Loại bỏ hoàn toàn Adware và Spyware trên hệ thống của bạn

Adware là một pop-up quảng cáo hiển thị trên máy tính hoặc trên quảng cáo. Spyware là một chương trình điều khiển các hoạt động và thông tin trên máy tính của bạn, sau đó gửi các thông tin này cho một máy tính từ xa khác.

Cả Adware và Spyware đều là những chương trình nguy hiểm. Một khi máy tính của bạn bị nhiễm Adware và Spyware, chúng sẽ bắt đầu tàn tấn công và phá hệ thống của bạn. Vậy làm sao để loại bỏ hoàn toàn Adware và Spyware trên hệ thống, mời bạn cùng tham khảo bài viết dưới đây của Quản trị mạng.

1. Ngắt toàn bộ kết nối Internet trên máy tính

Đóng tất cả cửa sổ trình duyệt và ứng dụng trên máy tính của bạn (bao gồm cả email), sau đó tiến hành ngắt toàn bộ kết nối Internet trên máy tính của bạn. Cách đơn giản nhất là rút dây mạng kết nối máy tính với modem hoặc router.

2. Sử dụng phương pháp gỡ bỏ cài đặt ứng dụng truyền thống

Một số chương trình, ứng dụng cài đặt trên máy tính của bạn có thể đính kèm theo cả adware và spyware mà bạn không hề hay biết. Do đó để "dọn sạch" adware và spyware, cách đơn giản nhất là gỡ bỏ cài đặt các chương trình này. Trước khi tiến hành gỡ bỏ cài đặt, mở **Control Panel** => **Program**, sau đó truy cập tùy

chọn **Uninstall or change a program** và kiểm tra các chương trình được cài đặt trên máy tính của bạn.

Nếu phát hiện các chương trình không mong muốn cài đặt trên máy tính, rất đơn giản bạn cần kích chuột phải vào tên chương trình đó rồi chọn **Uninstall** là xong.

Trên Windows Vista, truy cập tùy chọn **Programs and Features** để gỡ bỏ các ứng dụng, chương trình cài đặt không mong muốn.

Sau khi đã loại bỏ Adware và Malware, tiến hành khởi động lại máy tính của bạn lại là xong.

3. Sử dụng chương trình diệt virus để quét máy tính của bạn

Sau khi ngắt toàn bộ kết nối Internet, gỡ bỏ adware và spyware và khởi động lại máy tính của bạn, bước tiếp theo là sử dụng các chương trình diệt virus để quét toàn bộ hệ thống của bạn. Nếu chương trình diệt virus bạn đang sử dụng cho phép, bạn có thể quét toàn bộ hệ thống ở chế độ Safe Mode. Nếu chưa cài đặt chương trình diệt virus nào, bạn có thể lựa chọn tải và cài đặt các chương trình diệt virus trả phí hoặc các chương trình diệt virus miễn phí tốt nhất để sử dụng.

4. Sử dụng SmitFraudFix, MalwareBytes, và các công cụ khác

Phần lớn các phần mềm gián điệp (spyware) được phân phối thông qua Zlob family của Troijan downloader. SmitFraudFix là một trong những công cụ miễn phí loại bỏ các phiên bản Zlob có liên quan đến adware và spyware tốt nhất.

MalwareBytes hỗ trợ việc loại bỏ scareware, các phần mềm lừa đảo mà hijacks (không tặc) tấn công máy tính của bạn.

5. Giành quyền truy cập ổ đĩa

Mặc dù việc quét toàn bộ hệ thống của bạn ở chế độ Safe Mode là một giải pháp tốt, tuy nhiên vẫn chưa đủ để ngăn chặn một số phần mềm độc hại. Nếu adware (phần mềm quảng cáo) và spyware (phần mềm gián điệp) vẫn tồn tại trên hệ thống của bạn mặc sức bạn đã áp dụng đủ mọi cách mà vẫn không thể loại bỏ được chúng, giải pháp tiếp theo mà bạn có thể nghĩ đến là truy cập ổ đĩa mà không cần sự cho phép của adware và spyware.

