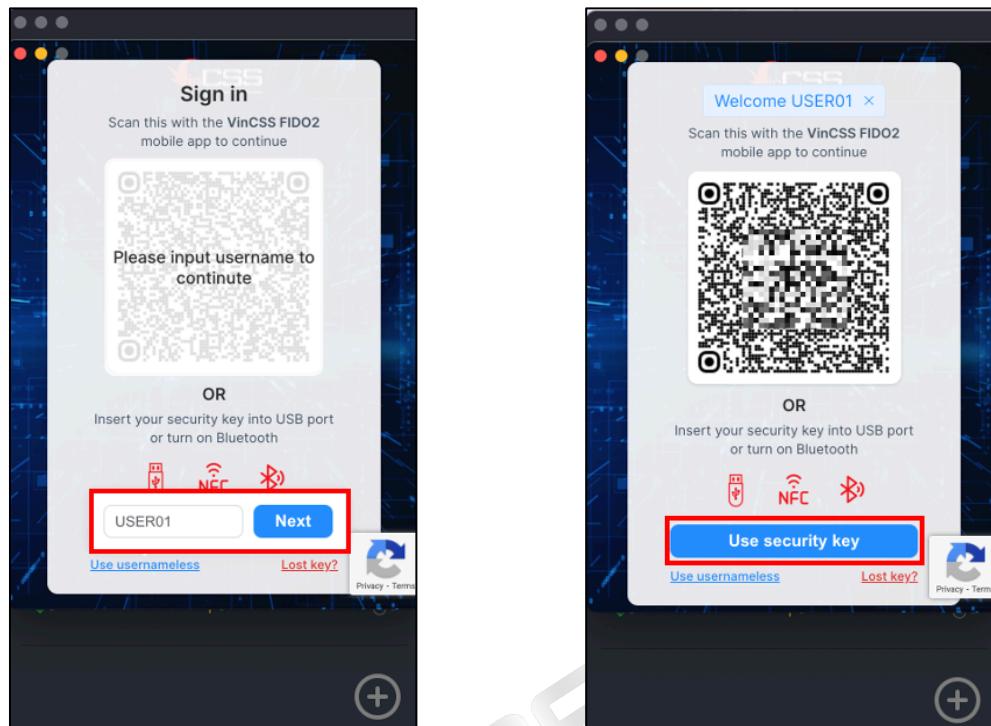


- Hoặc nhấn chuột phải vào biểu tượng VinCSS OVPN Client ở taskbar, chọn VPN profile cần kết nối, sau đó chọn **Connect**.



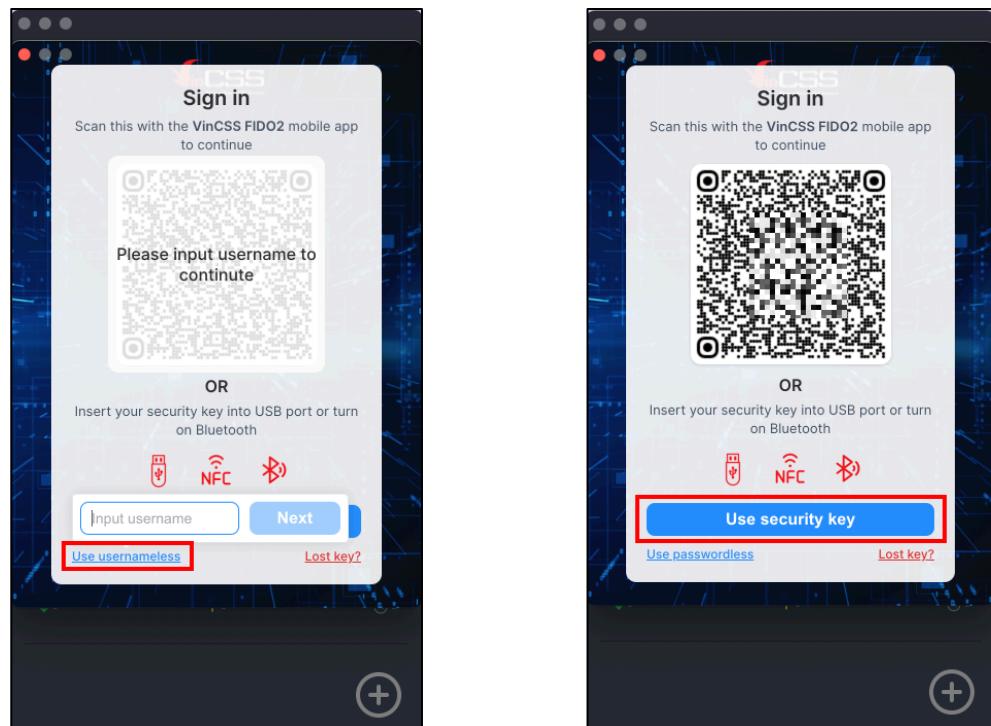
### III.3.1.2.1. Xác thực không mật khẩu

- Nhập **Username** (*không phân biệt chữ hoa, chữ thường*) rồi chọn **Next**. Sau đó chọn **Use security key** để tiếp tục.



### III.3.1.2.2. Xác thực không tên người dùng

- Người dùng có thể chọn phương thức đăng nhập khác bằng cách chọn **Use usernameless** để thay cho bước nhập **username** rồi chọn **Use security key**.

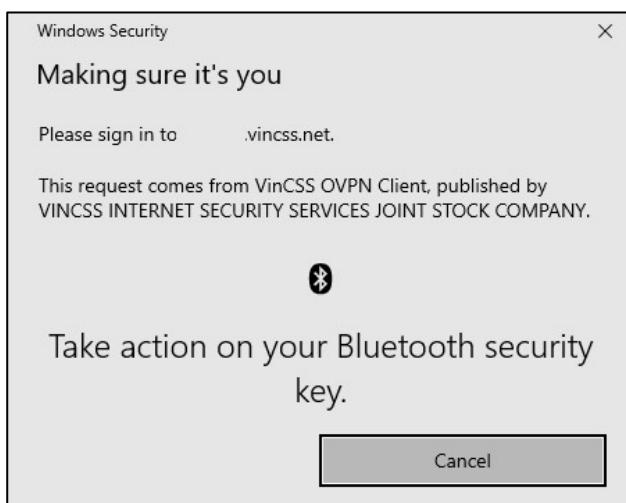


### III.3.1.2.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua kết nối Bluetooth.



- Quét dấu vân tay khi nhận được thông báo.



### III.3.1.2.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB. Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

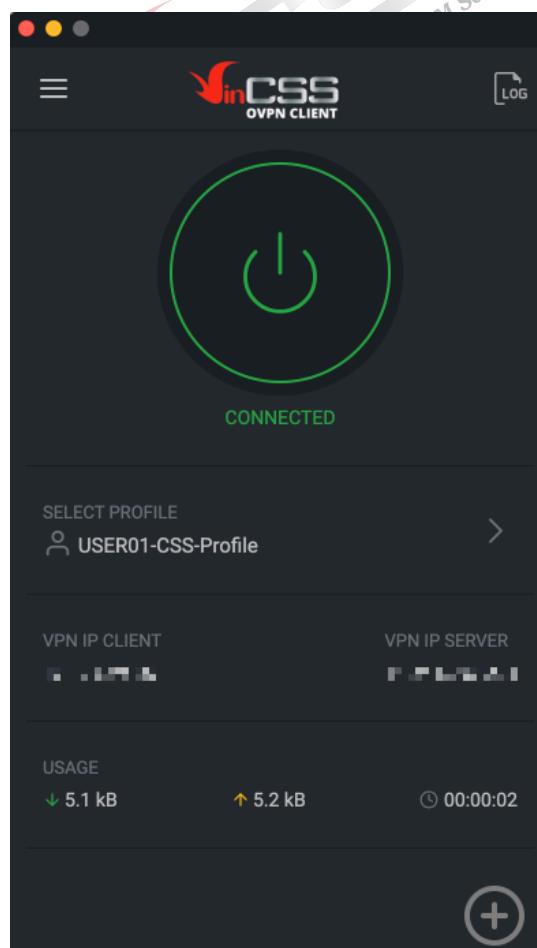


### III.3.1.2.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC. Chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



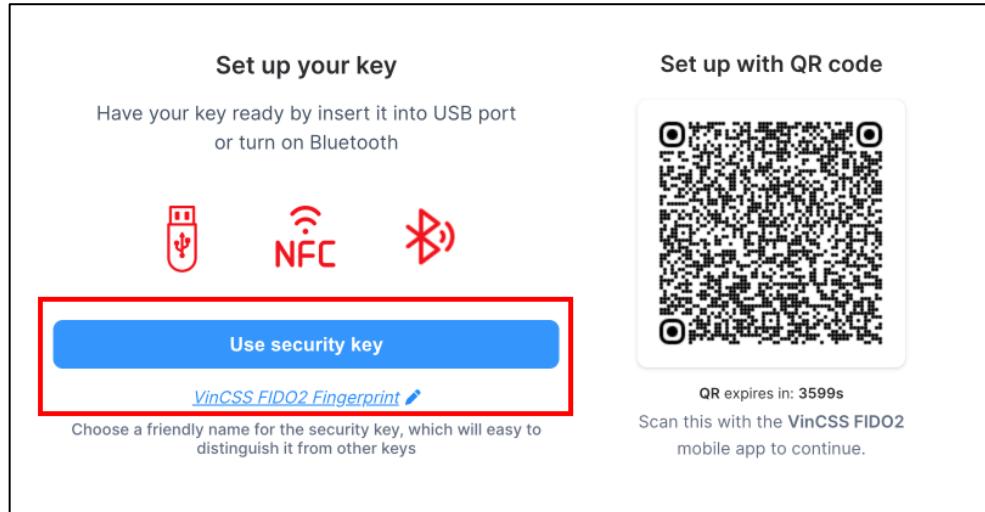
- Quá trình kết nối được tiến hành khi người dùng xác thực thành công. Kết nối VPN thành công, trên giao diện ứng dụng hiển thị trạng thái **CONNECTED**.



### III.3.2. macOS

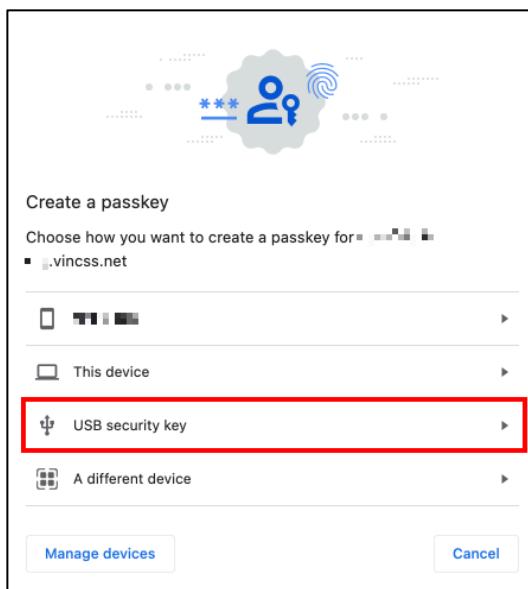
#### III.3.2.1. Đăng ký khóa bảo mật VinCSS FIDO2® Fingerprint (*Chỉ hỗ trợ kết nối USB*)

- Liên hệ người quản trị để lấy đường link đăng ký khoá được gửi cho người dùng qua email hoặc IM (*có hiệu lực trong 1 giờ*). Thay đổi tên khoá bảo mật và chọn **Use security key**.

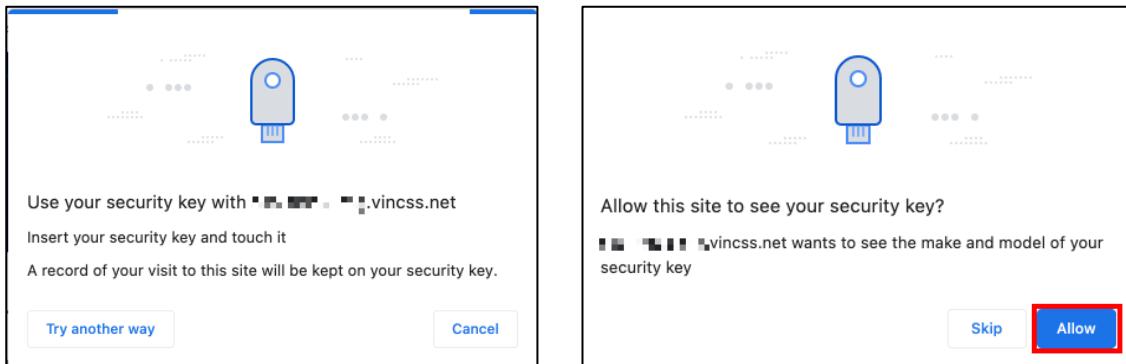


**Lưu ý:** Mặc định người quản trị sẽ gửi link đăng ký khoá bảo mật sử dụng được với tất cả các hình thức đăng nhập sau khi đăng ký khoá bảo mật thành công (Hình thức xác thực không mật khẩu (Tham khảo mục III.3.2.2.1.) và hình thức xác thực không tên người dùng (Tham khảo mục III.3.2.2.2.)).

