FE ONLINE

HƯỚNG DẪN SỬ DỤNG ỨNG DỤNG

FE ONLINE 2.0

FE CREDIT

Khởi tạo và quản lý khoản vay, thẻ tín dụng

Ü by VPBank

Tiện ích ngân hàng số

FE CREDIT

Hướng dẫn
CÁCH XỬ LÝ KHI THIẾT BỊ KHÔNG ĐÁP ỨNG ĐIỀU KIỆN BẢO MẬT THEO THÔNG TƯ 77 CỦA NHNN
trên ứng dụng FE ONLINE 2.0

1 Xử lý chế độ gỡ lỗi USB đang được bật (Chỉ có trên thiết bị Android)

1.1 Định nghĩa

Hỏi:

Cảnh báo **"chế độ gỡ lỗi USB"** là gì?

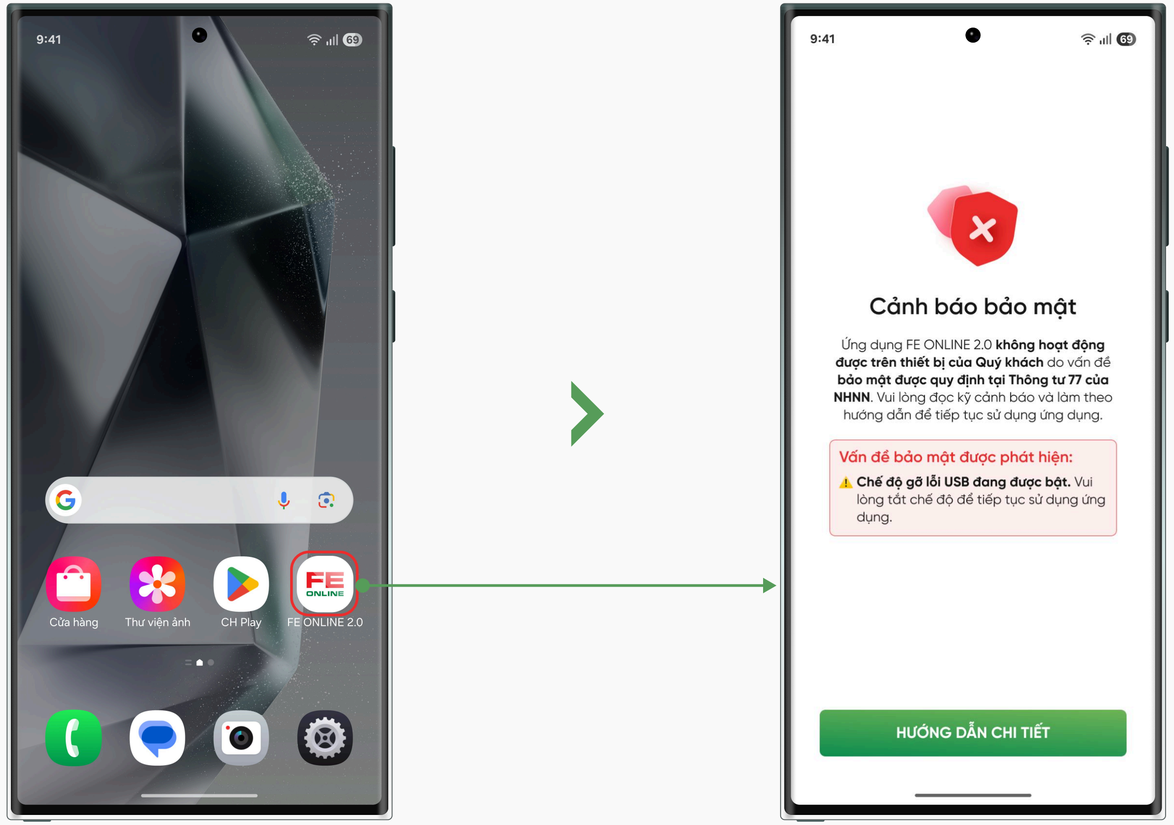
Đáp:

Đây là cảnh báo bảo mật nghiêm trọng khi hệ thống phát hiện thiết bị Android của bạn đang bật Chế độ Gỡ lỗi USB (USB Debugging).

