

LÀM GÌ KHI MÁY TÍNH BỊ NHIỄM ĐỘC

Quản Trị Mạng - Đôi khi người dùng có kinh nghiệm thực sự cũng không thể nhận ra một máy tính bị nhiễm virus thực sự hay không vì chúng có thể ẩn náu trong các file thông thường hoặc như các file chuẩn. Vậy triệu chứng của các máy tính bị nhiễm virus như thế nào, chúng tôi sẽ giới thiệu cho các bạn những vấn đề này trong bài, cùng với đó là cách khôi phục dữ liệu sau khi virus xâm nhập vào máy bạn và cách phòng chống dữ liệu để tránh bị các phần mềm độc hại xâm nhập.

Quản Trị Mạng - Đôi khi người dùng có kinh nghiệm thực sự cũng không thể nhận ra một máy tính bị nhiễm virus thực sự hay không vì chúng có thể ẩn náu trong các file thông thường hoặc như các file chuẩn. Vậy triệu chứng của các máy tính khi bị nhiễm virus như thế nào, chúng tôi sẽ giới thiệu cho các bạn những vấn đề này trong bài, cùng với đó là cách khôi phục dữ liệu sau khi virus xâm nhập vào máy bạn và cách phòng chống dữ liệu để tránh bị các phần mềm độc hại xâm nhập.

Các triệu chứng bị nhiễm

Có một số triệu chứng cho thấy rằng máy tính của bạn đã bị nhiễm. Nếu bạn phát hiện ra các hiện tượng lạ như chúng tôi liệt kê ra dưới đây thì đó chính là triệu chứng:

Các thông báo hoặc các ảnh không mong muốn được hiển thị một cách bất ngờ

Những âm thanh hoặc đoạn nhạc không bình thường được bật một cách ngẫu nhiên

Ổ CD-ROM của bạn đóng mở bất thường

Các chương trình chạy bất thành lình

Bạn nhận thông báo từ tường lửa cho biết rằng, một số ứng dụng nào đó đã cố gắng thực hiện kết nối Internet mặc dù bạn không khởi chạy nó.

Thêm vào đó, có một số triệu chứng chỉ thị rằng máy tính của bạn đã bị nhiễm thông qua email:

Các bạn thân của bạn cho biết rằng họ đã nhận được các thông báo từ địa chỉ của bạn mà bạn không hề gửi các thư đó.

Mailbox của bạn chứa rất nhiều các thông báo không có địa chỉ hoặc header của người gửi.

(Tuy vậy có thể các vấn đề này lại không bị gây ra bởi virus. Cho ví dụ, các thông báo bị tiêm nhiễm giả sử đến từ địa chỉ của bạn có thể lại được gửi từ một máy tính khác).

Có một số các triệu chứng khác chỉ thị rằng máy tính của bạn có thể bị tiêm nhiễm:

Máy tính thường xuyên bị đóng băng hoặc bất thành linh xuất hiện các lỗi

Máy tính chạy chậm khi các chương trình bắt đầu được bật

Không thể nạp hệ điều hành

Các file và thư mục bị xóa hoặc bị thay đổi nội dung

Không thể truy cập ổ đĩa cứng như thường lệ

Internet Explorer bị đóng băng hoặc các chức năng chạy một cách thất thường, nghĩa là bạn không thể đóng cửa sổ ứng dụng.

90% trong số các triệu chứng được liệt kê trên chỉ thị vấn đề phần cứng hoặc phần mềm. Mặc dù

các triệu chứng như vậy không chắc bị gây ra bởi virus nhưng bạn cần sử dụng một phần mềm chống virus để quét toàn bộ máy tính của mình.

Cần làm gì nếu bạn mắc các triệu chứng nhiễm trên

Nếu bạn thấy máy tính của mình chạy thất thường

Không nên sợ hãi! Nguyên tắc vàng này có thể tránh được vấn đề mất các dữ liệu quan trọng đã được lưu trong máy tính và giúp bạn tránh khỏi tình trạng stress không đáng có.

Hủy kết nối máy tính với Internet

Nếu máy tính được kết nối với mạng LAN, hãy hủy kết nối với mạng này.

Nếu máy tính không thể khởi động từ ổ đĩa cứng (lỗi khởi động), bạn hãy khởi động hệ thống trong chế độ Safe Mode hoặc từ đĩa khởi động của Windows.

Trước khi thực hiện bất cứ hành động nào, hãy backup toàn bộ dữ liệu quan trọng của bạn vào một ổ cứng ngoài (đĩa CD hoặc ổ USB,...).

Cài đặt phần mềm diệt virus trong trường hợp không cài đặt trước đó.

Download các nâng cấp mới nhất đối với phần cơ sở dữ liệu về virus. Nếu có thể, không sử dụng máy tính bị nhiễm để download mà bạn hãy sử dụng một máy tính khác để thực hiện công việc này. Điều này rất quan trọng vì bạn lại phải kết nối với Internet, virus có thể gửi các thông tin quan trọng đến các thành phần thứ ba hoặc có thể thực hiện gửi thư đến các địa chỉ trong danh sách các địa chỉ của bạn. Bạn cũng có thể lấy các nâng cấp về phần mềm chống virus từ các đĩa

CD-ROM của các hãng phần mềm hoặc những người chính đáng.

Thực hiện quét toàn bộ hệ thống.

Nếu không xuất hiện virus trong quá trình quét

Nếu không xuất hiện virus trong quá trình quét và các triệu chứng đã cảnh báo thì bạn có thể không có lý do gì phải phiền muộn về vấn đề virus. Hãy kiểm tra tất cả phần cứng và phần mềm đã được cài đặt trong máy tính. Download các bản vá của Windows bằng cách sử dụng Windows Update. Hủy bỏ cài đặt tất cả các phần mềm không có đăng ký khỏi máy tính và xóa các ổ đĩa chứa các file tạp nham.