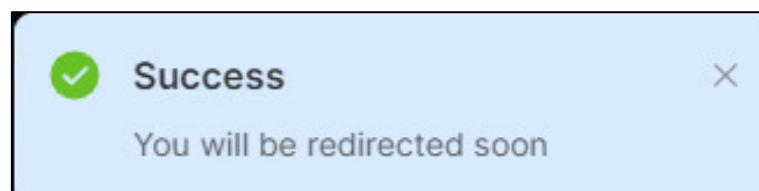
- Chọn **USB security key** để đăng ký bằng khoá bảo mật VinCSS FIDO2® Fingerprint.



- Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo. Sau đó nhấn **Allow** để tiếp tục.

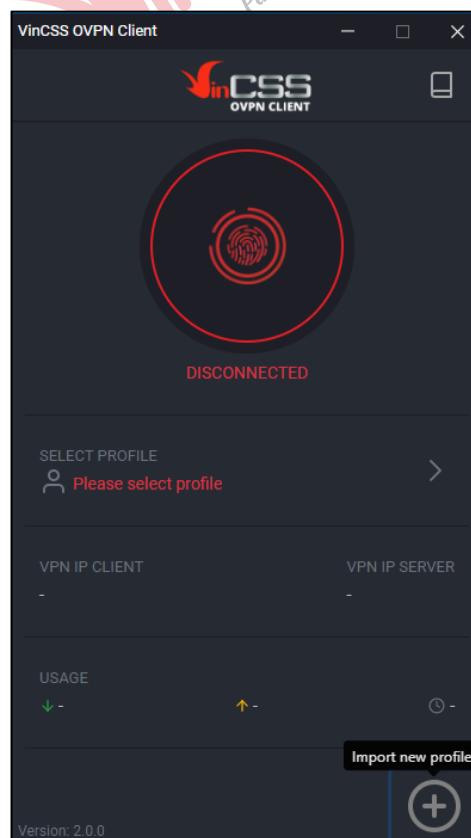


- Trên màn hình máy tính hiện pop-up thông báo người dùng đã đăng ký khoá bảo mật thành công.

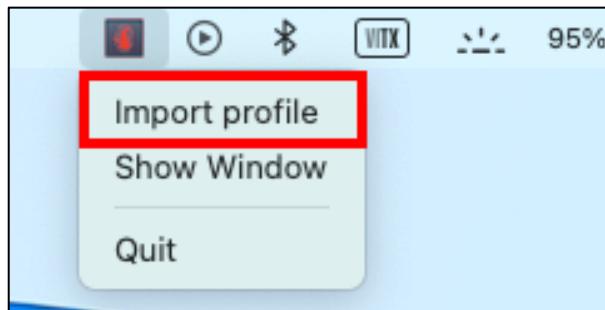


### III.3.2.2. Xác thực bằng khoá bảo mật VinCSS FIDO2® Fingerprint

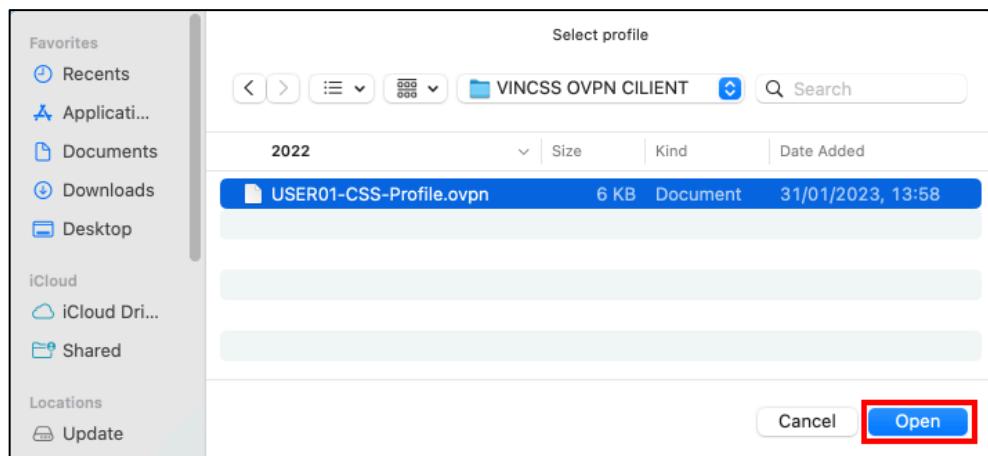
- Mở phần mềm VinCSS OVPN Client đã được cài đặt trong máy. Trên giao diện chính, nhấn vào dấu (+) để thêm mới profile.



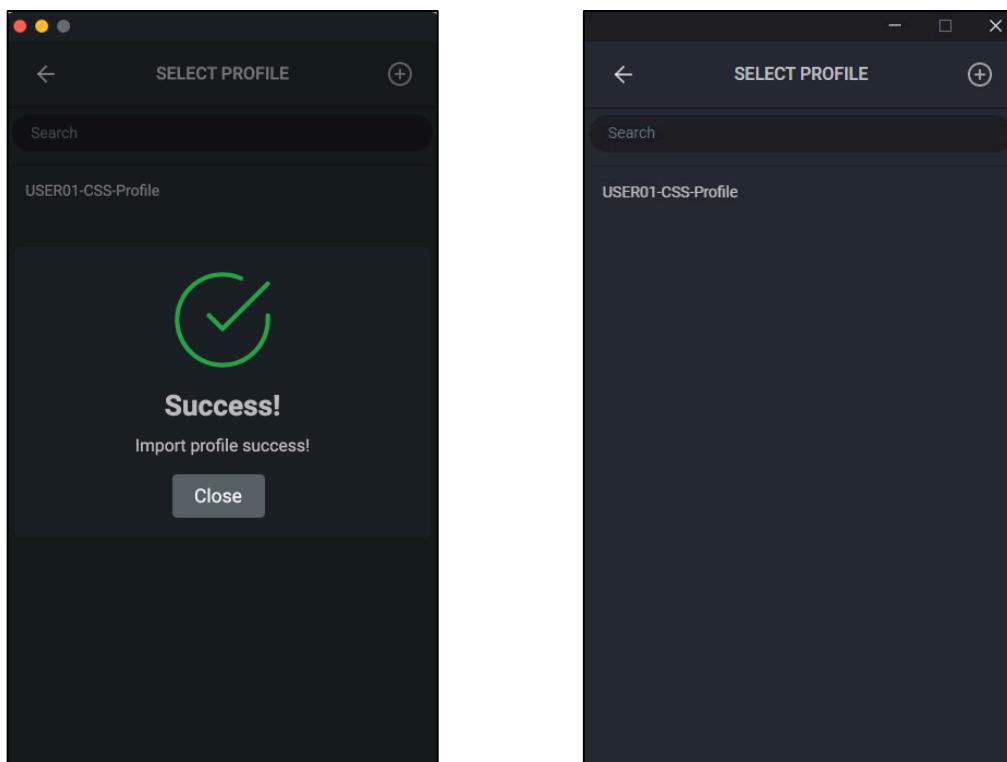
- Hoặc nhấp chuột phải vào biểu tượng VinCSS OVPN Client trên taskbar, chọn **Import profile**.



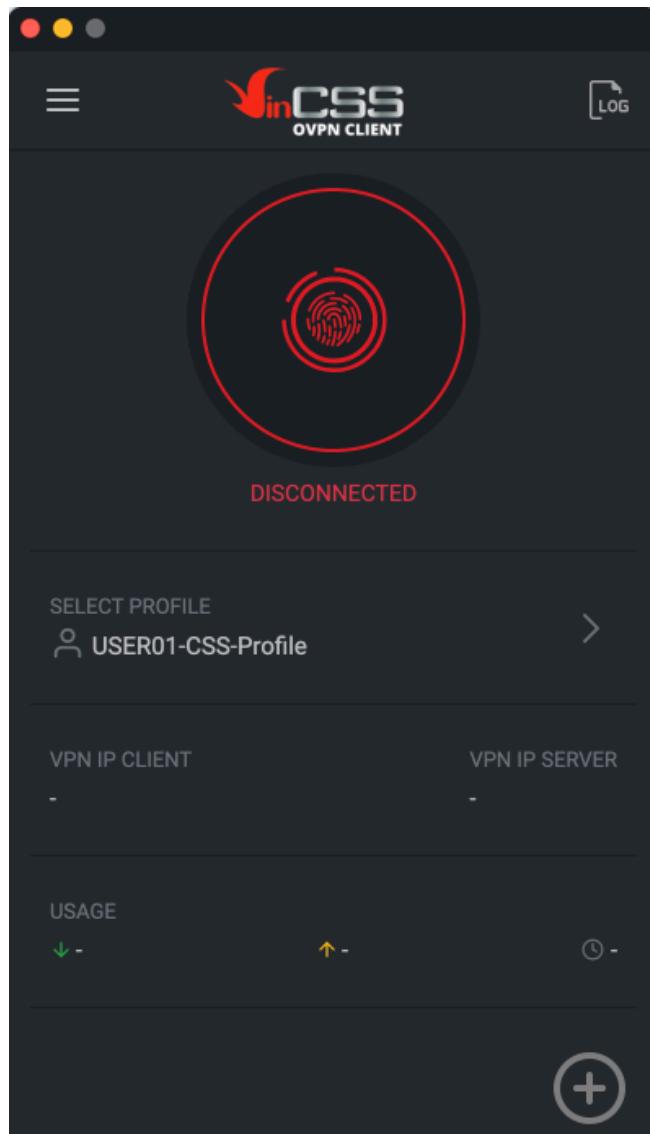
- Chọn profile được gửi bởi người quản trị (*file .ovpn*) và chọn **Open**.



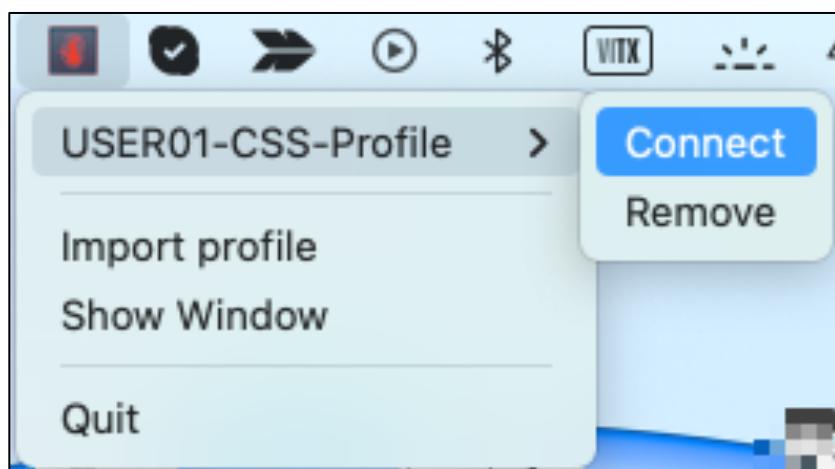
- Profile được thêm thành công, nhấn **Close** để đóng cửa sổ thông báo. Màn hình hiển thị tên profile trong danh sách.



- Nhấn vào biểu tượng vân tay màu đỏ trên giao diện ứng dụng để tiến hành kết nối VPN.