Khi bật chế độ này, thiết bị có thể bị truy cập và điều khiển thông qua cổng USB hoặc phần mềm từ xa, kể cả bởi mã độc đã tồn tại trong máy.

1 Xử lý chế độ gỡ lỗi USB đang được bật (Chỉ có trên thiết bị Android)

1.2 Hiển thị cảnh báo khi truy cập ứng dụng FE ONLINE 2.0

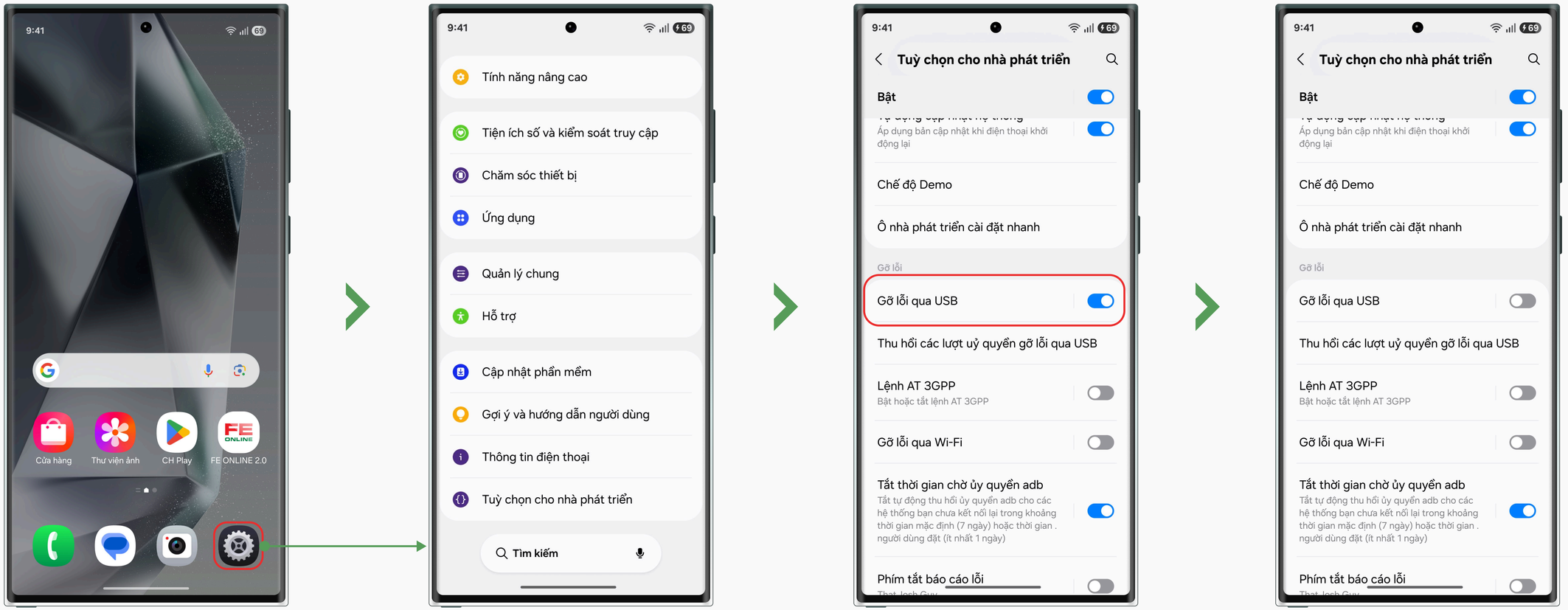


Người dùng khi truy cập vào ứng dụng **FE ONLINE 2.0**

Nếu thiết bị của bạn có dấu hiệu đang bật chế độ gỡ lỗi USB, hệ thống sẽ thể hiện cảnh báo sau đây

1 Xử lý chế độ gỡ lỗi USB đang được bật (Chỉ có trên thiết bị Android)

1.3 Tắt chế độ gỡ lỗi USB đang được bật



Bước 1

Thực hiện đóng ứng dụng, sau đó vào **"Cài đặt"**

Bước 2

Cuộn xuống dưới cùng, chọn mục **"Tuỳ chọn cho nhà phát triển"**

Bước 3

Cuộn xuống tìm và **"Tắt"** mục **"Gỡ lỗi qua USB"**

Bước 4

Tắt thành công, trở về màn hình chính và truy cập lại ứng dụng **FE ONLINE 2.0**

*Lưu ý: **Nếu không thấy mục "Tuỳ chọn cho nhà phát triển"**, hãy vào Cài đặt > Thông tin điện thoại > Thông tin phần mềm > Bấm 7 lần vào "Số hiệu bản dựng" cho đến khi hiện thông báo bạn đã là nhà phát triển, sau đó quay lại menu Cài đặt chính*