Cách tốt nhất để giành quyền truy cập ổ đĩa là sử dụng BartPE Bootable CD. Sau khi khởi động vào BartPE CD, bạn có thể truy cập File manager (quản lý tập tin), tìm các chương trình diệt virus bạn cài đặt và quét hệ thống của bạn một lần nữa. Hoặc xác định vị trí các tập tin và thư mục là "thủ phạm" và tiến hành xóa các tập tin, thư mục đó đi.

6. Hoàn tác Residual Damage (thiệt hại gián tiếp)

Sau khi đã chắc chắn các phần mềm độc hại: adware và spyware đã được loại bỏ hoàn toàn khỏi hệ thống của bạn, khi đó bạn có thể kết nối lại Internet trên hệ thống.

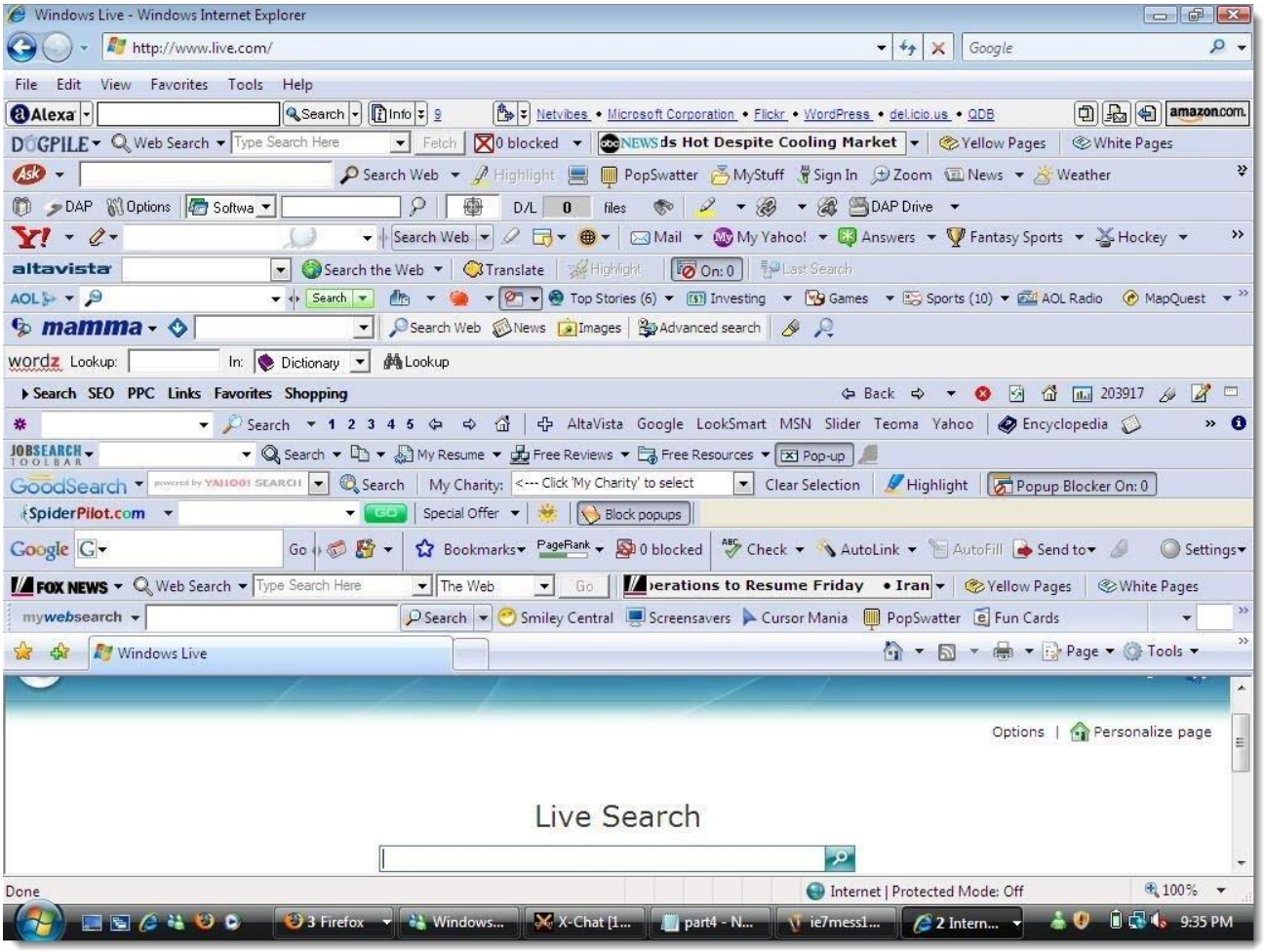
Trước khi tiến hành kết nối lại Internet, reset lại trình duyệt của bạn và trang chủ (homepage).

