# Hacking IOS

iOS là hệ điều hành di động được phát triển bởi Apple. Apple không cấp phép cài đặt iOS trên phần cứng không phải của Apple. Công ty đã tăng phạm vi sản phẩm của mình bằng cách bao gồm điện thoại di động, máy tính bảng và các thiết bị di động khác. Sự gia tăng nhanh chóng trong việc sử dụng các thiết bị Apple đã thu hút sự chú ý của những kẻ tấn công. Các lỗi thiết kế trong iOS khiến nó dễ bị tấn công bởi các ứng dụng độc hại, cấu hình mạng ẩn, các cuộc tấn công MITM, v.v. Kẻ tấn công có thể hack iOS để giành quyền truy cập cấp gốc vào các thiết bị Apple.

Phần này giới thiệu các nội dung sau: Apple iOS; bẻ khóa iOS; các loại, công cụ và kỹ thuật bẻ khóa; hướng dẫn bảo mật thiết bị iOS; và các công cụ theo dõi thiết bị iOS.

## Apple iOS

iOS là hệ điều hành di động của Apple, hỗ trợ các thiết bị của Apple như iPhone, iPod touch, iPad và Apple TV. iOS quản lý phần cứng thiết bị và cung cấp nhiều công nghệ cần thiết để triển khai ứng dụng gốc. Ở cấp độ cao nhất, iOS đóng vai trò trung gian giữa ứng dụng và phần cứng cơ bản. Các ứng dụng giao tiếp với phần cứng cơ bản thông qua một tập hợp các giao diện hệ thống được xác định rõ ràng. Giao diện người dùng dựa trên khái niệm thao tác trực tiếp, sử dụng cử chỉ cảm ứng đa điểm. Kiến trúc iOS bao gồm năm lớp: Ứng dụng Cocoa, phương tiện, dịch vụ cốt lõi, hệ điều hành và nhân lõi cũng như trình điều khiển thiết bị. Các lớp cấp thấp hơn chứa các dịch vụ và công nghệ cơ bản, trong khi các lớp cấp cao hơn xây dựng trên các lớp thấp hơn để cung cấp các dịch vụ và công nghệ phức tạp hơn.

Ứng dụng Cocoa: Lớp này chứa các khung chính giúp xây dựng các ứng dụng iOS. Các khung này xác định giao diện của ứng dụng, cung cấp cơ sở hạ tầng ứng dụng cơ bản, và hỗ trợ các công nghệ chính như đa nhiệm, nhập liệu bằng cảm ứng, đẩy thông báo và nhiều dịch vụ hệ thống cấp cao. Ứng dụng cacao sử dụng AppKit khuôn khổ.

Phương tiện: Lớp này chứa các công nghệ đồ họa, âm thanh và video cho phép trải nghiệm đa phương tiện trong ứng dụng.

Dịch vụ cốt lõi: Lớp này chứa các dịch vụ hệ thống cơ bản cho ứng dụng. Các dịch vụ chính là Core Foundation và Foundation framework (xác định các loại cơ bản mà tất cả các ứng dụng sử dụng). Các công nghệ riêng lẻ hỗ trợ các tính năng như mạng xã hội, iCloud, vị trí và kết nối mạng đều thuộc lớp này.

Hệ điều hành lõi: Lớp này chứa các tính năng cấp thấp mà hầu hết các công nghệ khác đều dựa trên đó. Các khung trong lớp này rất hữu ích khi xử lý rõ ràng các vấn đề về bảo mật hoặc giao tiếp với phần cứng và mạng bên ngoài. Các dịch vụ được cung cấp bởi lớp này phụ thuộc vào lớp Trình điều khiển thiết bị và hạt nhân.

Hạt nhân và Trình điều khiển thiết bị: Lớp thấp nhất của kiến ​​trúc iOS bao gồm kernel, trình điều khiển, BSD, hệ thống tệp, công nghệ cơ sở hạ tầng như mạng.

