1. **Trình bày khái niệm mạng không dây, thành phần mạng không dây và hoạt động cơ bản của mạng không dây;**

Mạng không dây (Wireless Network):

Mạng không dây là một hệ thống kết nối mà không cần sử dụng dây cáp vật lý để truyền tải dữ liệu giữa các thiết bị. Thay vì sử dụng cáp, mạng không dây sử dụng sóng radio, tia hồng ngoại, hoặc các phương tiện truyền tải không dây khác để truyền thông tin.

Thành Phần Cơ Bản của Mạng Không Dây:

Thiết bị Cuối (End Devices): Đây là các thiết bị sử dụng mạng không dây để truyền hoặc nhận dữ liệu, ví dụ như điện thoại di động, máy tính xách tay, máy tính bảng, thiết bị IoT (Internet of Things), vv.

Access Points (APs): Access Points là các thiết bị có nhiệm vụ kết nối các thiết bị cuối với mạng không dây. Chúng chuyển tiếp dữ liệu giữa thiết bị cuối và mạng có dây nếu cần thiết.

Router và Switch:

Router: Thiết bị chịu trách nhiệm chuyển tiếp dữ liệu giữa các mạng, đặc biệt là giữa mạng không dây và mạng có dây.

Switch: Thiết bị quản lý và chuyển tiếp dữ liệu trong cùng một mạng.

Antenna: Antenna được sử dụng để truyền và nhận sóng radio, chuyển đổi giữa tín hiệu điện và sóng radio và ngược lại.

Middleware và Protocol:

Middleware: Phần mềm giữa ứng dụng và hệ điều hành, cung cấp giao tiếp và quản lý tài nguyên.

Protocol: Quy tắc và quy định mà các thiết bị tuân theo để giao tiếp với nhau, đảm bảo tính tương thích và an toàn.

Hoạt Động Cơ Bản của Mạng Không Dây:

Truyền Thông Đa Hướng (Broadcasting): Dữ liệu được truyền tải qua không gian và có thể được nhận bởi nhiều thiết bị cùng một lúc.

Truyền Thông Đa Điểm (Point-to-Multipoint): Một thiết bị truyền dữ liệu đến nhiều thiết bị khác, ví dụ như khi một access point truyền dữ liệu đến nhiều thiết bị cuối.

Truyền Thông Điểm-Điểm (Point-to-Point): Dữ liệu được truyền giữa hai thiết bị cụ thể, ví dụ như truyền dữ liệu giữa hai điểm access point hoặc giữa một thiết bị cuối và một access point.

Tự Tổ Chức (Self-Organizing): Mạng không dây thường có khả năng tự tổ chức và thích ứng với biến đổi trong môi trường hoặc số lượng thiết bị kết nối.

1. **Phân tích về hình thức tấn công Deauthentication trên mạng không dây;**

Tấn công Deauthentication là một trong những hình thức tấn công phổ biến đối với mạng không dây, nhằm mục đích ngăn chặn thiết bị từ việc kết nối với mạng hoặc ngắt kết nối của chúng. Dưới đây là một phân tích chi tiết về tấn công Deauthentication trên mạng không dây:

\*\*1. Mục Tiêu của Tấn Công:

Ngắn hạn: Ngăn chặn hoặc ngắt kết nối của một hoặc nhiều thiết bị khỏi mạng không dây.

Dài hạn: Tạo điều kiện thuận lợi cho các tấn công khác như tấn công Man-in-the-Middle (MITM).

\*\*2. Cơ Chế Hoạt Động:

Gửi Gói Tin Deauthentication: Kẻ tấn công gửi các gói tin Deauthentication đến một hoặc nhiều địa chỉ MAC của thiết bị đang kết nối với mạng.

Mô Phỏng Từ Access Point: Gói tin Deauthentication thường được giả mạo để trông giống như chúng đến từ Access Point (AP) của mạng, để thiết bị kết nối bị nhầm lẫn.

