10 BƯỚC BẢO VỆ PC TRƯỚC KHI KẾT NỐI INTERNET

Internet cung cấp rất nhiều kiến thức bổ ích cho người sử dụng, nhưng đồng thời cũng là nguồn phát tán những sâu, virus, trojan, spyware.... Bởi rất nguyên nhân, hệ thống máy tính của bạn sẽ là miếng mồi ngon cho chúng. Do đó, hãy thực hiện những bước sau trước

Bước 1. Hãy tạo đĩa khởi động CD-ROM

Trước khi truy cập Internet, hãy nán lại vài phút để tạo một đĩa khởi động bằng ổ CD-ROM có chứa phiên bản mới nhất của chương trình diệt virus mà bạn yêu thích. Nếu vẫn muốn giữ tính đơn giản và miễn phí thì hãy sử dụng AVG và Avast hoặc các chương trình diệt virus trong nước cũng đem lại hiệu quả cao là D32 và BKAV, những phần mềm diệt virus hàng đầu như Norton hay MacAfee thì quá tuyệt vời nhưng chúng hơi "nặng" cả về giá cả cũng như dung lượng lưu trữ.

Để tiết kiệm thời gian, bạn cũng nên đưa thêm các công cụ diệt phần mềm gián điệp (spyware) như Spybot, và Adware. Một ý tưởng hay là bạn cũng nên đưa những bản cập nhật các trình điều khiển (driver) mới nhất cho card đồ hoạ, âm thanh,... Có tất cả những trình điều khiển phần cứng ở trong ổ đĩa CD-ROM. Bởi vì bạn không cần phải kết nối Internet để cài đặt các trình điều khiển cho PC.

Bước 2. Loại bỏ phần mềm không sử dụng

Điều đầu tiên cần làm là hãy dọn sạch sẽ PC của bạn. Nên gỡ bỏ toàn bộ các phần mềm dùng thử hay những phần mềm kèm thêm mà không có ý định sử dụng. Bởi những phần mềm dùng thử này đều đòi hỏi bạn phải kích hoạt hoặc đăng kí qua kết nối Internet. Trong một số trường hợp thì chúng tự động truy cập Internet mà không hỏi người sử dụng. Do đó, máy tính cũng rất dễ bị lây nhiễm virus. Để loại bỏ những chương trình không mong muốn ra khỏi hệ thống. Bạn chỉ cần vào Control Panel->Add/Remove Programs. Tiếp đó, hãy loại bỏ những phần mềm dùng thử hoặc các phần mềm không sử dụng và khởi động lại máy tính.

Bước 3. Cài đặt phần mềm diệt virus

Tiếp theo hãy cài đặt phần mềm diệt virus, diệt spyware mà bạn đã "burn" sang CD-ROM trong bước1. Sau đó tiến hành quét lại toàn bộ hệ thống để đảm bảo rằng hệ thống đều sạch sẽ và có khả năng miễn nhiễm với virus và spyware. Hầu hết các phần mềm chống virus, spyware đều có khả năng tự động phòng chống những hiểm hoạ và nguy cơ lây nhiễm. Bạn hãy bật chức năng tự động ngăn chặn spyware, virus của những phần mềm này.

Bước 4. Cài đặt phần mềm tường lửa

Trong Windows XP SP2 đều đã tích hợp sẵn một phần mềm tưởng lửa miễn phí khá tốt là Windows Firewall. Nếu muốn có thêm nhiều tình năng hơn chỉ cần chạy các phần mềm của hãng thứ 3 như ZoneAlarm hoặc SyGate. Phần mềm tường lửa cũng nên được để sẵn vào bộ đĩa CD-ROM được tạo ra trong bước 1. Hãy tiến hành cài đặt phần mềm tường lửa để bảo vệ hệ thống của bạn.

Bước 5. Cài đặt máy in và các thiết bị ngoại vi khác

Trước khi bạn kết nối vào Internet hãy cài đặt các thiết bị ngoại vi vào trong PC mới. Bởi sau kết nối Internet bạn mới tiến hành cài đặt các thiết bị ngoại vi thì chúng sẽ tự động kết nối vào trang cập nhật Windows. Chúng sẽ tự động tìm kiếm các thiết bị và đưa ra những đề nghị về nâng cấp các trình điều khiển mới và thích hợp cho từng phần cứng. Điều này thực sự là tốt và hữu dụng của Windows, nhưng rất có thể đó sẽ là một điểm yếu mà hacker có thể lợi dụng để xâm nhập vào máy tính của bạn.

