

Cyber Security

**An Ninh Mạng
Staying Safe Online**

NỘI DUNG

1. An ninh mạng là gì
2. Lừa đảo trên mạng
3. Mật khẩu an toàn
4. Nhận diện bằng nhiều mật khẩu
5. Cập nhật phần mềm
6. Sao lưu dữ liệu
7. Hướng dẫn tự bảo vệ bạn

1. An ninh mạng là gì

- An ninh mạng là việc giữ an toàn trực tuyến, vấn đề này rất thiết yếu trong thế giới digital ngày nay. Vì các mối đe dọa như: *vi phạm dữ liệu, đánh cắp danh tính và lừa đảo trực tuyến* thật là phổ biến.
- *Nhưng nếu luôn thực hành theo hướng dẫn rõ ràng và thiết thực sẽ giúp bạn tự bảo vệ mình.*
- *Cyber security and staying safe online are essential in today's digital world, where threats like data breaches, identity theft, and online scams are common. Here's a clear and practical guide to help you protect yourself*

2. Lừa đảo trên mạng

- Dùng tình cảm lòng thương hại qua các youtuber, email hay tin nhắn cơ quan từ thiện cá nhân, nhóm nhỏ.
- Mua sản phẩm trực tuyến hay cho *thử hàng không thích được trả lại hay giảm giá 50-90%* có thêm cò mồi khen giả.
- Được lợi những khoản tiền lớn như trúng số, đầu tư, công việc làm lương cao
- Đòi tiền nợ giả như etag, tiền phạt, mua hàng chưa trả tiền, bill quá hạn

2. Lừa đảo trên mạng

- Dùng người thân làm công cụ để đe dọa, hay ngay cả báo thiết bị dữ liệu sẽ không dùng được.
- Báo cáo lừa đảo: Liên lạc người thân trong gia đình, bạn bè, các tổ chức, người giúp đỡ – cơ quan chính phủ trình báo về lừa đảo, đe dọa.
- Theo Scamwatch, người dân Victoria đã mất hơn \$110 triệu vì các vụ lừa đảo vào năm 2023 và \$100 triệu lừa đảo vào năm 2024 (*theo vic.gov.au/stay-safe-online-tips-vietnamese*).
- Lừa đảo qua hình thức phone, quảng cáo, spam email, hay ngay cả qua những thông tin *được người thân vô tình chuyển qua bằng forward...*

2. Lừa đảo trên mạng

- Trong quý đầu 2024, có 588 vụ lừa đảo qua điện thoại khiến các nạn nhân mất tổng cộng 23,9 triệu đô la. Ngoài ra, hơn 10.000 cuộc gọi lừa đảo, 32.091 tin nhắn (theo [sbs.com.au/language/vietnamese/](https://www.sbs.com.au/language/vietnamese/) 29-12-24)
- Ngày càng có nhiều *kẻ lừa đảo sử dụng các tài khoản giả mạo* hoặc bị đánh cắp trên mạng xã hội, các nền tảng và ứng dụng nhắn tin để chiếm đoạt tiền bạc và thông tin cá nhân
- Tin nhắn, email và cuộc gọi phone lừa đảo được ghi nhận nhiều hơn, và *các vụ lừa đảo qua mạng xã hội*

2. Lừa đảo trên mạng

“ Bạn có thể nhận được tin nhắn trên mạng xã hội từ một người mà bạn chưa từng quen biết. Kẻ lừa đảo giả vờ là bạn bè, người thân, cố vấn tài chính hoặc đại diện của một doanh nghiệp cung cấp cơ hội việc làm,” NASC cho biết.



2. Lừa đảo trên mạng

- Công cụ mới giúp ngăn chặn lừa đảo và tiết kiệm hàng triệu đô la cho người dân Úc
- Để giảm thiểu thiệt hại này, chính phủ vừa công bố một **công cụ mới có tên là Sổ Đăng Ký Tên Người Gửi SMS Bắt Buộc (SMS Sender ID Register)**.
- Công cụ này yêu cầu các *nhà cung cấp dịch vụ viễn thông kiểm tra xem tên người gửi tin nhắn dưới danh nghĩa một tổ chức có khớp với thông tin đã đăng ký hợp pháp hay không.*

- “Tất cả chúng ta nếu đều đã từng nhận những tin nhắn lừa đảo giả danh các tổ chức uy tín hãy thông báo.
- *“Với **sổ đăng ký** bắt buộc này, những tin nhắn lừa đảo sẽ bị chặn hoặc bị đánh dấu, giúp người tiêu dùng tránh bị lừa đảo”*
- “Nhờ vậy, **sổ đăng ký** cũng sẽ giúp khôi phục niềm tin vào các tin nhắn từ các tổ chức uy tín và biến Úc trở thành một nơi mà những kẻ lừa đảo khó hoạt động hơn.”
- **Sổ đăng ký** được thiết kế để ngăn chặn những kẻ lừa đảo sử dụng tên của *những tổ chức đáng tin cậy, bao gồm ngân hàng, nhà cung cấp dịch vụ hoặc cơ quan chính phủ như ANZ, Linkt hay myGov* (theo sbs.com.au/language/vietnamese).



3. Mật khẩu an toàn

- Tạo **mật khẩu khó đoán và lưu trữ chúng an toàn** (bảo mật mạng hàng đầu)
 - * *Gồm ít nhất 8 đến 16 ký tự*
 - * *Cần chữ hoa và chữ thường, số 0-9*
 - * *Phải có các ký tự đặc biệt*
 - * *không dùng tên, ngày tháng sinh của mình*
- Thường các tổ chức uy tín có cài đặt hệ thống xem mật khẩu có an toàn đủ tiêu chuẩn không và ngay cả tự tạo – **generated mật khẩu lúc đầu, or reset**. Phải **thay đổi ngay** mật khẩu cung cấp trong lần đầu truy cập.

3. Mật khẩu an toàn

- Tạo **mật khẩu khó đoán và lưu trữ chúng an toàn** (bảo mật mạng hàng đầu)
 - * *Gồm ít nhất 8 đến 16 ký tự*
 - * *Cần chữ hoa và chữ thường, số 0-9*
 - * *Phải có các ký tự đặc biệt*
 - * *không dùng tên, ngày tháng sinh của mình*
- Thường các tổ chức uy tín có cài đặt hệ thống xem mật khẩu có an toàn đủ tiêu chuẩn không và ngay cả tự tạo – **generated mật khẩu lúc đầu, or reset**. Phải **thay đổi ngay** mật khẩu cung cấp trong lần đầu truy cập.