Đảm bảo rằng file HOSTS của bạn đã không bị tấn công.

7. Dọn dẹp trình duyệt

Ngay cả khi những cách trên hoạt động hiệu quả, tuy nhiên những phần mềm quảng cáo này có thể đã lây nhiễm vào trình duyệt của bạn và gỡ cài đặt chương trình cũng không thể loại bỏ được phần mềm quảng cáo. Để làm sạch trình duyệt,

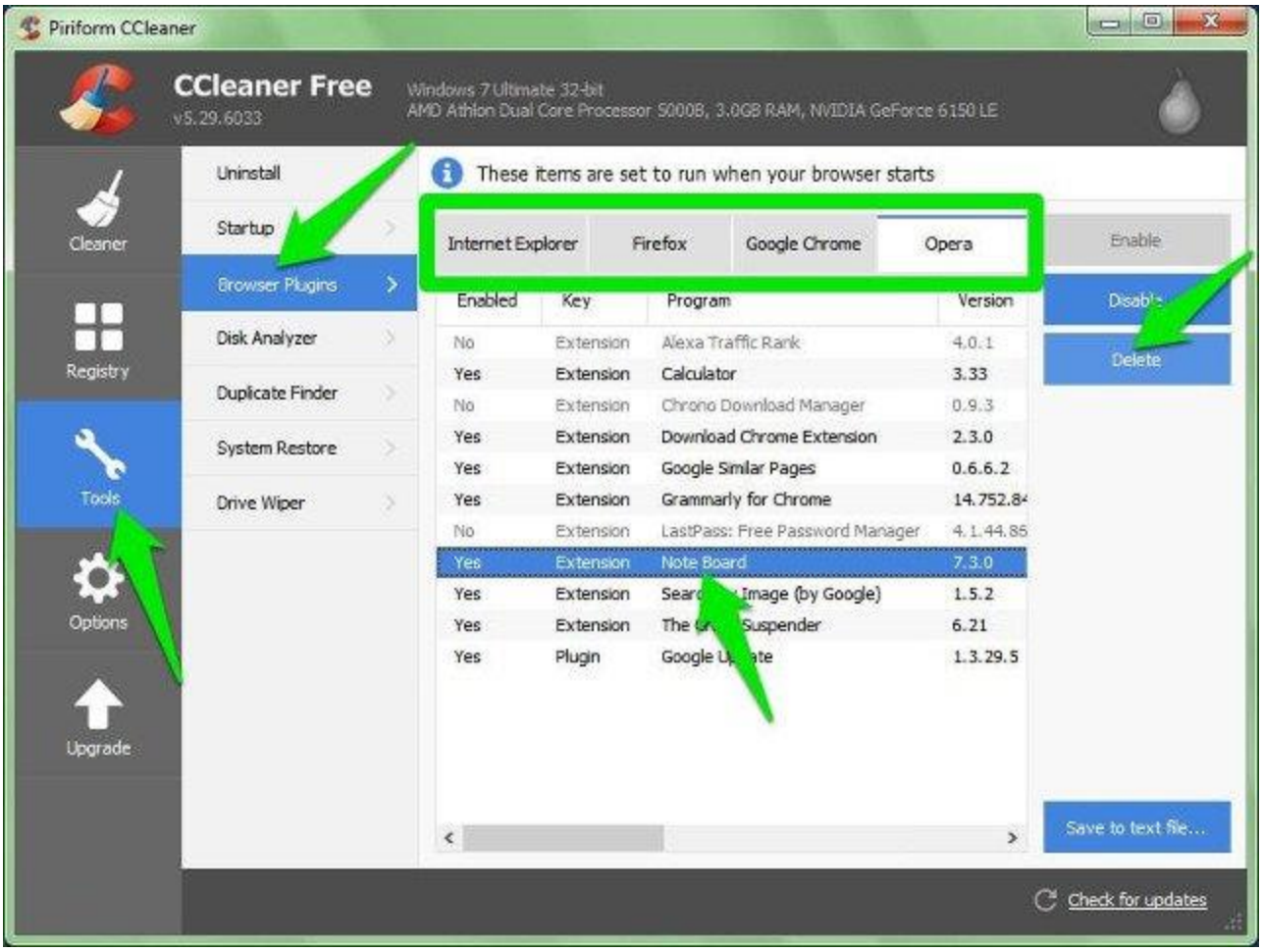
bạn chỉ cần reset công cụ tìm kiếm của nó (nếu nó đã thay đổi) và tìm kiếm các extension hoặc add on bạn không nhận ra.