Bước 6. Tạo mật khẩu mạnh cho tài khoản quản trị (Administrator)

Đây là một trong những điểm yếu của bảo mật trên những hệ thống Windows, tài khoản quản trị cho phép quản lý truy cập vào toàn bộ hệ thống và rất nguy hiểm. Hacker có thể lấy cắp thông tin về hệ thống, các virus, sâu, trojan, spyware... có thể tự động cài đặt và lây nhiễm vào hệ thống khi sử dụng tài khoản quản trị. Bạn không muốn bất cứ ai có có thể truy cập vào thiết lập quyền quản trị cho PC của bạn. Và trong hầu hết các mật khẩu đều có thể dễ dàng bị "bẻ khoá" bởi các hacker có trình độ.

Bước 7.Tạo tài khoản người dùng bị giới hạn, và sử dụng mật khẩu an toàn

Điều này cũng quan trọng như bảo vệ mật khẩu của tài khoản quản trị. Để phục vụ cho hoạt động hằng ngày, bạn không muốn sử dụng tài khoản quản trị. Thay vào đó, bạn muốn sử dụng tài khoản bị giới hạn và có mật khẩu để bảo vệ (mật khẩu này phải khác với mật khẩu của quản trị viên và cũng phải mạnh, không dễ đoán). Chính nhờ tải khoản bị giới hạn này mà máy tính của bạn sẽ chống lại được sự lây nhiễm hoặc cài đặt từ các phần mềm hiểm độc do sự giới hạn về quyền truy cập.

Bước 8. Tắt những dịch vụ Windows không cần thiết

Microsoft đã cố gắng tắt một số dịch vụ không cần thiết trong bản SP2, nhưng vẫn còn một số những dịch vụ không cần thiết vẫn hoạt động mặc định trên các PC. Nếu bạn muốn xem có bao nhiêu dịch vụ đang sử dụng. Chỉ cần sử dụng Task Manager (CTRL+ALT+DEL) và nhấn vào thẻ Processes. Hầu hết các ứng dụng, dịch vụ và các tiến trình... hoạt động ở chế độ nền đều sẽ hiển thị. Vấn đề ở đây chính là hầu hết những cuộc tấn công từ bên ngoài đều sử dụng và khai thác lỗ hổng từ các dịch vụ này. Hãy tắt các dịch vụ không cần thiết này để tiết kiệm tài nguyên hệ thống và phòng chống các cuộc tấn công từ xa.

Bước 9. Thiết lập một điểm phục hồi

Nếu như bạn thực xong 8 bước trên thì hãy thực hiện một điểm phục hồi bằng tiện ích System Restore. Để tạo một điểm phục hồi (Restore Point), bạn cần chạy System Restore bằng cách nhấn vào Start | All Programs | Accessories | System Tools | System Restore và làm theo đồ thuật hướng dẫn. Bước này thực sự quan trọng bởi lúc này hệ thống của bạn còn rất "sạch sẽ", nên nếu sau này hệ thống bị nhiễm virus, sâu, trojan... hay bị hỏng hóc thì điểm phục hồi này đúng là phao cứu sinh cho PC của bạn.

Bước 10. Cài đặt và cấu hình Router

Đây là bước cuối cùng và dường như không cần thiết mà lại phải đầu tư thêm chi phí. Nhưng

trong thời kỳ mà virus, sâu, trojan... đang thả sức tung hoành trên Internet thì cài đặt router phân cách ranh giới giữa bạn và thế giới bên ngoài là thực sự cần thiết. Kết nối trực tiếp PC với Internet đồng nghĩa rằng PC sẽ có một địa chỉ IP riêng, và điều này có thể ảnh hưởng tới hệ thống máy tính. Nhưng cài đặt thêm router khi kết nối băng thông rộng, router sẽ lấy địa chỉ IP thật đó và đưa cho PC mới một địa chỉ IP trong mạng LAN. Hơn nữa, router có tường lửa phần cứng giúp chặn đứng sự xâm nhập. Chính vì vậy, sử dụng router hoặc modem ADSL tích hợp sẵn router là một giải pháp an toàn và không đắt.

Minh Phúc