SỬ DỤNG KASPERSKY ANTIVIRUS HOÀN HẢO HƠN

Internet ngày càng trở nên nguy hiểm hơn với những đe dọa như: virus, trojan, hacker, keylogger, malware, spyware... Do vậy, bạn phải lựa chọn đúng chương trình anti-virus và hơn nữa, phải thiết lập, cấu hình "chiến binh" này sao cho thích hợp nhất. Kaspersky AntiVirus l

Internet ngày càng trở nên nguy hiểm hơn với những đe doa như: virus, trojan, hacker, keylogger, malware, spyware... Do vậy, bạn phải lựa chọn đúng chương trình anti-virus và hơn nữa, phải thiết lập, cấu hình "chiến binh" này sao cho thích hợp nhất. Kaspersky AntiVirus là một trong những lưa chon tốt vì được đánh giá khá cao trong danh sách các chương trình antivirus hiện nay với khả năng tìm và diệt đến 99% các loại virus bao gồm cả các mã virus, các hình thái virus khác kể cả backdoor/Trojan. Sau khi tải về và cài đặt, Kaspersky AntiVirus (KAV) sẽ hoạt động âm thầm và quét moi thứ đang hoat đông trên PC của ban. Các đối tương, tập tin, tài liêu ... sẽ được quét trước khi có sư truy xuất từ người dùng, do đó khi phát hiện lây nhiễm virus, hệ thống cũng không bi tổn hai do KAV sẽ nhanh chóng tóm gọn chúng. Giao diện chính của Kaspersky Antivirus Giao diên chính của KAV khá đơn giản với thẻ Protection (Hình 1) bao gồm các chức năng chính của KAV. Ban có thể bắt đầu quét tìm diệt nhanh bằng cách chon "Scan My Computer" hay quét các đối tượng xác định qua "Scan objects" (chức năng này thuận tiện khi bạn đã quét toàn bộ hệ thống rồi nhưng lại bổ sung thêm ổ cứng mới hay đĩa mềm, CD, DVD) hoặc quét luôn các ổ di động với "Scan removable drives". (Bạn đừng nên chủ quan với những dữ liệu từ ổ đĩa ngoài, chúng có thể làm hư hai cả hê thống của ban mà không thể khôi phục được). Trong cùng cửa sổ trên, ta có thể tìm thấy liên kết "Update Now". Chức năng này cho phép cập nhật dữ liệu virus mới nhất qua việc kết nối vào cơ sở dữ liệu từ máy chủ của Kaspersky thông qua Internet. Kaspersky cũng khác với các trình antivirus khác ở chỗ CSDL được cập nhật hằng ngày chứ không phải hằng tuần, hằng tháng. Thời gian cập nhật cũng rất nhanh vì dung lượng CSDL chỉ khoảng từ 3 đến 20KB. Ở phần bên dưới là Quarantine và Backup. Khi một virus được tìm thấy, tập tin bị nhiễm sẽ ngay lâp tức được đưa vào "vùng" Quarantine, tức là chúng sẽ được "giam giữ" nghiêm ngặt, tránh khả năng truy xuất từ người dùng, do đó không thể phát tán được. Bạn cũng nên tập thói quen truy câp vào thư mục Quarantine và xóa sạch tất cả tập tin bị lậy nhiễm đạng được lưu trữ trong đó. Ban cũng sẽ có quyền truy xuất đến phần Report, hỗ trơ báo cáo các hoat đông của trình KAV cho ban theo dõi. Thẻ Settings với khá nhiều thiết lập

- Cấu hình bảo vệ thời gian thực: Real-Time Protection hay bảo vệ thời gian thực có nghĩa là chương trình antivirus sẽ hoạt động ở phần nền của hệ thống và theo dõi mọi xử lý đang hoạt động trên máy tính. Nó sẽ âm thầm quét các tập tin, email, macro, script để chắc chắn rằng không có nguy hiểm nào ảnh hưởng đến hệ thống có thể lọt qua được. Để chức năng này hoạt động tốt, bạn phải chỉ dẫn cho trình antivirus cách thức hành động đối với các vấn đề khác nhau. Trước hết, kiểm tra chế độ Real-Time Protection ở các thẻ Files, Email, Macros, Scripts và Network. Ở 3 thẻ đầu là Files, Email, Macros, chọn Protection Level Settings là Recommended. Thiết lập này khá tốt, cung cấp độ bảo mật cao sử dụng hợp lý dung lượng tài nguyên hệ thống. Nếu bạn cảm thấy rằng mình đang làm việc trong một môi trường nguy hiểm, hãy chọn High Protection để tăng độ bảo vệ nhưng điều này sẽ làm giảm tốc độ của hệ thống. Với những người dùng không kết nối Internet hay mạng và cũng không thường xuyên chép dữ liệu từ bên ngoài vào trong khi làm việc cùng những chương trình với cấu hình được giữ nguyên mỗi ngày thì nên dùng thiết lập High Speed. Nó sẽ chiếm dụng rất ít tài nguyên hệ thống. Bạn cũng có thể chọn các hành động khi

