KASPERSKY LAB

Kaspersky® Internet Security 2015

HƯỚNG DẪN CÀI ĐẶT VÀ SỬ DỤNG

http://www.kaspersky.vn

Ngày cập nhật: Tháng 10 năm 2014

I. Cài đặt và kích hoạt bản quyền

Lưu ý trước khi cài đặt:

- ✓ Gỡ bỏ hết tất cả các phần mềm diệt virus của các hãng khác trên máy tính, nếu không quá trình cài đặt sẽ không thực hiện được.
- ✓ Đảm bảo ngày và thời gian trên máy tính phải đúng với hiện tại (bao gồm múi giờ của VN là (GMT +7) Bangkok, Ha Noi, Jakarta; đồng thời chỉnh giờ, ngày, tháng, năm đúng với hiện tại). Nếu thời gian sai dẫn đến quá trình kích hoạt bản quyền sẽ bị lỗi.
- ✓ Máy tính phải được kết nối Internet mới có thể kích hoạt được bản quyền.
- ✓ Việc chia sẻ mã số kích hoạt cho nhiều máy tính sử dụng cùng lúc, vượt quá số lượng cho phép của bản quyền sẽ dẫn đến việc mã số kích hoạt bị khóa hoàn toàn. Kaspersky không chịu trách nhiệm bảo hành các trường hợp này.
- ✓ Có thể chuyển bản quyền sang máy tính khác, tuy nhiên phải gỡ bỏ Kaspersky trên máy tính hiện tại ra.
- ✓ **Giữ kỹ thẻ bản quyền cẩn thận, để có thể kích hoạt lại Kaspersky nếu bạn cài đặt lại hệ điều hành hoặc chương trình. Nếu mất thẻ bản quyền Kaspersky sẽ từ chối bảo hành**
- ✓ Kaspersky Internet Security 2015 chỉ sử dụng cho máy tính cá nhân, không cài được cho máy chủ. Các doanh nghiệp nên dùng sản phẩm Kaspersky Endpoint Security for Business để sử dụng đúng chức năng tốt nhất của Kaspersky Lab.

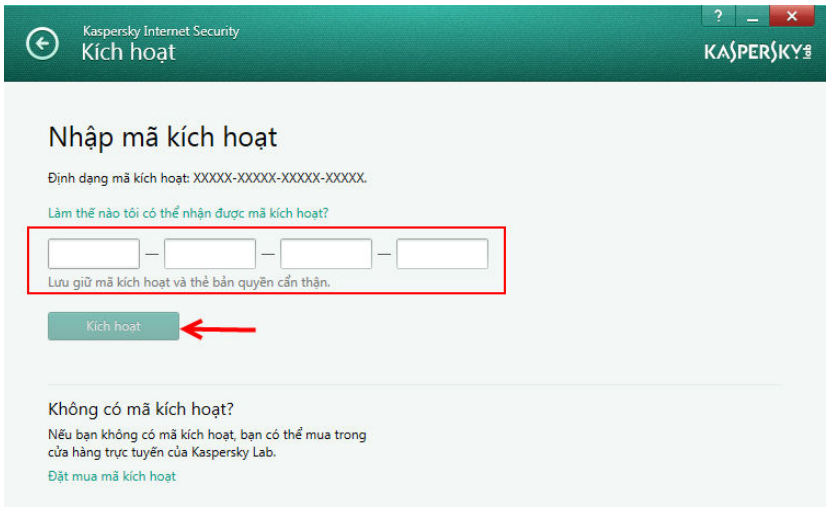
Cài đặt

Bỏ đĩa CD cài đặt vào máy tính, giao diện autorun tự động hiện lên như hình bên dưới (hoặc bạn chạy tập tin autorun.exe trong CD). Ngoài ra, bạn có thể tải về nguồn (source) cài đặt tại địa chỉ: www.kaspersky.vn

- ✓ Chọn **Cài đặt ngay** để bắt đầu quá trình cài đặt
- ✓ Tại cửa sổ "Chào mừng đến với Kaspersky Internet Security 2015" > bạn chọn **Cài đặt**
- ✓ Thông báo cài đặt thành công xuất hiện, bạn chọn **Hoàn tất** để qua bước kích hoạt bản quyền.

Kích hoạt bản quyền

Sau khi cài đặt thành công, giao diện kích hoạt bản quyền xuất hiện như hình bên dưới. Bạn điền mã bản quyền gồm 20 ký tự (cào nhẹ lớp tráng bạc trên thẻ cào bản quyền để có được mã kích hoạt này) > kế tiếp bạn chọn **Kích hoạt** để bắt đầu kích hoạt bản quyền.



Sau khi kích hoạt thành công, giao diện thông báo bản quyền đã được kích hoạt thành công xuất hiện (hình dưới). Bạn chọn **Hoàn tất** để hoàn thành quá trình cài đặt và kích hoạt bản quyền

<u>Lưu ý</u>: Khi kích hoạt thành công bản quyền, bạn nên giữ lại thẻ bản quyền cẩn thận để kích hoạt lại bản quyền trong trường hợp cài đặt lại Windows và phần mềm Kaspersky.

Các bước nên thực hiện sau khi cài đặt thành công chương trình

Sau khi cài đặt thành công chương trình Kaspersky, bạn nên thực hiện các hành động sau:

- ✓ **Kiểm tra trạng thái Kaspersky**: Biểu tượng  màu đỏ xuất hiện ở thanh taskbar (góc phải cuối màn hình) chứng tỏ là chương trình Kaspersky đang bảo vệ trong thời gian thực.
- ✓ **Cập nhật cơ sỡ dữ liệu cho chương trình**: Click chuột phải vào biểu tượng Kaspersky ở thanh taskbar (góc phải cuối màn hình) chọn **Cập nhật**. Lần đầu do dung lượng cập nhật khá lớn nên thời gian cập nhật khá lâu, những lần cập nhật sau này diễn ra rất nhanh chóng do dung lượng nhỏ.
- ✓ **Quét virus toàn bộ máy tính**: Sau khi cập nhật thành công, bạn nên tiến hành quét toàn bộ máy tính bằng cách mở giao diện chính của chương trình > chọn **Quét** > **Quét toàn bộ**. Bạn nên thực hiện bước này sau khi vừa cài đặt thành công chương trình Kaspersky, mục đích là giúp loại bỏ tất cả các chương trình, đoạn mã độc hại có trong máy tính (nếu có) đồng thời giúp Kaspersky ghi nhớ, đánh dấu các tập tin hiện có nhằm giúp chương trình hoạt động hiệu quả nhất.

Các lưu ý để sử dụng tốt chương trình

Kaspersky luôn bảo vệ máy tính của bạn trong thời gian thực. Tuy nhiên, trong quá trình sử dụng, bạn lưu ý các vấn đề sau để có thể phát huy hiệu quả hoạt động cao nhất của chương trình.

- ✓ **Đảm bảo chương trình được cập nhật thường xuyên**: nếu chương trình không được cập nhật thường xuyên, nó không có khả năng tiêu diệt virus mới.
- ✓ **Không tắt chương trình trong mọi thời điểm**: lúc bạn tắt chương trình Kaspersky đi, tại thời điểm đó, một số dòng virus có thể xâm nhập vào máy tính và vô hiệu quá hoạt động của chương trình và phá hủy dữ liệu dẫn đến khả năng không còn cứu chữa được nữa.
- ✓ **Định kỳ (một khoảng thời gian) quét toàn bộ máy tính một lần**: việc quét toàn bộ máy tính sẽ gia tăng hiệu quả hoạt động của chương trình, giúp chương trình loại bỏ hoàn toàn các đoạn mã độc hại, phát hiện lỗi hệ thống, lỗi chương trình, ghi nhớ tập tin,…
- ✓ **Liên hệ hỗ trợ kỹ thuật khi gặp sự cố**: liên hệ ngay đến trung tâm hỗ trợ khách hàng của Kaspersky Lab VN nếu bạn gặp vấn đề khi sử dụng sản phẩm.
- ✓ **Ngoài ra, đặt mật khẩu bảo vệ chương trình**, không cấu hình các tính năng của chương trình khi không hiểu rõ về chúng cũng là cách sử dụng hiệu quả chương trình.