2 Xử lý thiết bị đã bị jailbreak hoặc root

2.1 Định nghĩa

Hỏi:

Cảnh báo **“thiết bị đã bị jailbreak hoặc root”** là gì?

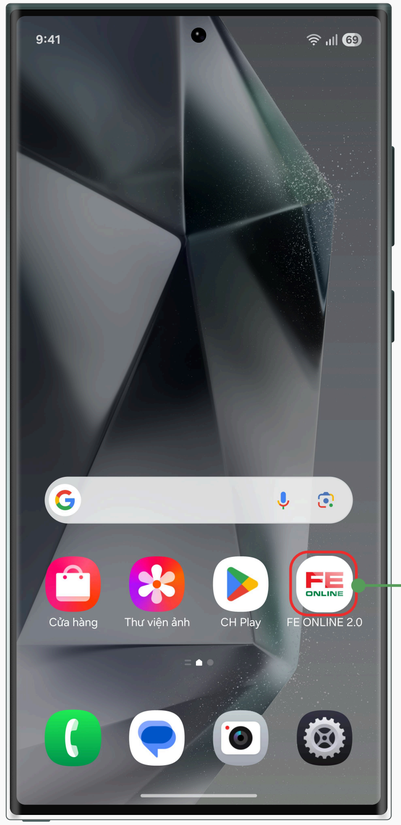
Đáp:

Đây là cảnh báo bảo mật quan trọng khi hệ thống FE ONLINE phát hiện thiết bị của bạn đã bị can thiệp sâu vào hệ điều hành – gọi là Root với Android hoặc Jailbreak với iOS.

Việc bẻ khóa hệ điều hành làm vô hiệu hóa nhiều cơ chế bảo vệ mặc định, khiến thiết bị trở nên dễ bị tấn công và không đáp ứng Điều kiện bảo mật theo Thông tư 77 của NHNN

2 Xử lý thiết bị đã bị jailbreak hoặc root

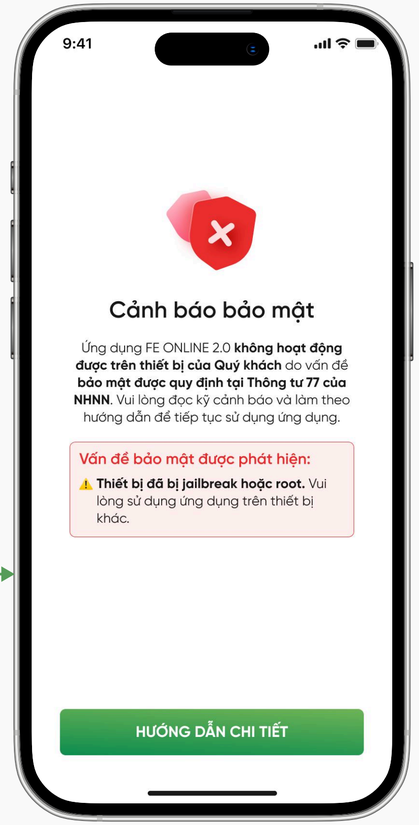
2.2 Hiển thị cảnh báo khi truy cập ứng dụng FE ONLINE 2.0



Người dùng khi truy cập vào ứng dụng **FE ONLINE 2.0**
(Đối với thiết bị Android)

Nếu thiết bị của bạn có dấu hiệu bị jailreak hoặc root, hệ thống sẽ thể hiện cảnh báo sau đây