\*\*3. Lợi Ích và Mục Đích:

Gây Phiền Hại: Tạo ra sự phiền hại và gây khó khăn cho người dùng khi họ mất kết nối.

Tấn Công MITM: Mở đường cho các tấn công Man-in-the-Middle khi thiết bị ngừng kết nối và sau đó cố gắng kết nối lại.

\*\*4. Phương Tiện Thực Hiện Tấn Công:

Sử Dụng Công Cụ:

Công cụ như Aircrack-ng, mdk3, và aireplay-ng thường được sử dụng để gửi gói tin Deauthentication.

Tấn công này có thể được thực hiện thông qua các card mạng không dây chế độ monitor.

\*\*5. Phòng Ngừa và Bảo Vệ:

Sử Dụng WPA3: Nâng cấp lên WPA3 nếu có khả năng, vì WPA3 cung cấp bảo mật mạnh mẽ hơn so với WPA2.

Cấu Hình Mạng An Toàn: Cài đặt các biện pháp bảo mật khác như 802.1X cho chứng thực và sử dụng mã hóa mạnh mẽ.

Giám Sát Mạng: Theo dõi liên tục hoạt động của mạng để phát hiện sớm bất kỳ hoạt động nghi ngờ nào.

**2.1) Phân tích các vấn đề an toàn khi sử dụng giao thức WEP trong mạng không dây;**

Giao thức WEP (Wired Equivalent Privacy) là một trong những giao thức bảo mật mạng không dây cổ điển. Tuy nhiên, WEP đã bị coi là không an toàn và dễ bị tấn công. Dưới đây là phân tích về các vấn đề an toàn khi sử dụng giao thức WEP:

\*\*1. Sử Dụng Mã Hóa Yếu:

Vấn Đề: WEP sử dụng mã hóa RC4 với khóa có kích thước chỉ 40-bit hoặc 104-bit, làm cho nó dễ bị tấn công và bẻ khóa.

Lời Giải: Mã hóa WPA2 hoặc WPA3 được coi là mạnh mẽ hơn và nên được ưu tiên sử dụng.

\*\*2. Khóa Tuyến Tính:

Vấn Đề: WEP sử dụng khóa tuyến tính để mã hóa dữ liệu, điều này làm cho nó dễ bị tấn công với kỹ thuật tấn công Keystream Prediction.

Lời Giải: Sử dụng giao thức bảo mật mạng không dây hiện đại như WPA2 hoặc WPA3, có cơ chế mã hóa mạnh mẽ và khóa động.

\*\*3. Tấn Công Korek:

Vấn Đề: Tấn công Korek là một kỹ thuật tấn công từ điển được sử dụng để tìm ra khóa WEP.

Lời Giải: Sử dụng mật khẩu mạnh và thường xuyên thay đổi để ngăn chặn tấn công từ điển.

\*\*4. Initialization Vector (IV) Dự Đoán:

Vấn Đề: WEP sử dụng IV để gia tăng độ ngẫu nhiên, nhưng con số IV giới hạn và dễ dự đoán, tạo điều kiện thuận lợi cho tấn công.

Lời Giải: Sử dụng giao thức có cơ chế quản lý IV mạnh mẽ hơn, như TKIP (Temporal Key Integrity Protocol) trong WPA.

\*\*5. Sự Đánh Bại bởi Airsnort và Aircrack:

Vấn Đề: Công cụ như Airsnort và Aircrack-ng được thiết kế để tận dụng các yếu điểm của WEP và dễ dàng bẻ khóa.

Lời Giải: Nâng cấp lên các giao thức bảo mật mạng không dây mạnh mẽ hơn như WPA2 hoặc WPA3.

\*\*6. Brute Force Attacks:

Vấn Đề: Tấn công Brute Force có thể được thực hiện để thử tất cả các khả năng của khóa WEP.

