Những điều cần biết khi dùng wifi nơi công cộng

Ngày nay các mạng wifi miễn được lắp đặt ở khắp mọi nơi, từ các quán cà phê, công viên giải trí, trung tâm mua sắm, thậm chí là trên xe bus,... Điều này rất tiện lợi cho người dùng chúng ta để có thể kết nối mạng ở khắp mọi nơi để lướt Facebook và làm việc. Tuy nhiên, việc sử dụng wifi miễn phí liệu có an toàn? Câu trả lời cho bạn là không an toàn một chút nào. Bởi lẽ khi chúng ta dùng wifi công cộng, những nguy cơ về an ninh bảo mật có thể không xảy ra với bạn ngay lúc đó, nhưng nó lại là mối nguy hiểm cho những ngày về sau. Chính vì vậy, khi muốn sử dụng wifi công cộng thì hãy ghi nhớ những điều sau.

- Dữ liệu của bạn có thể bị đánh cắp khi sử dụng Wifi công cộng?
- Tổng hợp cách đổi mật khẩu WiFi trên laptop hoặc điện thoại
- Đây là cách ngăn hacker đánh cắp dữ liệu của bạn khi sử dụng Wifi công cộng

1. Giữ hệ điều hành điện thoại của bạn được cập nhật nhất

Việc cập nhật hệ điều hành trên các thiết bị điện thoại thông minh như Android hoặc iPhone không chỉ giúp điện thoại của chúng ta cập nhật thêm nhiều tính năng mới, mà nó còn giúp điện thoại khắc phục các lỗ hổng và ngăn chặn việc đánh cắp thông tin bảo mật dữ liệu cá nhân. Việc cập nhật hệ thống này không chỉ chúng chúng ta có thể truy cập mạng công cộng an toàn mà còn cho tất cả các chương trình khác.

2. Sử dụng các phần mềm diệt virus trên điện thoại

Trước khi sử dụng các wifi công cộng, thì bạn nên cài đặt cho điện thoại của mình những phần mềm diệt virus cần thiết, để có thể bảo mật dữ liệu cá nhân trước sự xâm hại của hacker. Đối với người dùng iPhone thì việc này có thể không cần thiết, nhưng với những người dùng Android thì không tránh khỏi những phiền phức từ các phần mềm độc hại này mang lại. Khi chúng ta cài đặt những phần mềm vius cho điện thoại, thì những phần mềm này như một bức tường lửa bảo vệ và loại bỏ những phần mềm độc hại nếu chúng ta gặp phải.

Vậy nên, sử dụng wifi công cộng, không có gì là đảm bảo cho thiết bị của bạn không phải tiếp xúc với phần mềm độc hại. Các ứng dụng bảo mật di động có thể giảm thiểu việc này, bảo vệ thiết bị của bạn một cách tốt nhất bằng cách chủ động bảo vệ hoặc quét và xóa những phần mền độc hại vi phạm.

3. Những mạng wifi công cộng có tốc độ chậm càng ẩn chứa nhiều mối nguy hại

Khi bạn đăng nhập vào bất kỳ mạng wifi nào đang mở mà thấy rằng, kết nối mạng của bạn chậm như "rùa bò" kể cả khi kết nối với những trang web thông dụng nhất. Lúc này, tốt nhất bạn nên ngắt kết nối với mạng wifi đó đi.

Khi tốc độ chậm, chúng ta có thể nghĩ đến khả năng do router đã bị xâm nhập. Một lời giải thích khác có thể là bạn chưa kết nối với bộ định tuyến mà đang kết nối tới một thiết bị khác được đặt làm bộ định tuyến. Tốc độ chậm có thể bởi vì dữ liệu đang được định tuyến qua thiết bị khác.