Để reset công cụ tìm kiếm:

- Chuyển đến cài đặt của trình duyệt và tìm tiêu đề **Search** ở trong phần **General**.
- Chọn công cụ tìm kiếm muốn xóa (như Google) từ trình đơn thả xuống.

Để tìm extension hoặc add on phần mềm quảng cáo, bạn nên sử dụng công cụ của bên thứ ba để hiển thị tất cả các extension và plugin từ tất cả các trình duyệt trong một cửa sổ, bao gồm cả những extension ẩn. Có rất nhiều công cụ thứ ba giúp bạn thực hiện được điều này như trình quản lý plugin tích hợp của CCleaner.



- Mở CCleaner và chuyển đến phần **Tools** từ bảng điều khiển bên trái.
- Chọn Browser Plugins và bạn sẽ thấy tất cả các trình duyệt đã cài đặt ở thanh trên cùng và các plugin và extension ở bên dưới chúng.
- Xem từng trình duyệt và tìm kiếm những extension hoặc plugin bạn chưa từng cài đặt.
- Chọn những extension/plugin đó và nhấp vào nút **Delete** màu xanh ở bên phải để xóa.

Xem thêm:

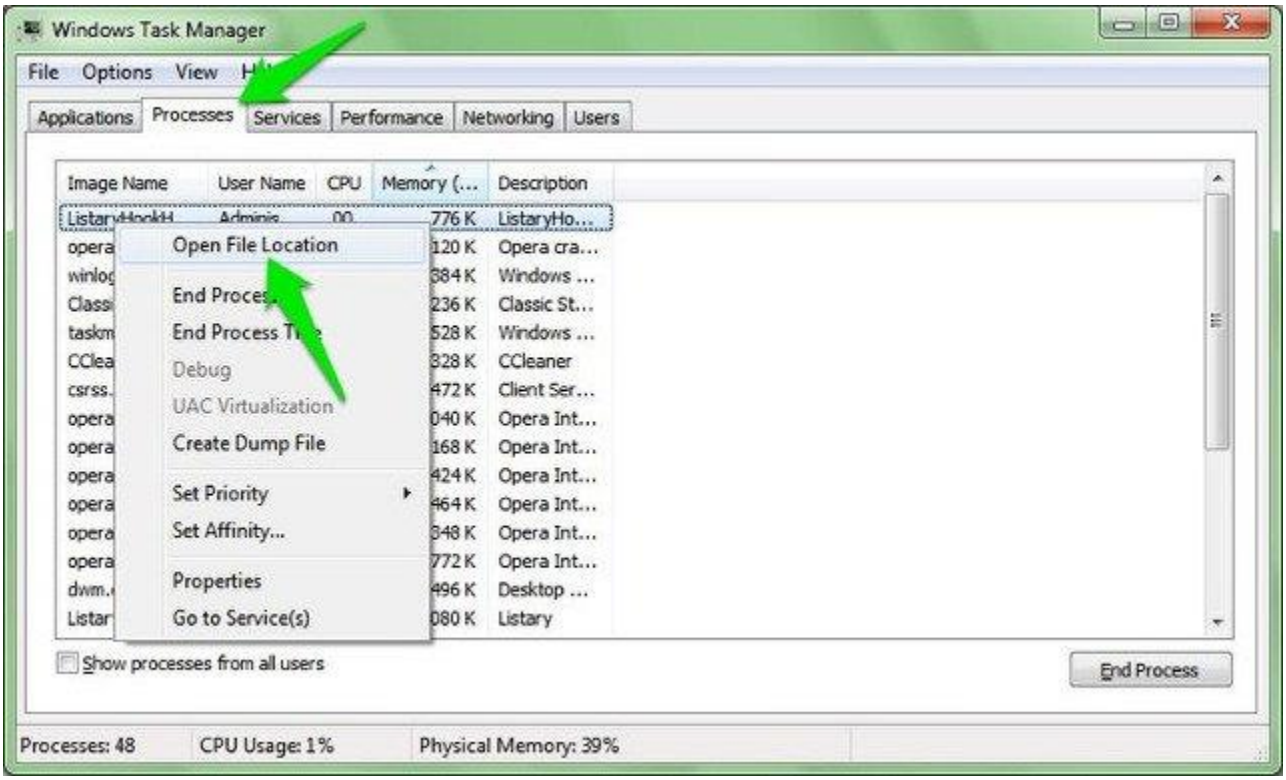
8. Kiểm tra Task Manager

Đối với những phần mềm quảng cáo thông thường thì những cách trên là đủ, nhưng nếu bạn vẫn thấy quảng cáo, thì có thể nó đang bị ẩn trong các dịch vụ hoặc

tiến trình nền. Bạn có thể kiểm tra các tiến trình nền trong Task Manager bằng cách nhấn tổ hợp phím **Ctrl + Shift + Esc** và chuyển đến tab **Processes**.

Tiếp theo, hãy tìm các tiến trình nền có vẻ bị ẩn, tuy nhiên rất khó để chỉ ra đúng tiến trình trình nền trừ khi bạn biết tên phần mềm quảng cáo vì Windows liệt kê tất cả các tiến trình của nó ở đây. Do vậy bạn nên tìm kiếm trên mạng các tên tiến trình bạn nghi ngờ và nếu nó không phải là tiến trình Windows, hãy thực hiện theo các bước dưới đây:

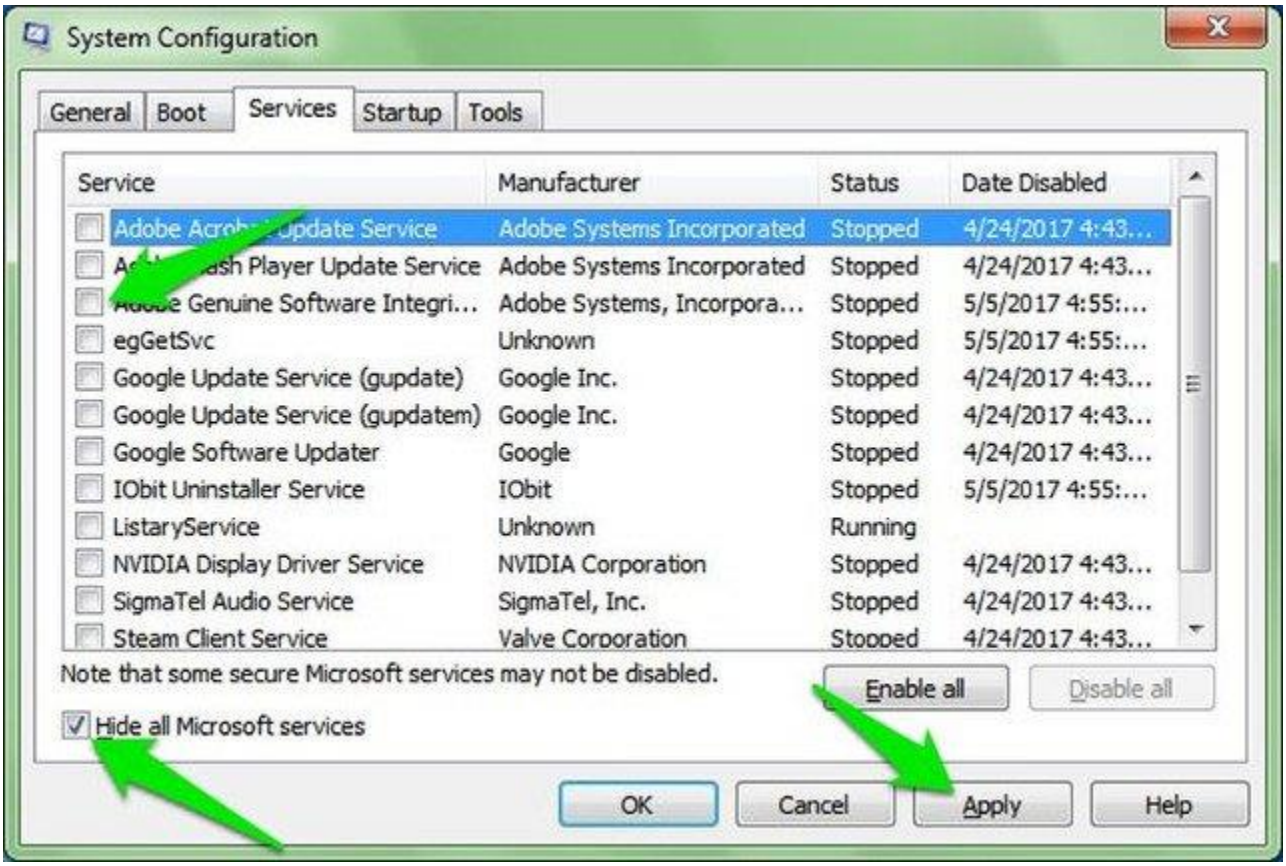
- Click chuột phải vào nó và chọn **Open File Location**.
- Xóa tất cả dữ liệu bạn thấy.
- Nếu không thể xóa nó, sau đó quay lại Task Manager để kết thúc tiến trình và sau đó thử xóa lại.