Nếu phát hiện virus trong quá trình quét

Một giải pháp chống virus tốt nhất sẽ được gửi đến bạn nếu trong quá trình quét thấy xuất hiện virus, bên cạnh đó là một vài tùy chọn để giải quyết với các đối tượng bị nhiễm.

Trong đại đa số các trường hợp, các máy tính cá nhân thường bị nhiễm bởi worm, các chương trình Trojan hoặc virus. Trong hầu hết các trường hợp như vậy, dữ liệu bị mất có thể đều được khôi phục thành công.

Một giải pháp chống virus hữu ích sẽ cung cấp tùy chọn giúp tẩy uế các đối tượng bị nhiễm, cách ly các đối tượng bị nhiễm, xóa worms và Trojans. Một báo cáo sẽ xuất hiện cung cấp tên của các phần mềm mã độc đã bị phát hiện trong máy tính của bạn.

Trong một số trường hợp, bạn có thể cần đến một tiện ích đặc biệt để khôi phục dữ liệu đã bị lỗi. Hãy ghé thăm các website của các hãng phần mềm chống virus, tìm kiếm thêm các thông tin về virus, Trojan hoặc worm đã nhiễm vào máy tính của bạn. download bất cứ tiện ích đặc biệt nào nếu có thể.

Nếu máy tính bị nhiễm bởi virus khai thác lỗ hổng của Microsoft Outlook Express, khi đó bạn có thể làm sạch toàn bộ máy tính bằng cách tẩy uế tất cả các đối tượng bị nhiễm, sau đó quét và tẩy uế các cơ sở dữ liệu mail máy khách. Cách làm này có thể bảo đảm rằng các chương trình mã độc không thể được kích hoạt trở lại khi các thông báo bị nhiễm trước khi quét được mở lại. Bạn cũng cần download và cài đặt các bản vá bảo mật cho Microsoft Outlook Express.

Tuy nhiên một số virus không thể remove khỏi các đối tượng bị nhiễm. Số virus này có thể làm hư hại đến các thông tin trên máy tính và không thể khôi phục các thông tin này. Nếu một virus không thể remove khỏi một file nào đó, cách tốt nhất lúc này là bạn hãy xóa file đó.

Nếu máy tính bị tấn công virus ở mức độ nguy hiểm

Một số virus và Trojan có thể gây ra một số hỏng hóc đối với máy tính:

Nếu bạn không thể khởi động máy tính từ ổ đĩa cứng của mình (lỗi khởi động), khi đó hãy thử khởi động từ đĩa khôi phục của Windows. Nếu hệ thống không thể nhận ra đĩa cứng của bạn thì virus có thể đã làm hư hại đến bảng partition của đĩa. Trong trường hợp này, hãy khôi phục lại bảng partition bằng tiện ích scandisk, đây là một chương trình Windows chuẩn. Nếu thao tác này vẫn không giúp ích gì bạn, khi đó hãy liên hệ với một dịch vụ khôi phục dữ liệu máy tính nào đó. Hãng máy tính của bạn thường cung cấp các thông tin liên hệ về các vấn đề như vậy.

Nếu bạn đã cài đặt một tiện ích quản lý đĩa, một số ổ đĩa logic của bạn có thể không hiện hữu khi bạn khởi động từ đĩa khôi phục. Trong trường hợp này, bạn cần phải tẩy uế tất cả các ổ đĩa có khả năng truy cập, sau đó khởi động lại từ ổ cứng của hệ thống và tẩy uế tiếp các ổ đĩa logic còn lại.

Khôi phục các file và các ứng dụng bị lỗi bằng cách backup các copy sau khi bạn đã quét ổ đĩa có chứa dữ liệu.

Khắc phục vấn đề bằng các công cụ Windows chuẩn

Kiểm tra tính toàn vẹn của hệ thống file trên ổ đĩa cứng (sử dụng chương trình CHKDSK) và sửa các lỗi hệ thống file. Nếu có rất nhiều lỗi thì bạn phải backup các file quan trọng nhất vào một ổ lưu động nào đó trước khi sửa lỗi.

Quét máy tính sau khi khởi động từ đĩa khôi phục Windows.

Sử dụng các công cụ Windows chuẩn, ví dụ như tiện ích scandisk.

Nếu không gì có thể trợ giúp

Nếu các triệu chứng được miêu tả ở trên vẫn xuất hiện sau khi bạn đã quét toàn bộ máy tính, đã kiểm tra tất cả các phần cứng cũng như phần mềm đã cài đặt và các ổ đĩa bằng các tiện ích của

Windows thì bạn cần phải gửi thông báo với những mô tả đầy đủ về vấn đề của mình tới trung tâm hỗ trợ kỹ thuật của hãng phần mềm chống virus của bạn.

Các chuyên gia phát triển phần mềm ở đây sẽ phân tích các file bị lây nhiễm được đề trình từ phía người nhận.

Sau khi trừ khử sự nhiễm

Khi đã trừ khử được vấn đề nhiễm của mình, hãy quét toàn bộ đĩa và thiết bị lưu trữ ngoài có thể bị nhiễm virus.

Hãy cấu hình thích hợp phần mềm chống virus đã được cài đặt trên máy tính.

Thao tác an toàn trong khi sử dụng máy tính.

Tất cả các cách xử trí này sẽ giúp bạn ngăn chặn được máy tính của mình bị nhiễm trong tương lai.