3. Mật khẩu an toàn

- Tốt nhất nên tạo một ***hệ thống mật khẩu*** cho riêng mình để dễ nhớ FL.DD.MM@Site
- Nhớ phải ***lưu trữ lại và giữ nhiều phiên bản*** – cho người tin tưởng nhất biết - để truy tìm khi mình không dùng được lúc bất trắc.
- Với mọi người ***mật khẩu quên*** là vấn đề thường xuyên có nhất là người cao tuổi. Mà nhiều hệ thống chỉ cho ***nhập không quá 3 lần sẽ khóa account*** lại. Nên vấn đề tạo ***một hệ thống mật khẩu dễ nhớ*** cho mình và an toàn là rất quan trọng.
- Mật khẩu thường mã hóa có thể đổi ***show*** để đánh chính xác, ***không save mật khẩu*** cho app quan trọng

Sign in

or [create an account](#)

☒ Remember me

Sign in



Sign in with Google

[Forgotten your password?](#)

User Login

Username

• • • • •

☐ Remember

[Forgot Password ?](#)

SUBMIT

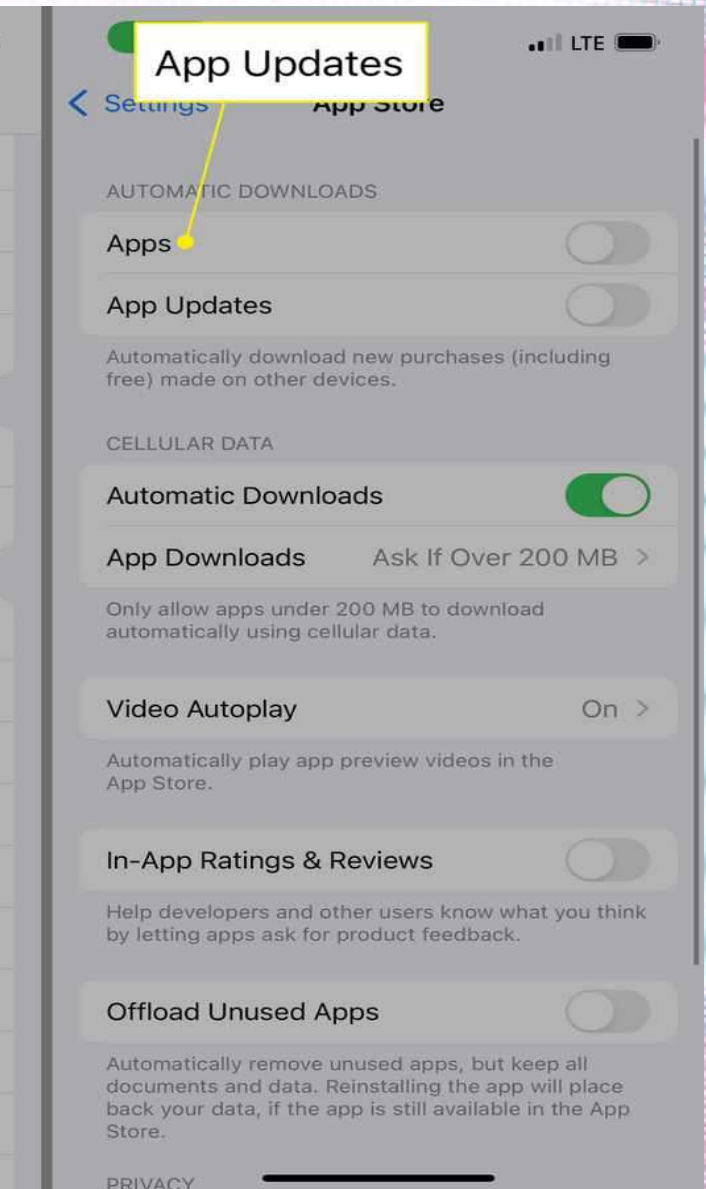
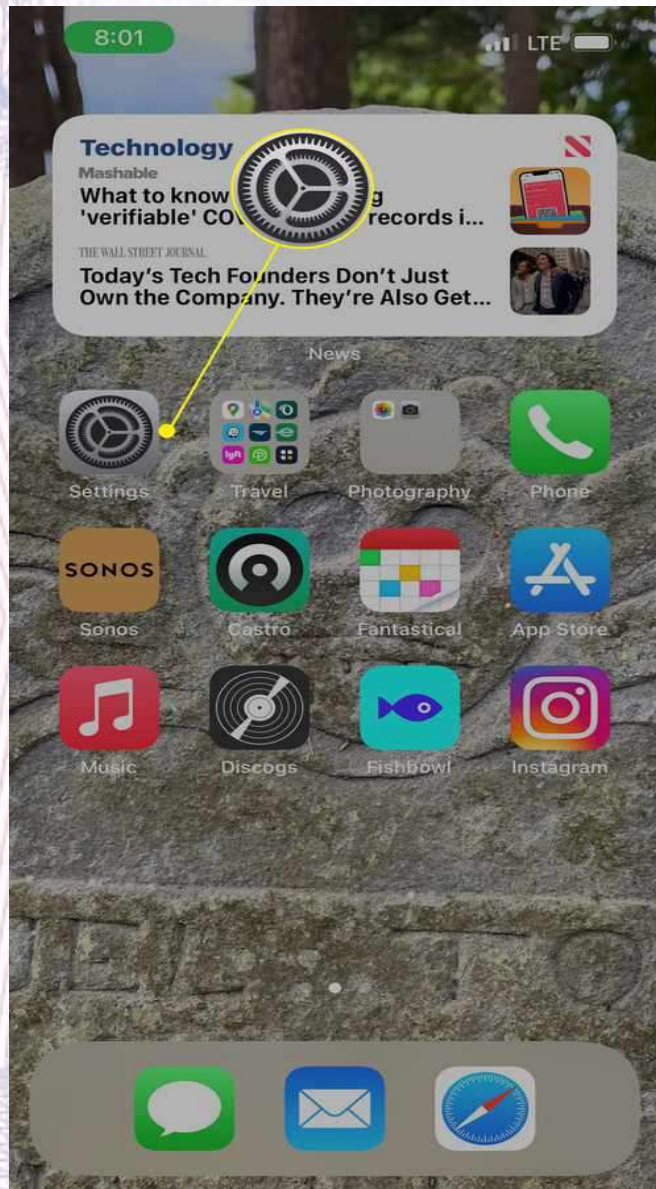


4. Nhận diện bằng nhiều mật khẩu

- Dùng nhiều yếu tố để xác định quyền truy cập thiết bị hay dữ liệu
 - * câu hỏi phụ bảo mật : nơi làm, ở, sanh ra v...v
 - * thêm pin, mật khẩu phụ
 - * dùng vân tay, mắt v... v
 - * nhắn SMS, email để chấp nhận quyền dùng
- Tạo **mật khẩu để mở dữ liệu lưu trữ hay tạo chế độ quyền truy cập** - access control user, admin, hoặc dấu kín – *hidden file*

