1 GIỜ DÀNH CHO BẢO MẬT

Dành ra khoảng 1 tiếng đồng hồ, bạn có thể loại bỏ đa số những mối đe doạ trong quá trình sử dụng máy tính và duyệt web. Sau đây là 10 thủ thuật nhanh giúp bạn tạo lớp bảo vệ cho phần cứng, phần mềm và cả dữ liệu máy tính. 1. Cài đặt mảnh vá tự đ

Dành ra khoảng 1 tiếng đồng hồ, bạn có thể loại bỏ đa số những mối đe doạ trong quá trình sử dụng máy tính và duyệt web. Sau đây là 10 thủ thuật nhanh giúp bạn tạo lớp bảo vệ cho phần cứng, phần mềm và cả dữ liệu máy tính. 1. Cài đặt mảnh vá tự động. Hãy đảm bảo rằng Windows được lên cấu hình để tự động nâng cấp. Trong Win XP, nhấn Start/Control Panel/Security Settings và chọn Automatic Updates. Trong Win 2000, chọn Start/Settings/Control Panel/Automatic Updates. Bạn cũng có thể chọn để Windows chỉ nâng cấp sau khi đã cảnh báo bạn hoặc nâng cấp theo kiểu thủ công. 2. Đừng chờ đợi hệ điều hành. Nếu máy tính của bạn đã ở trong tình trạng "ngủ đông" trong vài ngày, đừng đợi Windows tự động nâng cấp mà phải chủ động tìm tới nó ngay sau khi khởi động. Microsoft giới thiệu các bản cập nhật vào ngày thứ Ba thứ hai trong mỗi tháng. 3. Sử dụng trình bảo mật của Win XP. Một trong những tính năng nổi bật nhất của Windows XP Service Pack 2 là WindowsSecurityCenter- ứng dụng cảnh báo khi bạn loại bỏ tường lửa hoặc các ứng dụng phòng chống virus đã cũ. Tuy nhiên, tường lửa của Windows XP chỉ có tác dụng đối với virus xâm nhập từ ngoài vào. Để có giải pháp bảo mật toàn diện, bạn nên loại bỏ tường lửa của Windows XP và sử dụng phần mềm tường lửa của hãng thứ ba (ví dụ ZoneAlarm của Zone Lab). 4. Đảm bảo hiển thị phần đuôi của tệp tin. Không ít loại virus giả dạng những tệp tin "hiền lành" thông qua việc chèn định dạng tệp tin khác vào cuối mỗi tệp tin (ví dụ funnycartoon.jpg.exe). Thông thường ở những máy mặc định ẩn phần đuôi tệp tin, bạn chỉ nhìn thấy '.jpg' chứ không nhìn thấy '.exe'. Để đối phó với những virus kiểu này, mở Windows Explorer, chọn Tools/Folder Options/View và nhấn bỏ chọn Hide file extensions for known file types. 5. An toàn với trình duyệt. Trình duyệt IE phiên bản mới nhất hỗ trợ khá tốt các ActiveX và các đoạn mã tạo "hiệu ứng" như JavaScript. Chính vì vậy, bạn nên sử dụng IE một cách an toàn hơn bằng cách lựa chọn tính năng bảo mật cao cho trình duyệt. Để thực hiện, chọn Tools/Internet Options/Security/Custom Level/High. Đối với người dùng Firefox, cách tốt nhất để loại bỏ các đoạn mã có hại là cài đặt tiện ích hỗ trợ (addin) NoScript của Giorgio Maone. Đây là phần mềm hoàn toàn miễn phí, bạn có thể tải về từ địa chỉ www.noscript.net. 6. Thận trọng khi sử dụng email. Nếu máy tính của bạn bị lây nhiễm hoặc trở thành nguồn phát tán virus thì con đường chính là thông qua email. Hãy tuân thủ những nguyên tắc bảo mật khi sử dụng email: không nhấn chuột vào những đường link nghi vấn, quét các tệp tin đính kèm trước khi tải về máy… Một lưu ý quan trọng là bạn nên tắt chế độ xem trước trong các trình duyệt email. Khá nhiều thông điệp phát tán virus ngay cả khi xuất hiện ở dạng xem trước (preview). Trong Microsoft Outlook 2003, chọn View/Reading pane Off. Trong Outlook Express 6, chọn View/Layout và loại bỏ tuỳ chọn Show Preview Pane. Tương tự, trong Mozilla Thunderbird, chọn View/Layout và bỏ chọn Message pane'(hoặc nhấn phím). Hãy đọc email ở dạng ký tự thuần tuý (plain text). Nguyên nhân là do các đoạn mã nguy hại thường được tin tặc chủ ý cài lẫn vào các đoạn mã HTML. Trong Outlook 2003, chọn Tools/Options/Preferences/E-mail Options và chọn Read all standard mail in plain text. Trong Outlook Express 6, chọn Tools/Options/Read và chọn Read all messages in plain text. Đối với Mozilla Thunderbird, chọn View/Message Body As/Plain Text.