II. Mô tả các tính năng của chương trình Kaspersky Internet Security 2015

Phiên bản Kaspersky Internet Security 2015 có các tính năng bảo vệ như sau:

- **Chống virus cho tập tin**: Bảo vệ an toàn tập tin hệ điều hành, dữ liệu trên máy tính, phát hiện, xử lý virus tấn công từ ổ cứng di động, mạng LAN,…
- **Chống virus cho thư điện tử**: Phát hiện, xử lý các email chứa mã độc.
- **Chống virus cho web**: Phát hiện, xử lý, ngăn không cho truy cập đến các địa chỉ web độc hại cũng như tải về các tập tin độc hại từ Internet.
- **Chống virus cho tin nhắn**: Phát hiện, xử lý các đoạn mã, đường link, tập tin độc hại lây nhiễm qua các chương trình chát (Yahoo, Skype,…)
- **Kiểm soát ứng dụng**: Quản lý các ứng dụng được cài đặt tên máy tính giúp phát hiện các ứng dụng tiềm tàng nguy hiểm.
- **Chống lừa đảo**: Ngăn chặn truy cập đến các địa chỉ web lừa đảo cũng như phát hiện và ngăn các email lừa đảo.

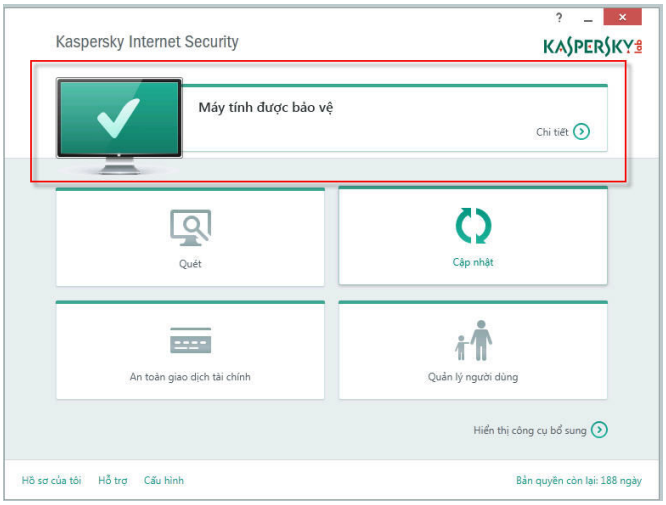
- **Chủ động bảo vệ**: Tính năng phân tích hành vi giúp phát hiện các đối tượng nguy hiểm dù chúng chưa có trong cơ sỡ dữ liệu của chương trình.
- **An toàn giao dịch tài chính**: Chạy các trang web internet banking của các ngân hàng, trang web thanh toán, mua hàng trực tuyến trong chế độ an toàn với một môi trường ảo hoàn toàn, khi bạn chạy trong chế độ an toàn, phần mềm độc hại, hacker không có cách nào lấy đi tiền bạc của bạn.
- **Kiểm soát người dùng**: Quản lý thời gian và nội dung truy cập của con cái bạn. Bạn có thể cấm con bạn sử dụng máy tính, Internet, chương trình vào các khoảng thời gian nào đó trong ngày. Bạn cũng có thể ngăn con bạn truy cập đến các địa chỉ web chỉ định, ngăn tải về các tập tin,….
- **Tường lửa cá nhân**: Quản lý, giám sát chặt chẽ luồng dữ liệu vào và ra máy tính qua việc định nghĩa các quy tắc cho các gói tin cũng như cho các ứng dụng. Quản lý chặt chẽ các đường mạng kết nối Internet.
- **Chống tấn công mạng**: Ngăn chặn hacker từ mạng Internet cũng như mạng nội bộ xâm nhập điều khiển máy tính của bạn, lấy đi các thông tin quan trọng trên máy tính.
- **Quét lỗ hổng bảo mật**: Phát hiện, xử lý các lỗ hổng bảo mật của hệ điều hành cũng như của các phần mềm được cài đặt trên máy tính.
- **Chống thư rác**: Phát hiện và xử lý các email rác gửi đến email của bạn.
- **Chặn quảng cáo**: Ngăn chặn các quảng cáo gây phiền toán cho bạn khi bạn truy cập web.
- **Giám sát mạng**: Giám sát chi tiết luồng dữ liệu vào và ra máy tính, các trang web và IP đang truy cập, các công được mở,…
- **Bảo vệ dữ liệu nhập vào**: đảm bảo các dữ liệu quan trọng mà bạn nhập vào từ bàn phím vật lý không thể bị lấy cắp, lưu lại bởi hacker, keylogger
- **Giám sát hệ thống**: không phục hành động được gây ra bởi phần mềm độc hại
- **Bảo vệ với điện toán đám mây**: tương tác với người sử dụng: chỉ một thao tác đơn giản, bạn sẽ dễ dàng kiểm tra độ tin cậy, danh tiếng, mức độ sử dụng của một chương trình, một trang web thông qua mạng Kaspersky Security Network trên toàn cầu.

III. Một số tùy chỉnh thường sử dụng

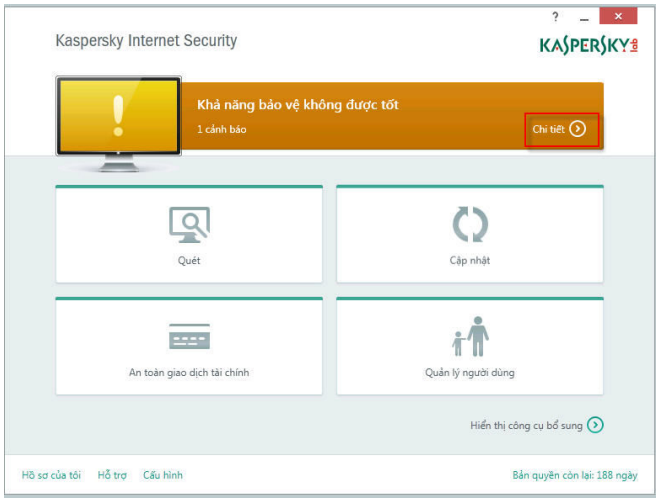
1. Xem trạng thái bảo vệ máy tính của chương trình

Mở giao diện chương trình, bạn sẽ thấy ngay lập tức trạng thái bảo vệ của chương trình Kaspersky. Việc xem trạng thái bảo vệ giúp bạn xác định: máy tính có gặp nguy hiểm không? các thành phần bảo vệ có tắt không? cơ sở dữ liệu có cập nhật tới thời điểm gần nhất không? bản quyền còn bao nhiêu ngày sử dụng?

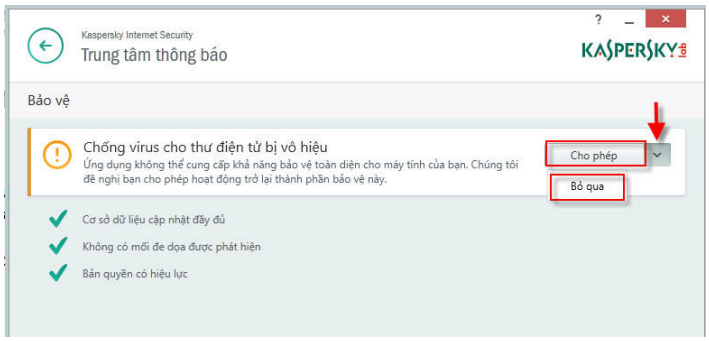
Bạn để ý xem màu của hình máy tính trên giao diện chính chương trình: nếu là màu xanh > máy tính an toàn; nếu là màu vàng hoặc đỏ > máy tính đang gặp một số vấn đề cũng như các mối nguy hiểm.



Nếu chương trình thông báo “Khả năng bảo vệ không được tốt”, bạn nhấn chuột vào để xem lý do vì sao chương trình Kaspersky báo như vậy.



Ví dụ bên dưới: Máy tính không được an toàn do vài tính năng thành phần bị tắt, cụ thể là tính năng Chống virus cho thư điện tử > Bạn chọn **Cho phép** nếu muốn khôi phục tính năng bị tắt (ngoài ra, bạn có thể chọn **Bỏ qua** nếu cảm thấy tính năng này thật sự không cần thiết > điều này đồng nghĩa với việc Kaspersky sẽ không có khả năng bảo vệ máy tính nếu virus lây nhiễm qua con đường email).