5. Cập nhật phần mềm

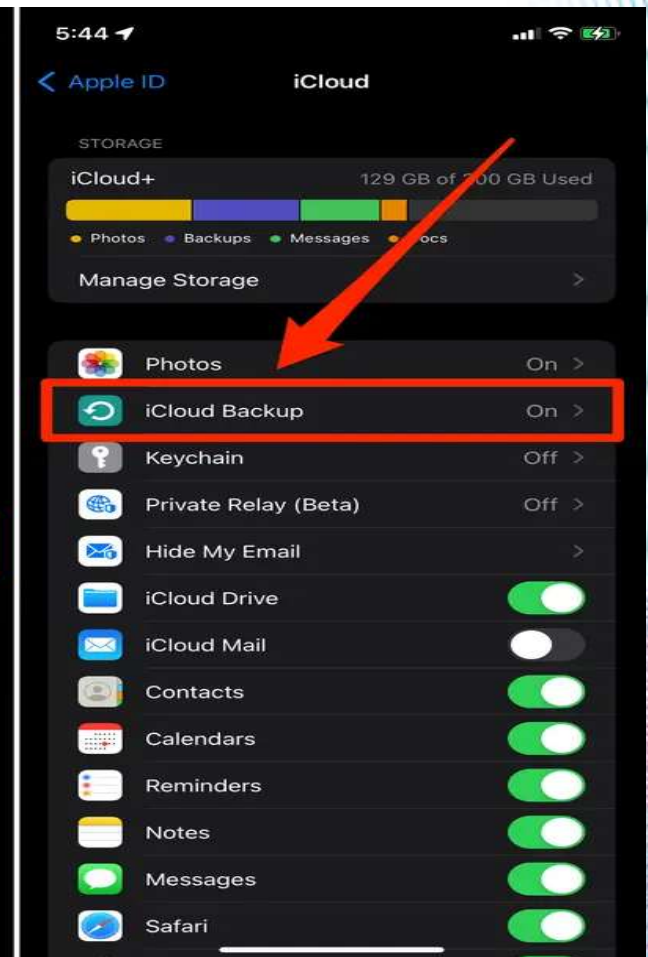
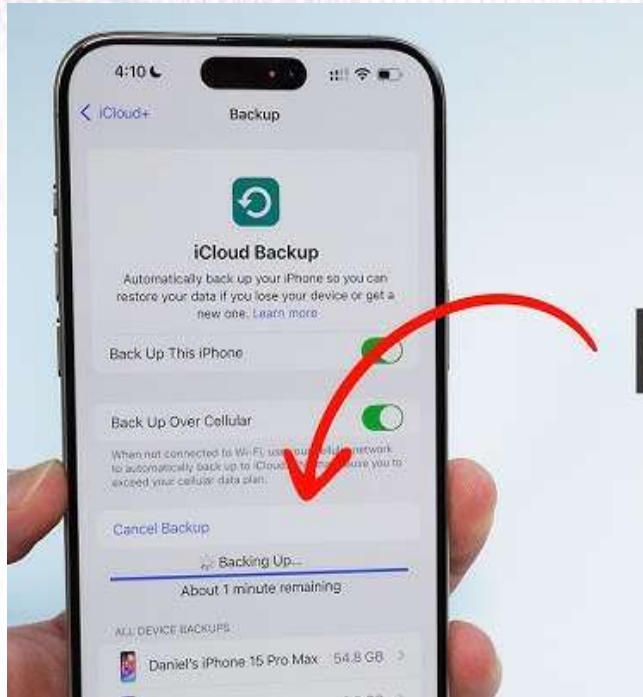
- Cập nhật phần mềm của thiết bị : *khắc phục các điểm yếu hoặc lỗ hổng trong phần mềm* của thiết bị.
- Thường phần mềm sau một thời gian sử dụng *lúc nào cũng bị phát hiện sai sót*. Do đó phần mềm và thiết bị thường ra loại version mới mỗi năm.
- Trong *setting của các thiết bị thường có mục chọn lựa cho phép hoặc không tự cập nhật phần mềm* mỗi khi có chương trình thay đổi.

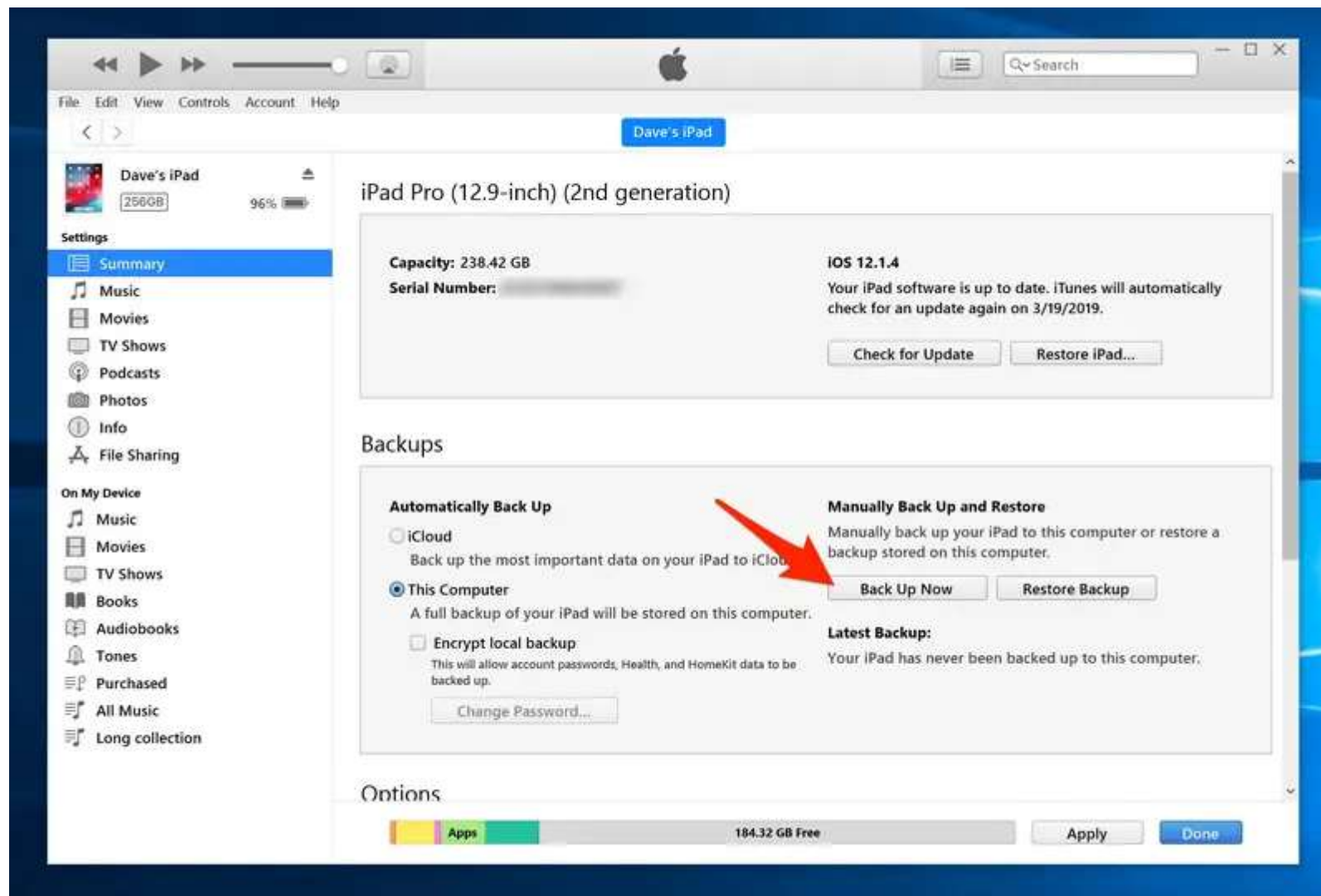


6. Sao lưu dữ liệu

- Sao lưu **cục bộ** (*local hard disk*) trên máy tính
- Sao lưu **trực tuyến** – *google drive, cloud*
- Giữ backup trên **USB** hay *external hard drive*
- **Lưu giữ thường xuyên** mỗi ngày, tuần, tháng và giữ nhiều bản để có thể truy cập trở lại.
- Những gì **quan trọng** về thông tin cá nhân, mật khẩu, chứng từ tài chính v...v
- Lưu những thông tin liên lạc **contact cần thiết**.
- Các thiết bị cũng có chứng năng **backup và restore**.
- Luôn **tự bảo vệ chính mình** khi tham gia trực tuyến.