Lời Giải: Sử dụng mật khẩu mạnh, kết hợp chữ, số và ký tự đặc biệt để khó khăn hóa quy trình Brute Force.

\*\*7. Khả Năng Phục Hồi Mật Khẩu:

Vấn Đề: WEP cho phép dễ dàng phục hồi mật khẩu từ dữ liệu thu được từ gói tin.

Lời Giải: Sử dụng giao thức mạng không dây có khả năng ẩn thông tin mật khẩu hiệu quả hơn, chẳng hạn như WPA2 hoặc WPA3.

**Phân tích về hình thức tấn công Man in the middle trên mạng không dây;**

Tấn công Man-in-the-Middle (MITM) là một hình thức tấn công nơi kẻ tấn công đứng giữa hai bên truyền thông và theo dõi, thay đổi, hoặc chặn thông tin truyền qua giữa chúng mà không bị phát hiện. Trong môi trường mạng không dây, MITM có thể được thực hiện một cách tương đối dễ dàng. Dưới đây là phân tích về hình thức tấn công Man-in-the-Middle trên mạng không dây:

Cách Thức Thực Hiện Tấn Công MITM trên Mạng Không Dây:

ARP Spoofing/Poisoning:

Kẻ tấn công gửi các gói tin ARP (Address Resolution Protocol) giả mạo để làm cho địa chỉ IP tương ứng với địa chỉ MAC của mình, làm cho thiết bị mục tiêu tin rằng nó gửi dữ liệu đến địa chỉ MAC của kẻ tấn công.

DNS Spoofing:

Kẻ tấn công có thể thay đổi câu trả lời DNS để chuyển hướng người dùng đến các trang web giả mạo và thu thập thông tin đăng nhập.

Wi-Fi Phishing:

Kẻ tấn công tạo ra một mạng Wi-Fi giả mạo có tên giống như mạng công cộng, khiến người dùng kết nối vào mạng giả mạo để thu thập thông tin đăng nhập.

SSL Stripping:

Kẻ tấn công có thể giả mạo trang web không sử dụng HTTPS và chuyển hướng người dùng sang phiên bản không bảo mật của trang web để đánh cắp thông tin.

Packet Sniffing:

Kẻ tấn công có thể sử dụng công cụ chặn gói tin để đọc và theo dõi thông tin truyền qua mạng, bao gồm cả thông tin đăng nhập và dữ liệu cá nhân.

Session Hijacking:

Kẻ tấn công có thể chiếm đoạt phiên đăng nhập của người dùng để lợi dụng quyền truy cập và thực hiện các hoạt động trái phép.

Các Biện Pháp Bảo Vệ chống Tấn Công MITM trên Mạng Không Dây:

Sử Dụng HTTPS:

Sử dụng kết nối HTTPS để mã hóa dữ liệu giữa người dùng và máy chủ, ngăn chặn kẻ tấn công đọc thông tin truyền qua mạng.

Sử Dụng VPN:

Sử dụng một mạng riêng ảo (VPN) để mã hóa toàn bộ giao tiếp giữa thiết bị và mạng, ngăn chặn tấn công MITM.

Chống ARP Spoofing:

Sử dụng các công cụ và kỹ thuật như ARP spoofing detection để phát hiện và ngăn chặn tấn công ARP Spoofing.

Kiểm Tra Chứng Thực Mạng:

Sử dụng các phương tiện chứng thực mạng như 802.1X để đảm bảo rằng chỉ những thiết bị được ủy quyền mới có thể kết nối vào mạng.

Sử Dụng Mạng 4G/5G:

Chuyển sang sử dụng mạng di động 4G hoặc 5G thay vì Wi-Fi công cộng khi cần tính an toàn cao hơn.

Kiểm Tra Điểm Truy Cập:

Kiểm tra kỹ các điểm truy cập Wi-Fi trước khi kết nối và tránh kết nối vào các mạng không dây không xác đáng tin cậy.