2. Đặt mật khẩu bảo vệ cho chương trình

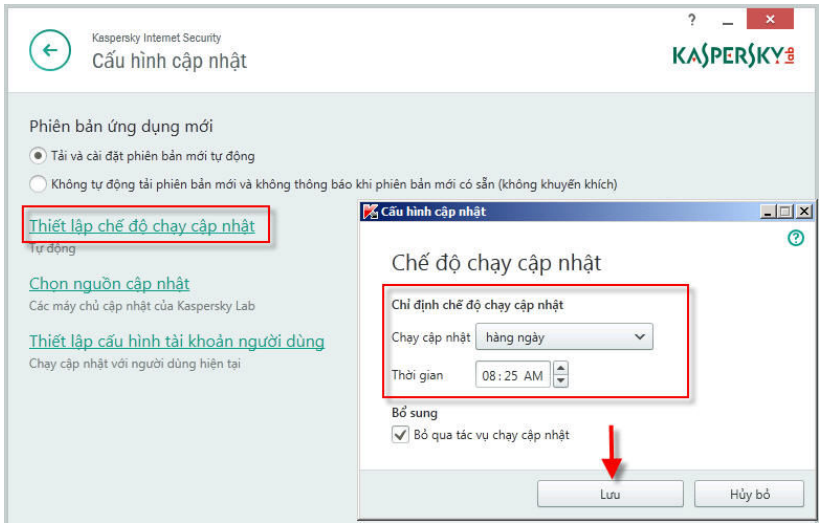
Mật khẩu bảo vệ chương trình là cần thiết nếu như bạn không muốn người khác can thiệp tắt (mở), chỉnh sửa, gỡ bỏ chương trình, gây ảnh hưởng đến hiệu quả bảo vệ của Kaspersky. Ngoài ra, đặt mật khẩu bảo vệ là bắt buộc nếu bạn cấu hình tính năng Kiểm soát người dùng.

Mở giao diện **Cầu hình** > Chọn **Tổng quát** > Chọn **Thiết lập mật khẩu bảo vệ** > Sau đó điền vào mật khẩu bảo vệ chương trình. Lưu ý: bạn nên chọn hết các dòng trong **Phạm vi mật khẩu** (xem hình dưới).

3. Tùy chỉnh lịch cập nhật virus theo ý bạn (Update)

Mặc định, chế độ Cập nhật của Kaspersky là tự động (chương trình định kỳ kết nối đến máy chủ để kiểm tra và tự động tải về bản cập nhật mới). Để tiết kiệm tài nguyên hệ thống, và tránh trình trạng cập nhật nhiều lần trong ngày có thể làm cho máy tính chạy chậm trong khoảng thời gian cập nhật, bạn có thể tạo một lịch cập nhật riêng theo ý của bạn.

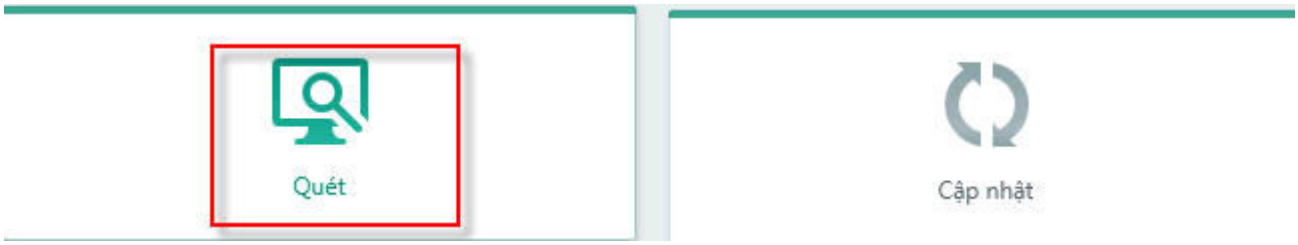
Mở giao diện **Cấu hình** > Chọn **Bổ xung** > Chọn **Cập nhật** > giao diện tiếp theo chọn **Thiết lập chế độ chạy cập nhật**. Tại đây, bạn có thể tạo một lịch theo ý mình. Lưu ý, bạn không nên cấu hình cho chương trình trong khoảng thời gian dài không được cập nhật, như thế sẽ ảnh hưởng đến hiệu quả diệt virus mới của chương trình.

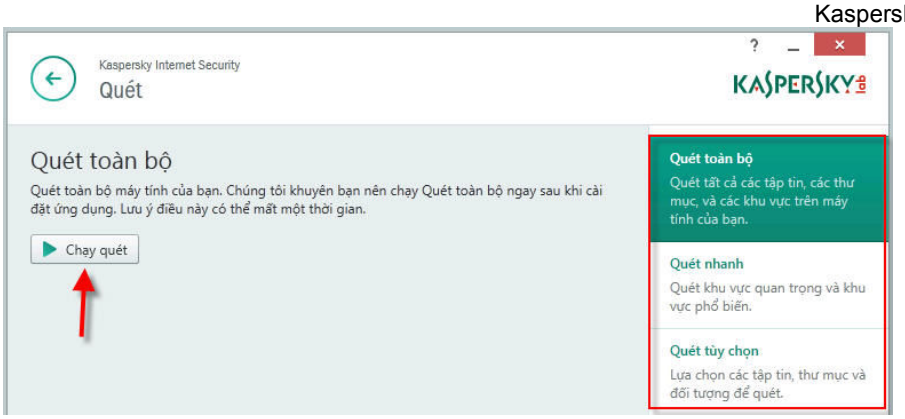


Ngoài ra, Kaspersky hỗ trợ bạn cập nhật offline (dành cho các máy tính khi cập nhật online dung lượng lớn bị lỗi). Vui lòng liên hệ địa chỉ hotro@kaspersky.vn để được hướng dẫn

4. Thực hiện một thao tác quét máy tính (Scan)

Lần đầu tiên sau khi cài Kaspersky vào máy tính, bạn nên tiến hành thực hiện Quét toàn bộ máy tính. Nhấn chuột phải vào My Computer > **Quét virus**. Hoặc bạn mở giao diện chương trình Kaspersky > **Quét** > **Quét toàn bộ** (hình dưới)





Kaspersky bảo vệ máy tính trong thời gian thực, vì thế bạn không cần thực hiện Quét toàn bộ máy tính nhiều lần, có thể chỉ một lần đầu tiên là đủ (bạn cũng có thể thực hiện Quét toàn bộ những lần sau với khoảng cách thời gian quét hợp lý, ví dụ như vài tháng quét toàn bộ một lần).

Lưu ý: Trong khi thực hiện Quét toàn bộ máy tính, Kaspersky sẽ chiếm dụng thêm tài nguyên hệ thống, vì thế với các máy tính có cấu hình yếu, quá trình quét toàn bộ máy tính có thể làm cho máy tính của bạn hoạt động hơi chậm hơn bình thường. Bạn nên chọn thời gian quét toàn bộ máy tính cho hợp lý để không ảnh hưởng đến công việc (Vd: Vào giờ nghỉ trưa chẳng hạn)

Lần đầu tiên, quét toàn bộ máy tính diễn ra tương đối lâu và tùy thuộc vào dung lượng dữ liệu trên máy tính. Tuy nhiên, những lần quét sau diễn ra khá nhanh. Ở lần đầu tiên Kaspersky có cơ chế đánh dấu tập tin, những lần quét sau, Kaspersky sẽ bỏ qua không quét các tập tin không bị truy cập và chỉnh sửa kể từ lần quét toàn bộ trước đó.

Bạn cũng có thể chọn **Quét nhanh** (hình trên) để cho chương trình chỉ quét các khu vực quan trọng (tập tin hệ điều hành, tập tin của các phần mềm trên máy tính, tập tin khởi động cùng máy tính, boot sector)

5. Tắt một tính năng mà bạn không muốn sử dụng

Giả sử, bạn không muốn sử dụng các tính năng Chống thư rác, Chống virus cho thư điện tử, Kiểm soát ứng dụng, hoặc một tính năng nào đó của chương trình vì bạn không có nhu cầu hoặc cảm thấy không cần thiết.