## Bẻ khóa iOS

Bẻ khóa được định nghĩa là quá trình cài đặt một bộ bản vá kernel đã sửa đổi cho phép người dùng chạy các ứng dụng của bên thứ ba không được nhà cung cấp hệ điều hành ký. Đó là quá trình vượt qua các giới hạn của người dùng do Apple đặt ra, chẳng hạn như sửa đổi hệ điều hành, đạt được đặc quyền quản trị viên và cài đặt các ứng dụng được phê duyệt không chính thức thông qua "tải bên". Bạn có thể thực hiện bẻ khóa bằng cách sửa đổi hạt nhân hệ thống iOS. Một lý do để bẻ khóa các thiết bị iOS như iPhone, iPad và iPod Touch là để mở rộng bộ tính năng bị hạn chế bởi Apple và App Store của hãng. Bẻ khóa cung cấp quyền truy cập root vào HĐH và cho phép tải xuống các ứng dụng, chủ đề và tiện ích mở rộng của bên thứ ba không có sẵn thông qua Apple App Store chính thức. Bẻ khóa cũng loại bỏ các hạn chế hộp cát, cho phép các ứng dụng độc hại truy cập vào thông tin và tài nguyên di động bị hạn chế. Người ta có thể sử dụng các công cụ như Cydia, Hexxa Plus, ApricotiOS, Yuxigon, Sileo, Trimgo, v.v. để bẻ khóa các thiết bị iOS. Bẻ khóa, giống như root, đi kèm với nhiều rủi ro bảo mật và các rủi ro khác đối với thiết bị của bạn, bao gồm:

Làm mất hiệu lực bảo hành điện thoại của bạn

Hiệu suất kém

Nhiễm phần mềm độc hại

“Bẻ gạch” thiết bị

## Các loại bẻ khóa

Ba loại bẻ khóa được thảo luận dưới đây:

■ Khai thác đất người dùng

Userland Exploit sử dụng lỗ hổng trong ứng dụng hệ thống. Nó cho phép truy cập ở cấp độ người dùng nhưng không cho phép truy cập ở cấp độ iboot. Bạn không thể bảo mật thiết bị iOS trước cách khai thác này vì không có gì có thể gây ra vòng lặp chế độ khôi phục. Chỉ các bản cập nhật chương trình cơ sở mới có thể vá các lỗ hổng như vậy.

Khai thác iBoot

Kiểu khai thác này có thể được kết nối một nửa nếu thiết bị có bootrom mới. Jailbreak iboot cho phép truy cập ở cấp độ người dùng và cấp độ iboot. Cách khai thác này lợi dụng lỗ hổng trong iBoot (bộ tải khởi động thứ ba của iDevice) để hủy liên kết công cụ ký mã. Các bản cập nhật chương trình cơ sở có thể vá các lỗi khai thác như vậy.

Khai thác bootrom

Bootrom Exploit sử dụng lỗ hổng trong SecureROM (bộ tải khởi động đầu tiên của iDevice) để vô hiệu hóa kiểm tra chữ ký, lỗ hổng này có thể được sử dụng để tải bản vá chương trình cơ sở NOR. Các bản cập nhật chương trình cơ sở không thể vá các lỗi khai thác như vậy. Bẻ khóa bootrom cho phép truy cập ở cấp độ người dùng và cấp độ iboot. Chỉ có bản cập nhật phần cứng bootrom của Apple mới có thể vá lỗi khai thác này.

## Kỹ thuật bẻ khóa

Bẻ khóa không giới hạn

Trong quá trình bẻ khóa không dây, nếu người dùng tắt và bật lại thiết bị, thiết bị sẽ

khởi động hoàn toàn và kernel sẽ được vá mà không cần sự trợ giúp của máy tính; nói

cách khác, thiết bị sẽ được jailbreak sau mỗi lần khởi động lại.