**3) Phân tích các vấn đề an toàn khi sử dụng giao thức WPA trong mạng không dây**

Giao thức WPA (Wi-Fi Protected Access) được phát triển để cải thiện tính an toàn so với WEP và là một tiêu chuẩn bảo mật mạng không dây phổ biến. Tuy nhiên, cũng có một số vấn đề an toàn cần được xem xét khi sử dụng WPA. Dưới đây là phân tích các vấn đề an toàn chính:

\*\*1. Kỹ Thuật Tấn Công Brute Force:

Vấn Đề: Tấn công Brute Force có thể được thực hiện để thử tất cả các khả năng của mật khẩu WPA, đặc biệt là khi mật khẩu yếu.

Lời Giải: Sử dụng mật khẩu mạnh, kết hợp chữ, số và ký tự đặc biệt để khó khăn hóa quy trình Brute Force.

\*\*2. Khả Năng Sử Dụng Mật Khẩu Dễ Đoán:

Vấn Đề: Người sử dụng có thể chọn mật khẩu dễ đoán hoặc sử dụng mật khẩu mặc định, làm cho nó dễ bị tấn công.

Lời Giải: Khuyến khích người dùng sử dụng mật khẩu mạnh và không sử dụng mật khẩu mặc định.

\*\*3. Tấn Công Deauthentication và Disassociation:

Vấn Đề: Kẻ tấn công có thể sử dụng tấn công Deauthentication hoặc Disassociation để đưa thiết bị người dùng ra khỏi mạng, tạo điều kiện cho các tấn công khác.

Lời Giải: Theo dõi và phát hiện tấn công, sử dụng cơ chế tăng cường bảo mật mạng để giảm thiểu tác động của tấn công này.

\*\*4. Sử Dụng WPA với TKIP:

Vấn Đề: Mặc dù TKIP được thiết kế để thay thế WEP, nhưng nó đã bị coi là không an toàn do một số lỗ hổng bảo mật đã được phát hiện.

Lời Giải: Ưu tiên sử dụng giao thức WPA2 hoặc WPA3 với AES (Advanced Encryption Standard) thay vì TKIP.

\*\*5. Tấn Công Man-in-the-Middle (MITM):

Vấn Đề: Tấn công MITM có thể được thực hiện để đánh cắp thông tin truyền qua mạng không dây.

Lời Giải: Sử dụng giao thức WPA2 hoặc WPA3, kết hợp với tính năng 802.1X để cung cấp chứng thực và bảo vệ chống lại tấn công MITM.

\*\*6. Khả Năng Sử Dụng Kỹ Thuật Phục Hồi Mật Khẩu (PMKID):

Vấn Đề: Một số công cụ tấn công có thể sử dụng kỹ thuật PMKID để thu thập thông tin và tấn công mật khẩu.

Lời Giải: Cập nhật thiết bị và hệ thống để ngăn chặn kỹ thuật PMKID và sử dụng mật khẩu mạnh.

**3.2)Phân tích các vấn đề an toàn khi sử dụng giao thức WPA2 trong mạng không dây;**

WPA2 (Wi-Fi Protected Access 2) là một giao thức bảo mật mạng không dây được thiết kế để thay thế cho WPA (Wi-Fi Protected Access) và cung cấp mức bảo mật cao hơn đối với mạng Wi-Fi. Tuy nhiên, cũng có những vấn đề an toàn mà người quản trị mạng và người sử dụng cần phải xem xét:

KRACK Attacks (Key Reinstallation Attacks):

Vấn Đề: KRACK là một loại tấn công mà kẻ tấn công có thể tái thiết lập khóa mã hóa và thu được quyền truy cập không ủy quyền vào mạng.

Giải Pháp: Các bản vá đã được phát hành để khắc phục lỗ hổng này. Người quản trị mạng cần đảm bảo rằng thiết bị và phần mềm của họ đã được cập nhật.