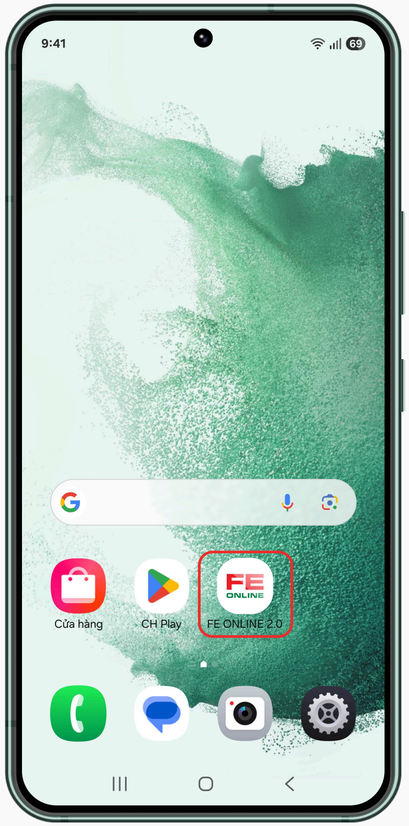
Người dùng khi truy cập vào ứng dụng **FE ONLINE 2.0**
(Đối với thiết bị IOS)

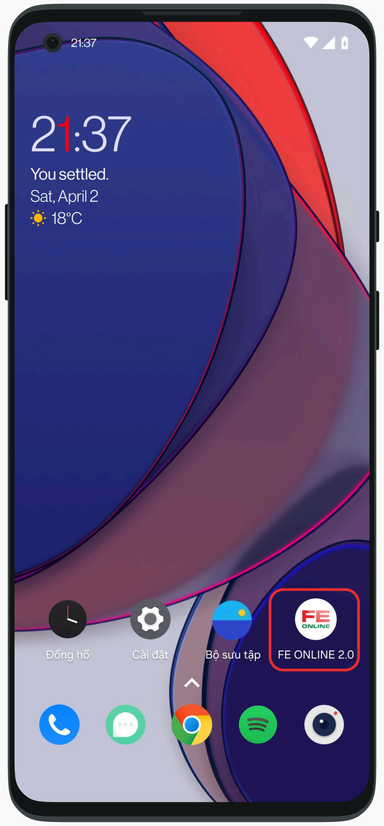


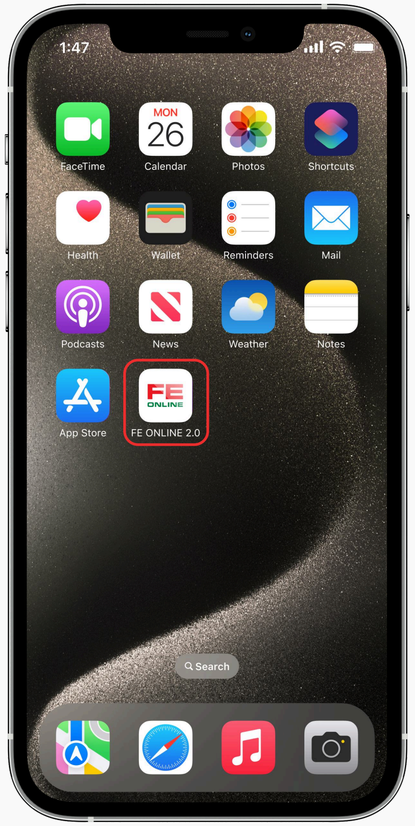
Nếu thiết bị của bạn có dấu hiệu bị jailreak hoặc root, hệ thống sẽ thể hiện cảnh báo sau đây

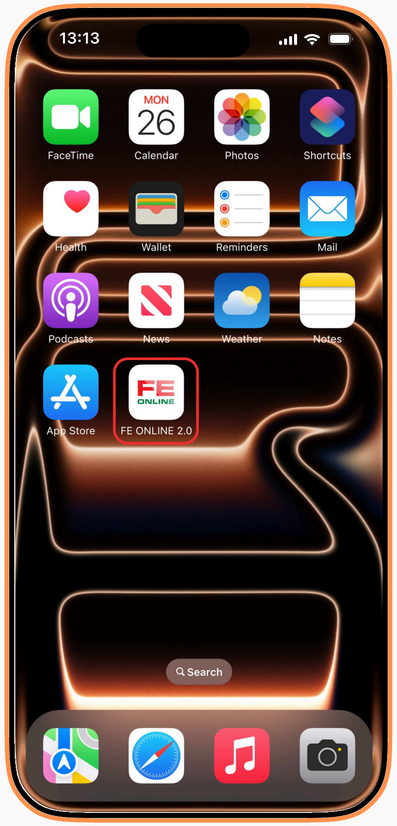
2 Xử lý thiết bị đã bị jailbreak hoặc root