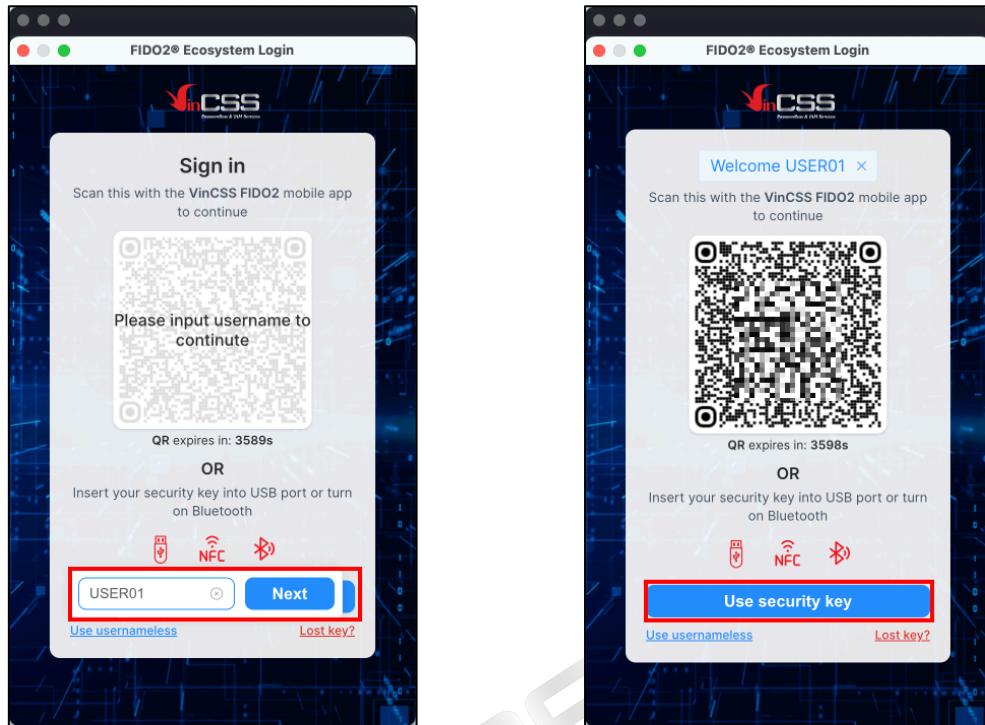


- Hoặc nhấp chuột phải vào biểu tượng VinCSS OVPN Client ở taskbar, chọn VPN profile cần kết nối, sau đó chọn **Connect**.



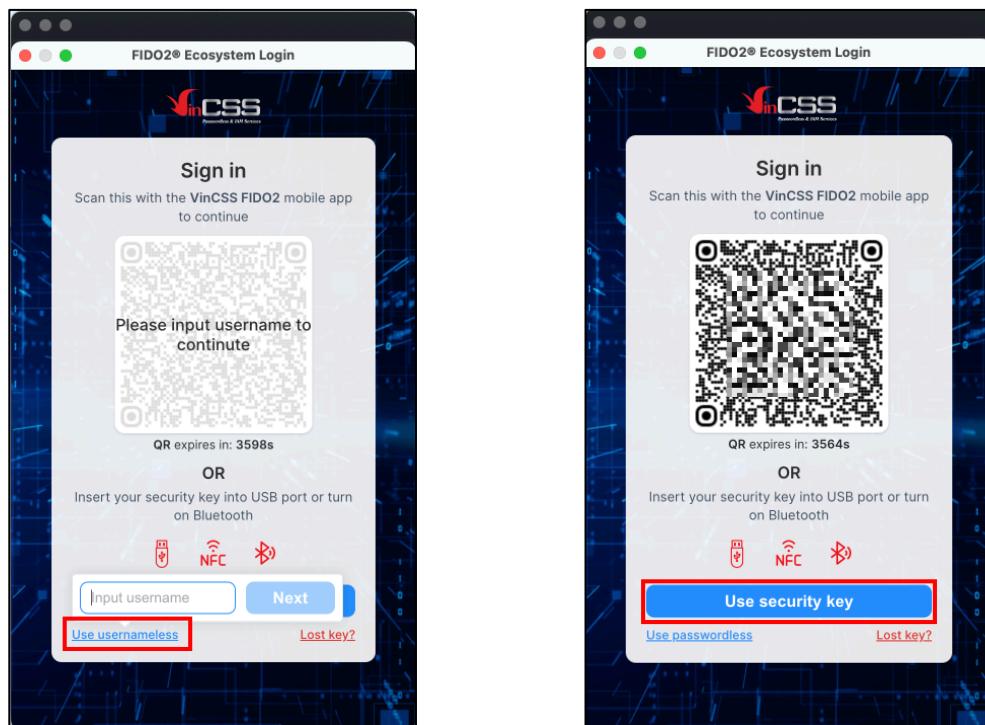
### III.3.2.2.1. Xác thực không mật khẩu

- Nhập **Username** (*không phân biệt chữ hoa, chữ thường*) rồi chọn **Next**. Sau đó chọn **Use security key** để tiếp tục.



### III.3.2.2.2. Xác thực không tên người dùng

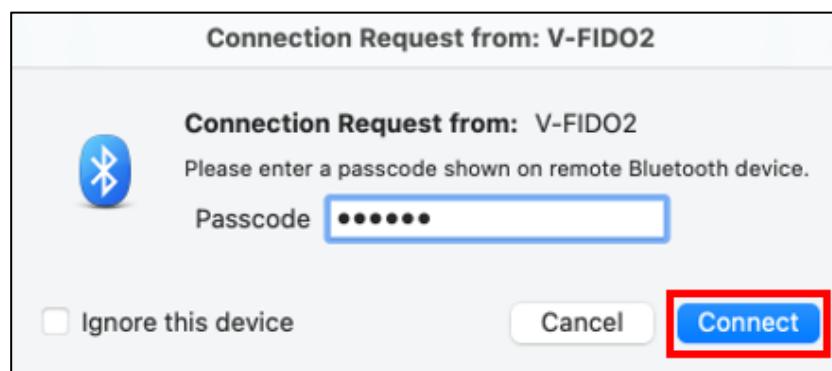
- Hoặc có thể chọn phương thức xác thực khác bằng cách chọn **Use usernameless** để thay cho bước nhập **username** rồi chọn **Use security key**.



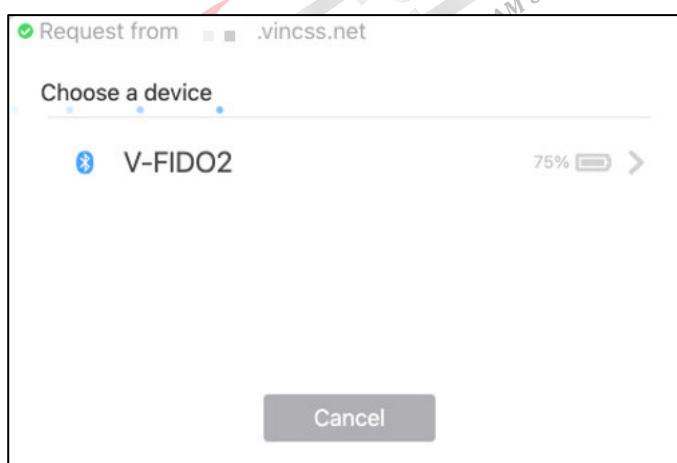
### III.3.2.2.2.1. Sử dụng qua kết nối Bluetooth

- Chạm và giữ vào phần quét vân tay (*khoảng 5-8 giây*) của khoá bảo mật cho đến khi đèn báo nháy sáng xanh. Khoá bảo mật đang ở trong trạng thái chờ ghép nối. Nhập mã ghép đôi (*Mã ghép đôi được ghi ở mặt sau của khóa bảo mật*) để kết nối rồi chọn **Connect**.

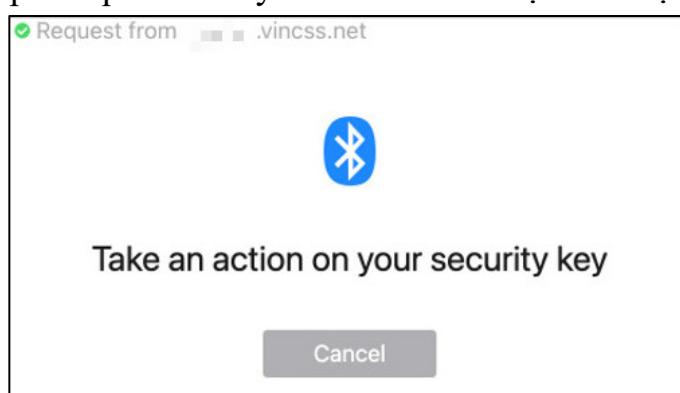
**Lưu ý:** macOS không hỗ trợ kết nối Bluetooth của khoá bảo mật trước đó. Chỉ có thể hỗ trợ kết nối Bluetooth của khoá bảo mật qua ứng dụng VinCSS OVPN Client tại bước này).



- Người dùng nhấn chọn vào tên của khoá bảo mật để kết nối.

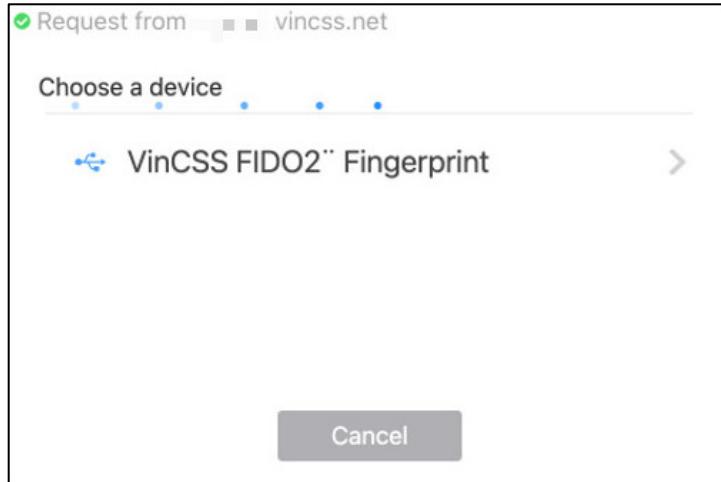


- Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

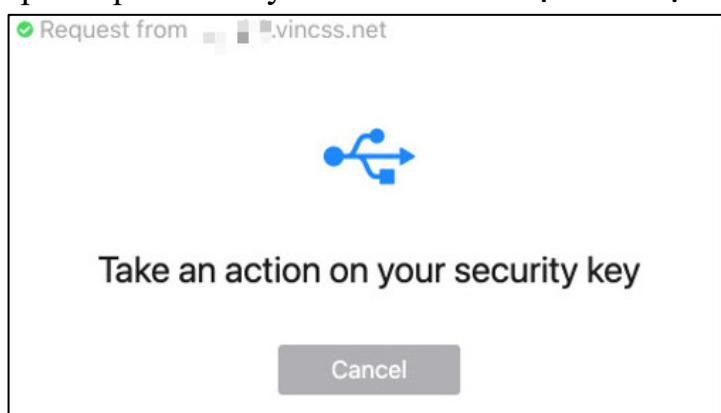


### III.3.2.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB. Chọn thiết bị cần kết nối.



- Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

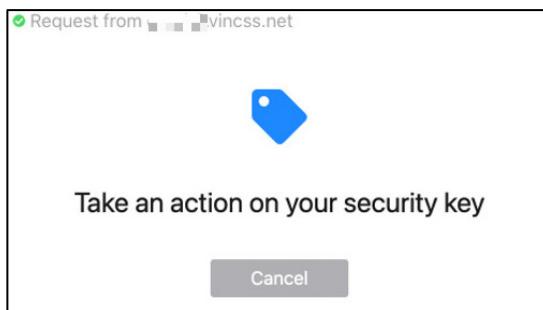


### III.3.2.2.3. Sử dụng qua kết nối NFC

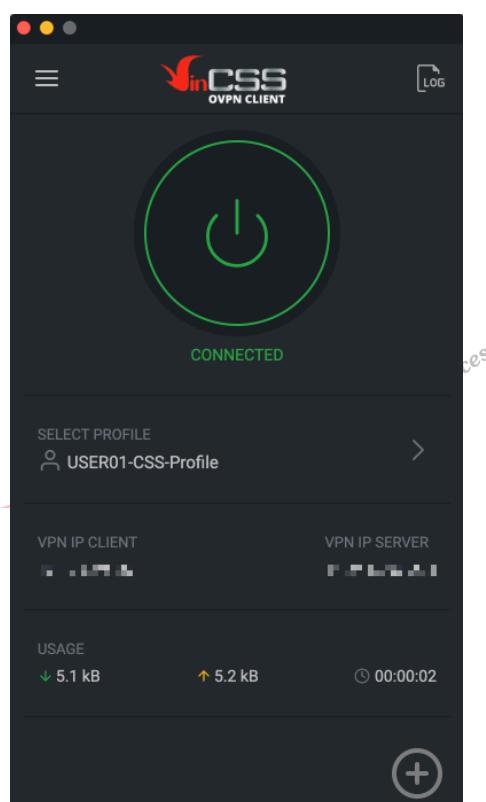
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chọn thiết bị cần kết nối.



- Chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Kết nối VPN thành công, trên giao diện ứng dụng hiển thị trạng thái **CONNECTED**.



### III.4. Xác thực 2 yếu tố tài khoản Facebook

#### III.4.1. Đăng ký khoá bảo mật

- Đăng nhập vào <https://www.facebook.com/>, sau đó vào phần **Cài đặt > Bảo mật và đăng nhập** bên menu trái.



- Tại mục **Xác thực 2 yếu tố**, chọn **Chỉnh sửa** ở phần **Dùng tính năng xác thực 2 yếu tố**.

The screenshot shows the 'Bảo mật và đăng nhập' (Security and Login) settings page on Facebook. On the left sidebar, under 'Cài đặt' (Settings), 'Bảo mật và đăng nhập' (Security and Login) is selected. In the main content area, there are several sections: 'Để xuất' (Export), 'Nơi bạn đã đăng nhập' (Places you've logged in from), 'Đăng nhập' (Logins), and 'Xác thực 2 yếu tố' (Two-factor authentication). The 'Xác thực 2 yếu tố' section contains two items: 'Dùng tính năng xác thực 2 yếu tố' (Use the two-factor authentication feature) and 'Đăng nhập hợp lệ' (Allow trusted logins). The 'Chỉnh sửa' (Edit) button for the first item is highlighted with a red box.

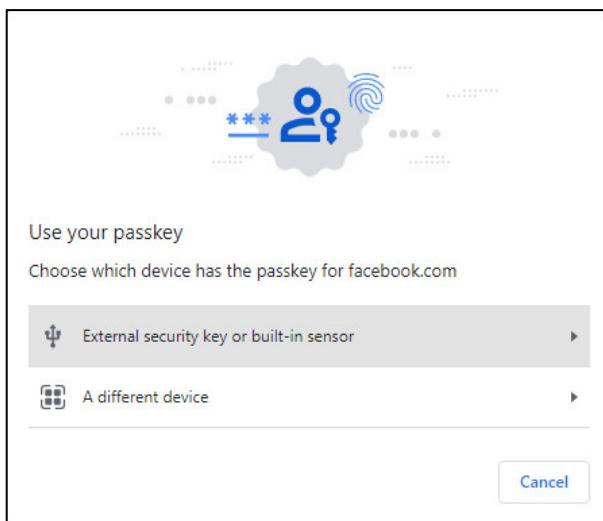
- Từ danh sách **Chọn phương thức bảo mật**, chọn **Sử dụng khóa bảo mật**.

The screenshot shows the 'Chọn phương thức bảo mật' (Select security method) screen. It lists three options: 'Ứng dụng xác thực' (Authenticator app), 'Tin nhắn văn bản (SMS)' (Text message (SMS)), and 'Khóa bảo mật' (Security key). The 'Khóa bảo mật' section contains a description: 'Sử dụng khóa bảo mật vật lý để không ai có thể truy cập trái phép vào tài khoản Facebook của bạn. Bạn sẽ không cần nhập mã nữa.' (Use a physical security key so no one can illegally access your Facebook account. You won't need to enter a code again.) and a 'Sử dụng khóa bảo mật' (Use a security key) button, which is highlighted with a red box.

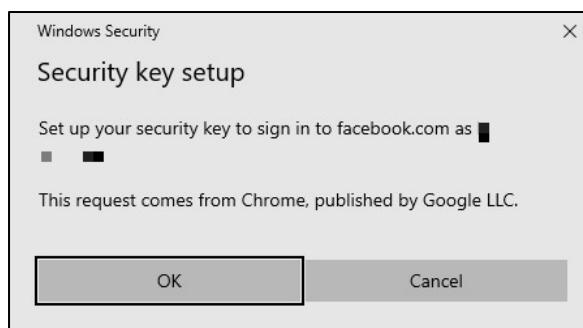
- Ở hộp thoại **Xác thực hai yếu tố**, chọn **Đăng ký khóa bảo mật**.

The screenshot shows the 'Xác thực 2 yếu tố' (Two-factor authentication) setup dialog. It has a heading 'Cắm khóa bảo mật' (Insert security key) with a USB drive icon. Below it, a text box says: 'Nếu có khóa bảo mật USB, bạn có thể dùng khóa để bảo vệ tài khoản Facebook của mình.' (If you have a USB security key, you can use it to protect your Facebook account.) At the bottom, there are two buttons: 'Quay lại' (Back) and 'Đăng ký khóa bảo mật' (Register security key), which is highlighted with a red box.

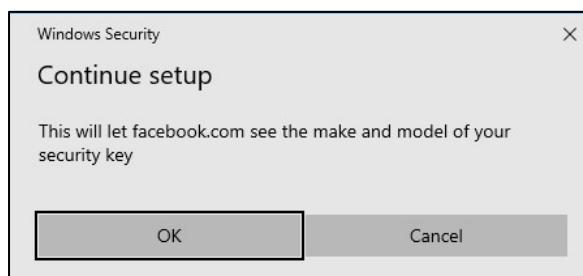
- Chọn **External security key or built-in sensor** để thiết lập khoá bảo mật.



- Để tiếp tục quá trình đăng ký, nhấn **OK**.

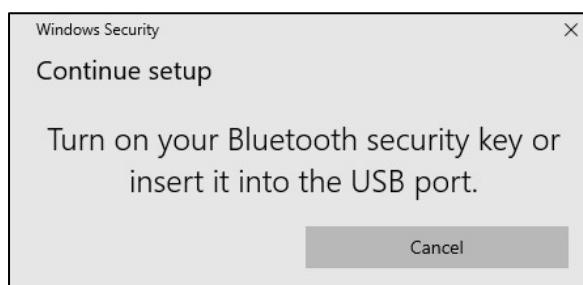


- Nhấn **OK** để tiếp tục.

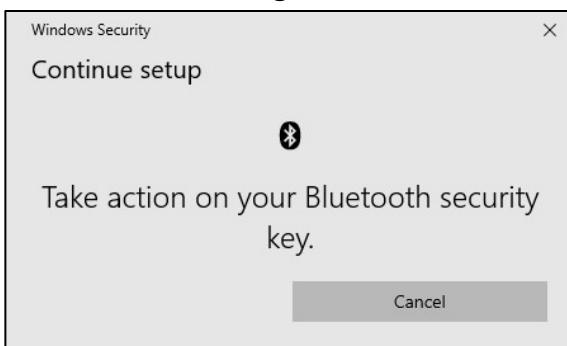


### III.4.1.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint vào máy tính thông qua Bluetooth.

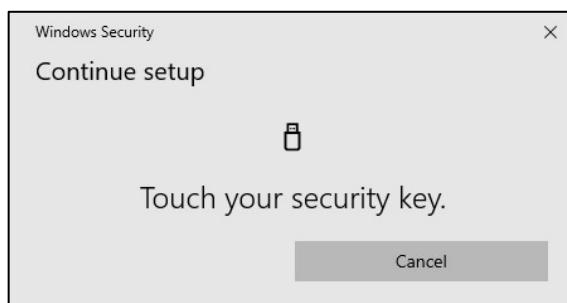


- Quét vân tay khi nhận được thông báo.



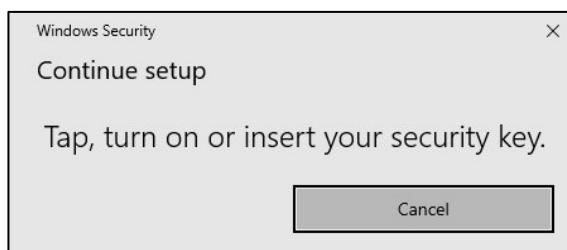
### III.4.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB. Chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



### III.4.1.3. Sử dụng qua kết nối NFC

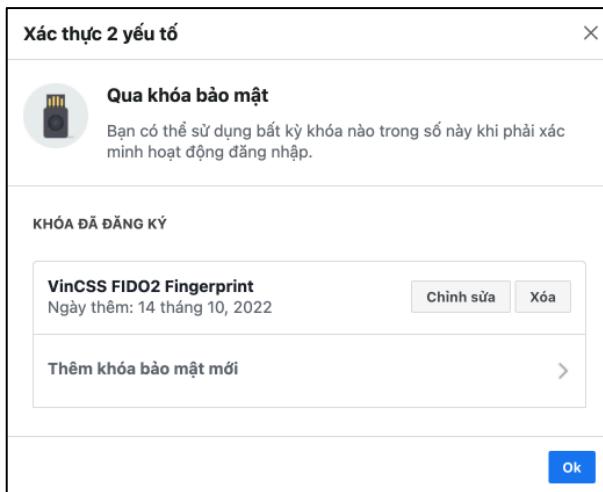
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật để phân biệt giữa các khoá, sau đó nhấn **Lưu** để lưu lại thông tin khoá.

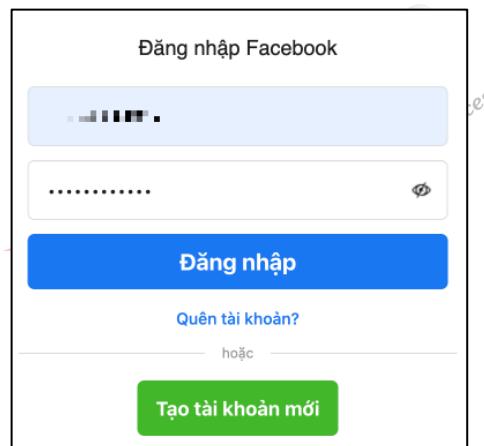


- Thông tin khoá bảo mật đã được đăng ký thành công.

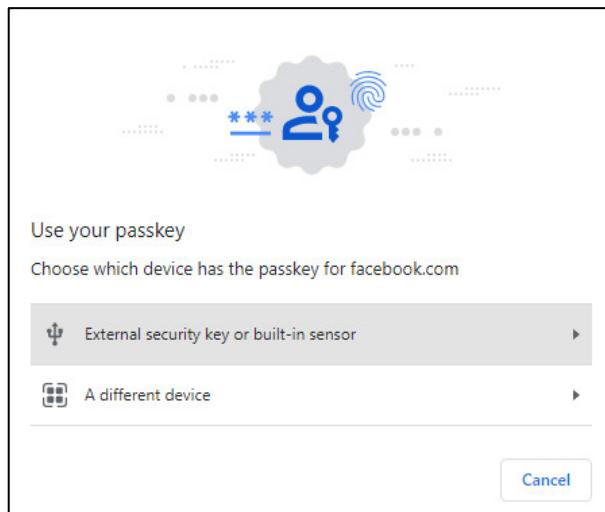


### III.4.2. Xác thực 2 yếu tố với dịch vụ Facebook

- Truy cập <https://www.facebook.com/>, đăng nhập với tài khoản và mật khẩu.



- Sau khi nhập mật khẩu, trình duyệt yêu cầu người dùng thực hiện xác thực bằng khoá bảo mật. Chọn **External security key or built-in sensor**.

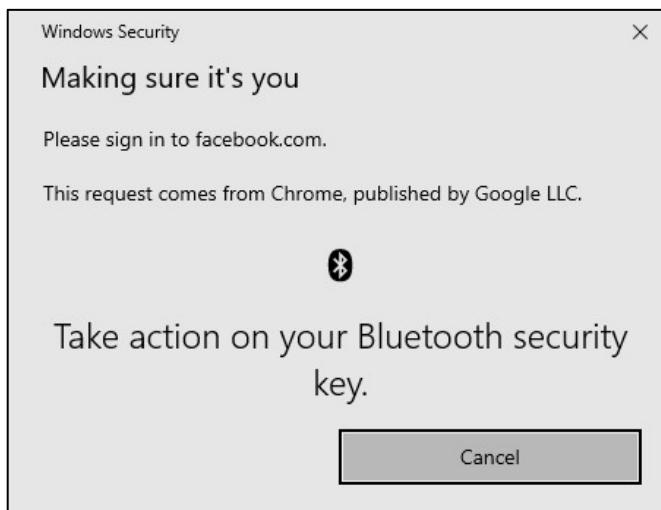


### III.4.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua kết nối Bluetooth.



- Quét vân tay khi nhận được thông báo.