4. Không nên mua sắm trực tuyến hoặc sử dụng chuyển khoản ngân hàng

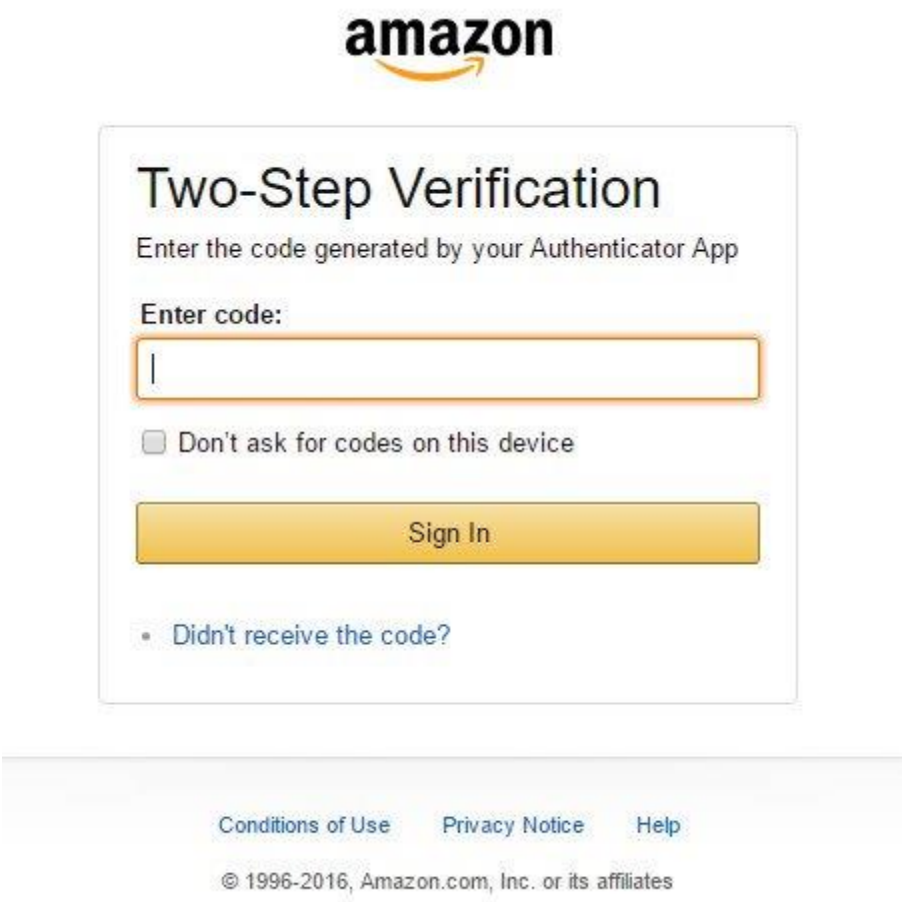
Không nên sử dụng mạng wifi công cộng khi mua hàng trực tuyến hoặc chuyển khoản ngân hàng. Khi bạn thực hiện những thao tác này trên những thiết bị wifi miễn phí, là bạn đang vô tình cho những kẻ tội phạm được biết những thông tin bảo mật của bạn thông qua các thiết bị đó, chúng có thể đánh cắp được một số dữ liệu không được mã hóa theo cách của họ tại thời điểm kết nối không an toàn.

Chính vì vậy, ở bất kỳ thời điểm nào, hay bất cứ đâu, nếu bạn muốn sử dụng những ứng dụng mua hàng trực tuyến hay chuyển khoản ngân hàng thì cách tốt nhất và an toàn nhất cho bạn đó là nên kết nối dữ liệu di động để sử dụng. Bên cạnh đó bạn cũng có thể sử dụng một mạng riêng ảo (VPN) để mã hóa tất cả lưu lượng Internet của bạn.

Nếu bạn muốn sử dụng dịch vụ ngân hàng trực tuyến, hãy sử dụng những ứng dụng chính thức của ngân hàng cung cấp như: Internet Banking.

5. Sử dụng xác thực hai yếu tố

Đây là cách mà có thể giúp bạn chắc chắn với những thao tác trên các dịch vụ trực tuyến mà có thể bạn đang sử dụng. Tương tự, họ có thể chắc chắn rằng đó là bạn đang cố gắng đăng nhập, hoặc thực hiện một giao dịch ngân hàng.



