**BẢO VỆ DỮ LIỆU CÁ NHÂN TRÊN ĐIỆN THOẠI DI ĐỘNG**

250

[](https://antoanthongtinhaiphong.gov.vn/wp-content/uploads/2022/04/tip1.jpg)

Điện thoại di động đã trở thành vật dụng vô cùng hữu ích trong thời đại công nghệ số, tuy nhiên, các tính năng của nó có thể gây mất an toàn với quyền riêng tư của người dùng. Người dùng cần thận trọng và tăng cường quyền riêng tư cho điện thoại của mình. Sau đây là một số mẹo bảo mật quan trọng để ngăn chặn những kẻ gian lận đánh cắp thông tin cá nhân và tiền của người dùng từ điện thoại di động.

**Cảnh giác với kẻ mạo danh**

Nếu người dùng đột nhiên nhận được cuộc gọi nói rằng họ là thành viên trong gia đình và nói rằng họ đang rất cần tiền. Người dùng nên cảnh giác bởi giọng nói thường không giống nhau. Nếu nghe thấy giọng lạ, người dùng cần thận trọng và có thể tiếp tục nghe từ đầu dây bên kia. Khi đó, người dùng có thể nhận ra giọng của người lạ sẽ rất khẩn khoản và họ sẽ hướng dẫn cách gửi tiền cho họ ngay lập tức.



Ngay sau khi cúp máy, người dùng hãy gọi lại đến số của người đó từ danh bạ của mình để xác minh trực tiếp xem có phải họ vừa gọi cho mình hay không.

Ngoài ra, hãy gọi lại đến số mà người lạ vừa gọi đến, nếu không thể kết nối cuộc gọi hoặc gọi mà không bắt máy thì chính xác đó là kẻ lừa đảo mạo danh.

**Tránh sử dụng dây sạc điện thoại ở nơi công cộng**

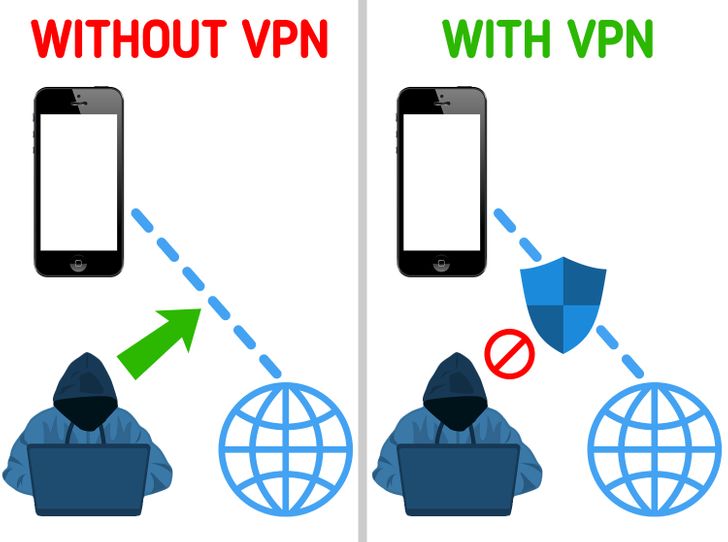
Nhiều nơi công cộng có sẵn dây sạc cho người dùng. Tuy nhiên, những kẻ lừa đảo thường thiết lập các ki-ốt giả ở những nơi công cộng để đánh lừa người dùng. Tại đầu nhận của dây có thể được kết nối với máy tính để tin tặc truy cập vào thiết bị của người dùng và thậm chí cài đặt phần mềm độc hại.



Rất khó để phân biệt trạm sạc giả với trạm thật và đó là lý do tại sao người dùng nên tránh sử dụng chúng ở nơi công cộng.

**Nên sử dụng VPN khi đăng nhập vào Wifi công cộng**

Nhiều tin tặc có thể giả mạo Wifi công cộng để đánh cắp thông tin cá nhân của người dùng. Vì thế, người dùng nên sử dụng giải pháp VPN để dữ liệu không thể đọc được khi được gửi trên mạng công cộng. Người dùng cũng có thể chuyển vùng ẩn danh trên internet để hạn chế việc lịch sử web bị theo dõi.