Thực hiện: Vào phần cấu hình của chương trình > chọn **Trung tâm bảo vệ** > kéo thanh trượt và chọn tính năng mà bạn cần tắt > tắt tính năng như hình bên dưới (ví dụ về việc vô hiệu quá trính năng Chống thư rác)

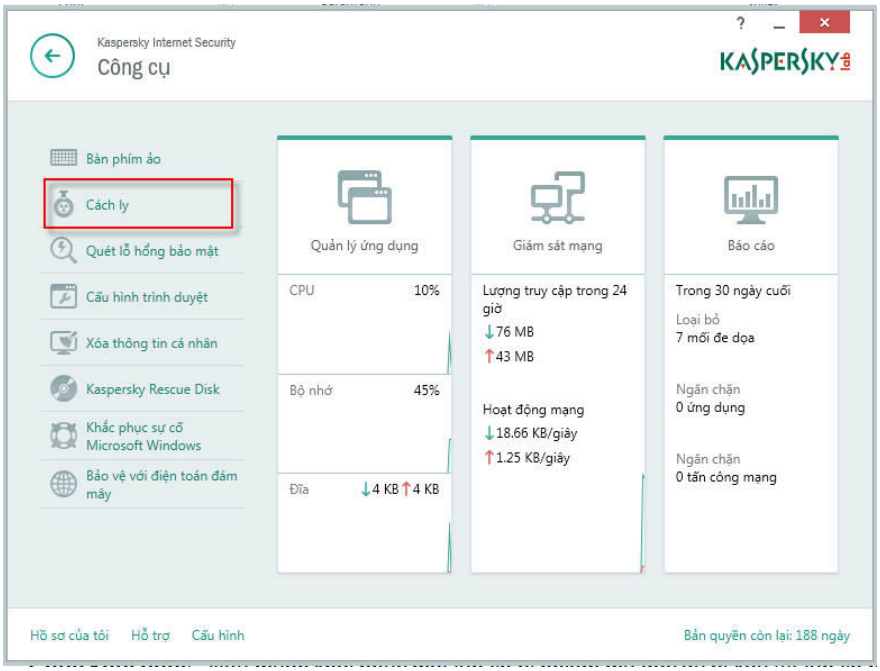
Lưu ý: Bạn chỉ thật sự tắt tính năng nào đó khi bạn không cần đến và bạn cảm thấy nó dư thừa (Ví dụ: tắt chống virus cho thư điện tử, chống thư rác vì bạn không dùng email; tắt tính năng Kiểm soát ứng dụng, Chống

lừa đảo,… vì bạn là người sử dụng máy tính có kinh nghiệm và quản lý tốt các trang web truy cập hoặc các ứng dụng được cài trên máy tính,…)

Dù tắt tính năng nào đi nữa: 4 tính năng quan trọng chính sau đây bạn không thể tắt vì sẽ làm ảnh hưởng nghiêm trọng đến hiệu quả hoạt động của chương trình: **Chống virus cho tập tin, Chống virus cho web, Chống virus cho thư điện tử (nếu có dùng trình email), Chống virus cho tin nhắn (nếu có dùng các chương trình Chát)**.

6. Quản lý các tập tin bị Kaspersky xử lý

Khi Kaspersky xử lý một tập tin độc hại, chương trình không xóa vĩnh viễn tập tin đó (trừ trường hợp bạn gỡ bỏ chương trình Kaspersky ra khỏi máy thì các tập tin đó sẽ bị xóa vĩnh viễn). Mặc định các tập tin mã độc bị Kaspersky xử lý sẽ được lưu trữ tại khu vực Cách ly với một định dạng đặt biệt, không gây hại cho máy tính. Từ giao diện chính của chương trình, bạn nhấn **Hiển thị công cụ bổ sung vào** phần **Cách ly** (hình dưới).



- Tại đây sẽ lưu trữ thông tin tất cả các tập tin bị nhiễm độc và bị Kaspersky tẩy xóa.

  ✓ **Chọn khôi phục** : Nếu muốn khôi phục một tập tin bị nhiễm mã độc đã bị xóa (vì tập tin này rất quan trọng với bạn)

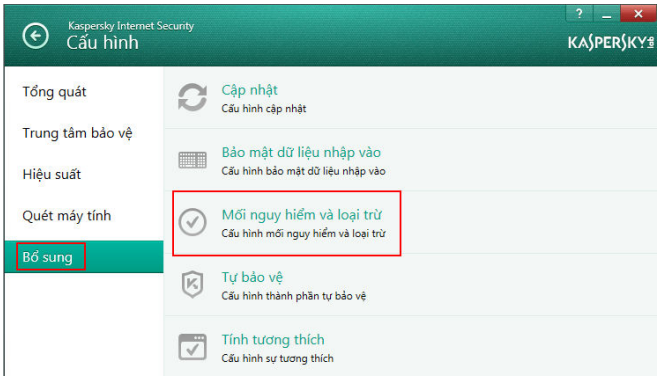
  ✓ **Chọn Xóa**: Nếu bạn muốn xóa vĩnh viễn tập tin này (không còn khả năng khôi phục tập tin)

- ✓ **Lưu ý**: Trước khi khôi phục một tập tin bị nhiễm mã độc, bạn nhấn chuột phải vào biểu tượng Kaspersky ở góc phải cuối màn hình > chọn **Tạm ngưng bảo vệ…** đồng thời bạn phải chấp nhận rủi ro rằng tập tin bị nhiễm độc này có khả năng phá hoại hệ thống. Khuyến cáo: trường hợp bạn có tập tin làm việc quan trọng (excel,…) bị Kaspersky xóa vì nhiễm virus, bạn nên liên hệ đến Kaspersky Lab VN để được cung cấp các phương pháp hỗ trợ hiệu quả.

7. Đưa một chương trình, một thư mục vào vùng tin tưởng

Có trường hợp Kaspersky nhận dạng lầm một ứng dụng chứa mã độc và xóa tập tin chạy của chương trình đó đi hoặc ngăn một số hoạt động của chương trình, làm chương trình hoạt động không đúng cách. Cũng có trường hợp bạn có một thư mục ABC, một số tập tin lưu trữ trong thư mục này bị Kaspersky nhận dạng có chứa mã độc. Tuy nhiên, những tập tin này rất quan trọng với bạn và bạn không muốn chúng bị Kaspersky xóa đi.

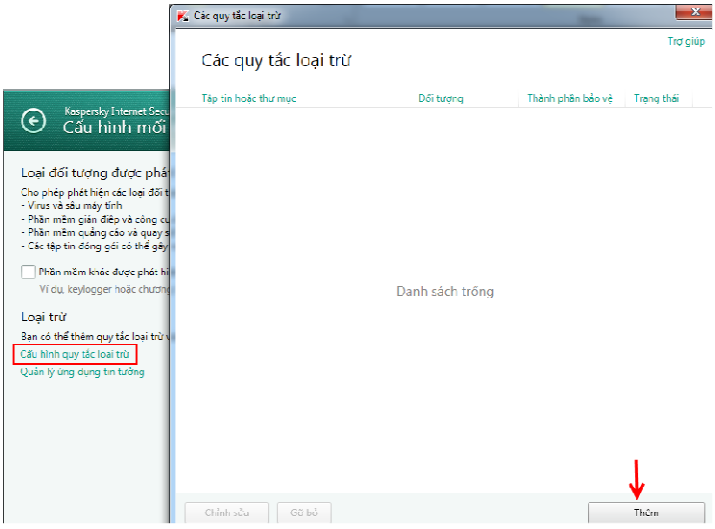
Để giải quyết 2 trường hợp trên, bạn có thể đưa chương trình, thư mục đó vào vùng tin tưởng của Kaspersky. Mở giao diện **Cấu hình** của chương trình > Chọn **Bổ xung** > chọn **Mối nguy hiểm và loại trừ** (hình dưới)

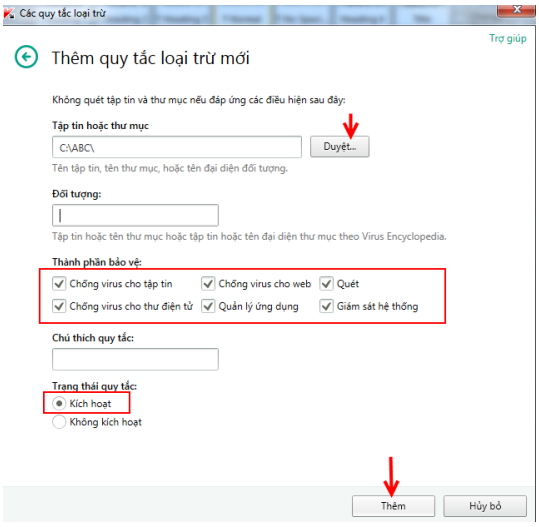


Tại đây có 2 lựa chọn: hoặc là cấu hình tin tưởng cho tập tin chạy chương trình (có định dạng .exe) hoặc là cấu hình tin tưởng một thư mục nào đó

Vd 1: Cấu hình tin tưởng thư mục ABC

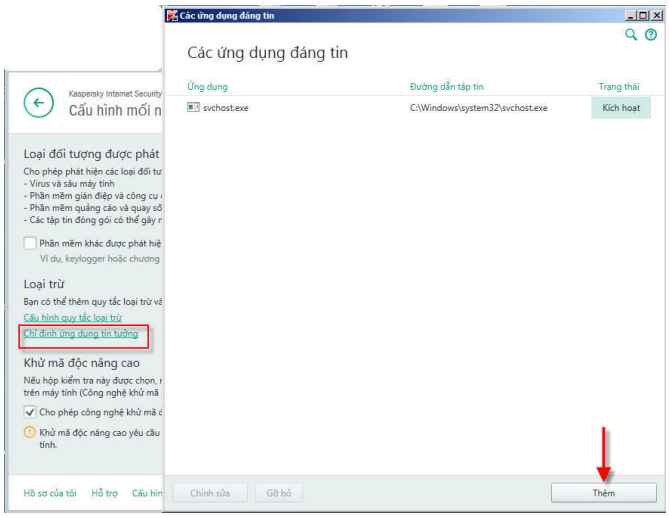
Chọn **Cấu hình quy tắc loại trừ** > **Thêm** > **Chọn Duyệt** > tìm đến thư mục ABC cần cấu hình tin tưởng > cuối cùng chọn **Thêm** (hình dưới)