Brute Force Attacks (Tấn Công Brute Force):

Vấn Đề: Một kẻ tấn công có thể thử mọi khả năng của mật khẩu để đánh giá sự an toàn của mạng.

Giải Pháp: Sử dụng mật khẩu mạnh, kích thước đủ lớn và kích thước ký tự đa dạng. Cài đặt các biện pháp phòng ngừa như tạm thời khóa tài khoản sau một số lần đăng nhập thất bại.

Dictionary Attacks (Tấn Công Từ Điển):

Vấn Đề: Kẻ tấn công sử dụng từ điển các mật khẩu phổ biến để thử đăng nhập.

Giải Pháp: Sử dụng mật khẩu phức tạp và không dễ dàng đoán được. Thường xuyên thay đổi mật khẩu.

Khả Năng Tấn Công DoS (Denial of Service):

Vấn Đề: Kẻ tấn công có thể tạo ra lưu lượng mạng lớn để làm cho mạng trở nên chậm chạp hoặc không khả dụng.

Giải Pháp: Sử dụng các biện pháp bảo vệ chống tấn công DDoS và giám sát liên tục tình trạng mạng.

Sự Rò Rỉ Thông Tin:

Vấn Đề: Có thể xảy ra sự rò rỉ thông tin nhạy cảm nếu giao thức không được cấu hình đúng.

Giải Pháp: Sử dụng mã hóa mạnh mẽ, cài đặt chế độ WPA2-Enterprise khi có thể, và giữ bản vá và cấu hình hệ thống cập nhật.

Sự Yếu Đuối trong Quản Lý Mật Khẩu:

Vấn Đề: Mật khẩu yếu có thể dễ dàng bị tấn công.

Giải Pháp: Sử dụng mật khẩu mạnh, có chiều dài đủ và thường xuyên thay đổi.

Để tăng cường bảo mật mạng không dây, ngoài việc sử dụng WPA2, người quản trị mạng cũng nên xem xét việc triển khai các biện pháp bảo mật bổ sung như WPA3, sử dụng 802.1X cho chứng thực mạng, giám sát liên tục và tạo lập chính sách bảo mật mạng.

**4)Phân tích các vấn đề an toàn khi sử dụng thiết bị di động iOS; Trình bày các giải pháp nâng cao an toàn khi sử dụng thiết bị di động iOS trong mạng không dây;**

Vấn Đề An Toàn Khi Sử Dụng Thiết Bị Di Động iOS:

Phishing và Malware:

Vấn Đề: Người sử dụng có thể nhận được email, tin nhắn giả mạo để lừa đảo thông tin cá nhân hoặc cài đặt malware.

Giải Pháp: Cẩn thận khi mở các liên kết không rõ nguồn gốc, sử dụng ứng dụng chống malware và duyệt web an toàn.

Kết Nối Mạng Không Dây Bất An:

Vấn Đề: Kết nối đến mạng không dây không an toàn có thể tạo rủi ro bị đánh cắp thông tin cá nhân.

Giải Pháp: Sử dụng mạng Wi-Fi đã được xác minh và kích hoạt tính năng VPN để tăng cường bảo mật truyền dữ liệu.

Quản Lý Quyền Riêng Tư:

Vấn Đề: Ứng dụng yêu cầu quyền truy cập vào thông tin cá nhân mà không cần thiết.

Giải Pháp: Kiểm tra và cấu hình cẩn thận quyền truy cập ứng dụng trong Cài đặt, hạn chế quyền truy cập nếu cần.

Thiết Lập Mật Khẩu Yếu:

Vấn Đề: Sử dụng mật khẩu dễ đoán hoặc không đủ mạnh.

Giải Pháp: Sử dụng mật khẩu mạnh, kích thước đủ lớn, kết hợp chữ, số và ký tự đặc biệt.

Cập Nhật Phần Mềm Đều Đặn:

Vấn Đề: Không cập nhật phần mềm iOS đều đặn có thể tạo rủi ro về bảo mật.