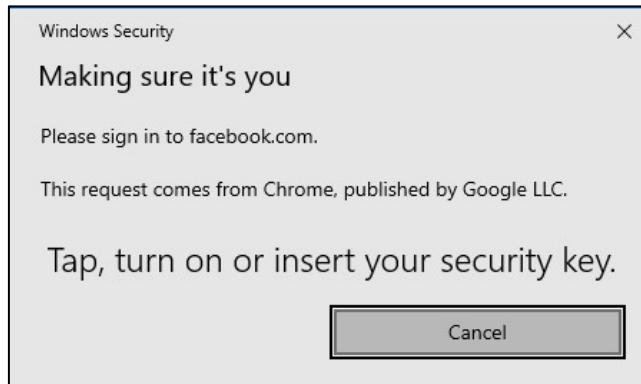
### III.4.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



### III.4.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



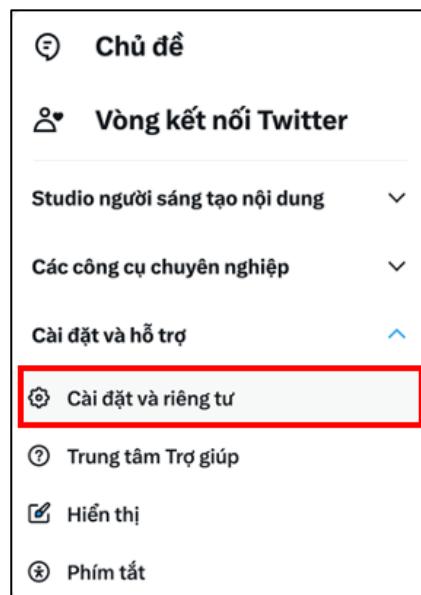
- Xác thực thành công. Chọn **Không lưu** rồi nhấn **Tiếp tục**.



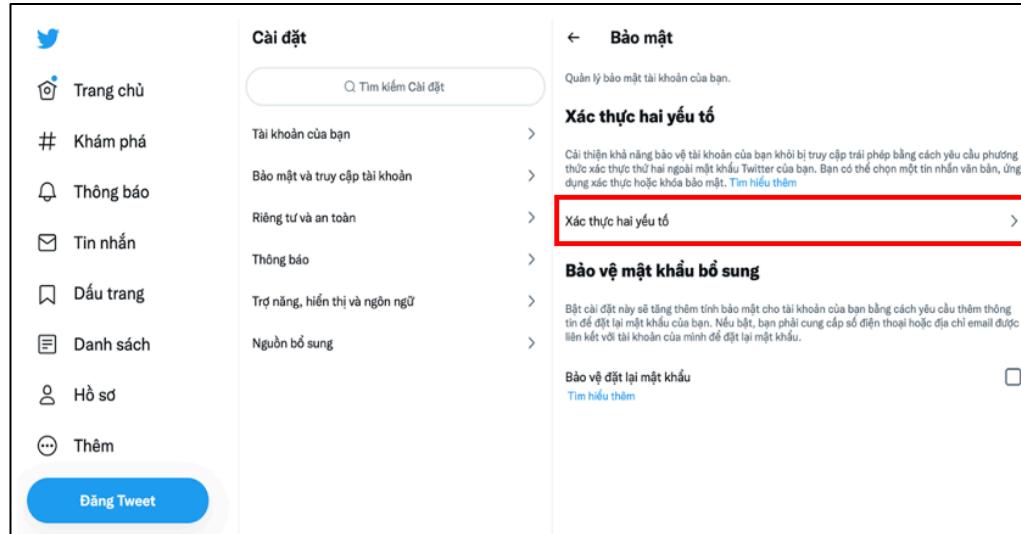
## III.5. Xác thực 2 yếu tố với Twitter

### III.5.1. Đăng ký khoá bảo mật

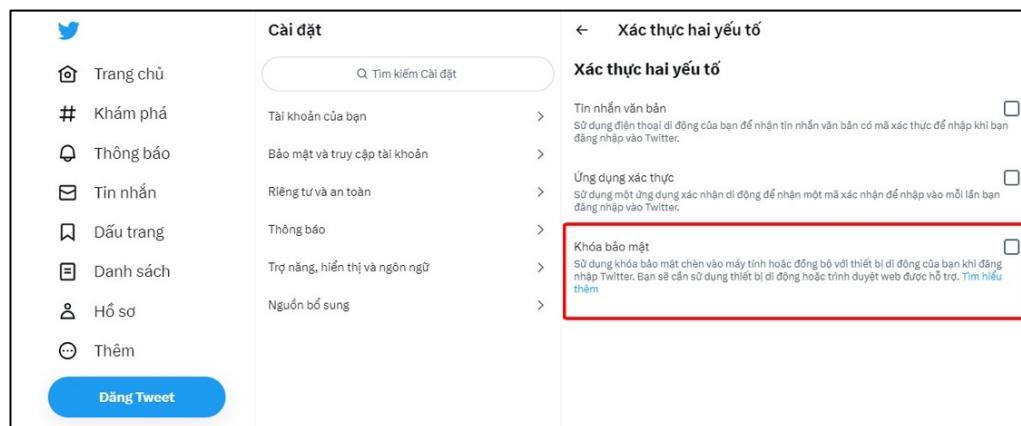
- Đăng nhập vào <https://twitter.com>, sau đó chọn **Thêm > Cài đặt và hỗ trợ > Cài đặt và riêng tư**.



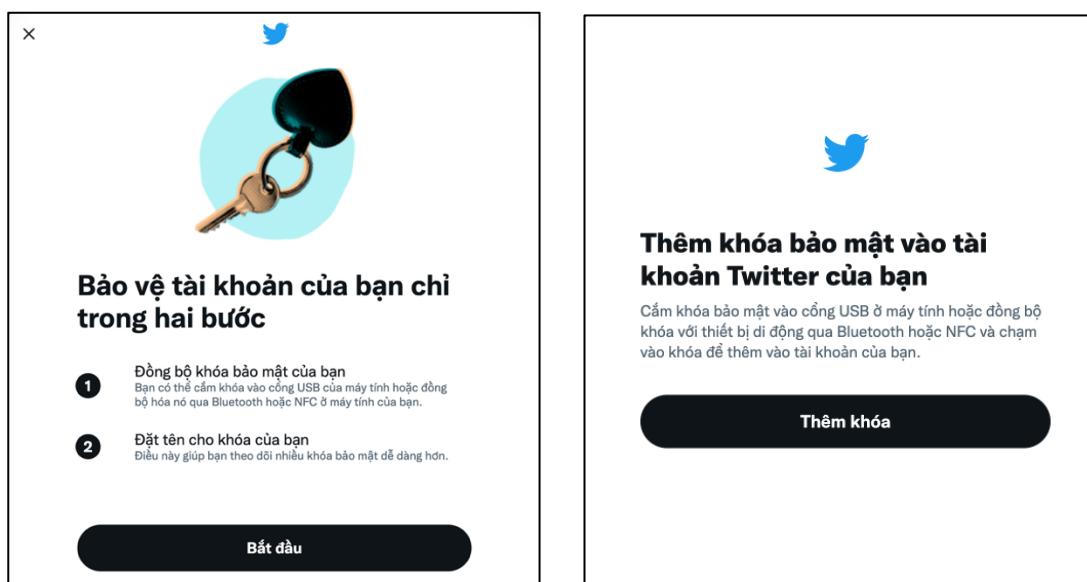
- Chọn **Bảo mật và truy cập tài khoản > Bảo mật > Xác thực hai yếu tố.**



- Tại mục **Xác thực hai yếu tố**, chọn tính năng **Khoá bảo mật**.



- Ở bảng thông báo, chọn **Bắt đầu > Thêm khoá** để bắt đầu quá trình đăng ký khoá bảo mật.

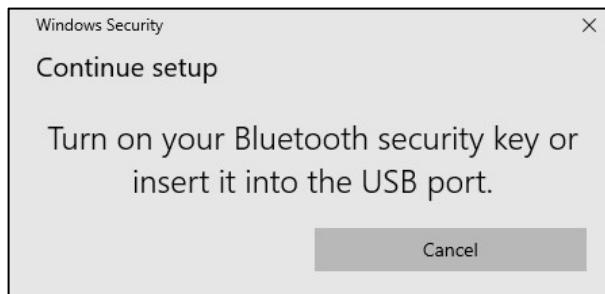


- Nhấn **OK** để tiếp tục.

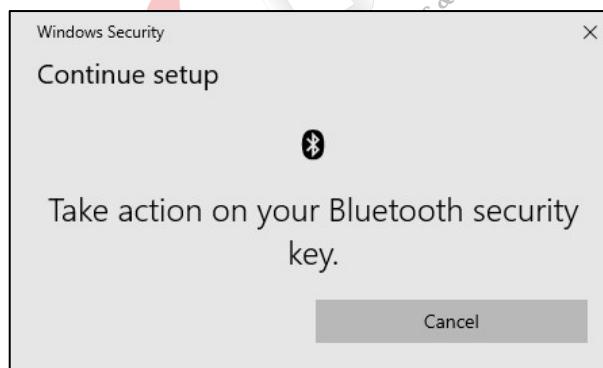


### III.5.1.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật với máy tính thông qua Bluetooth.

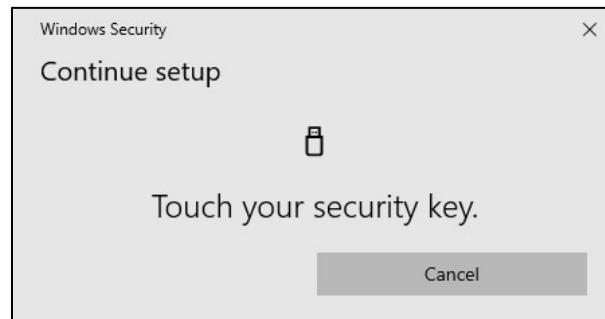


- Quét vân tay khi nhận được thông báo.



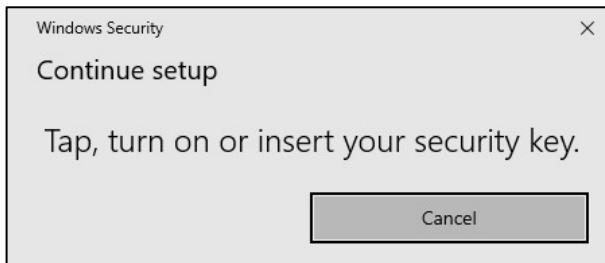
### III.5.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.

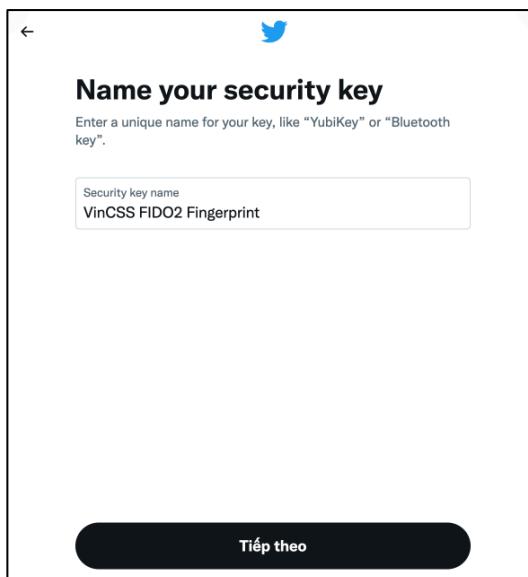


### III.5.1.3. Sử dụng qua kết nối NFC

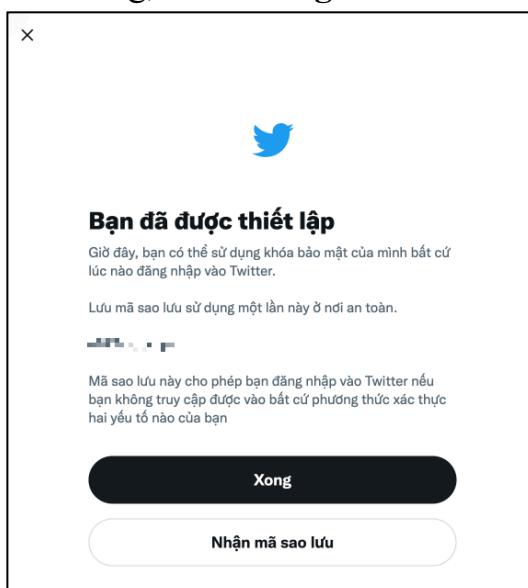
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho khoá bảo mật để phân biệt giữa các khoá, sau đó nhấn **Tiếp theo** để lưu lại thông tin khoá.