**Nên sử dụng ứng dụng quản lý mật khẩu**

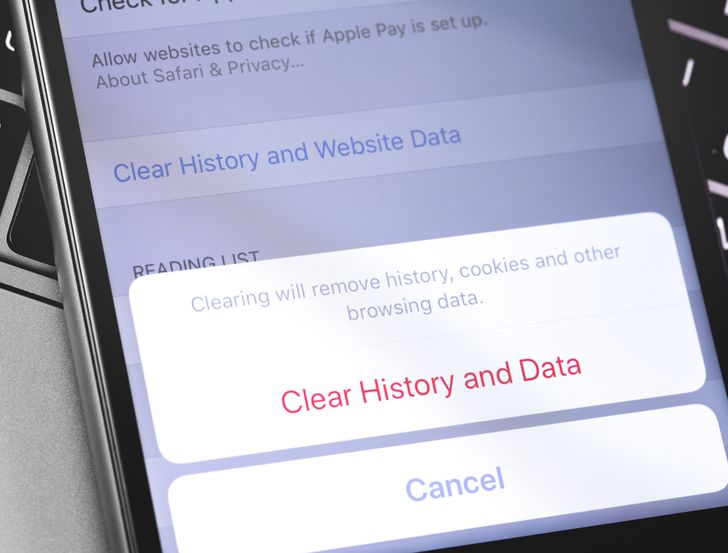
Đa số người dùng đều sử dụng mật khẩu dễ đoán, dễ nhớ và sử dụng chung một mật khẩu trên nhiều tài khoản của mình. Điều đó dẫn đến việc tin tặc dễ dàng đánh cắp mật khẩu gây rò rỉ hàng loạt tài khoản. Người dùng không nên tạo mật khẩu dễ dàng và không được lưu mật khẩu vào sổ ghi chú của điện thoại, nên sử dụng [ứng dụng quản lý mật khẩu](http://antoanthongtin.vn/lo-hong-attt/cac-ung-dung-quan-ly-mat-khau-tren-android-co-the-bi-danh-lua-104922).



Ứng dụng này không chỉ giúp tạo mật khẩu mạnh cho người dùng mà còn lưu trữ tất cả trong cơ sở dữ liệu được mã hóa. Mật khẩu duy nhất người dùng cần nhớ là mật khẩu mở khóa cơ sở dữ liệu.

**Thường xuyên xóa lịch sử web, cookie và bộ nhớ cache**

Tin tặc thường sẽ sử dụng các cookie đã lưu để truy cập vào thiết bị của người dùng nếu không tìm thấy mật khẩu của người dùng. Bởi cookie lưu trữ nhiều thông tin cá nhân như thông tin chi tiết ngân hàng của người dùng, điều mà tin tặc có thể sử dụng để thực hiện các giao dịch bất chính.



Tin tặc cũng có thể theo dõi người dùng trực tuyến và một khi chúng biết người dùng truy cập trang web nào, chúng sẽ gửi email hoặc tin nhắn lừa đảo tới họ.

Những email này có vẻ như được gửi từ một dịch vụ mà người dùng đang sử dụng và yêu cầu họ cung cấp thêm chi tiết thông tin cá nhân. Nhiều người có thể bị lừa khi cung cấp thông tin chi tiết và đó là cách những kẻ lừa đảo đánh cắp tiền của người dùng. Đó là lý do tại sao người dùng nên dọn dẹp trình duyệt thường xuyên và không bao giờ sử dụng tính năng ghi nhớ mật khẩu của tôi.

**Chỉ tải ứng dụng từ Apple store hoặc Cửa hàng Google Play**

Rất nhiều ứng dụng được tạo bởi các nguồn chưa được xác minh có thể gây ra các mối đe dọa lớn cho thiết bị của người dùng. Mối đe dọa đầu tiên là mã độc, vì một ứng dụng chưa được xác minh không phải lúc nào cũng được hệ thống bảo mật trên điện thoại kiểm tra.



Ngoài ra, nhiều ứng dụng giả mạo được tạo ra trông giống hệt như ứng dụng thật và tìm cách xâm nhập vào thiết bị của người dùng để lấy cắp tiền. Điều duy nhất họ sẽ yêu cầu là chi tiết đăng nhập và sau khi người dùng gửi đi, tin tặc sẽ có quyền truy cập vào thiết bị của bạn.

**Thiết lập ứng dụng xóa từ xa trên điện thoại**

Nếu điện thoại của người dùng bị đánh cắp hoặc bị mất, hãy ứng dụng lệnh xóa từ xa để có thể xóa tất cả dữ liệu cá nhân, phòng khi rơi vào tay kẻ xấu. Không chỉ vậy, những ứng dụng này có thể ngăn kẻ trộm khôi phục các tệp đã xóa, đồng thời đưa điện thoại về cài đặt gốc. Tuy nhiên, điện thoại cần được bật và kết nối với mạng và quá trình xóa có thể gặp trục trặc nếu điện thoại ở chế độ trên máy bay hoặc không có kết nối.



**Không nên bật chế độ Bluetooth liên tục**

Điều nguy hiểm và phổ biến nhất có thể xảy ra là tin tặc có thể truy cập vào thông tin cá nhân của người dùng nếu thiết bị của họ cho phép kết nối Bluetooth. Chúng cũng có thể phát tán phần mềm độc hại trên thiết bị của người dùng, khiến người dùng không thể sử dụng được.



Tất cả các thiết bị sử dụng Windows, iOS, Android và Linux đều có thể bị ảnh hưởng nếu chế độ Bluetooth luôn được bật. Vì thế, người dùng cần cẩn thận khi bật chế độ Bluetooth, chỉ nên dùng khi thực sự cần.