How to Back up





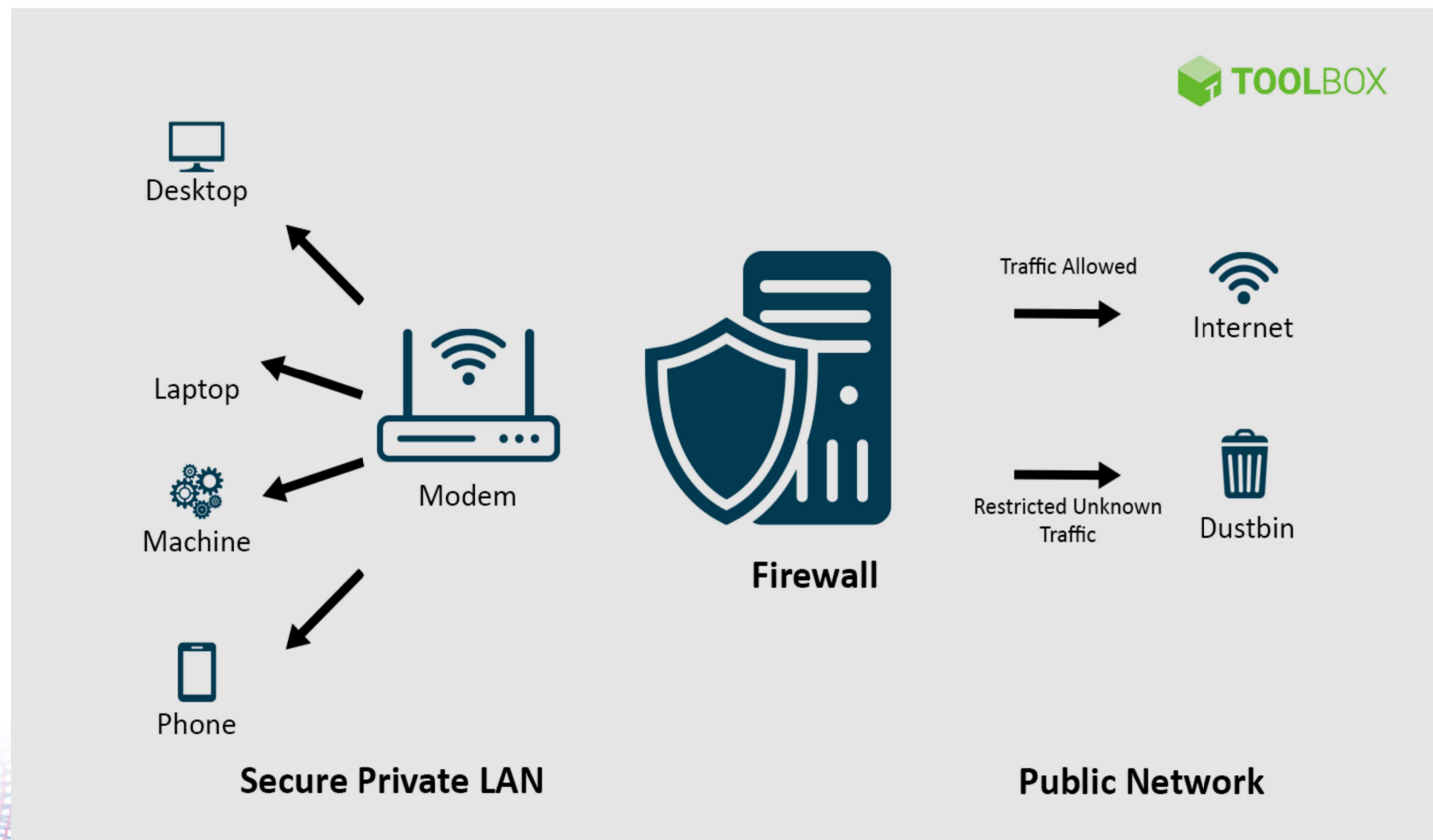
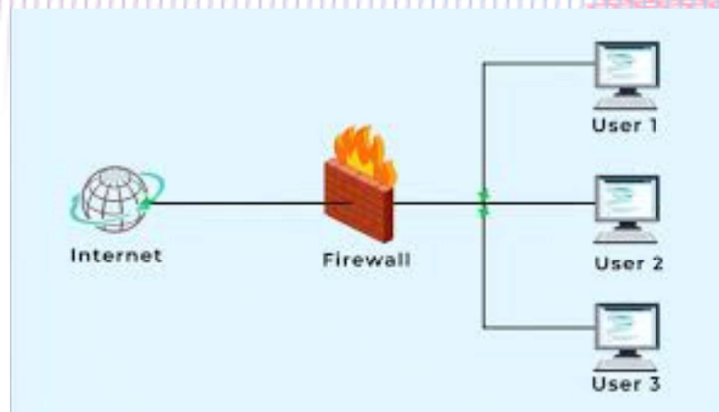
How to easily Transfer Files or **Backup Datas** from **iPhone/iPad** devices to **Windows** 10/11 computers ?