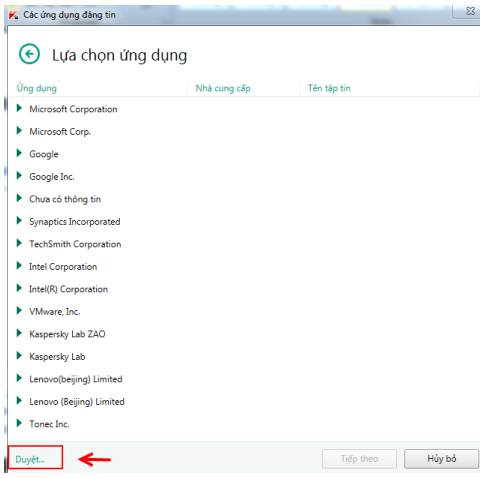




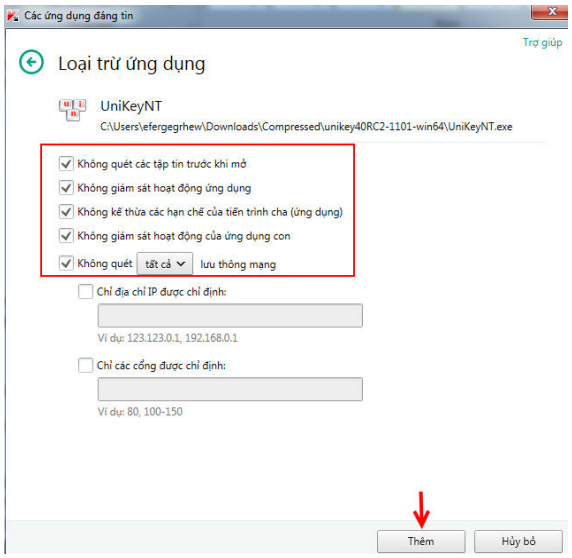
Vd 2: Cấu hình tin tưởng chương trình Unikey

Để thêm một ứng dụng vào vùng tin tưởng của Kaspersky, bạn chọn **Quản lý ứng dụng tin tưởng** > Chọn **Thêm** > Sau đó chọn **Duyệt** để tìm đến đường dẫn chứa tập tin chạy có định dạng *.exe của ứng dụng Unikey cần cấu hình tin tưởng (ngoài ra, bạn có thể chọn các ứng dụng đã được Kaspersky liệt kê sẵn)





Sau khi đã chọn xong ứng dụng cần cấu hình tin tưởng, bước tiếp theo bạn đánh dấu chọn tất cả các dòng như hình dưới (bạn cũng có thể chọn vài hành động loại trừ mà bạn nghĩ là phù hợp). Sau khi cấu hình xong, Kaspersky sẽ bỏ qua không quét các hành động đã loại trừ khi ứng dụng Unikey chạy.



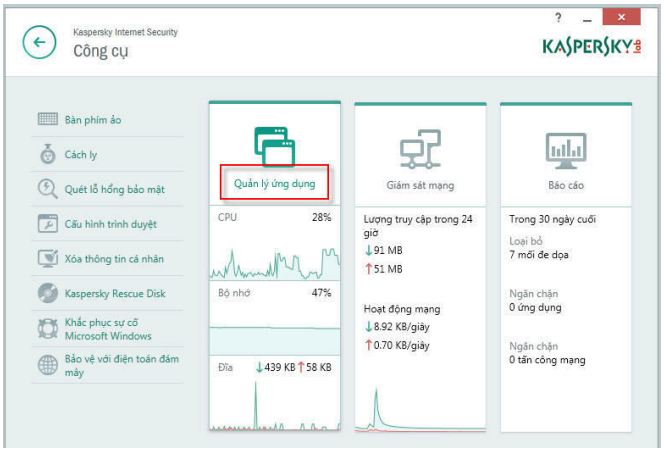
Lưu ý: Chỉ những chương trình thật sự tin tưởng bạn mới thêm vào khu vực loại trừ, trường hợp bạn cấu hình tin tưởng nhầm vào chương trình có chứa mã độc sẽ rất nguy hiểm đối với máy tính.

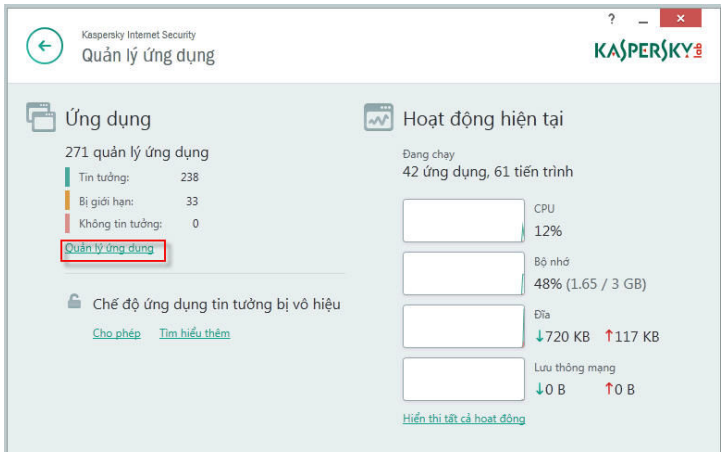
8. Cấu hình mức độ tin tưởng của Kaspersky với các ứng dụng được cài đặt trên máy tính

Khi một ứng dụng được chạy lần đầu tiên trên máy tính, Kaspersky sẽ phân tích ứng dụng và đưa vào 3 nhóm chính:

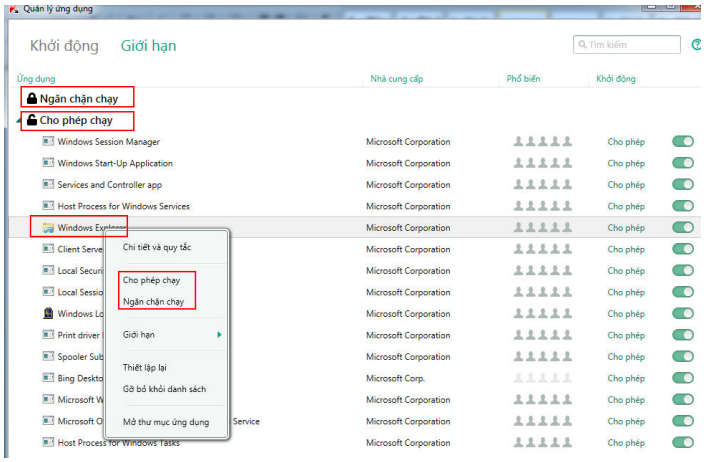
- ✓ **Tin tưởng**: Bao gồm các ứng dụng có chữ ký số cũng như các ứng dụng nằm trong cơ sở dữ liệu tin tưởng của Kaspersky.
- ✓ **Không tin tưởng**: Bao gồm những ứng dụng nguy hiểm, bị Kaspersky liệt vào những phần mềm độc hại.
- ✓ **Ứng dụng không biết**: Bao gồm danh sách các chương trình được phát triển bởi các hãng nhỏ, ít được biết đến và không có một chữ ký số. Đối với các ứng dụng này, Kaspersky chỉ có thể tạo ra các quy tắc kiểm soát cho chúng khi bạn chạy chúng ở lần đầu tiên. Lúc đó, chương trình mới biết được là hành động của ứng dụng là tin cậy hay không tin cậy, dựa trên cơ sở đó Kaspersky sẽ quyết định các mức độ truy cập của ứng dụng đến tài nguyên hệ thống.