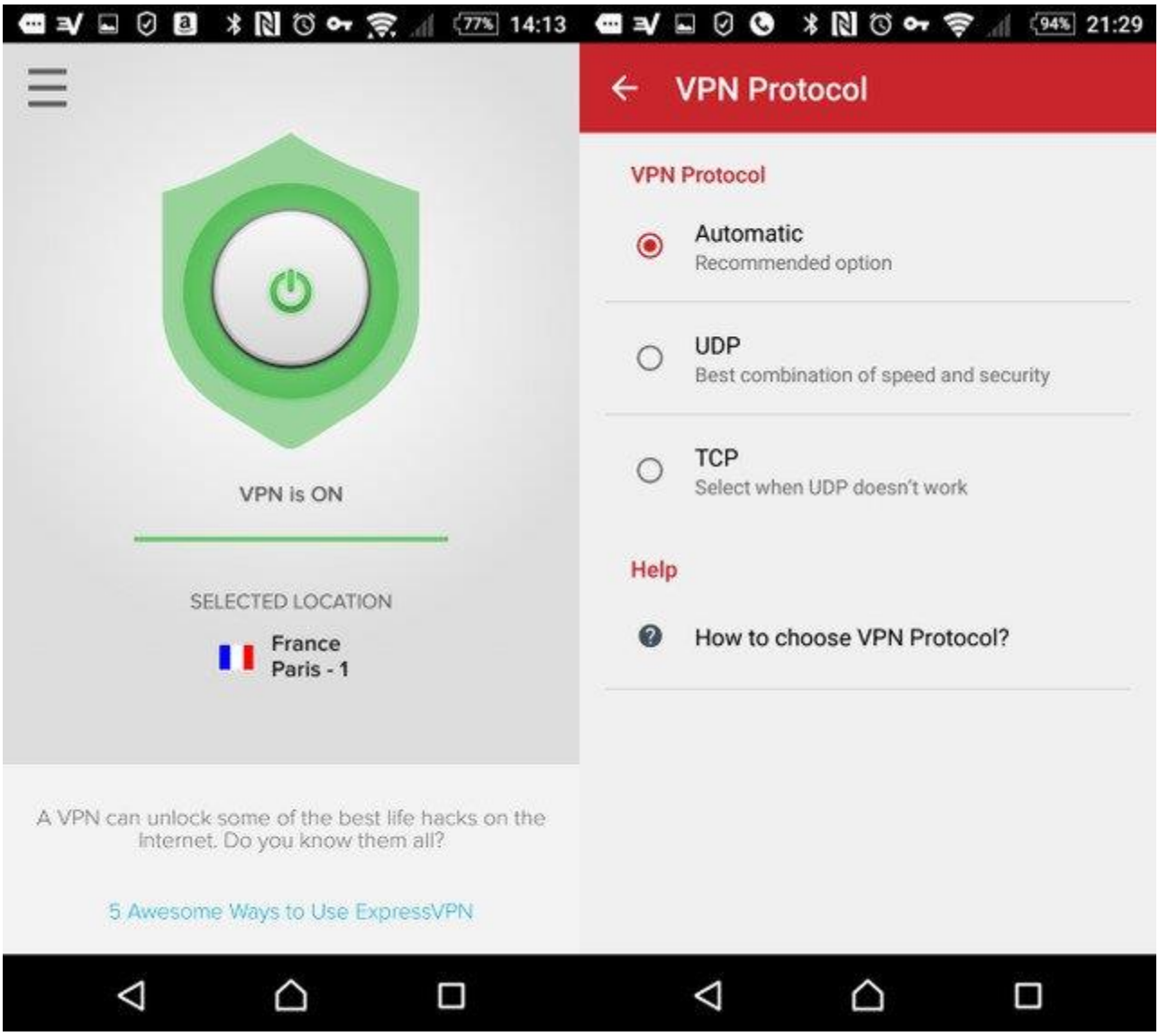
Hai yếu tố được sử dụng trong tiêu chuẩn 2FA thường là thứ mà bạn biết (thông tin đăng nhập của bạn) và thứ bạn có (mã được tạo ra trên điện thoại của bạn hoặc tin nhắn văn bản được gửi qua công ty trực tuyến, ngân hàng hoặc dịch vụ khác). Khi đã nhập đúng, bạn có thể chắc chắn rằng bạn đang sử dụng một trang web đảm bảo.

Xác thực 2 yếu tố thường được cung cấp bởi các công ty trực tuyến có kiến thức về bảo mật. Tuy nhiên, lưu ý rằng hoạt động được thực hiện sau khi đăng nhập 2 yếu tố có thể dễ dàng quan sát được bởi chủ sở hữu của một bộ định tuyến hoặc mạng giả. Do đó, bạn vẫn không được bỏ qua những lưu ý quan trọng khác khi tiếp xúc với các mạng Wi-Fi mở.

6. Tắt kết nối wifi nếu chúng ta không vào mạng

Khi chúng ta không sử dụng wifi nữa thì hãy tắt kết nối trên điện thoại, đây là một việc làm rất đơn giản, nhưng nhiều người thường quên hoặc lười tắt. Khi tắt kết nối wifi chúng ta có thể tránh được những khả năng xâm phạm của những phần mềm độc hại không mong muốn vào trong thiết bị của mình một cách an toàn nhất.

7. Không bao giờ kết nối với Wi-Fi công cộng mà không dùng VPN



Phần lớn những nguy hiểm từ việc sử dụng wifi công cộng chúng ta có thể phòng tránh được nếu sử dụng mạng VPN. Những ứng dụng này có thể được sử dụng để kết nối với máy chủ VPN an toàn, do đó mã hóa lưu lượng truy cập của bạn khi nó rời khỏi thiết bị của bạn. VPN có nhiều mục đích từ tránh proxy để vượt qua khu vực bị chặn. Chúng cũng là công cụ bảo mật tốt nhất mà bạn có để duyệt Internet một cách yên tâm nhất.