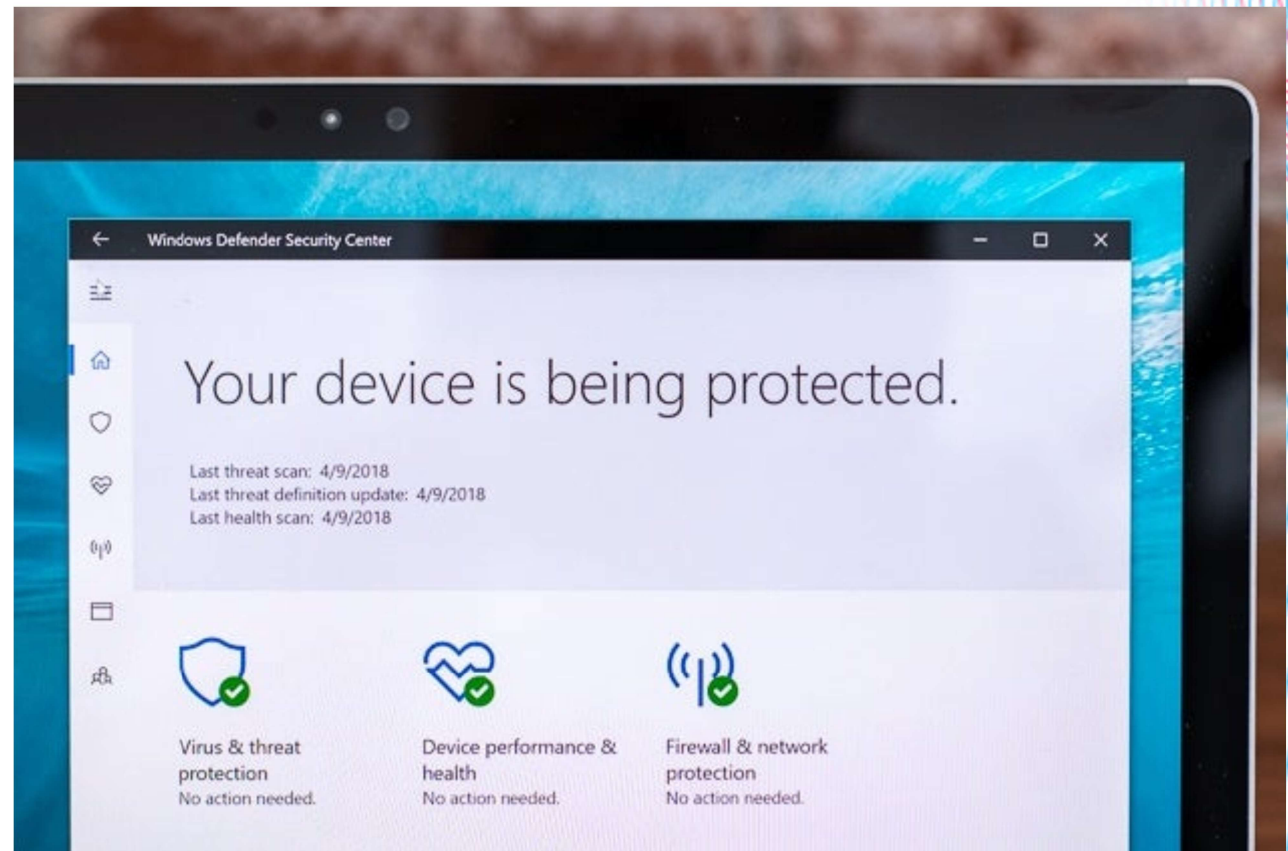
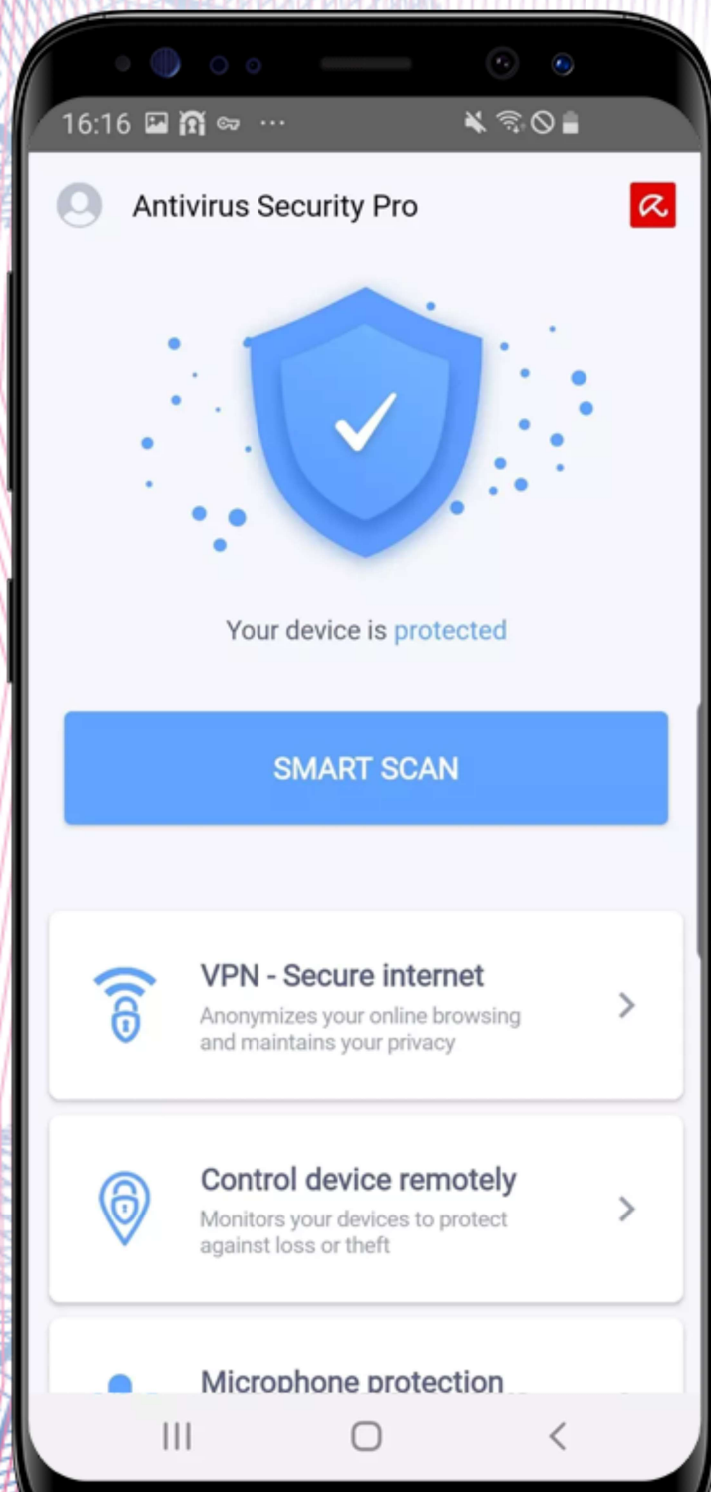


<https://www.youtube.com/watch?v=3AkvwZK9nMU>

7. Hướng dẫn tự bảo vệ bạn

- Install reputable ***antivirus software and enable your firewall.***
- These tools help ***block malicious programs and un-authorized access.***
- Không nên cho những ***ứng dụng online hay social media tự động thay đổi settings*** để bảo vệ an toàn cho chính mình, gia đình và bạn bè.
- Không cho ứng dụng ***chế độ theo dõi nơi (location)*** từ mạng hay apps – vô tình bị share info.
- Kiểm soát việc ***mở máy chụp hình tự động***





Settings



Wallpaper

Home and lock screen wallpaper



Themes

Themes • Wallpapers • Icons



Home screen

Layout • App icon badges



Lock screen

Screen lock type



Biometrics and security

Face recognition • Fingerprints



Privacy

Permission management



Location

Location permissions • Location requests



Google

Google services



Accounts and backup

Manage accounts • Smart Switch



Advanced features

Android Auto • Side key

Location



Location



On



App permissions



Improve accuracy

Use Wi-Fi and Bluetooth for more accurate location detection.