2.3 Hướng xử lý









Vui lòng **sử dụng thiết bị khác** để truy cập ứng dụng FE ONLINE 2.0
hoặc **có thể khôi phục cài đặt gốc** đối với thiết bị đã bị jailbreak hoặc root

3 Xử lý trường hợp ứng dụng FE ONLINE 2.0 được cài đặt từ nguồn không chính thức

3.1 Định nghĩa

Hỏi:

Cảnh báo **"Ứng dụng FE ONLINE 2.0 được cài đặt từ nguồn không chính thức"** là gì?

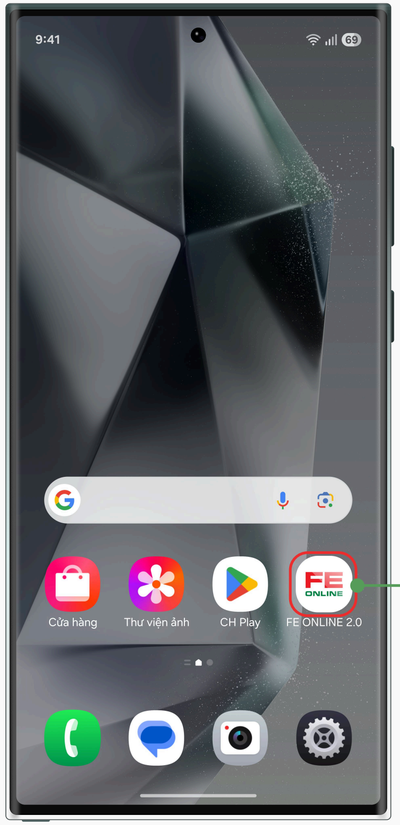
Đáp:

Đây là cảnh báo bảo mật nghiêm trọng khi hệ thống phát hiện ứng dụng FE ONLINE 2.0 của bạn không được tải và cài đặt thông qua các cửa hàng ứng dụng được FE CREDIT phân phối chính thức:

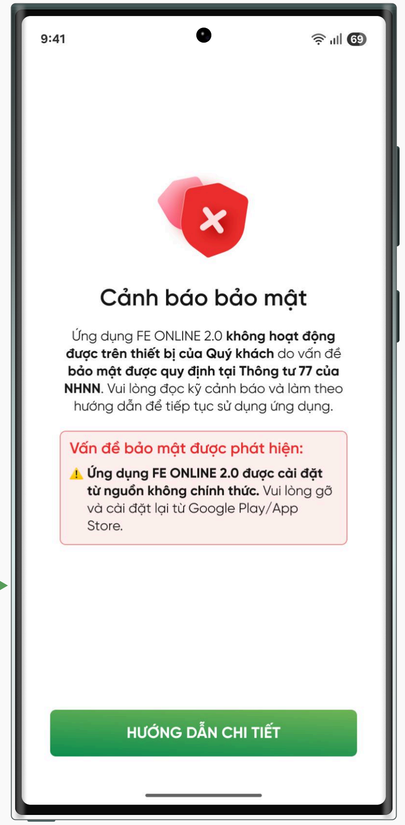
- Hệ điều hành Android (Play Store)
- Hệ điều hành iOS (App Store)

3 Xử lý trường hợp ứng dụng FE ONLINE 2.0 được cài đặt từ nguồn không chính thức

3.2 Hiển thị cảnh báo khi truy cập ứng dụng FE ONLINE 2.0

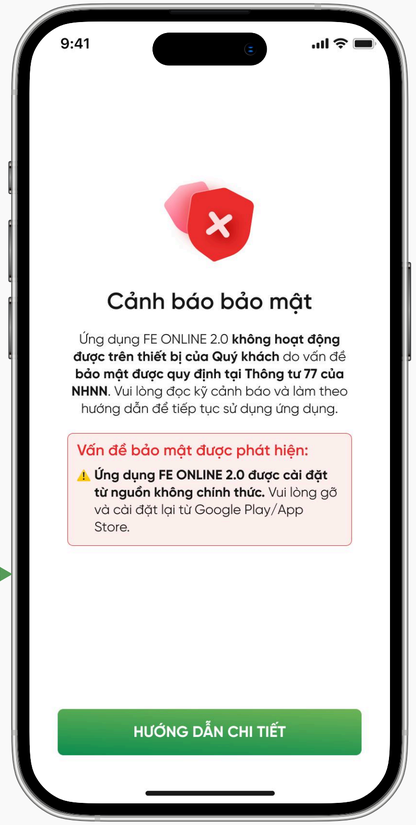


Người dùng khi truy cập vào ứng dụng **FE ONLINE 2.0**
(Đối với thiết bị Android)