Bẻ khóa một nửa

Trong bản bẻ khóa bán kết nối, nếu người dùng tắt và bật lại thiết bị, thiết bị sẽ khởi động hoàn toàn. Nó sẽ không còn có kernel được vá lỗi nữa nhưng vẫn có thể sử dụng được cho các chức năng bình thường. Để sử dụng các addon đã bẻ khóa, người dùng cần khởi động thiết bị với sự trợ giúp của công cụ bẻ khóa.

■ Bẻ khóa có dây buộc

Với phương pháp bẻ khóa có dây buộc, nếu thiết bị tự khởi động, thiết bị sẽ không còn nhân được vá và có thể bị kẹt ở trạng thái khởi động một phần; để khởi động nó hoàn toàn và với kernel đã được vá, về cơ bản nó phải được "bẻ khóa lại" bằng máy tính (sử dụng tính năng "boot tethered" của công cụ bẻ khóa) mỗi khi nó được bật.

Bẻ khóa bán không ràng buộc

Bẻ khóa bán không dây cũng tương tự như bẻ khóa nửa dây. Trong kiểu bẻ khóa này, khi thiết bị khởi động lại, kernel sẽ không được vá. Tuy nhiên, kernel có thể được vá mà không cần dùng máy tính; nó được vá bằng ứng dụng được cài đặt trên thiết bị.

## Bẻ khóa iOS 13.2 bằng Cydia

Nguồn: https://www.cydiafree.com

Cydia là một ứng dụng phần mềm dành cho iOS cho phép người dùng tìm và cài đặt các gói phần mềm (bao gồm ứng dụng, tùy chỉnh giao diện và tiện ích mở rộng hệ thống) trên iPhone, iPod Touch hoặc iPad đã jailbreak. Nó là giao diện đồ họa của Công cụ đóng gói nâng cao (APT) và hệ thống quản lý gói dpkg, có nghĩa là các gói có sẵn trong Cydia được cung cấp bởi một hệ thống kho lưu trữ phi tập trung (còn gọi là nguồn) liệt kê các gói này.

Bạn có thể bẻ khóa iOS 13.2 bằng Cydia theo các bước sau:

-Trên iPhone hoặc iPad, hãy mở trình duyệt Safari



Từ thanh địa chỉ, truy cập cydiafree.com



Bây giờ, cuộn xuống trang web và nhấp vào nút "Cydia Tải xuống iOS 13" để chuyển sang trang tiếp theo



Bấm vào nút "Cydia Download iOS 13" trên trang đó để truy cập trang tải xuống

Trên trang tải xuống Cydia, bạn sẽ được cung cấp các hướng dẫn cần thiết để cài đặt Cydia iOS 13. Hãy làm theo các hướng dẫn đó theo đúng thứ tự để hoàn tất quá trình cài đặt

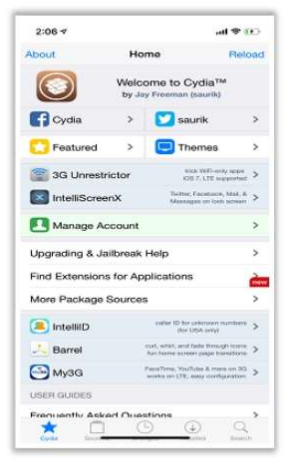


Bây giờ, gõ Cydia vào ô đặt tên cho biểu tượng ứng dụng. Nhấn vào nút Thêm và đóng trình duyệt Safari



Xác định vị trí biểu tượng Cydia trên màn hình chính của bạn





## Bẻ khóa iOS 13.2 bằng Hexxa Plus

Nguồn: https://pangu8.com

Hexxa Plus là Trình giải nén Repo bẻ khóa cho iOS 13.2, cho phép bạn cài đặt các chủ đề, chỉnh sửa và ứng dụng. Nó tương thích với iOS 13 và các phiên bản cao hơn lên đến iOS 13.2.3 bao gồm cả iOS 13.3 beta. Đây là phương pháp phổ biến nhất để cài đặt các ứng dụng jailbreak mà không cần jailbreak untethered hoặc semi-untethered. Bạn có thể cài đặt ứng dụng jailbreak iOS 13.2 bằng cách giải nén repos. Có nhiều kho lưu trữ bẻ khóa trong Hexxa plus với hàng ngàn chỉnh sửa, chủ đề, trò chơi và sớm.