Recent location requests



Google

Location services



Emergency Location Service

On



Google Location Accuracy

On



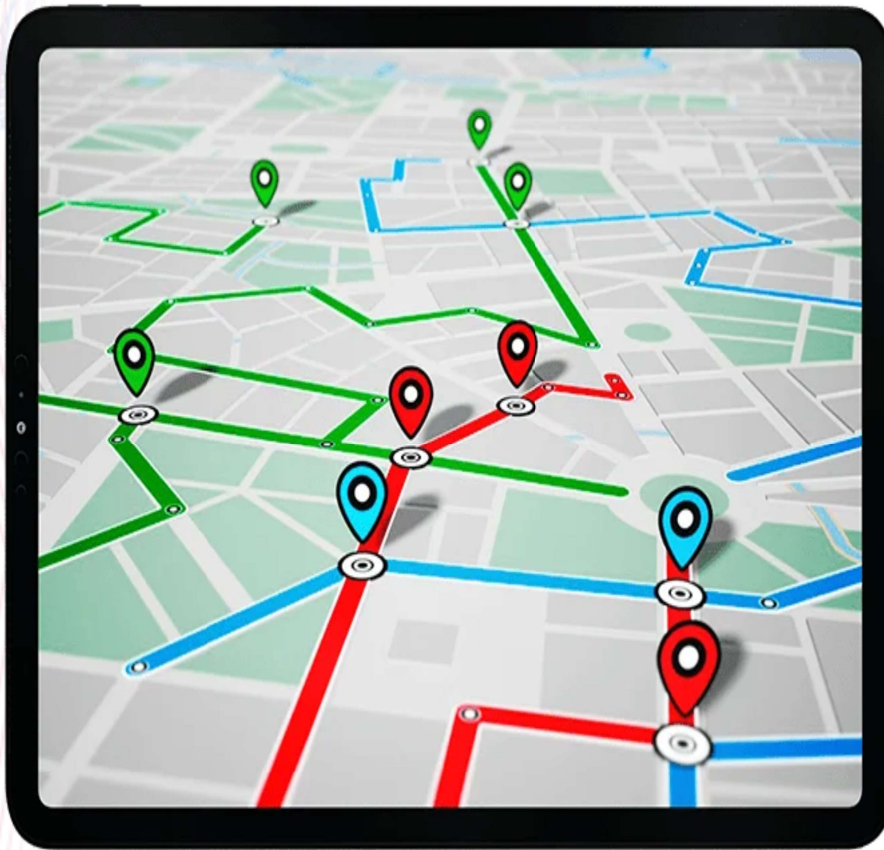
Google Location History

On



Google Location Sharing

On



Location trackers, while useful for safety and convenience, can be misused to stalk, harass, or control individuals, especially in situations involving domestic violence or coercive control. These tools, like Life360 and Find My iPhone, can be employed by perpetrators to monitor and track victims without their knowledge or consent.



- Trojan is a type of malware that is often disguised, in this case as legitimate software or program. Once installed on a device, it can ***give hackers full remote access to a person's computer.***
- UNSW cybersecurity expert Professor Salil Kanhere says that we shouldn't assume Trojan attacks only occur in spy thriller movie plots. It is, he says, happening frequently to ordinary people today.
- “What is alarming is that it also gives them remote access to your computer, including peripherals ***such as your webcam – meaning they can essentially watch whatever is on the other side of the lens.*** This type of attack is known as camfecting

7. Video Hướng dẫn cách lưu trữ

- Backup contact list on gmail

<https://www.youtube.com/watch?v=8CmaulMRopE>

- Contact phone from Iphone cloud

<https://www.youtube.com/watch?v=WtFwbqE4Cjw>

- Move mobile contacts to gmail account

<https://www.youtube.com/watch?v=EMAhgNVDYoA%3D%3D>

- Move mobile contacts to gmail account

<https://www.youtube.com/watch?v=EMAhgNVDYo>

Một số cách đề phòng tự bảo vệ an toàn

- Nhận biết những nguy hiểm lừa đảo
- Cảnh thận để không bị đánh cắp thông tin
- Cảnh thận khi truy cập mạng tránh bị dẫn tới những trang mạng không tốt – quảng cáo, lừa đảo, khiêu dâm.
- Thường xuyên delete bỏ những tin, email rác
- Lưu giữ lại thông tin quan trọng chỗ an toàn để kiểm khi cần

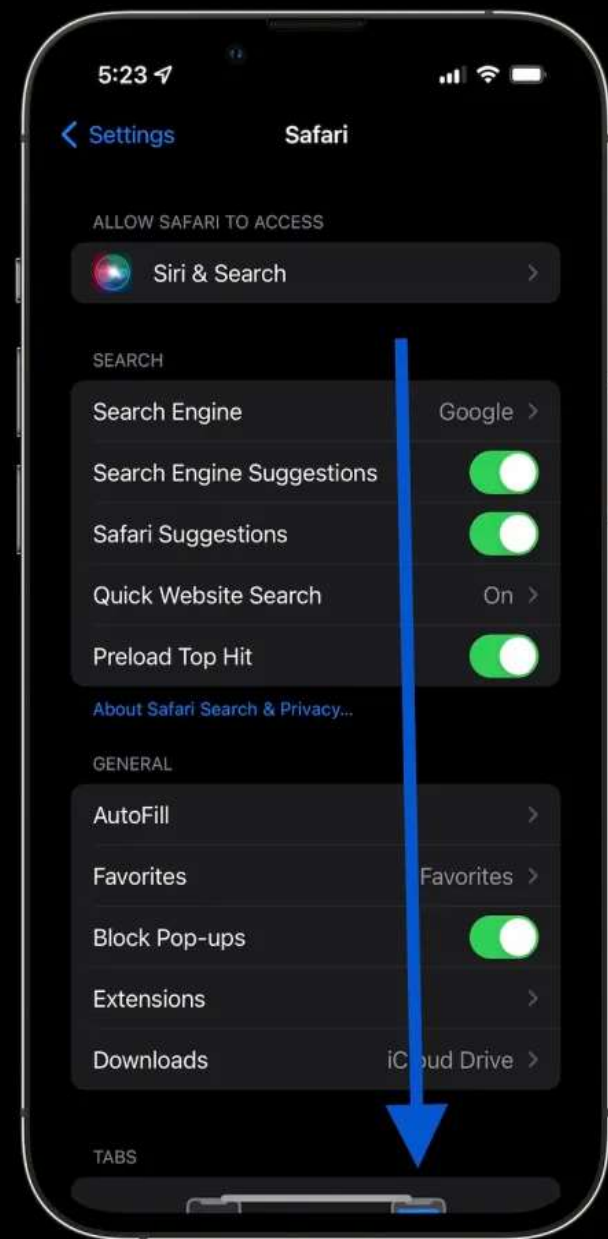
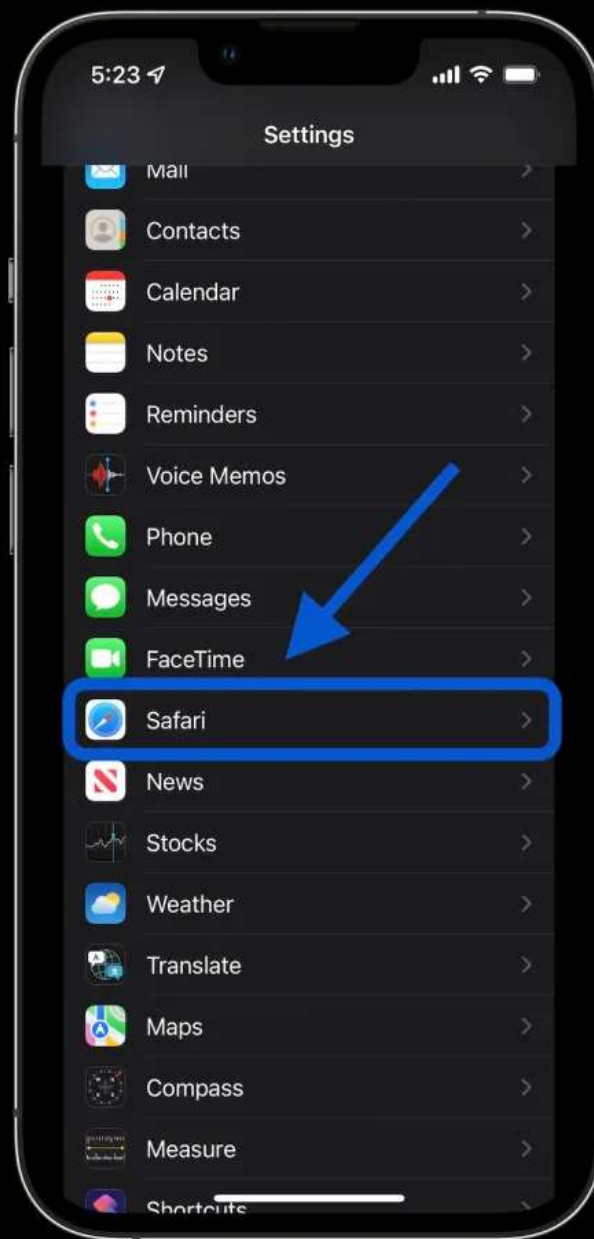