Giải Pháp: Bật chế độ tự động cập nhật hoặc kiểm tra thường xuyên để cài đặt bản vá mới nhất.

Giải Pháp Nâng Cao An Toàn Khi Sử Dụng Thiết Bị Di Động iOS trong Mạng Không Dây:

Sử Dụng Mã Hóa:

Kích hoạt mã hóa thiết bị trong Cài đặt để bảo vệ dữ liệu khi thiết bị bị mất hoặc bị đánh cắp.

Kích Hoạt Touch ID hoặc Face ID:

Sử dụng tính năng xác minh bằng vân tay hoặc nhận diện khuôn mặt để tăng cường bảo mật.

Quản Lý Thiết Bị Từ Xa:

Kích hoạt tính năng "Find My iPhone" để có thể quản lý và xóa dữ liệu từ xa nếu thiết bị bị mất.

Sử Dụng Ứng Dụng VPN:

Kích hoạt dịch vụ VPN để bảo vệ dữ liệu khi kết nối vào mạng không dây công cộng.

Kiểm Tra Ứng Dụng Trong App Store:

Tải ứng dụng chỉ từ App Store chính thức để tránh cài đặt phần mềm độc hại.

Tắt Các Tính Năng Không Cần Thiết:

Tắt các tính năng như Bluetooth, Wi-Fi, và Airdrop khi không sử dụng để giảm rủi ro tấn công.

Chế Độ Công Cộng:

Chuyển đổi sang chế độ công cộng (Public Wi-Fi) trong Cài đặt khi kết nối vào mạng không dây công cộng để tăng cường bảo mật.

Bằng cách thực hiện các giải pháp trên, người sử dụng thiết bị di động iOS có thể nâng cao mức độ an toàn và bảo mật của họ khi sử dụng trong mạng không dây.

**4.2) Phân tích các vấn đề an toàn khi sử dụng thiết bị di động android; Trình bày các giải pháp nâng cao an toàn khi sử dụng thiết bị di động android trong mạng không dây**

Vấn Đề An Toàn Khi Sử Dụng Thiết Bị Di Động Android:

1 Malware và Phần Mềm Độc Hại:

Vấn Đề: Ứng dụng không an toàn hoặc nguồn không đáng tin cậy có thể chứa malware và phần mềm độc hại.

Giải Pháp: Tải ứng dụng chỉ từ Google Play Store, cập nhật hệ điều hành và ứng dụng thường xuyên, sử dụng ứng dụng chống malware.

2 Tấn Công Man-in-the-Middle (MITM):

Vấn Đề: Kẻ tấn công có thể thực hiện MITM để đánh cắp thông tin truyền qua mạng không dây.

Giải Pháp: Sử dụng kết nối HTTPS, sử dụng mạng 4G/5G an toàn hơn, tránh kết nối vào mạng Wi-Fi không an toàn.

3 Lỗ Hổng Bảo Mật Thiết Bị:

Vấn Đề: Lỗ hổng bảo mật trong hệ điều hành Android hoặc các ứng dụng có thể bị tận dụng.

Giải Pháp: Cập nhật hệ điều hành và ứng dụng, sử dụng thiết bị hỗ trợ cập nhật thường xuyên.

4 Quyền Truy Cập Ứng Dụng Quá Mức:

Vấn Đề: Một số ứng dụng yêu cầu quyền truy cập không cần thiết vào thông tin cá nhân.

Giải Pháp: Kiểm tra và cấu hình quyền truy cập ứng dụng trong cài đặt Android, chỉ cấp quyền cần thiết.

5 Mất Thiết Bị và Đánh Cắp Dữ Liệu:

Vấn Đề: Mất điện thoại hoặc bị đánh cắp có thể dẫn đến mất mát dữ liệu nhạy cảm.