Mở giao diện **Chính** của chương trình > chọn **Hiển thị công cụ bổ sung** > chọn **Quản lý ứng dụng** > chọn **Quản lý ứng dụng**

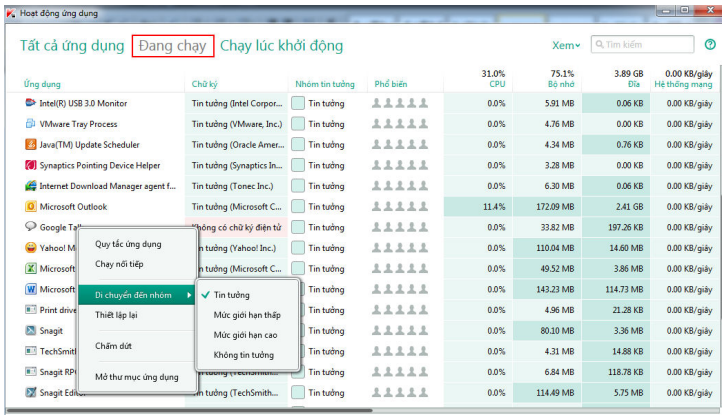




Tại đây, Kaspersky phân loại sẵn cho bạn 2 nhóm ứng dụng: Ngăn chặn chạy và Cho phép chạy. Nhấn chuột phải vào một ứng dụng > Bạn có thể cấu hình cho phép sử dụng hoặc ngăn sử dụng một ứng dụng nào đó



Ngoài ra, tính năng Quản lý ứng dụng còn giúp bạn xem được một cách rõ ràng trạng thái các ứng dụng đang chạy trên máy tính, mỗi ứng dụng chiếm bộ nhớ RAM là bao nhiêu? chiếm CPU là bao nhiêu? trạng thái của ứng dụng có đáng tin hay không? Click chuột phải vào biểu tượng Kaspersky chọn **Công cụ** > chọn **Hoạt động ứng dụng** > chọn thẻ **Đang chạy**. Nếu bạn nhấn chuột phải vào một tiến trình đang chạy, bạn có thể chấm dứt hoạt động của tiến trình hoặc cấu hình lại mức độ tin tưởng (ví dụ chuyển từ mức Tin tưởng sang các mức trạng thái khác).



- ✓ **Tin tưởng**: Ứng dụng được phép hoạt động toàn quyền trên hệ thống.
- ✓ **Mức giới hạn thấp**: Ứng dụng chỉ được phép thực hiện một số hoạt động như truy cập đến một số tiến trình khác, kiểm soát hệ thống, ẩn truy cập mạng.
- ✓ **Mức giới hạn cao**: Các ứng dụng của nhóm này đòi hỏi sự cho phép của người dùng cho hầu hết các hành động mà ảnh hưởng đến hệ thống, một số hành động không được phép thực hiện.
- ✓ **Không tin tưởng**: Ứng dụng không được phép hoạt động.

Ngoài ra, bạn có thể cấu hình cho tính năng này hoạt động ở chế độ Ứng dụng tin tưởng: khi kích hoạt chế độ này, chỉ những ứng dụng có trong cơ sở dữ liệu các ứng dụng tin tưởng của Kaspersky mới được phép chạy, tất cả các ứng dụng khác sẽ bị vô hiệu. Mở giao diện chính của chương trình > chọn **Quản lý ứng dụng** > chọn **Cho phép** trong phần Chế độ ứng dụng tin tưởng (hình dưới)

9. Cấu hình tính năng Chống thư rác

Tính năng chống thư rác tích hợp với các chương trình gửi nhận mail phổ biến sau: Microsoft Outlook, Outlook Express, Thunderbird, The Bat!, giúp phát hiện và xử lý thư rác tại ngay máy tính người dùng.

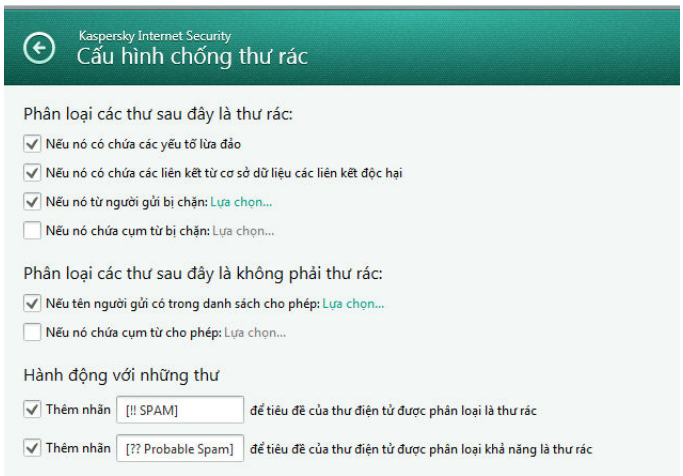
Tùy chỉnh phương pháp nhận dạng thư rác

Khả năng chống thư rác của Kaspersky dựa vào cơ sở dữ liệu được cập nhật hàng ngày. Một email được đánh giá là thư rác nếu:

- ✓ Địa chỉ người gửi có trong danh sách bị chặn của Kaspersky (được cập nhật hàng ngày).
- ✓ Nếu email gửi có chứa đường link dẫn đến trang web lừa đảo hoặc trang web khả nghi.

- ✓ Bạn có thể chỉ định một địa chỉ nào đó là thư rác: Tại dòng “Nếu nó từ người gửi đã bị chặn” > Nhấn **Chọn** để tiến hành cấu hình.
- ✓ Bạn cũng có thể chỉ định: nếu một email chứa từ hay cụm từ nào đó thì sẽ nhận dạng nó sẽ là thư rác: Chọn dòng “Nếu nó chứa cụm từ bị chặn” > Nhấn **Chọn** để tiến hành cấu hình.

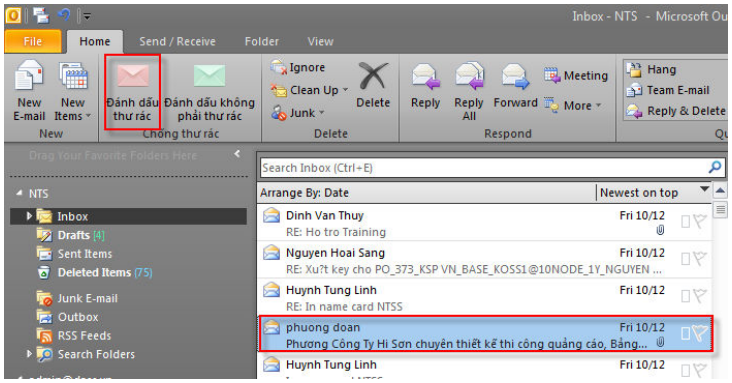
Để tiến hành tùy chỉnh lại cấu hình, bạn vào phần cấu hình của Kaspersky > **Trung tâm bảo vệ** > **Chống thư rác** > **Cấu hình nâng cao** (hình dưới).



- **Thực hiện Huấn luyện thư rác** (Ví dụ cho Microsoft Outlook)

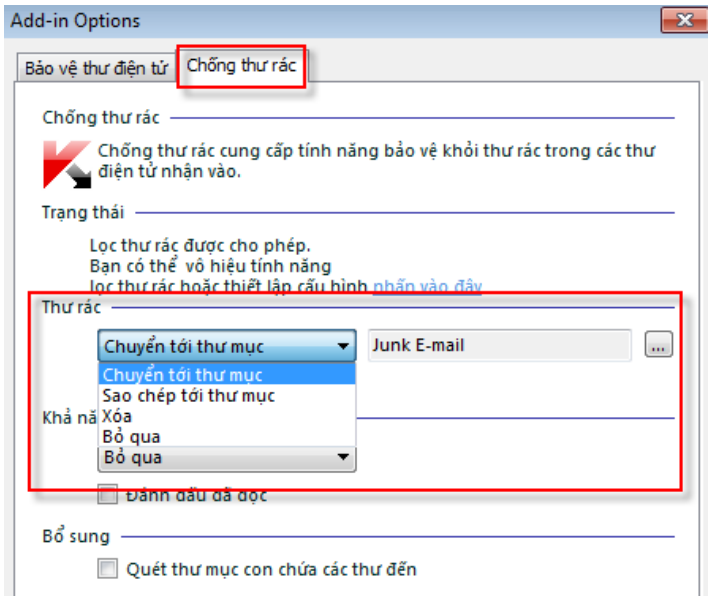
Ngoài khả năng nhận dạng dựa trên cơ sở dữ liệu hiện có và các tùy chỉnh ở trên, Kaspersky còn cho phép người dùng tiến hành huấn luyện cho Kaspersky, chỉ cho chương trình biết là những địa chỉ email nào là thư rác, những email nào không phải là thư rác.

Huấn luyện thư rác trên giao diện chương trình Outlook: Vd: Bạn đang sử dụng Microsoft Outlook 2010 > bạn chọn email mà cho là thư rác (Kaspersky bỏ sót) > chọn **Thư rác** (hình dưới). Ngược lại nếu một email bị đánh dấu nhầm là **Thư rác** > bạn chọn email đó sau đó chọn **Không phải thư rác**.