chương trình tìm thấy virus. Mặc dù phương thức tốt nhất là xóa các tập tin bị lây nhiễm ngay nhưng ban nên lưa chon và xác đinh rằng tập tin bị nhiễm không quan trong và có thể xóa đi bằng cách chon Prompt User for Action. Cách này giúp ban đưa các tập tin quan trong nhưng bi nhiễm vào phần bảo quản (Quarantine) để tìm cách "xóa bẩn" chúng. Trong thẻ Network, ban có thể lưa chon để nhân được thông báo khi có dấu hiệu tấn công mạng xảy ra. Tùy chon này hữu ích nhưng đôi khi lai gây phiền hà cho ban khá nhiều vì những thông báo kể cả khi đang xem một bộ phim. - Thiết lập trong thẻ Settings: Thiết lập quét định kỳ Trong thẻ Configure Scan My Computer này, người dùng có thể thiết lập quét hệ thống đinh kỳ. Chức năng này rất đáng giá và hữu ích. Ban không thể nào đều đăn nhớ chính xác ngày đã quét hê thống và mất thời gian vào việc này một cách thủ công. Hơn nữa, tạ có thể thiết lập KAV không thực hiện công việc quét hệ thống khi đang chơi một game năng nề nào đó hay sử dụng các chương trình xử lý phức tạp. -Cấu hình cập nhật Tất cả những cập nhật sẽ được hoàn tất tư động mà không cần ban phải thao tác thủ công. Đánh dấu Schedule Updates để có thể cập nhật dữ liêu mới nhất. Tại phần Quarantine & Backup Settings, cấu hình Kaspersky để quét các đối tương sau khi CSDL virus mới được cập nhật. Song song đó cũng cần đặt khoảng thời gian lưu trữ các tập tin bi nhiễm và dung lương lưu trữ cho chúng. Những thiết lập này tùy thuộc vào người dùng và dung lương, tài nguyên hê thống của mỗi người sử dụng. - Các phần thiết lập bổ sung Phần Additional Settings hỗ trơ ban thiết lập kích hoạt Kaspersky ngay khi khởi động vì nếu kích hoạt thủ cộng, sẽ có lúc ban quên đi và hệ thống sẽ hứng chịu nguy cơ tấn công. Ngoài ra, để ngăn chặn bất kỳ vấn đề nào, đánh dấu chon vào thiết lập hiển thi AntiVirus Scan Status trong khay hệ thống System Tray. Ban có thể theo dõi viêc quét virus và những hoat đông trên máy tính của mình. Tuy nhiên việc này sẽ khai thác tài nguyên bô nhớ RAM, do đó hê thống của ban cần có RAM ít nhất là 512MB trở lên. Một tính năng hữu ích nữa là người dùng laptop có thể thiết lập Kaspersky không thực hiện quét khi pin laptop sắp hết. - Các thiết lập bổ sung rất hữu ích của Kaspersky Antivirus Không chỉ áp dụng cho Kaspersky mà phần hướng dẫn trên, ban có thể tùy biến để áp dụng cho nhiều chương trình antivirus khác như BitDefender Pro 10, NOD32, AVG Pro... và luôn nhớ 9 quy tắc chung sau đây khi dùng các trình antivirus, cũng là 9 quy tắc bảo mật cho hệ thống của bạn: 1. Luôn luôn đặt trình antivirus tư đông được kích hoạt khi Windows khởi đông (Startup) 2. Nếu tài nguyên hê thống manh mẽ, hãy luôn thiết lập chế đô bảo mật cao nhất 3. Đinh kỳ quét virus thường xuyên để đảm bảo không có virus nào lây nhiễm trên hệ thống 4. Thiết lập trình antivirus cập nhật cơ sở dữ liêu virus mỗi ngày qua internet 5. Khi cài đặt hay mở bất kỳ tập tin nén nào, hãy tao thói quen phải chuột và quét với trình antivirus trước 6. Hãy xóa tất cả tập tin bi lây nhiễm. Việc "xóa bẩn" hay chuyển vào phần Quarantine chỉ dành cho các tập tin và tài liêu quan trong 7. Khi cài đặt lại hê điều hành, hãy cài trình antivirus ngay sau đó trước khi cài đặt các phần mềm, tiên ích khác 8. Đừng bao giờ kết nối vào internet khi không có trình antivirus nào đang hoat đông 9. Chỉ khóa tam trình antivirus trong những trường hợp tối cần thiết như ban cần toàn bô tài nguyên hê thống để xử lý môt công việc nào đó. THANH TRƯC