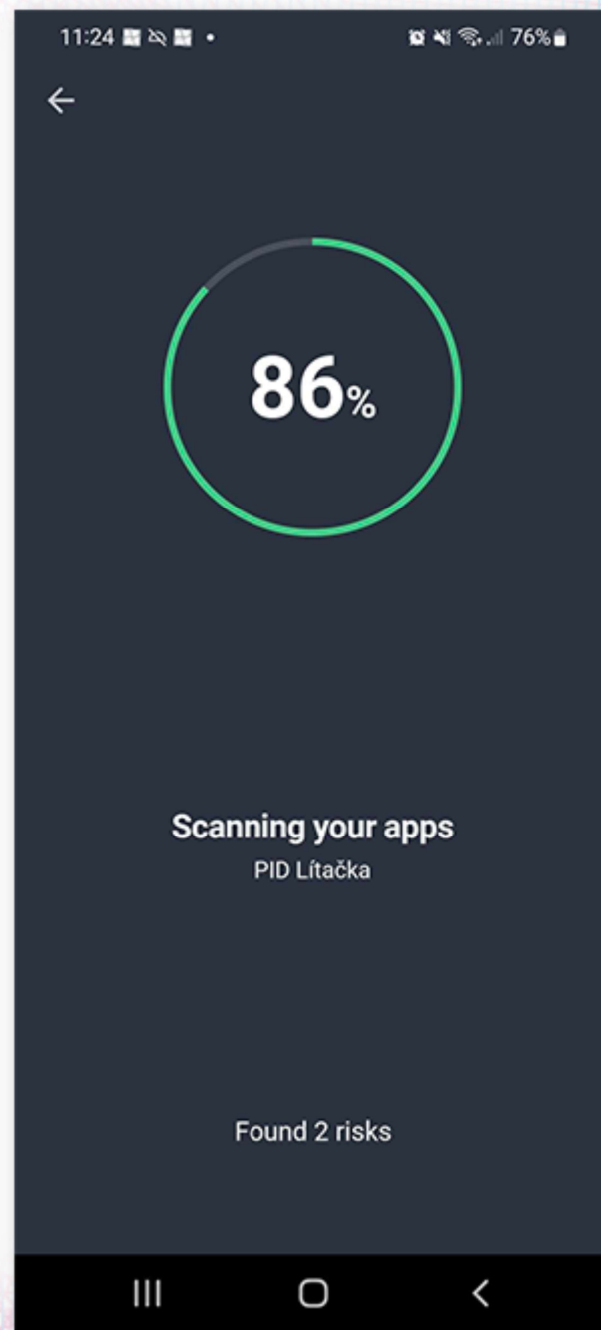
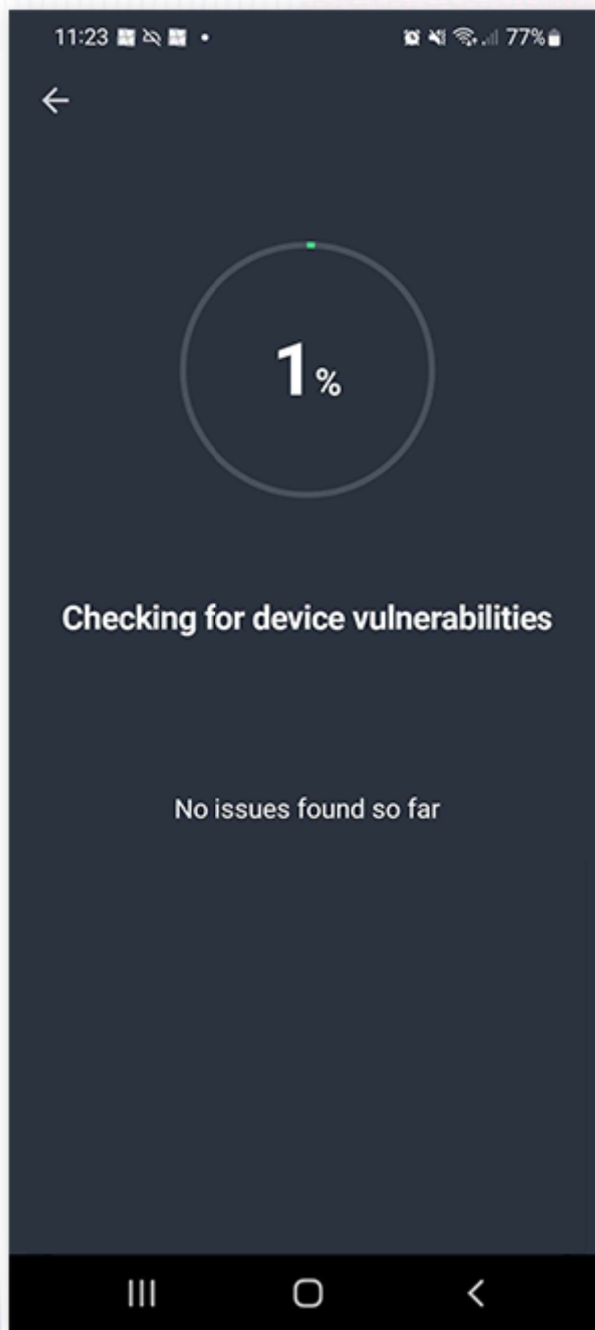
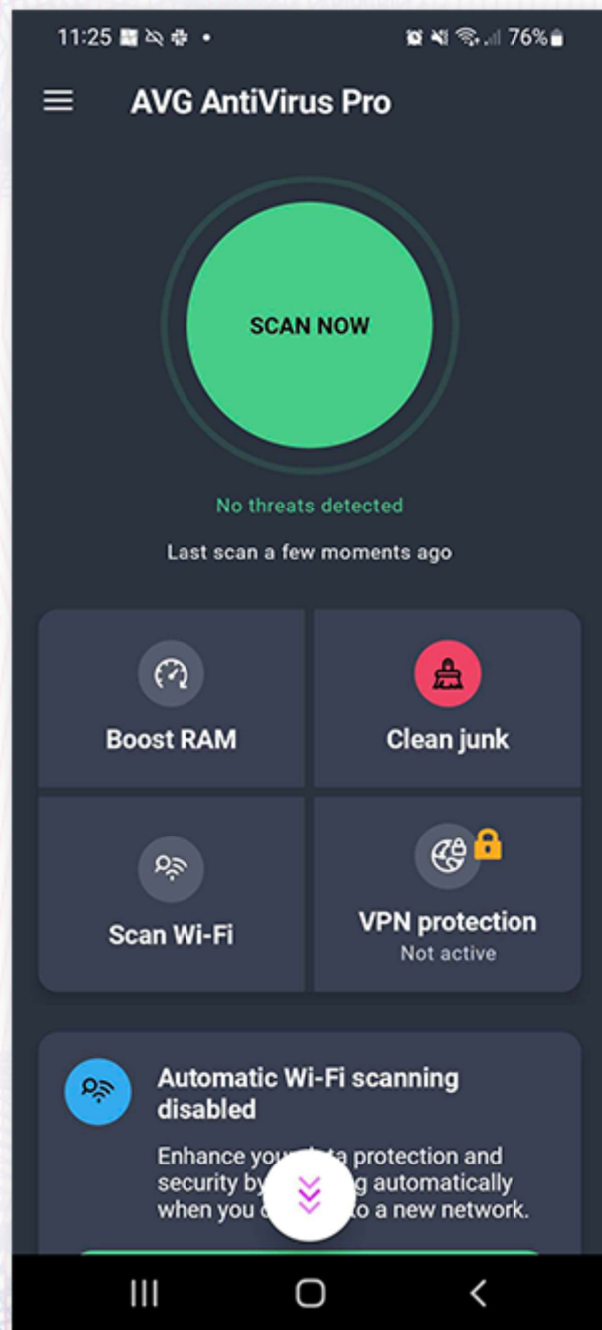
**PHÒNG TRÁNH QUÉT
MÃ QR LỪA ĐẢO** 
khi sử dụng
HOME PayLater