Nếu ứng dụng FE ONLINE trên thiết bị của bạn được cài đặt từ nguồn không chính thức, hệ thống sẽ thể hiện cảnh báo sau đây

Người dùng khi truy cập vào ứng dụng **FE ONLINE 2.0**
(Đối với thiết bị IOS)



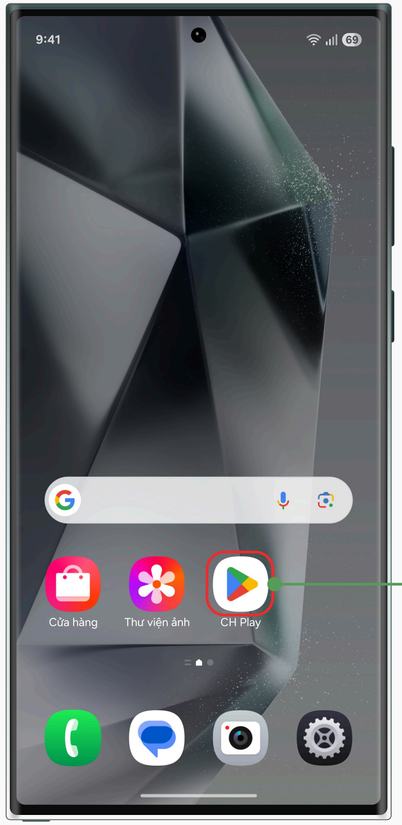
Nếu ứng dụng FE ONLINE trên thiết bị của bạn được cài đặt từ nguồn không chính thức, hệ thống sẽ thể hiện cảnh báo sau đây