- **Tùy chỉnh hành động xử lý của Kaspersky khi phát hiện thư rác**

Khi phát hiện một email là thư rác, mặc định chương trình sẽ bỏ qua email (không xóa thư mà chỉ thêm chữ [!! SPAM] vào tựa đề). Để thay đổi tùy chỉnh hành động của Kaspersky đối với thư rác bạn làm như sau: Nếu đang dùng Mirosoft Outlook 2010, bạn mở chương trình Outlook > Vào **File** > **Option** > **Add-ins** > **Add-ins options** > chọn thẻ Chống thư rác (hình dưới). Với Outlook 2007 bạn chọn **Tools** > **Option**



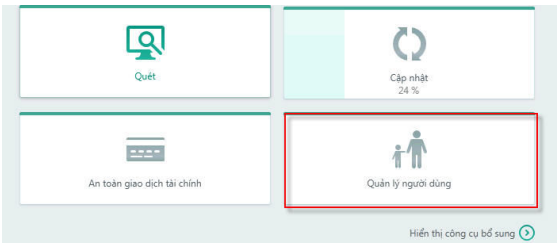
- ✓ Nếu bạn chọn **Chuyển tới thư mục** > Khi phát hiện thư rác, Kaspersky sẽ chuyển thư rác đến một thư mục chỉ định nào đó (Vd: bạn di chuyển tất cả thư rác đến thư mục Junk Email).
- ✓ Nếu chọn **Sao chép tới thư mục** > Khi phát hiện thư rác, Kaspersky sẽ copy thư rác đến một thư mục chỉ định nào đó.
- ✓ Nếu bạn chọn **Xóa** > Khi phát hiện thư rác, Kaspersky sẽ xóa ngay thư rác đó.
- ✓ Nếu bạn chọn **Bỏ qua** > Khi phát hiện thư rác, Kaspersky sẽ chỉ thêm vào chữ SPAM ở tựa đề email

Chúng tôi khuyến khích bạn nên chọn chế độ **Chuyển tới thư mục** để tránh trường hợp Kaspersky xóa đi các email bị nhận dạng lầm hoặc trong vài trường hợp bạn muốn đọc lại thư rác (Vd: tuy địa chỉ xx@abc.com đúng là thư rác nhưng bạn muốn đọc thư này vì nó chứa các nội dung quảng cáo bạn quan tâm).

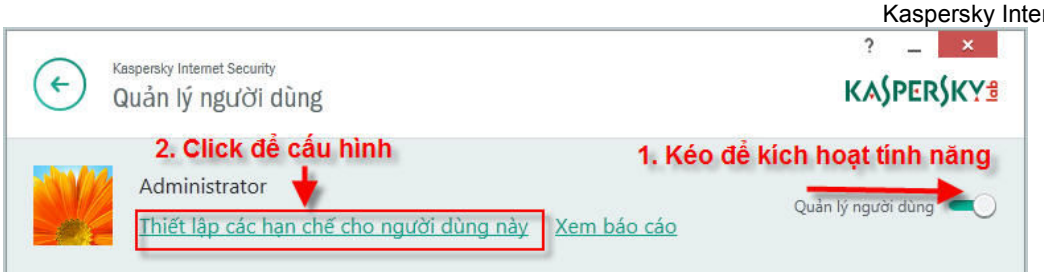
10. Cấu hình tính năng Quản lý người dùng (Parental Control)

Tính năng Quản lý người dùng giúp các bậc cha mẹ quản lý thời gian và nội dung truy cập Internet của con cái mình. Những trang web sex, cờ bạc, bạo lực sẽ bị cấm truy cập, bạn cũng có thể đặt ra lịch khoảng thời gian nào được phép truy cập Internet, truy cập máy tính của con cái. Bạn cũng có thể giám sát lịch sử truy cập web, ứng dụng của con mình

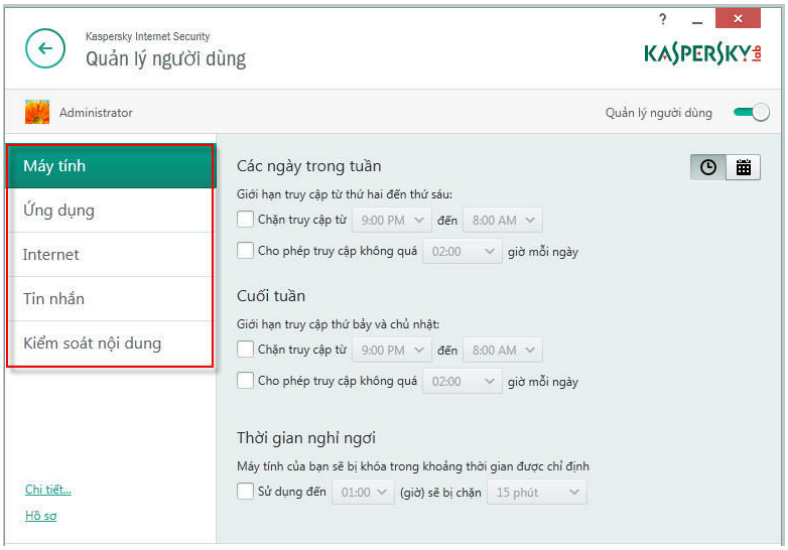
Mặc định tính năng này không được kích hoạt, để cấu hình, bạn vào giao diện chính của chương trình > Chọn **Quản lý người dùng** > giao diện tiếp theo, bạn điền vào mật khẩu và chọn **Tiếp tục** > Tiếp theo bạn chọn phạm vi áp dụng của mật khẩu > chọn **Tạo mật khẩu** (hình dưới).



Bước tiếp theo, danh sách các account trên máy tính sẽ hiển thị. Bạn muốn cấu hình quản lý account nào thì tiến hành kích hoạt tính năng, sau đó click chuột vào account để cấu hình (hình dưới)



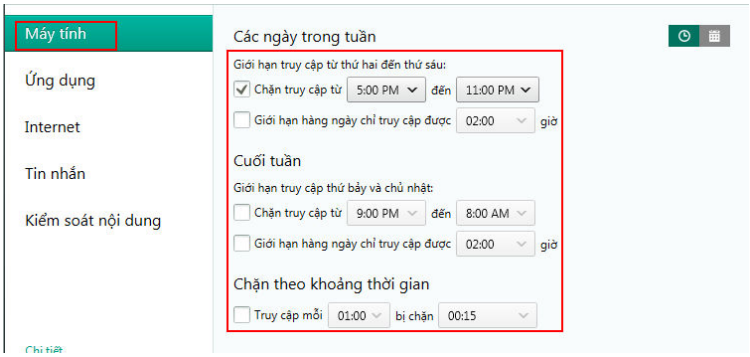
Giao diện tiếp theo bạn chọn mục cần cầu hình (hình dưới)



Cấu hình thời gian con cái được phép sử dụng máy tính

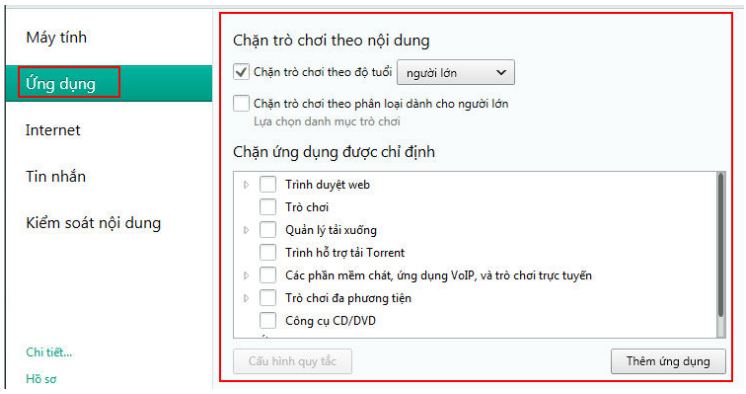
Bằng cách cấu hình trong phần **Máy tính**, bạn có thể đặt ra chính sách khoảng thời gian nào trong ngày con bạn được phép sử dụng máy tính. Hình dưới cấu hình khoảng thời gian từ 5h tối đến 11h tối, từ thứ 2 đến thứ 6, con bạn không được phép sử dụng máy tính (khoảng thời gian còn lại được phép sử dụng)

Ngoài ra, bạn cũng có thể giới hạn tổng thời gian sử dụng máy tính hàng ngày được phép bằng cách chọn vào dòng **Giới hạn hàng ngày chỉ truy cập được** sau đó chỉ định số giờ (Ví dụ: bạn cho con bạn một ngày chỉ truy cập máy tính 2h. Lúc này Kaspersky chỉ cho con bạn truy cập máy tính trong 2h/ngày – con bạn có thể truy cập vào nhiều thời điểm trong ngày nhưng tổng thời gian không được phép quá 2h/ngày, nếu tổng truy cập quá 2h/ngày > máy tính sẽ bị khóa truy cập). Bạn cũng có thể cấu hình chặn truy cập theo khoảng thời gian (Ví dụ: Truy cập mỗi 1h sẽ bị chặn trong 15 phút)