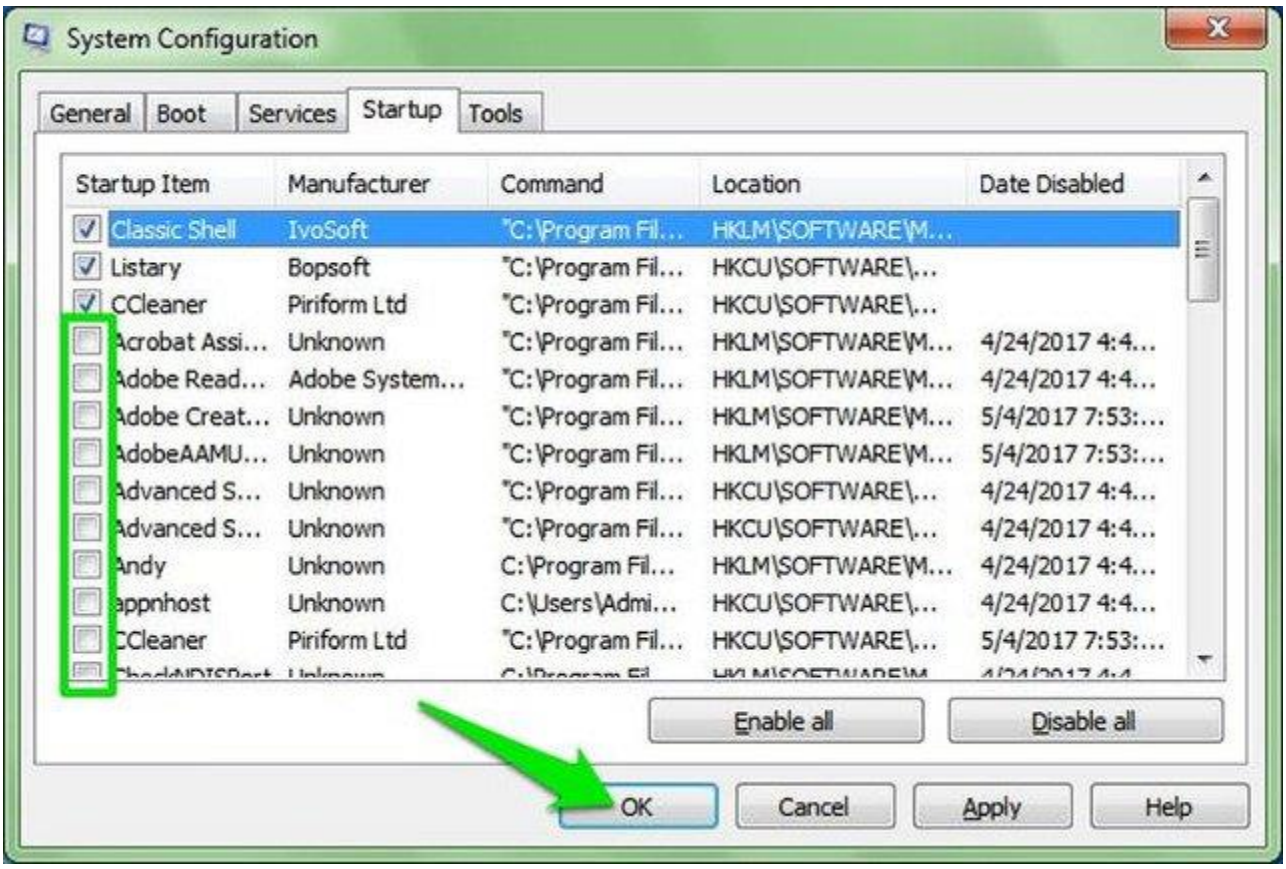
9. Tắt các chương trình và dịch vụ khởi động

Cách này đã được nhiều người sử dụng để vô hiệu hóa các chương trình quảng cáo và giả mạo và nó có thể khắc phục được vấn đề của bạn.

- Nhấn các phím **Windows + R** và nhập **msconfig** vào hộp thoại **Run** để mở cửa sổ cấu hình hệ thống.
- Chuyển đến tab **Services** tại đây và chọn hộp checkbox bên cạnh **Hide all Microsoft services**.
- Xem danh sách này và bỏ chọn tất cả các dịch vụ bạn không nhận ra hoặc không cần khởi động cùng hệ thống.
- Click vào nút **Apply** bên dưới để xác nhận thay đổi.



Chuyển sang tab **Startup** và bạn sẽ thấy tất cả các chương trình khởi động. Người dùng Windows 8 và 10 sẽ phải mở **Task Manager** và chuyển đến tab **Startup items** để xem các chương trình khởi động. Chỉ cần bỏ chọn hộp checkbox bên cạnh các chương trình khởi động không được công nhận và áp dụng các thay đổi.



Bạn sẽ phải khởi động lại máy tính để các thay đổi này có hiệu lực và xem các phần mềm quảng cáo có dừng hay không. Nếu thấy hiệu quả, bạn nên chạy AdwCleaner để tìm các phần mềm quảng cáo vì khi dừng dịch vụ, nó không bị ẩn khởi trình dọn dẹp nữa.

10. Khởi động ở chế độ Safe Mode

Nếu các cách trên không hiệu quả, bạn có thể thử khởi động máy tính ở chế độ Safe Mode. Khi ở trong chế độ Safe Mode, nó chỉ tải các file hệ thống và driver cần thiết, rất hiếm khi các chương trình giả mạo có thể "sống sót" trong chế độ Safe Mode. Sau đó chạy AdwCleaner từ Safe Mode để loại bỏ các phần mềm quảng cáo.