Hexxa Plus cho phép bạn cài đặt Cydia và các ứng dụng Bẻ khóa phổ biến lên các phiên bản iOS mới nhất của bạn thông qua phương pháp trích xuất mã nhà phát triển. Bạn phải cài đặt trình quản lý ứng dụng của bên thứ ba như zJailbreak để cài đặt Hexxa Plus.

Các bước cài đặt Hexxa Plus

Bước 1-Tải xuống ứng dụng zJailbreak. Cung cấp mật mã thiết bị của bạn cho bước này.

Bước 2 - Nhấp vào nút sao chép trên https://ios.cyrepo.tk/ Cydia repo



Bước 03- Vào Extract Repo và chọn nó. Dán repo Cydia đã sao chép

Bước 04- Giải nén Cydia repo bằng cách nhấp vào nút OK. Bây giờ, hãy nhấn vào nút Cài đặt

để cài đặt Cydia

Bước 05- Cuối cùng, bạn có thể thấy biểu tượng ứng dụng Cydia trên màn hình chính



Công cụ bẻ khóa

■ Apricot (quả mơ)

Nguồn: https://pangu8.com

Apricot là một hệ điều hành nhân bản dựa trên web dành cho iPhone mới nhất. Nó hỗ trợ các thiết bị iOS 13.2. Người dùng có thể chạy đồng thời phiên bản iOS nhân bản này với iOS 13.2 mặc định. Các tính năng của Apricot mang lại trải nghiệm thực tế cho iPhone chạy iOS 13.2 của bạn.



Một số công cụ Jailbreak iOS bổ sung như sau:

Yuxigon (https://yuxigon.com)

Sileo (https://cydia-app.com)

Trimgo (https://pangu8.com)

Bregxi (https://pangu8.com)

Yalu (<https://pangu8.com>)

# Hack thiết bị iOS

Những kẻ tấn công sử dụng nhiều phương pháp khác nhau để khai thác lỗ hổng iOS. Họ sử dụng các công cụ chuỗi khai thác nhằm vào các lỗ hổng bảo mật khác nhau để xâm nhập vào các lớp bảo vệ kỹ thuật số iOS khác nhau. Họ cũng cài đặt phần mềm độc hại như phần mềm gián điệp và Trojan để hack thiết bị iOS.

## Hack bằng Spyzie

Nguồn: https://www.spyzie.com

Những kẻ tấn công sử dụng nhiều công cụ trực tuyến khác nhau như Spyzie để hack các thiết bị di động iOS mục tiêu. Spyzie cho phép kẻ tấn công hack SMS, nhật ký cuộc gọi, trò chuyện trong ứng dụng, GPS, v.v. Công cụ này tương thích với tất cả các loại thiết bị iOS như iPhone, iPad và iPod. Những kẻ tấn công hack thiết bị mục tiêu từ xa ở chế độ ẩn mà không cần bẻ khóa thiết bị.

## Hack mạng bằng Network Analayzer Pro

Nguồn: <https://apps.apple.com>

Network Analyser Pro là một công cụ phát hiện thiết bị Wi-Fi giúp phát hiện tất cả địa chỉ và tên của thiết bị LAN cùng với các dịch vụ Bonjour/DLNA mà chúng cung cấp. Nó bao gồm các công cụ chẩn đoán tiêu chuẩn như ping, traceroute, quét cổng, tra cứu DNS và whois. Network Analyser Pro cho phép kẻ tấn công thu thập thông tin như thiết bị được kết nối với mạng, địa chỉ IP, NetBIOS, mDNS (Bonjour), LLMNR và tên DNS của chúng. Nó cũng giúp quét các cổng phổ biến nhất hoặc phạm vi cổng do người dùng chỉ định và phát hiện các cổng đóng, tường lửa và mở.

