KHÔI PHỤC MÁY TÍNH KHI BỊ NHIỄM TROJAN HOẶC VIRUS

Trojan

Trojan hoặc Virus có thể xảy ra đối với bất cứ ai. Việc xem xét một số lượng lớn các virus và Trojan có trên Internet tại một thời điểm nào đó nó là không tưởng đối với bất cứ ai. Sự nhận thức muộn cho thấy bạn đã có thể làm một công việc tốt hơn trong việc bảo vệ bản thân bạn, nhưng điều đó chỉ có thể giúp bạn chút ít trong tình trạng khó khăn của bạn hiện hành. Khi bạn biết rằng máy tính của bạn đã bị nhiễm Trojan hoặc virus thì bạn nên làm gì?

Nếu bạn biết rằng chương trình nguy hiểm cụ thể đã xâm hại máy tính của bạn, bạn có thể viếng thăm một vài trang web chống virus và tải một công cụ để xóa bỏ chúng. Mặc dù vậy nhưng ở đây bạn sẽ không thể nhận ra được phần mềm cụ thể nào. Không may mắn nữa là những chọn lựa của bạn còn bị giới hạn, tuy nhiên nếu bạn tuân theo các bước hướng dẫn của QuanTriMang.com dưới đây thì bạn có thể bảo vệ được máy tính và các file của bạn.

1. Gọi hỗ trợ CNTT

Nếu bạn có một đơn vị hỗ trợ CNTT thì bạn hãy báo cho họ ngay lập tức và làm theo các chỉ dẫn của họ.

2. Hủy kết nối máy tính của bạn với Internet

Phụ thuộc vào loại Trojan horse hay virus nào tấn công vào máy tính của bạn mà kẻ xâm nhập có thể truy cập vào thông tin cá nhân của bạn và có thể sử dụng máy tính của bạn để tấn công các máy tính khác. Bạn có thể dừng hoạt động này bằng việc tắt kết nối truy cập Internet. Cách tốt nhất để thực hiện vấn đề này là hủy bỏ kết nối vật lý bằng cáp hoặc đường điện thoại, nhưng bạn cũng có thể đơn giản vô hiệu hóa kết nối mạng của bạn bằng nhiều cách khác.

3. Sao chép các file quan trọng

Ở thời điểm này, bạn cần phải mất một ít thời gian để sao chép các file của bạn, đây là một ý tưởng tốt vào lúc này. Nếu có thể, bạn nên copy toàn bộ ảnh, các tài liệu, Internet favorites… và tạo chúng trong một đĩa CD hoặc lưu chúng trong các thiết bị lưu trữ mở rộng khác như USB. Cần phải nhớ rằng các file này sẽ không thể được tin tưởng khi chúng đã bị nhiễm.

4. Cài đặt một chương trình chống virus và quét máy tính của bạn

Từ khi máy tính của bạn bị nhiễm một chương trình nguy hiểm mà bạn không rõ. Biện pháp an toàn nhất là cài đặt một chương trình chống virus từ một nguồn an toàn như là CD-ROM. Bạn sẽ phải viếng thăm cửa hàng máy tính hoặc thiết bị lưu trữ gần đó để mua phần mềm. Có nhiều sự lựa chọn nhưng tất cả chúng nên cần cung cấp cho bạn những công cụ cần thiết.

Sau khi bạn cài đặt phần mềm, quét toàn bộ máy tính của bạn. Lúc đầu quét bạn sẽ phấn khởi tìm ra các chương trình nguy hiểm. Lý tưởng, chương trình chống virus sẽ tháo bỏ các file nguy hiểm này ra khỏi máy tính của bạn.

Nếu chương trình này thành công trong việc gỡ bỏ các file nguy hiểm hay định vị được chúng thì bạn có thể làm theo các bước phòng ngừa trong Bước 7 (được nêu ở dưới) để ngăn chặn các mối hiểm họa khác. Trong trường hợp xấu nếu các chương trình chống virus không định vị và gỡ bỏ được các file nguy hiểm thì bạn nên làm theo các chỉ dẫn trong các bước tiếp theo.

5. Cài đặt lại hệ điều hành

Nếu các bước trước không có kết quả gì với máy tính của bạn thì chỉ còn cách là bạn cài đặt lại hệ điều hành. Mặc dù hành động này sẽ làm mất tất cả các chương trình và các file nhưng nó là cách tốt để bảo đảm máy tính của bạn thoát khỏi những mối nguy hiểm từ phía sau và những thay đổi của kẻ xâm nhập vào máy tính của bạn. Trước khi thực hiện việc cài đặt lại, bạn phải chú ý rằng tất cả các chương trình và các thiết lập để bạn có thể quay trở lại máy tính như ban đầu.

Nó cũng cần thiết phải cài lại phần mềm chống virus và áp dụng bất kỳ các bản vá nào mà có sẵn. Hãy tìm các bài viết trước đây của QuanTriMang hướng dẫn bạn "10 bước bảo vệ PC trước khi kết nối Internet" để có thêm sự hỗ trợ.

6. Hoàn trả lại các file

Phần mềm ZoneAlarm

Nếu bạn làm một đĩa CD trong bước 3 thì bây giờ bạn có thể hoàn trả lại các file của bạn. Trước khi đặt các file này trên máy tính của bạn bạn nên quét chúng với phần mềm chống virus an toàn để bảo đảm chúng không bị nhiễm khi hoàn trả lại vào máy tính.

7. Bảo vệ máy tính

Để ngăn chặn các mối nguy hiểm trong tương lai, bạn nên tuân theo các phòng ngừa sau:

Không mở các file đính kèm không rõ nguồn gốc trong emai.

Không truy cập vào các liên kết không rõ nguồn gốc

Hãy thường xuyên cập nhật phần mềm chống virus

Sử dụng tường lửa (Có thể bật tường lửa sẵn có trong Windows hoặc dùng các phần mềm miễn phí như ZoneAlarm).

Cập nhật liên tục các bản vá lỗi của Windows bằng cách truy cập http://windowsupdate.microsoft.com