Giải Pháp: Sử dụng tính năng khóa màn hình, cài đặt tính năng xóa từ xa và sao lưu dữ liệu.

**Giải Pháp Nâng Cao An Toàn Khi Sử Dụng Thiết Bị Di Động Android trong Mạng Không Dây:**

6 Sử Dụng Mã Hóa Đối Với Dữ Liệu:

Kích hoạt mã hóa dữ liệu trên thiết bị để bảo vệ thông tin cá nhân khi bị mất hoặc đánh cắp.

7 Sử Dụng VPN:

Sử dụng dịch vụ VPN để mã hóa dữ liệu truyền qua mạng và bảo vệ khỏi tấn công MITM.

8 Cập Nhật Hệ Điều Hành và Ứng Dụng:

Thực hiện cập nhật hệ điều hành và ứng dụng đều đặn để bảo vệ khỏi các lỗ hổng bảo mật đã được vá.

9 Sử Dụng Tính Năng "Find My Device":

Bật tính năng "Find My Device" để theo dõi và quản lý thiết bị từ xa khi bị mất hoặc đánh cắp.

10 Chỉ Tải Ứng Dụng Từ Nguồn Tin Cậy:

Tải ứng dụng chỉ từ Google Play Store hoặc các nguồn đáng tin cậy để tránh malware.

11 Chế Độ "Unknown Sources":

Tắt chế độ "Unknown Sources" trong cài đặt để ngăn chặn cài đặt ứng dụng từ nguồn không xác đáng tin cậy.

12 Kiểm Tra Quyền Truy Cập Ứng Dụng:

Kiểm tra và cấu hình cẩn thận quyền truy cập của ứng dụng để ngăn chặn lợi dụng thông tin cá nhân.

13 Sử Dụng Mạng Wi-Fi An Toàn:

Tránh kết nối vào mạng Wi-Fi công cộng không an toàn. Nếu cần, sử dụng VPN khi kết nối.

10. Sử Dụng Tính Năng Biometric:

Sử dụng tính năng nhận diện vân tay (Fingerprint) hoặc nhận diện khuôn mặt (Face Unlock) để tăng cường bảo mật đăng nhập vào thiết bị.

11. Chế Độ Guest:

Khi chia sẻ thiết bị, sử dụng tính năng Chế độ Khách (Guest Mode) để hạn chế quyền truy cập và bảo vệ thông tin cá nhân.

12. Tắt Bluetooth và Wi-Fi Khi Không Sử Dụng:

Tắt Bluetooth và Wi-Fi khi không sử dụng để ngăn chặn tấn công từ xa và giảm tiềm ẩn của thiết bị trong các mạng không dây không an toàn.

13. Hạn Chế Công Cụ Phát Sóng:

Tắt chế độ Hotspot hoặc chia sẻ mạng di động khi không sử dụng để giảm rủi ro tấn công từ mạng không dây.

14. Sử Dụng Tính Năng "App Permissions":

Kiểm tra và quản lý quyền truy cập ứng dụng thông qua tính năng "App Permissions" trong cài đặt Android.

15. Sao Lưu Thường Xuyên:

Thực hiện sao lưu dữ liệu quan trọng thường xuyên, để có thể khôi phục thông tin khi cần thiết sau mất mát hoặc đánh cắp.

16. Sử Dụng Ứng Dụng Antivirus và Antimalware:

Cài đặt và sử dụng ứng dụng chống virus và phần mềm độc hại để quét và bảo vệ thiết bị.

17. Tối Ưu Hóa Cài Đặt Bảo Mật:

Cấu hình cẩn thận các tùy chọn bảo mật trong cài đặt Android, bao gồm cả tùy chọn khóa màn hình và bảo vệ dữ liệu.

18. Xem Xét Các Thiết Lập "Google Security":

Kiểm tra và cập nhật các cài đặt bảo mật có sẵn trong tài khoản Google của bạn, bao gồm cả xác minh hai yếu tố (2FA).