Kết hợp 7 "phòng tuyến" để bảo vệ máy tính

Nhiều người sử dụng máy tính thường nghĩ rằng sau khi cài đặt phần mềm diệt virus lên máy tính là có thể hoàn toàn yên tâm về vấn đề bảo mật tổng thể, bởi vì chúng đã giúp bảo vệ máy tính theo thời gian thực. Điều này không đúng, vì theo các chuyên gia trong lĩnh vực an toàn thông tin, các mã độc gián điệp luôn dễ dàng qua mặt các phần mềm diệt virus, và ý kiến của họ là bạn nên sử dụng kết hợp nhiều phương pháp bảo vệ máy tính. Sau đây là 7 phương pháp quan trọng nhất mà bạn nên quan tâm và áp dụng cho chiếc máy tính của mình.

1. Sử dụng phần mềm diệt virus

Đây là phương pháp bảo vệ cơ bản nhất, giúp ngăn chặn virus tấn công và được sự hỗ trợ trực tiếp từ bộ phận kỹ thuật của dịch vụ chăm sóc khách hàng. Các trình duyệt Internet luôn tồn tại những lỗ hổng, nhất là những tiện ích được cài đặt trên trình duyệt, virus và phần mềm độc hại có thể lợi dụng những lỗ hổng này để xâm nhập vào máy tính. Phần mềm diệt virus với dữ liệu được cập nhật thường xuyên sẽ giúp ngăn chặn có hiệu quả những trường hợp virus lợi dụng lỗ hổng trình duyệt này.

2. Luôn bật tính năng UAC

User Account Control (UAC) là một tính năng quản lý máy tính có mục đích ngăn chặn những thay đổi trái phép vào máy tính, được Microsoft giới thiệu đầu tiên trên hệ điều hành Windows Vista. Đối với một số người dùng, nhất là người dùng Windows XP, bảng thông báo UAC khi kích hoạt một ứng dụng nào đó có vẻ khá phiền toái, tuy nhiên, chính tính năng UAC này lại có khả năng ngăn chặn phần mềm độc hại và những thay đổi hệ thống khi không được phép rất hiệu quả. Và lời khuyên là bạn không nên vô hiệu hóa tính năng này trên các hệ điều hành Windows Vista/7/8. Cùng với phần mềm diệt virus, tính năng UAC là một lớp bảo mật rất quan trọng.

3. Luôn bật tính năng tường lửa

Hệ điều hành Windows đã cung cấp sẵn cho người dùng một tường lửa khá hiệu quả nên bạn không cần phải cài đặt thêm tường lửa của bên thứ ba. Trong quá trình sử dụng Windows, bạn nên bật tính năng Windows Firewall, giúp ngăn chặn những kết nối không mong muốn, bảo vệ Windows và các phần mềm khác trên máy tính khỏi sự tấn công, khai thác lỗ hổng của phần mềm độc hại và hệ thống dịch vụ mạng. Bên cạnh việc bật tính năng tường lửa, bạn cần phải thiết lập chính xác các tính năng liên quan đến mạng Home, Work hoặc Public network. Nếu chọn tùy chọn Home khi kết nối mạng wifi ở một quán cà phê, máy tính của bạn sẽ chia sẻ tập tin với người khác trong mạng wifi của quán cà phê. Tùy chọn Public giúp ngăn chặn người khác truy cập vào những tài nguyên chia sẻ trong máy tính của bạn.

4. Gỡ cài đặt ứng dụng Java

Java là một ứng dụng rất phổ biến và đang được rất nhiều người trên thế giới sử dụng. Tuy nhiên, trong quá khứ ứng dụng Java luôn có nhiều lỗ hổng bảo mật nghiêm trọng, luôn bị các nhóm tội phạm mạng lợi dụng triệt để để chèn mã độc và xâm nhập vào hệ thống máy tính. Hiện tại, Oracle đang phải thường xuyên

vá những lỗ hổng nghiêm trọng cho Java 7. Nếu có cài đặt Java, bạn có thể vào Control Panel để gỡ ứng dụng này hoặc vô hiệu hóa tiện ích Java trên trình duyệt. Tuy nhiên, có thể bạn cần Java để làm môi trường hỗ trợ cho một phần mềm nào đó, trường hợp này bạn không thể gỡ bỏ nó và phải tăng cường các biện pháp bảo vệ khác.

5. Thiết lập chế độ cập nhật tự động cho các phần mềm

Các phần mềm sử dụng hàng ngày như Internet Explorer, Mozilla Firefox, Google Chrome, Adobe Flash, Adobe PDF Reader, Microsoft Office... có thể gặp những rủi ro về vấn đề bảo mật, nên việc thiết lập chế độ tự động cập nhật là rất quan trọng. Đối với trình duyệt web, bạn cũng nên thường xuyên kiểm tra các tiện ích (plug-in, addon) rồi cập nhật chúng ngay lập tức khi phát hiện phiên bản mới. Để việc cập nhật diễn ra tự động, bạn sử dụng tính năng Windows Updates trong nhóm System and Security trong Control Panel.

6. Luôn cẩn thận với các chương trình muốn tải về và cài đặt

Bạn chỉ nên tải về và cài đặt những phần mềm, chương trình của các hãng phần mềm danh tiếng, và phải tải trực tiếp từ trang web chính thức cung cấp phần mềm đó. Nếu tải phần mềm từ một trang web khác hoặc do người khác cung cấp đường dẫn, bạn rất dễ vướng phải những phần mềm độc hại, phần mềm đã bị chèn mã độc hại hay mã quảng cáo. Bên cạnh đó, bạn cũng cần nên cẩn thận đối với việc tải những tập tin đính kèm qua e-mail và không nên mở những tập tin thực thi đính kèm.

7. Không sử dụng những phần mềm "lậu"

Khi sử dụng những phần mềm "lậu" được chia sẻ trên các dịch vụ lưu trữ hoặc qua mạng ngang hàng peer-to-peer, nguy cơ tiềm ẩn là rất cao. Chúng có thể chứa mã độc của các nhóm cracker, hacker nhằm ăn cắp thông tin trên máy tính của nạn nhân.

BÙI THANH LIÊM