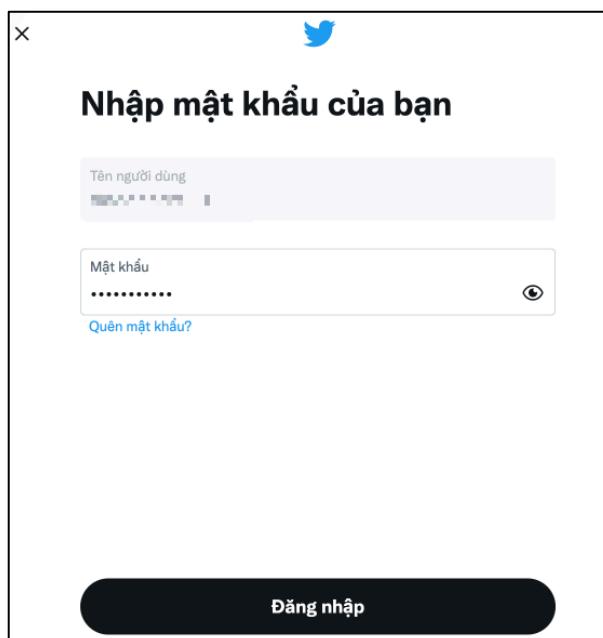


- Đăng ký khoá thành công, nhấn **Xong** để hoàn thành.



### III.5.2. Xác thực 2 yếu tố với dịch vụ Twitter

- Truy cập <https://twitter.com> rồi đăng nhập với tài khoản và mật khẩu.



#### III.5.2.1. Sử dụng qua kết nối Bluetooth

- Người dùng kết nối khoá bảo mật với máy tính thông qua Bluetooth.



- Quét vân tay khi nhận được thông báo.



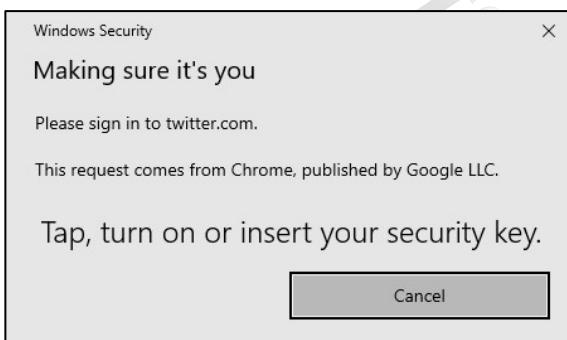
### III.5.2.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



### III.5.2.3. Sử dụng qua kết nối NFC

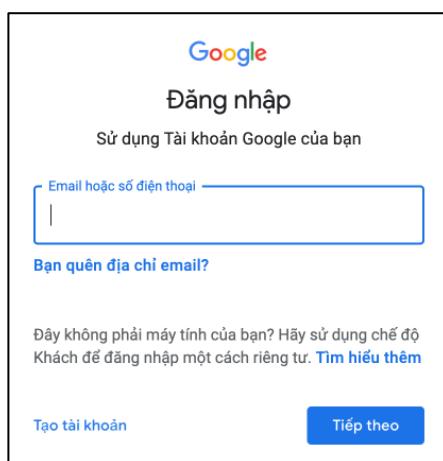
- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



## III.6. Xác thực 2 yếu tố với Google

### III.6.1. Đăng ký khoá bảo mật

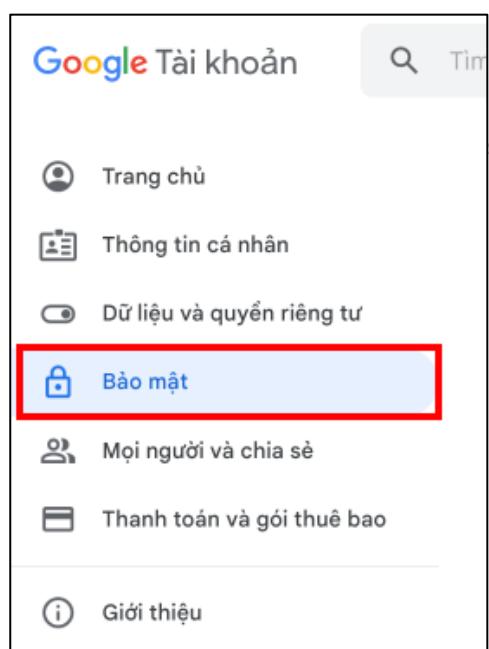
- Truy cập vào <https://accounts.google.com/>, đăng nhập với tài khoản và mật khẩu.



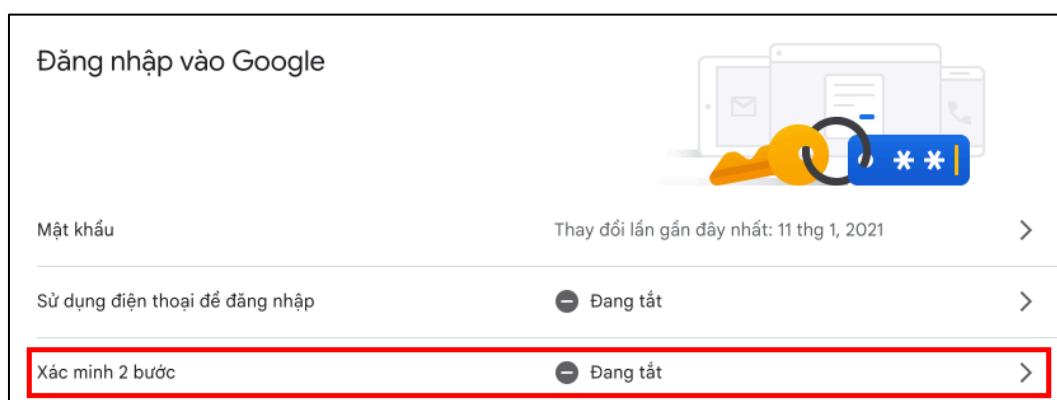
- Bấm vào biểu tượng account góc trên bên phải, chọn **Quản lý Tài khoản Google của bạn**.



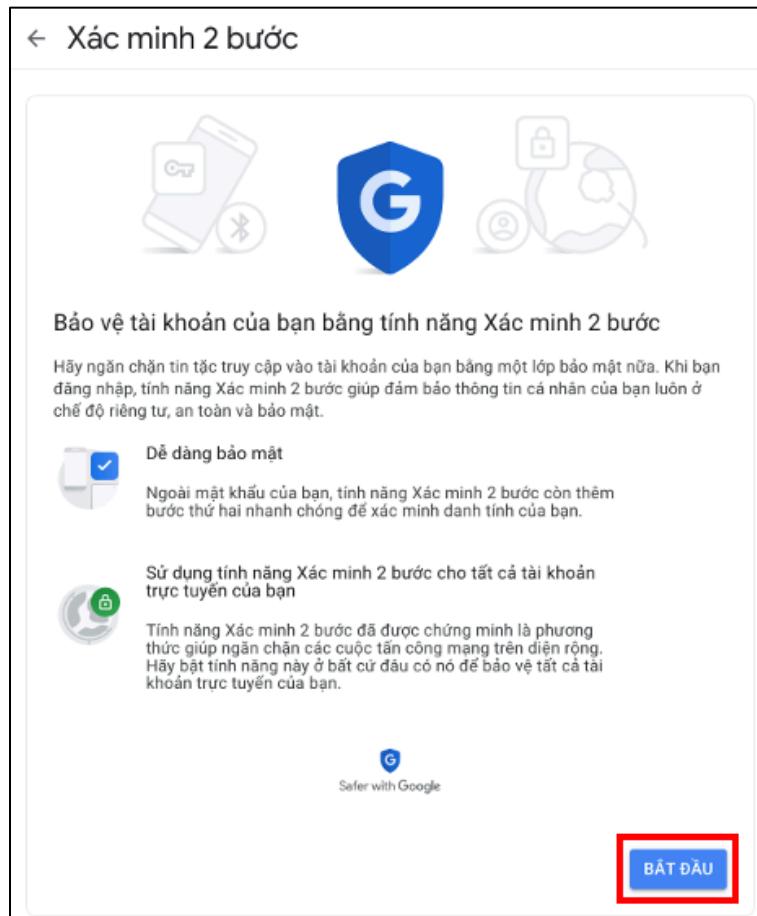
- Chọn mục **Bảo mật** tại menu bên trái.



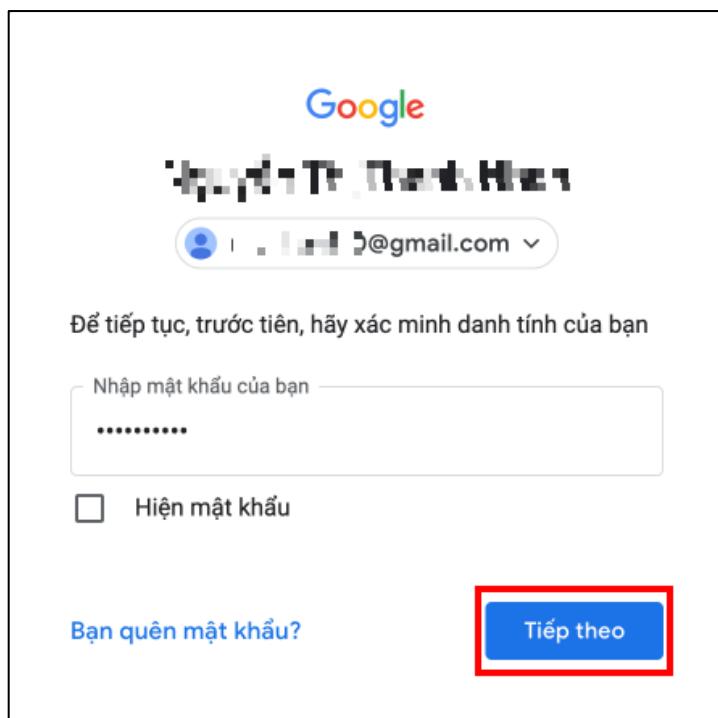
- Chọn mục **Xác minh 2 bước** để thiết lập xác thực hai yếu tố.



- Trong trường hợp chưa đăng ký xác thực 2 bước trước đó, cần xác minh danh tính của người dùng trước khi thiết lập khoá bảo mật. Nhấn **Bắt đầu**.



- o Nhập mật khẩu để xác minh danh tính và nhấn **Tiếp theo**.



Để tiếp tục, trước tiên, hãy xác minh danh tính của bạn

Nhập mật khẩu của bạn

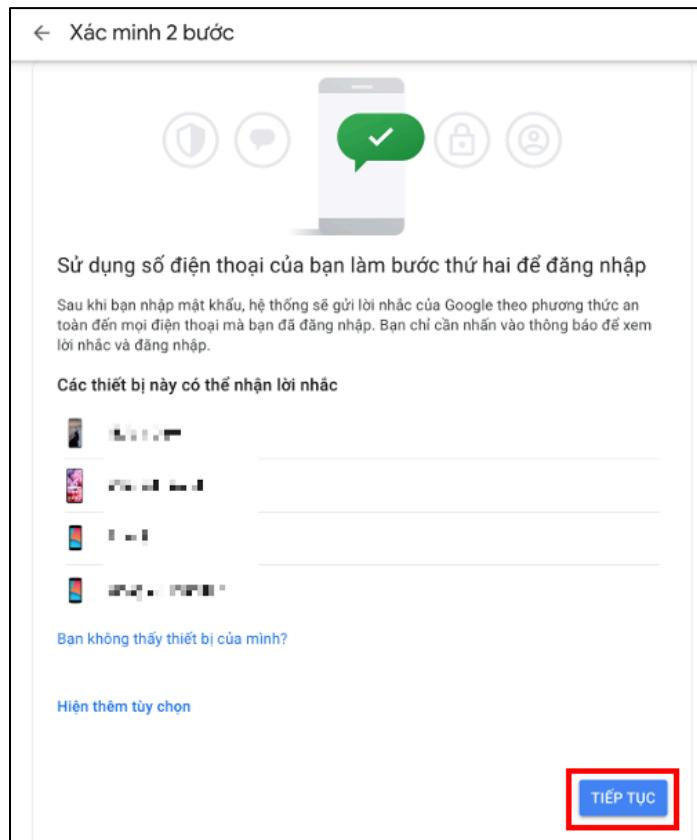
.....