Một số cách đề phòng tự bảo vệ an toàn

- Use *anti-virus, defender clean up cache, history, password hay thông tin trên browser trước* và sau khi dùng.
- Tránh **dùng free Wi-Fi**
- Cẩn thận khi chia sẻ thông tin cá nhân cho những người khác.
- Suy xét chọn lựa cẩn thận khi mua hàng online
- ***Không đưa chi tiết tài chính*** cho những công ty trả phí, bill tự động.
- Mở một ***account dùng tạm*** thời để chi trả online.





Windows Security



Home



Virus & threat protection



Account protection



Firewall & network protection



Device security



Device performance & health



Family options



Protection history



Virus & threat protection

Protection for your device against threats.



Current threats

No current threats.

Last scan: 8/23/2022 10:07 AM (quick scan)

0 threat(s) found.

Scan lasted 2 minutes 36 seconds

57195 files scanned.

Quick scan

[Scan options](#)

[Allowed threats](#)

[Protection history](#)

- Paypal does **not charge** the buyer/sender anything to pay an invoice. Fees are paid by the recipient. US fees are 2.9% of the payment plus 30 cents domestically.
- Paypal offers you ***fraud protection through their Buyer Protection program***, although if the payment is for a physical item you must return it to the seller and prove that it has been delivered to get the refund.
- Instant transfer through Interac (and possibly other systems) is ... instant, at least domestically, while the speed of Paypal payments depends on how you back your account. If you use a Paypal balance or a credit card to back your payment, it will be instant, but if you only back your PP with a bank account you have written an “e-cheque” which must clear the banking system. *This can take a few days and if you and the seller are in different countries, as much as ten days.*
- Paypal anonymizes the financial information of both buyer and seller. (<https://www.quora.com/For-online-payments-is-it-better-to-do-it-through-my-bank-or-Paypal>)

Một số cách đề phòng tự bảo vệ an toàn

- *Không dùng chính xác ngày tháng năm sinh hay tên, nơi ở thật trên những trang social media.*
- *Kiểm soát cẩn thận những người muốn kết bạn nhất là FaceBook*
- Thận trọng với những *quảng cáo free, thử hàng vì đa số là scam*. Ngay như trial anti-virus software Norton, AVG, AVAST sau thời gian trial nếu không dùng tiếp tục khi bỏ sẽ phá hủy thiết bị và phần mềm của bạn, tự disconnect các cổng liên lạc và phần mềm cho OS.



- **Cybercriminals are always looking for the new weak link and social media** is a point of vulnerability for many businesses. As it becomes more common for **social media to be used for and by businesses, the opportunity for cybercriminals** to use social media in their attacks grows.
- **Social media is an essential tool for networking, events, advertising, keeping up with trends and more.** However, with the rise of remote working and **personal smart devices, social media data breaches are fast becoming a risk** of which companies need to be aware.
- **What is a data breach?**
- **Data breaches are the result of a cyber-attack where criminals gain unauthorized access to a computer system or network and steal private, sensitive, or confidential personal and financial information**
 - Facebook estimates that anywhere from 50 million to 100 million of its monthly active user accounts are fake duplicates. As of late 2020, almost half of all consumers worldwide expect to be hit by a data breach. (source: <https://netacea.com/blog/the-rise-of-social-media-data-breaches/>)



Một số cách đề phòng tự bảo vệ an toàn

- *Cẩn thận với những survey* có những chi tiết nhỏ hay bí ẩn để lấy cắp thông tin của mình.
- Khi phát hiện có những *thay đổi bất thường* trong hoạt động của máy hay lúc truy cập thông tin. Nên tắt máy ngay và *checking virus, scan hệ thống* để tránh bị hacker xâm nhập.
- Báo cáo lại với The National Anti-Scam Centre

Who is the National Anti-Scam Centre?

The National Anti-Scam Centre is where government and industry work together to protect Australians from scams. We're harnessing shared resources and smarter analytics to identify blind spots, strengthen weak links and use data to react faster, stopping scams before they happen.

Our aim is to make Australia a harder target for scammers.

For more information about how to avoid or report a scam, visit the Scam watch website <https://www.nasc.gov.au/>



STOP. CHECK. PROTECT.

Three small steps to keep Australia safe from scammers.

Scam alert: ACCC phone numbers spoofed by scammers

Be confident connected

- Beware of spam voice mail or messages
- Beware of financial discussion on phone, email and message and website
- Apply Best Practices for Online Behaviour

STOP – CHECK – PROTECTED

Be confident and happy ONLINE