## Tin cậy iOS

iOS Trustjacking là một lỗ hổng có thể bị kẻ tấn công khai thác để đọc tin nhắn và email cũng như lấy thông tin nhạy cảm như mật khẩu và thông tin xác thực ngân hàng từ một địa điểm ở xa mà nạn nhân không hề hay biết. Lỗ hổng này khai thác tính năng "iTunes Wi-Fi Sync", theo đó nạn nhân kết nối điện thoại của mình với bất kỳ máy tính đáng tin cậy nào (có thể là của một người bạn hoặc bất kỳ tổ chức đáng tin cậy nào) đã bị kẻ tấn công lây nhiễm.

Khi thiết bị iOS đang cố gắng kết nối với máy tính, thiết bị sẽ hiển thị hộp thoại trên màn hình với các tùy chọn "Tin cậy" và "Không tin cậy". Khi nhấp vào Tin cậy, nó sẽ thiết lập kết nối giữa các thiết bị để chia sẻ thông tin.



Sau khi thiết lập kết nối và bật đồng bộ iTunes Wi-Fi trên máy tính, thiết bị có thể tiếp tục liên lạc với máy tính đó ngay cả sau khi bị ngắt kết nối vật lý.



Sau khi nạn nhân nhấp vào "Tin cậy", kẻ tấn công sẽ có quyền truy cập vào thiết bị iOS được kết nối thông qua máy tính bị nhiễm, quá trình này sẽ tiếp tục cho đến khi điện thoại đặt lại cài đặt kết nối. Dữ liệu và hoạt động trên màn hình của thiết bị bị xâm nhập sau đó có thể được giám sát từ máy tính để bàn mà người dùng không hề hay biết. Hệ thống bị nhiễm có thể cho phép kẻ tấn công đọc được hoạt động của người dùng ngay cả khi thiết bị nằm ngoài vùng liên lạc. Nó cũng có thể cho phép kẻ tấn công sao lưu hoặc khôi phục dữ liệu để đọc lịch sử SMS, ảnh đã xóa và ứng dụng. Kẻ tấn công cũng có thể thay thế các ứng dụng gốc của thiết bị bằng các ứng dụng độc hại từ PC đã kết nối trước đó.

## Phần mềm độc hại iOS

■ Phần mềm độc hại Clicker Trojan

Nguồn: https://www.notebookcheck.net

Phần mềm độc hại Clicker Trojan đã lây nhiễm 17 ứng dụng trên Apple Store. Tất cả các ứng dụng độc hại này đều sử dụng mô-đun Trojan nhấp chuột để tạo lưu lượng truy cập web giả mạo nhằm mục đích tạo doanh thu quảng cáo cho các trang web cụ thể. Clicker Trojan là một phần mềm độc hại tự động mở các trang web ở chế độ nền và nhấp vào liên kết quảng cáo mà người dùng không hề hay biết. Những kẻ tấn công thu được lợi ích tài chính thông qua số lần trả tiền cho mỗi lần nhấp chuột vào các trang web.

## Trident (cây đinh ba)

Nguồn: https://blog.malwarebytes.com

Trident là một phần mềm gián điệp tinh vi khai thác các lỗ hổng trong iPhone để theo dõi người dùng. Những lỗ hổng này cho phép kẻ tấn công bẻ khóa iPhone mục tiêu từ xa và cài đặt phần mềm gián điệp độc hại như Pegasus. Trident có khả năng kiểm soát hoàn toàn thiết bị di động mục tiêu và cho phép kẻ tấn công giám sát và theo dõi tất cả hoạt động của người dùng. Nó cũng cho phép kẻ tấn công ghi lại âm thanh, chụp ảnh màn hình và giám sát tất cả các cuộc gọi điện thoại và tin nhắn SMS.