Hiện mật khẩu

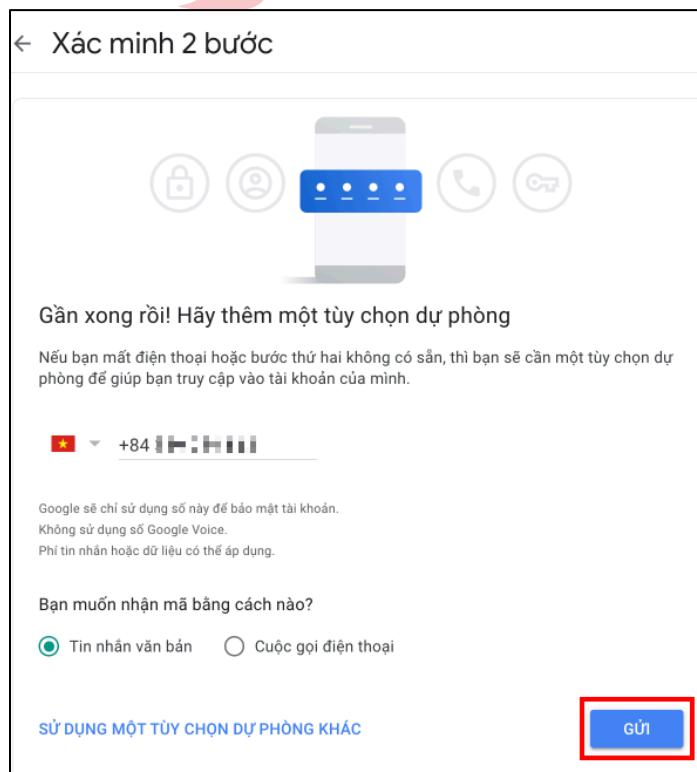
[Bạn quên mật khẩu?](#)

**Tiếp theo**

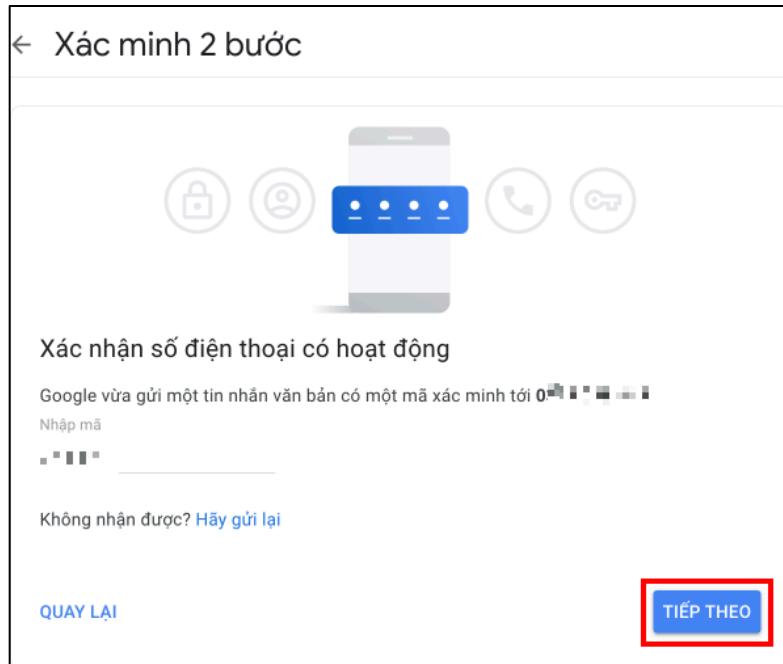
- Nhấn **Tiếp tục** để sử dụng số điện thoại làm bước thứ 2 để đăng nhập.



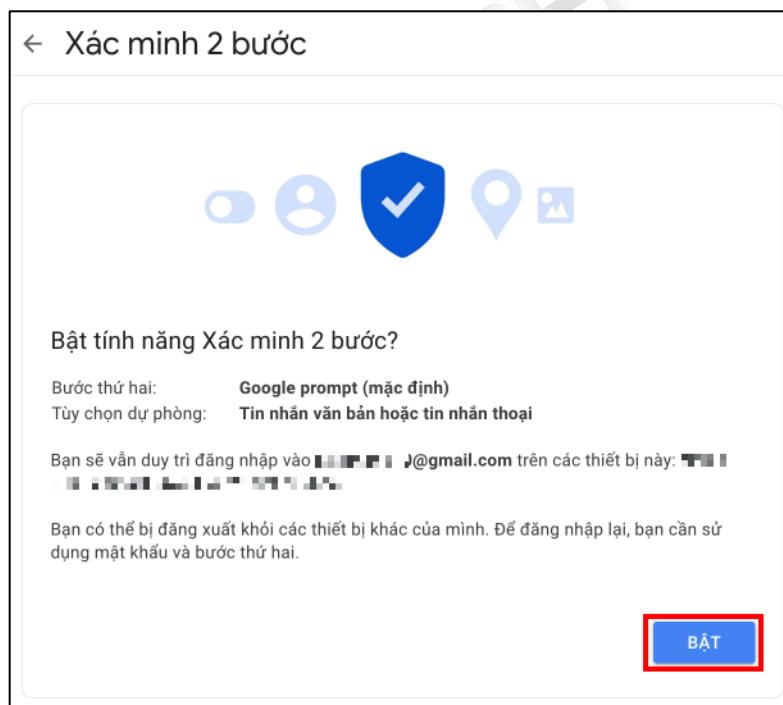
- Nhập số điện thoại và lựa chọn cách nhận mã rồi nhấn **Gửi** (*mặc định nhận bằng tin nhắn văn bản*).



- Nhập mã xác minh được gửi về điện thoại và nhấn **Tiếp theo**.



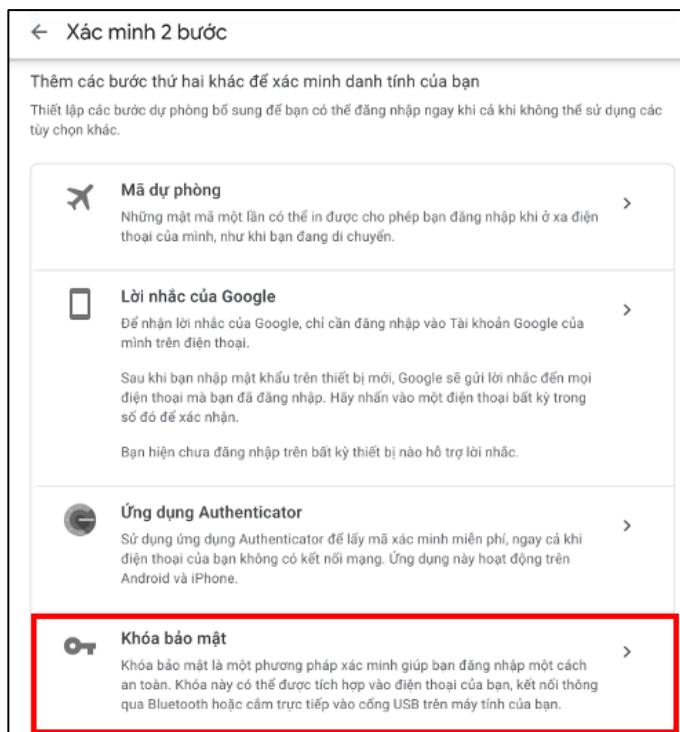
- Nhấn vào **Bật** để bật Xác minh 2 bước.



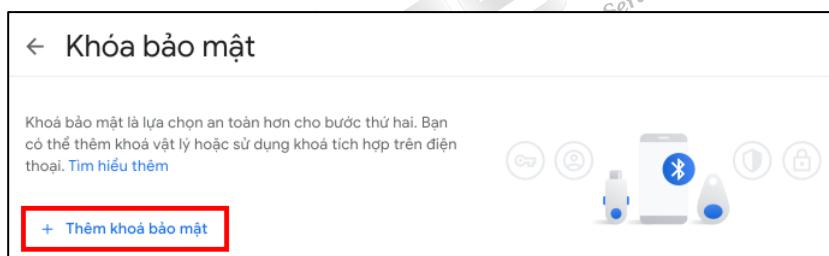
- Hoàn thành bước xác minh.



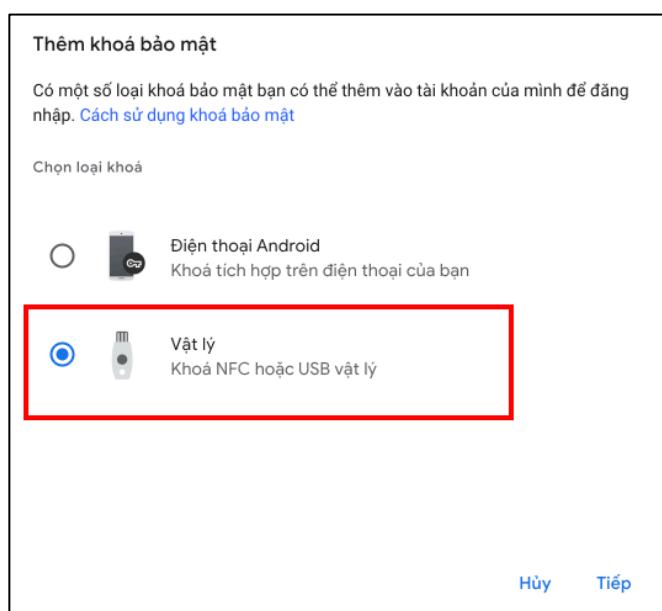
- Ở mục xác minh 2 bước, chọn **Khoá bảo mật**.



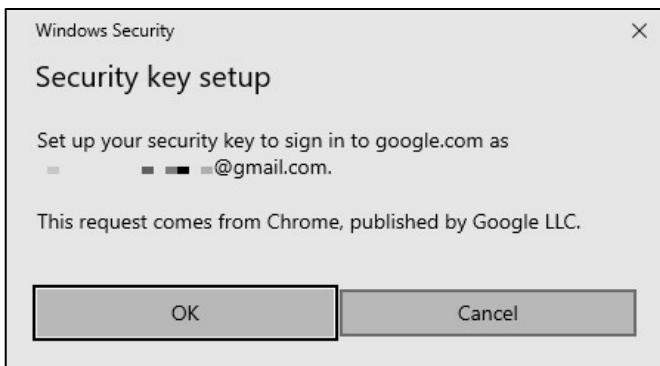
- Ở mục Khoá bảo mật chọn **Thêm khoá bảo mật**.



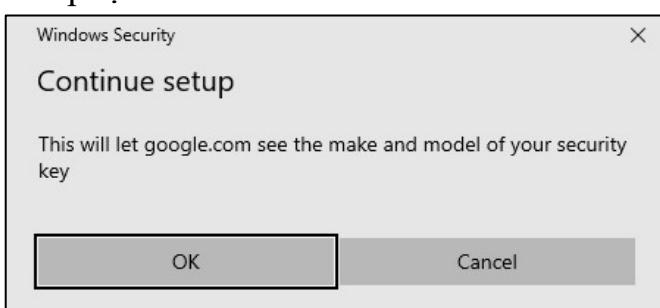
- Chọn **Vật lý** rồi nhấn **Tiếp** để thêm khóa bảo mật.



- Nhấn **OK** để tiếp tục quá trình đăng ký.

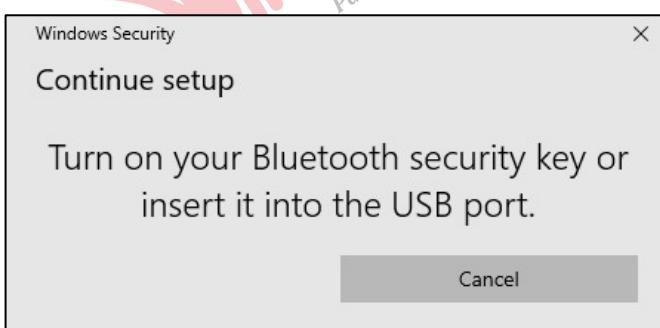


- Nhấn **OK** để tiếp tục.

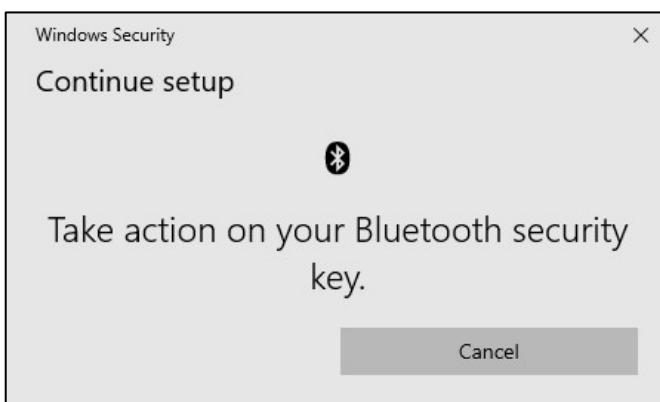


### III.6.1.1. Sử dụng qua kết nối Bluetooth

- Người dùng kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua Bluetooth.