3 Xử lý trường hợp ứng dụng FE ONLINE 2.0 được cài đặt từ nguồn không chính thức

3.3 Cài đặt lại ứng dụng FE ONLINE 2.0 *(Đối với thiết bị Android)*

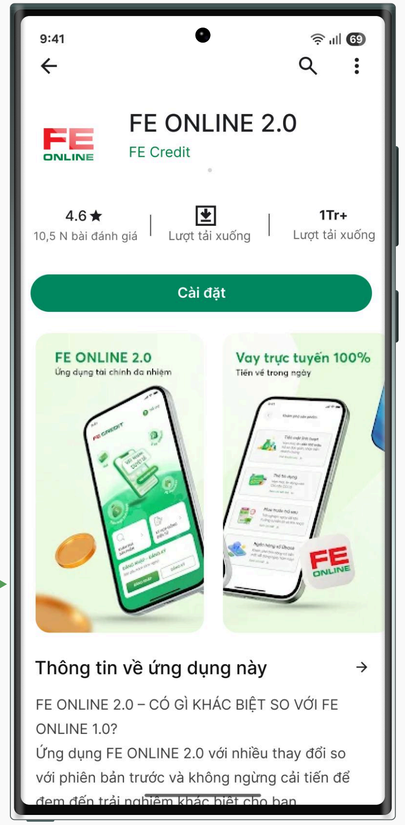
Bước 1

Gỡ cài đặt ứng dụng **FE ONLINE 2.0** hiện tại



Bước 2

Truy cập vào ứng dụng **CH Play**



Bước 3

Cài đặt và truy cập lại ứng dụng **FE ONLINE 2.0**

3 Xử lý trường hợp ứng dụng FE ONLINE 2.0 được cài đặt từ nguồn không chính thức

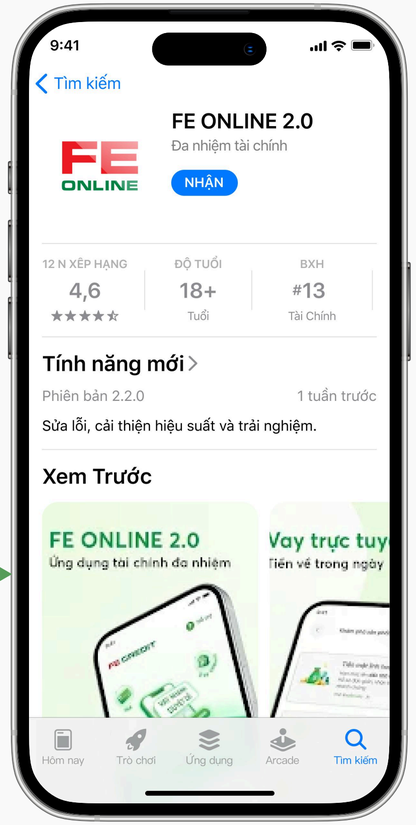
3.4 Cài đặt lại ứng dụng FE ONLINE 2.0 *(Đối với thiết bị IOS)*

Bước 1

Gỡ cài đặt ứng dụng
FE ONLINE 2.0 hiện tại

Bước 2

Truy cập vào ứng dụng
App Store



Bước 3

Cài đặt và truy cập lại
ứng dụng **FE ONLINE 2.0**

4 Xử lý thiết bị đã bị can thiệp hệ thống

4.1 Định nghĩa

Hỏi:

Cảnh báo **“Thiết bị đã bị can thiệp hệ thống”** là gì?

Đáp:

Đây là cảnh báo bảo mật nghiêm trọng khi hệ thống phát hiện có hành vi can thiệp trái phép vào quy trình vận hành hoặc cấu trúc dữ liệu của ứng dụng FE ONLINE 2.0.

Việc can thiệp này cho phép mã độc tự động sửa đổi thông tin giao dịch, đánh cắp mật khẩu hoặc "đọc trộm" mã OTP ngay khi ứng dụng đang hoạt động, gây rủi ro mất tiền trong tài khoản của bạn.

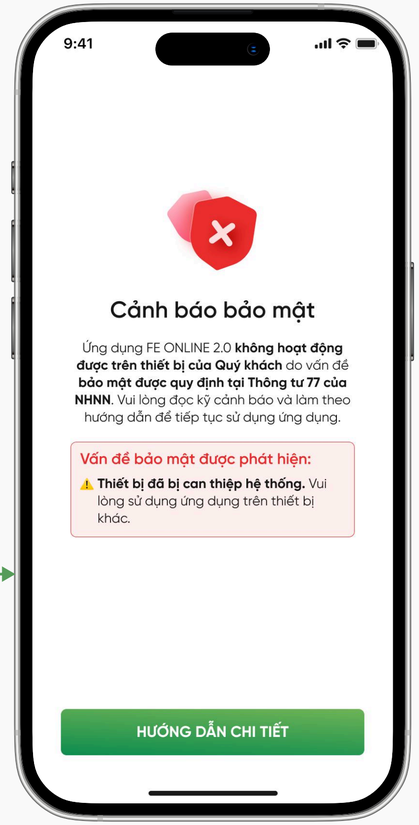
4 Xử lý thiết bị đã bị can thiệp hệ thống

4.2 Hiển thị cảnh báo khi truy cập ứng dụng FE ONLINE 2.0

Người dùng khi truy cập vào ứng dụng **FE ONLINE 2.0**
(Đối với thiết bị Android)

Nếu thiết bị của bạn bị can thiệp hệ thống, hệ thống sẽ thể hiện cảnh báo sau đây

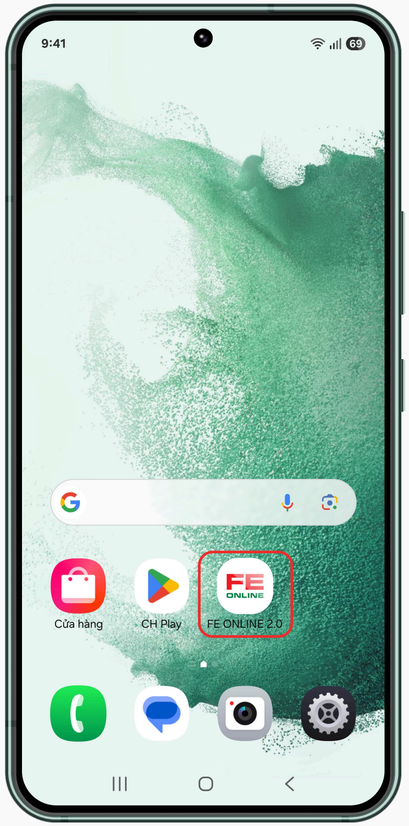
Người dùng khi truy cập vào ứng dụng **FE ONLINE 2.0**
(Đối với thiết bị IOS)