Một số phần mềm độc hại iOS bổ sung như sau:

Cuộc di cư

XcodeGhost

Kiểm tra

KeyRaider

AceDeceiver Trojan

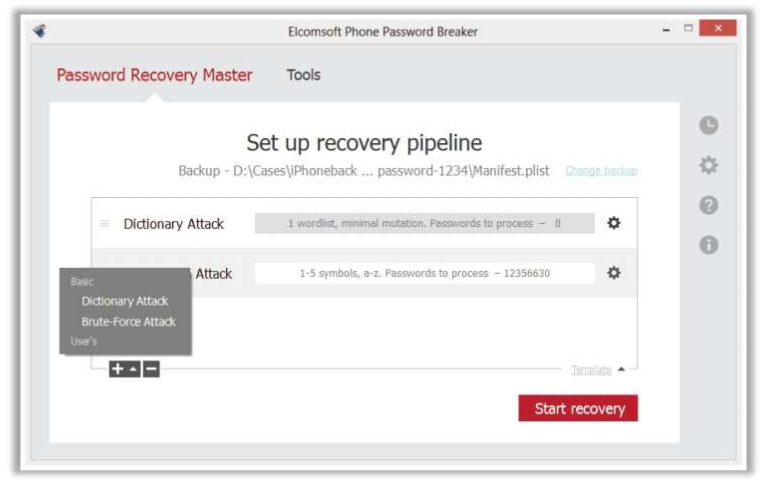
# Công cụ hack iOS

Dưới đây là thảo luận về nhiều công cụ khác nhau được kẻ tấn công sử dụng để hack các thiết bị di động iOS mục tiêu:

## Máy cắt điện thoại Elcomsoft

Nguồn: https://www.elcomsoft.com

Elcomsoft Phone Breaker cho phép kẻ tấn công thực hiện việc thu thập thiết bị iOS một cách hợp lý và không dây, đột nhập vào các bản sao lưu được mã hóa cũng như lấy và phân tích các bản sao lưu, dữ liệu được đồng bộ hóa và mật khẩu từ Apple iCloud. Nó cho phép kẻ tấn công phá mật khẩu và giải mã các bản sao lưu iOS bằng khả năng tăng tốc GPU. Sử dụng công cụ này, kẻ tấn công có thể giải mã Chuỗi khóa iCloud và tin nhắn cùng các tệp và tài liệu đa phương tiện từ iCloud.



Một số công cụ bổ sung để hack thiết bị iOS được liệt kê bên dưới:

Fing – Network Scanner (https://apps.apple.com)

Network Analyzer Master Lite (https://apps.apple.com)

Spyic (https://spyic.com)

iWepPRO (https://apps.apple.com)

Frida (<https://www.frida.re>)

# Bảo mật thiết bị iOS

Dưới đây là một số nguyên tắc quan trọng giúp bạn bảo mật thiết bị iOS và dữ liệu của chúng khỏi những kẻ tấn công:

+Kích hoạt tính năng Passcode Lock trên iPhone của bạn. Đi tới Settings → Touch ID & Passcode Lock, sau đó chạm vào Turn Passcode On.

+Đặt mật mã riêng cho ứng dụng chứa dữ liệu nhạy cảm

+Vô hiệu hóa Javascript và tiện ích bổ sung từ trình duyệt web

+Luôn tải xuống ứng dụng từ Apple App Store

+Đặt Auto-Lock Timeout để nhập mật mã sau một thời gian đã đặt. Đi tới Settings -> General → Auto-Lock

+Sử dụng thiết bị iOS trên mạng Wi-Fi được bảo mật và bảo vệ

+Không lưu trữ dữ liệu nhạy cảm trên cơ sở dữ liệu phía máy khách

+Không truy cập các dịch vụ web trên mạng bị xâm nhập

+Không mở liên kết hoặc tệp đính kèm từ các nguồn không xác định

+Chỉ triển khai các ứng dụng của bên thứ ba đáng tin cậy trên thiết bị iOS

+Thay đổi mật khẩu root iPhone mặc định từ Alpine

+Không bẻ khóa hoặc root thiết bị của bạn nếu được sử dụng trong môi trường doanh nghiệp