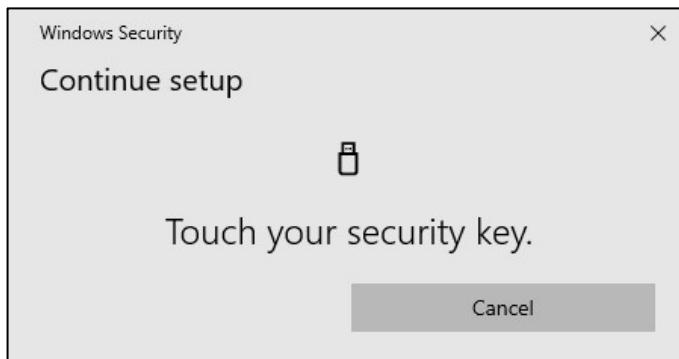


- Quét vân tay khi nhận được thông báo.



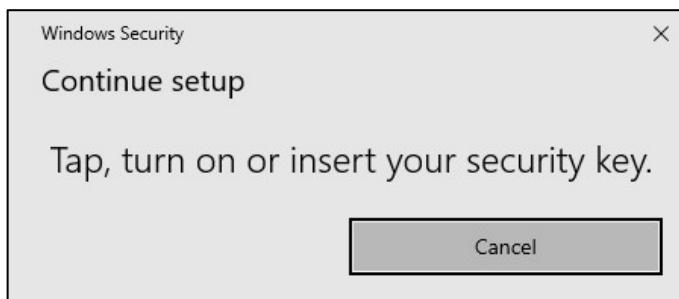
### III.6.1.2. Sử dụng qua kết nối USB

- Kết nối khoá bảo mật với máy tính thông qua dây kết nối USB, chạm vào phần quét vân tay trên khoá bảo mật khi nhận được thông báo.



### III.6.1.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Đặt tên cho thiết bị khoá bảo mật để dễ phân biệt trong trường hợp người dùng sử dụng đồng thời nhiều khóa (*tối đa 20 ký tự*), sau đó nhấn **Tiếp**.



- Chọn **Tiếp** để hoàn thành quá trình đăng ký khoá bảo mật.

Đã thêm khoá bảo mật



Tính năng Xác minh 2 bước hiện đã bật cho tài khoản của bạn. Bây giờ, bạn đã có thể dùng khoá bảo mật.

Giữ khoá bảo mật bên mình để bạn luôn có thể đăng nhập vào Tài khoản Google của mình.

[Quay lại](#) [Tiếp](#)

- Chọn **Tiếp** để hoàn tất đăng ký. Từ thời điểm này mọi dịch vụ của Google yêu cầu người dùng đăng nhập phải xác thực với cả mật khẩu và khóa bảo mật.

Cách đăng nhập bằng khoá bảo mật thông qua USB

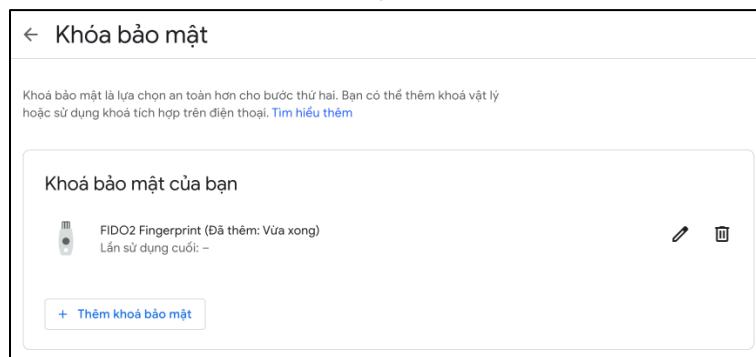


Bạn cũng có thể cắm khoá trực tiếp vào thiết bị mà bạn đang đăng nhập.

- Hãy cắm khoá bảo mật vào cổng USB trên thiết bị. Bạn có thể cần cáp hoặc đầu chuyển đổi.
- Nếu bạn thấy thông báo từ dịch vụ Google Play, hãy nhấn vào OK.
- Nếu khoá có vòng tròn đệm màu vàng, hãy chạm vào vòng tròn đệm đó. Nếu khoá có nút, hãy nhấn vào nút đó.
- Nếu khoá không có bất kỳ đặc điểm nào trong số này, hãy tháo và cắm lại khoá để kết nối.

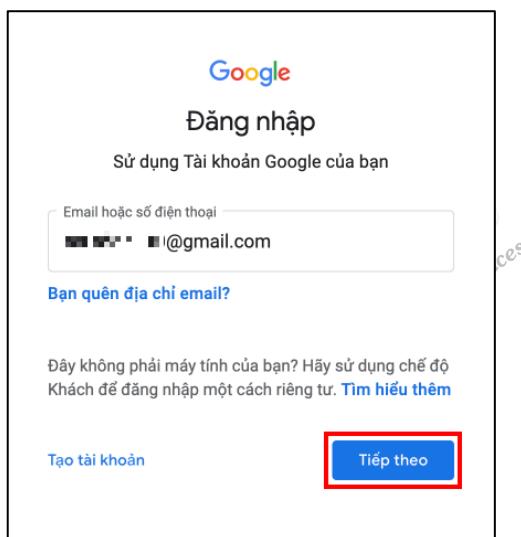
[Quay lại](#) [Tiếp](#)

- Đăng ký khoá bảo mật thành công.



### III.6.2. Xác thực 2 yếu tố với dịch vụ Google

- Truy cập vào <https://accounts.google.com/> rồi đăng nhập bằng tài khoản và mật khẩu.



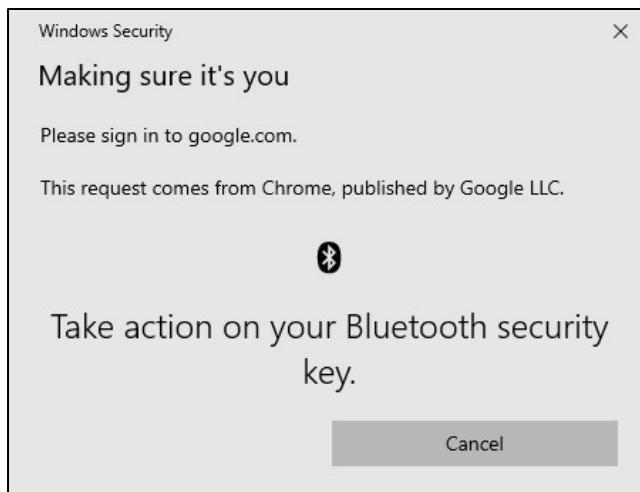
- Sau khi xác thực với mật khẩu, trình duyệt yêu cầu người dùng thực hiện xác thực bằng khoá bảo mật.

#### III.6.2.1. Sử dụng qua kết nối Bluetooth

- Kết nối khoá bảo mật VinCSS FIDO2® Fingerprint với máy tính thông qua Bluetooth.



- Quét vân tay khi nhận được thông báo.



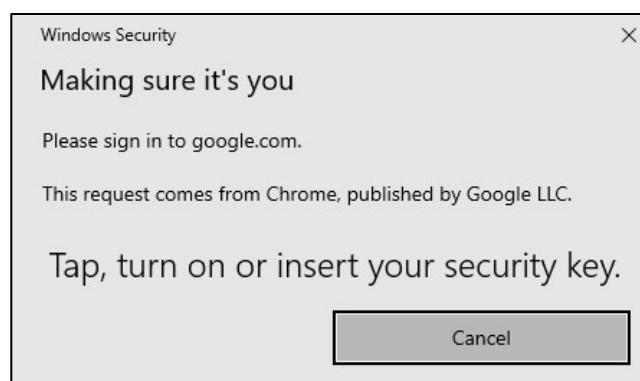
### III.6.2.2. Sử dụng qua kết nối USB

- Kết nối VinCSS FIDO2® Fingerprint vào máy tính thông qua dây USB. Chạm vào phần quét vân tay trên khoá bảo mật VinCSS FIDO2® Fingerprint khi nhận được thông báo.

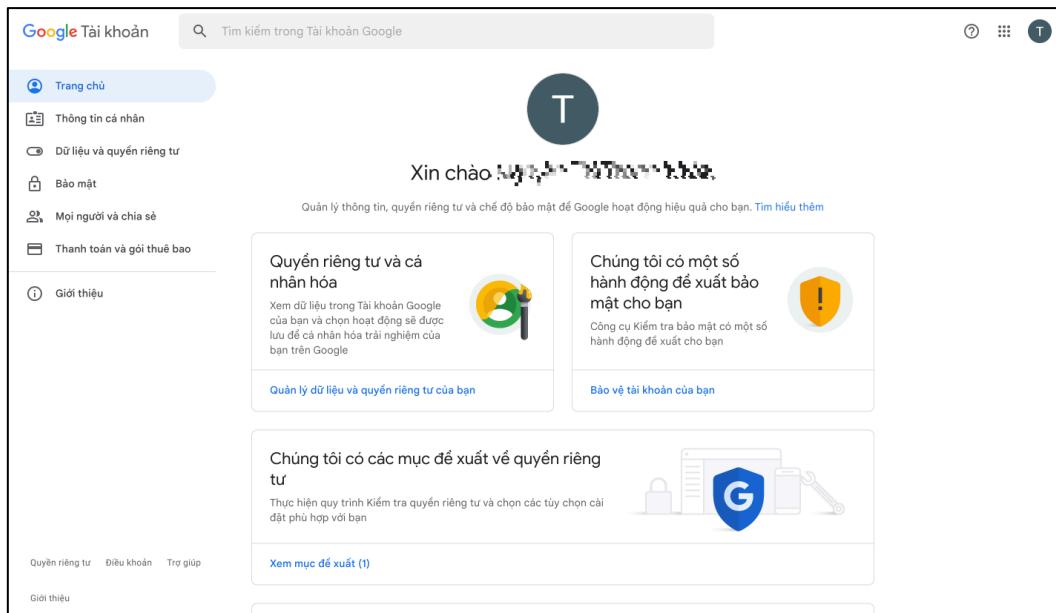


### III.6.2.3. Sử dụng qua kết nối NFC

- Kết nối khoá bảo mật với máy tính thông qua đầu đọc NFC, chạm khoá bảo mật vào đầu đọc NFC khi nhận được thông báo.



- Quá trình đăng nhập thành công, người dùng vào được tài khoản.



The screenshot shows the Google Account Settings page. At the top, there's a search bar labeled "Tim kiếm trong Tài khoản Google". On the left, a sidebar lists options: Trang chủ, Thông tin cá nhân, Dữ liệu và quyền riêng tư, Bảo mật, Mọi người và chia sẻ, Thanh toán và gói thuê bao, and Giới thiệu. The main content area has a large circular profile picture placeholder with a letter 'T'. Below it, a message says "Xin chào **Nguyễn Văn Hùng**". A note states: "Quản lý thông tin, quyền riêng tư và chế độ bảo mật để Google hoạt động hiệu quả cho bạn. [Tim hiểu thêm](#)". There are two main sections: "Quyền riêng tư và cá nhân hóa" (with a green and yellow icon) and "Chúng tôi có một số hành động để xuất bảo mật cho bạn" (with a yellow shield icon). Both sections have descriptive text and links like "Quản lý dữ liệu và quyền riêng tư của bạn" and "Bảo vệ tài khoản của bạn". At the bottom, there's a section titled "Chúng tôi có các mục để xuất về quyền riêng tư" (with a blue shield icon) and a link "Xem mục để xuất (1)". Navigation links at the bottom include "Quyền riêng tư", "Điều khoản", "Trợ giúp", and "Giới thiệu".

## THAM KHẢO

- Hệ sinh thái VinCSS FIDO2®:

<https://passwordless.vincss.net>

- Kênh Youtube VinCSS:

[https://www.youtube.com/channel/UCNtS\\_7d4GtyecE2HCpJSr7g](https://www.youtube.com/channel/UCNtS_7d4GtyecE2HCpJSr7g)

- Các câu hỏi thường gặp:

<https://passwordless.vincss.net/hotro>

- Hướng dẫn sử dụng ứng dụng VinCSS OVPN Client:

<https://github.com/VinCSS-Public-Projects/FIDO2-Public-Documents/tree/main/VinCSS-OVPN-Client>