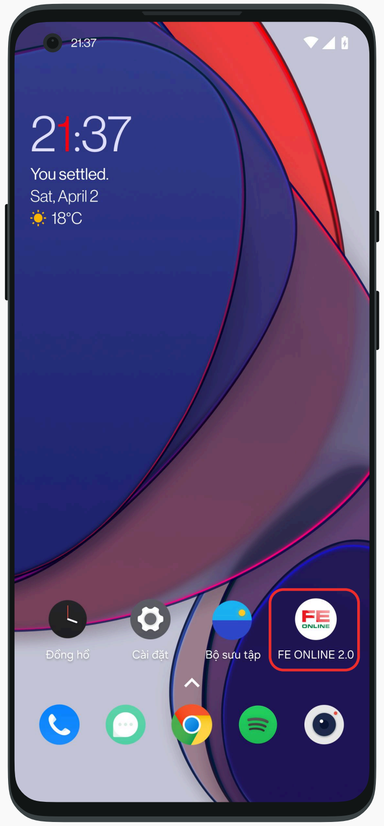


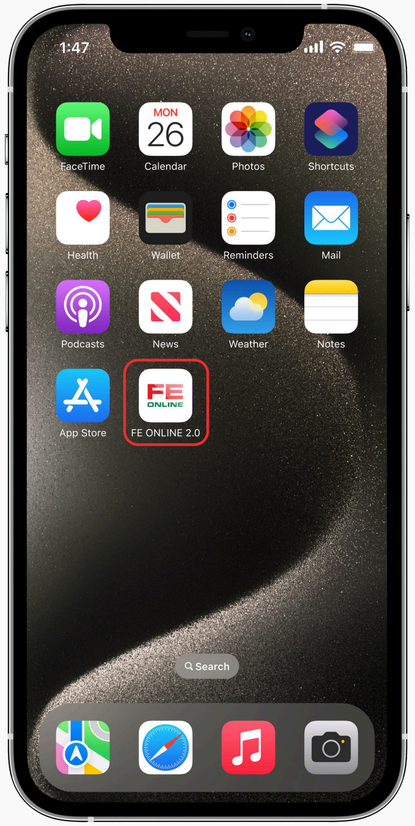
Nếu thiết bị của bạn bị can thiệp hệ thống, hệ thống sẽ thể hiện cảnh báo sau đây

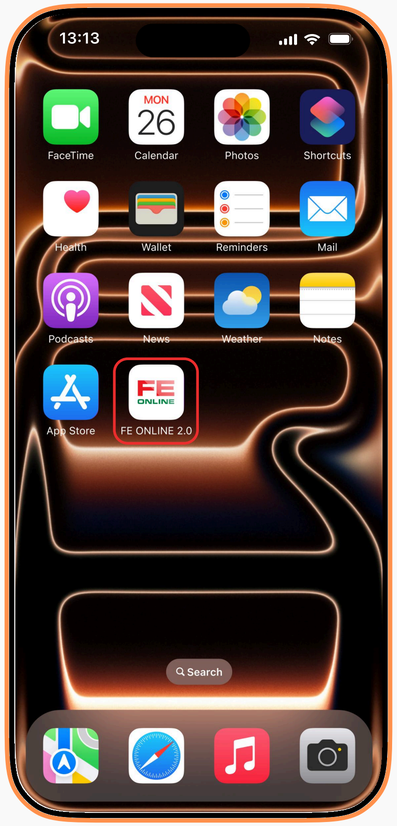
4 Xử lý thiết bị đã bị can thiệp hệ thống

4.3 Hướng xử lý









Vui lòng **sử dụng thiết bị khác** để truy cập ứng dụng FE ONLINE 2.0
hoặc **có thể khôi phục cài đặt gốc** đối với thiết bị đã bị can thiệp hệ thống