+Định cấu hình Tìm iPhone của tôi và sử dụng nó để xóa thiết bị bị mất hoặc bị đánh cắp

+Kích hoạt tính năng phát hiện Bẻ khóa và cũng bảo vệ quyền truy cập vào tài khoản AppleID và Google, được gắn với dữ liệu nhạy cảm

+Vô hiệu hóa dịch vụ iCloud để dữ liệu doanh nghiệp nhạy cảm không được sao lưu lên đám mây (lưu ý rằng dịch vụ đám mây có thể sao lưu tài liệu, thông tin tài khoản, cài đặt và tin nhắn)

+Kích hoạt chức năng Yêu cầu tham gia mạng; điều này ngăn bạn kết nối ngẫu nhiên với các mạng Wi-Fi có sẵn. Đi tới Cài đặt → Wi-Fi → Yêu cầu tham gia mạng

+Thường xuyên cập nhật hệ điều hành cho thiết bị của bạn với các bản vá bảo mật do Apple phát hành. Để nhận bản cập nhật, hãy kết nối với App Store. Đối với iOS 5 trở lên, có thể nhận các bản cập nhật thông qua Cài đặt → Chung→ Cập nhật phần mềm

+Kích hoạt tính năng Xóa dữ liệu trên iPhone của bạn để xóa tất cả dữ liệu và cài đặt sau 10 lần thử. Đi tới Cài đặt → Touch ID & Mật mã → Xóa dữ liệu

+Tắt tính năng Voice Dial trên iPhone để ngăn kẻ tấn công truy cập vào điện thoại mà không nhập mật mã. Đi tới Cài đặt Touch ID & Passcode, sau đó Turn Voice Dial để TẮT

+Xóa Bộ nhớ đệm bàn phím trên iPhone của bạn để xóa tất cả các lần nhấn phím được ghi lại. Đi tới Cài đặt chung → Đặt lại, chạm vào Đặt lại từ điển bàn phím, sau đó Xác nhận trên màn hình cảnh báo

+Tắt tính năng gắn thẻ địa lý (lưu trữ dữ liệu dựa trên vị trí trong hình ảnh) trên iPhone. Đi tới Cài đặt → Quyền riêng tư → Dịch vụ định vị, sau đó chuyển Camera sang TẮT

+Kích hoạt cài đặt bảo mật và quyền riêng tư của Safari trên iPhone. Đi tới Cài đặt Safari. Tại đây, bạn có thể thực hiện các thao tác sau: Bật Chặn cửa sổ bật lên, Tắt mật khẩu và Tự động điền, Bật cảnh báo trang web lừa đảo, Chặn cookie, Xóa lịch sử và dữ liệu trang web, v.v.

+Kích hoạt tính năng Không theo dõi để giữ cho việc duyệt web của bạn ở chế độ riêng tư. Đi tới Cài đặt → Safari rồi bật tùy chọn Không theo dõi

+Tắt Bluetooth khi không sử dụng. Đi tới Cài đặt Bluetooth, sau đó chuyển nó sang TẮT

+Tắt Wi-Fi khi không sử dụng. Đi tới Cài đặt → Wi-Fi, sau đó chuyển nó sang TẮT

+Vô hiệu hóa trợ lý cá nhân Siri của Apple. Đi tới Cài đặt → → Touch ID & Mật mã rồi chuyển "Cho phép truy cập khi bị khóa" thành TẮT.