11. Ngăn chặn Adware và Spyware

Sau khi loại bỏ phần mềm quảng cáo, học cách tránh các phần mềm này trong tương lai cũng là một cách "phòng bệnh hơn chữa bệnh". Bạn có thể thực hiện theo cách cách dưới đây:

Nếu thấy nghi ngờ bất kỳ chương trình, phần mềm nào hãy tìm kiếm trên Google

Một quy tắc rất đơn giản nhưng hiệu quả để giữ an toàn trên Internet là khi nghi ngờ một ứng dụng hoặc file nào đó, cách tốt nhất là tìm kiếm trên Google hơn là tải và tự kiểm tra. Công thức tìm kiếm đơn giản là "chương trình x có phải là phần mềm độc hại hay quảng cáo?".

Tránh tải các phần mềm crack

Nếu bạn thích truy cập vào các trang web torrent để "ăn cắp" các bản sao các ứng dụng hợp pháp trả phí, thì có thể bạn sẽ bị lây nhiễm các phần mềm quảng cáo và độc hại.

Những phần mềm crack của các chương trình trả phí thường bị nhiễm phần mềm độc hại và quảng cáo, gây nguy hại nghiêm trọng cho máy tính. Do vậy, bạn chỉ nên tải các chương trình từ trang web chính và không tải các chương trình crack.

Không nên tải bất cứ thứ gì được đề xuất

Internet đầy rẫy những quảng cáo yêu cầu bạn tải một chương trình tuyệt vời để nhận được những lợi ích tốt nhất, chẳng hạn như "tải chương trình kiếm tiền này để trở thành triệu phú" hoặc "bot tự động x miễn phí này sẽ làm các công việc x tự động", v.v… Nếu bạn nghe theo những lời dụ dỗ này, thì có cơ hội bạn sẽ phải dọn dẹp hoặc reset lại máy tính.

Đọc các bước khi cài đặt chương trình

Có nhiều phần mềm quảng cáo lẻn vào cùng chương trình hợp pháp như là một phần mềm đính kèm. Trong khi cài đặt chương trình hợp pháp, nó sẽ lừa bạn để xác định cài đặt nó. Giải pháp đơn giản là trong khi cài đặt bất cứ chương trình nào, hãy kiểm tra các bước thật cẩn thận và tìm kiếm các checkbox yêu cầu bạn cài đặt các chương trình khác cùng với chương trình chính.

Trình cài đặt cũng có thể trực tiếp yêu cầu cài đặt một chương trình cụ thể và chỉ cung cấp cho bạn tùy chọn click vào **Next** hoặc **Decline**, bạn nên chọn **Decline.**

Ngoài ra, nếu trình cài đặt có tùy chọn **Custom Installer** hoặc tương tự, hãy chọn tùy chọn này. Chương trình có thể không đề xuất tùy chọn này, nhưng đây là mẹo để đảm bảo bạn chưa bỏ tích các chương trình ẩn.

Kiểm tra các bước cài đặt bằng cách thủ công là điều quan trọng, và bạn nên làm điều đó mỗi lần cài đặt chương trình. Tuy nhiên, có một cách nhanh hơn là cài đặt ứng dụng **Unchecky** để tự động từ chối hoặc bỏ chọn các chương trình đi kèm đề xuất.

Loại bỏ phần mềm quảng cáo, độc hại càng sớm càng tốt là rất quan trọng không chỉ bởi vì nó gây phiền nhiễu cho bạn mà còn khiến bạn tải nhiều phần mềm quảng cáo hơn và thậm chí là phần mềm độc hại có thể gây hại cho máy tính hoặc ăn cắp dữ liệu của bạn.

Mặc dù cách cách ở trên đủ để loại bỏ bất kỳ phần mềm quảng cáo nào, nhưng bạn cũng nên khôi phục máy tính về thời điểm trước hoặc reset để loại bỏ bất kỳ loại phần mềm quảng cáo hoặc độc hại nào.