+Tắt tùy chọn tự động điền trong Safari. Đi tới Cài đặt → Safari → Tự động điền và sau đó chuyển nó sang TẮT

+Sử dụng xác thực hai yếu tố. Đi tới Cài đặt → ID Apple của bạn →→ Mật khẩu & Bảo mật, nhập mật khẩu của bạn rồi chuyển "Bật xác thực hai yếu tố" thành BẬT

+Cài đặt phần mềm VPN để mã hóa tất cả lưu lượng truy cập Internet của bạn

+Cài đặt ứng dụng Vault để ẩn dữ liệu quan trọng được lưu trữ trên thiết bị di động iOS của bạn

Đặt lại kết nối bằng cách điều hướng đến Cài đặt → → Chung → Đặt lại Đặt lại vị trí & Quyền riêng tư nếu có bất kỳ hoạt động đáng ngờ nào đc tìm thấy

Lưu ý: Các đường dẫn ở trên để việc bật/tắt các tính năng tương ứng có thể thay đổi tùy theo Phiên bản iOS hoặc thiết bị được sử dụng.

# Công cụ bảo mật thiết bị iOS

## Bảo mật di động Avira

Nguồn: https://www.avira.com

Công cụ Avira Mobile Security cung cấp các tính năng như bảo vệ web, bảo vệ danh tính, phát hiện các trang web lừa đảo nhắm mục tiêu cá nhân bạn, bảo mật email, theo dõi thiết bị của bạn, xác định hoạt động, sắp xếp bộ nhớ thiết bị, sao lưu tất cả danh bạ của bạn, v.v. cho tất cả iOS thiết bị.



Một số công cụ bảo mật thiết bị iOS bổ sung như sau:

Norton Security cho iOS (https://us.norton.com)

LastPass Password Manager (https://www.lastpass.com)

Lookout Personal for iOS (https://www.lookout.com)

McAfeeⓇ Mobile Security (https://www.mcafee.com)

Trend Micro Mobile Security (<https://www.trendmicro.com>)

# Công cụ theo dõi thiết bị iOS

Một số công cụ theo dõi thiết bị iOS được liệt kê bên dưới:

## Tìm iPhone của tôi

Nguồn: https://support.apple.com

Tìm iPhone của tôi là công cụ theo dõi thiết bị iOS cho phép bạn sử dụng một thiết bị iOS khác để theo dõi iPhone, iPad, iPod touch hoặc Mac bị mất hoặc bị thất lạc và bảo vệ dữ liệu của chúng. Để sử dụng công cụ này, bạn cần cài đặt ứng dụng trên một thiết bị iOS khác, mở ứng dụng và đăng nhập bằng ID Apple của bạn. Nó giúp bạn xác định vị trí thiết bị bị thất lạc của mình trên bản đồ, khóa thiết bị từ xa, phát âm thanh, hiển thị thông báo và xóa tất cả dữ liệu trên đó.

Tìm iPhone của tôi cũng bao gồm Chế độ mất để định vị iDevice chạy iOS 6 trở lên. Chế độ mất khóa thiết bị bị thất lạc của bạn bằng mật mã và hiển thị thông báo tùy chỉnh như số điện thoại liên hệ trên màn hình khóa. Khi ở Chế độ mất, thiết bị của bạn cũng theo dõi vị trí của thiết bị để bạn có thể xem lịch sử vị trí gần đây của thiết bị từ ứng dụng Tìm iPhone của tôi.

Cách thiết lập Tìm iPhone, iPad, iPod touch, Apple Watch, AirPods

1. Bắt đầu ở Màn hình chính của bạn

2. Nhấn vào Cài đặt → [tên của bạn] → iCloud. Nếu bạn đang sử dụng iOS 10.2 trở xuống, hãy đi tới Cài đặt iCloud

3. Cuộn xuống phía dưới và nhấn Tìm iPhone của tôi

4. Trượt để bật Tìm iPhone của tôi và Gửi vị trí cuối cùng

Một số công cụ theo dõi thiết bị iOS bổ sung như sau:

Phonty (https://phonty.com)

SpyBubble (https://thespybubble.com)

Prey Find my phone tracker GPS (https://apps.apple.com)

iHound (http://ihoundgps.com)

FollowMee GPS Location tracker (https://apps.apple.com)