Cấu hình ngăn trò chơi hoặc ứng dụng con cái không được phép sử dụng

Bằng cách cấu hình trong phần **Ứng dụng** > bạn có thể chặn các game, các ứng dụng mà con bạn không được phép chạy (có thể ngăn theo phân loại độ tuổi hoặc theo phân loại danh mục – được phân loại sẵn bởi Kaspersky, bạn cũng có thể chỉ định theo ý bạn)

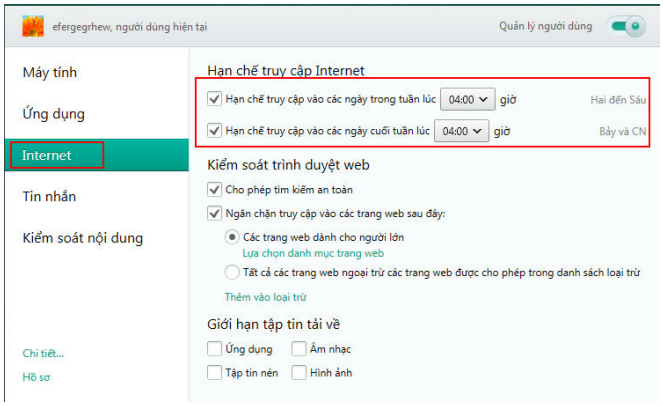


Cấu hình thời gian con cái được phép truy cập Internet

Tạo ra chính sách giúp bạn quản lý thời gian được phép truy cập Internet của con cái. Cấu hình thời gian được phép sử dụng Internet khác với thời gian sử dụng máy tính ở chổ:

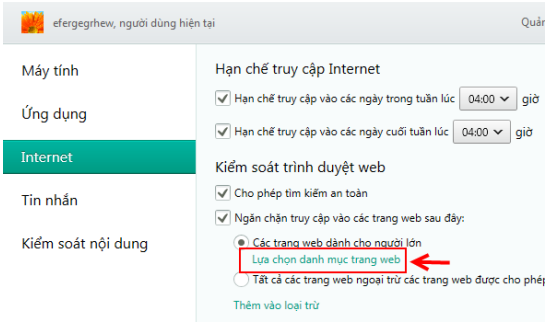
- ✓ Không cho sử dụng máy tính > sẽ ngăn không cho con bạn đăng nhập vào máy tính
- ✓ Không cho sử dụng Internet > vẫn đăng nhập được vào máy tính bình thường nhưng ngăn không có khả năng truy cập Internet.

Cấu hình: Vào phần **Internet** > Hình dưới đang cấu hình chỉ cho phép truy cập internet mỗi ngày 4 giờ



Chặn các trang web nguy hiểm theo chuẩn quốc tế của Kaspersky Lab

Trong phần **Internet** > chọn **Lựa chọn danh mục trang web** > tại đây bạn có thể cấu hình ngăn các trang web không được phép truy cập theo phân loại đánh giá sẵn có của Kaspersky (hình dưới)

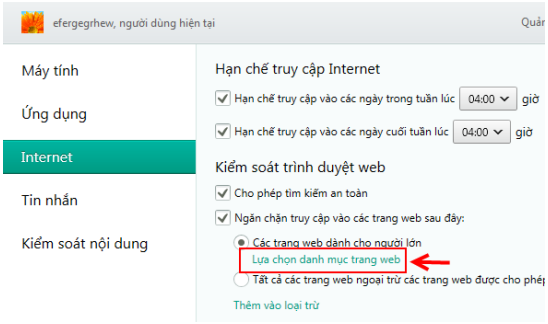


Chặn các trang web theo chính sách riêng của bạn

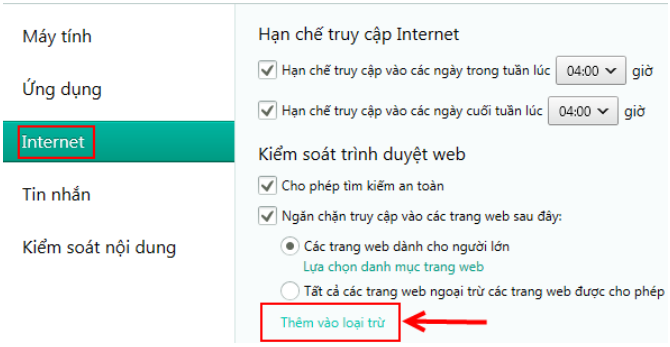
Ngoài việc chặn dựa theo chuẩn đánh giá, phân loại của Kaspersky ở trên, bạn cũng có thể chặn theo các chính sách riêng của bạn:

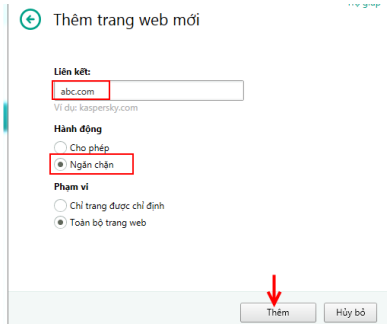
- ✓ **Chính sách 1: Ngăn chặn truy cập một số trang web chỉ định nào đó, các trang web còn lại được phép truy cập**.

Cấu hình: Vào phần **Internet** > Click **Lựa chọn danh mục trang web** > Bạn check bỏ hết các dòng > Sau đó bỏ chọn hết tất cả danh mục



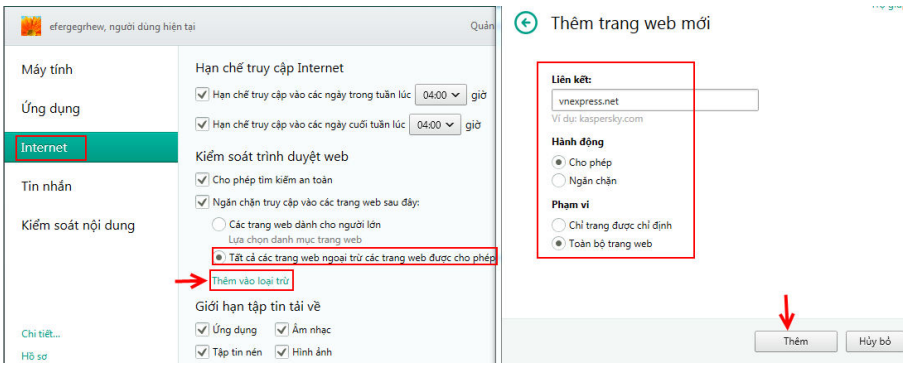
Tiếp theo trong bạn chọn vào dòng **Thêm vào loại trừ** > chọn **Thêm** > sau đó điền vào địa chỉ trang web cần ngăn truy cập sau đó chọn **Ngăn chặn** > cuối cùng chọn **Thêm** để hoành thành thao tác (hình dưới)





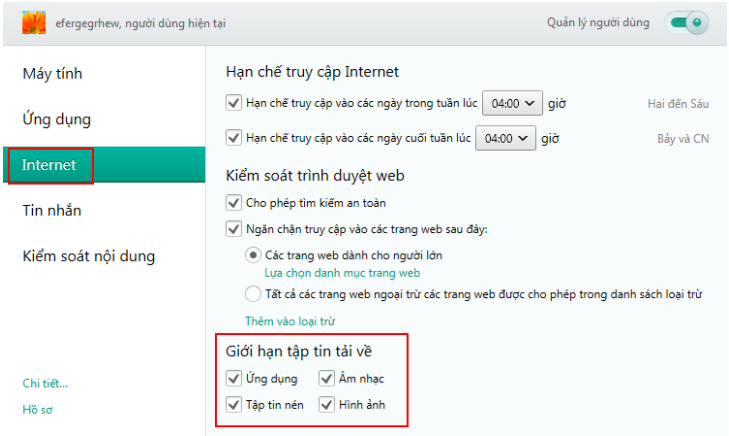
- ✓ **Chính sách 2: Chỉ cho truy cập những trang web mà bạn cho phép, tất cả các trang web còn lại sẽ bị ngăn lại**.

Cấu hình: Vào phần **Internet** và cấu hình như hướng dẫn bên dưới. Lúc này con bạn chỉ được truy cập các trang web mà bạn đã cấu hình cho phép, tất cả các trang web còn lại sẽ bị ngăn truy cập



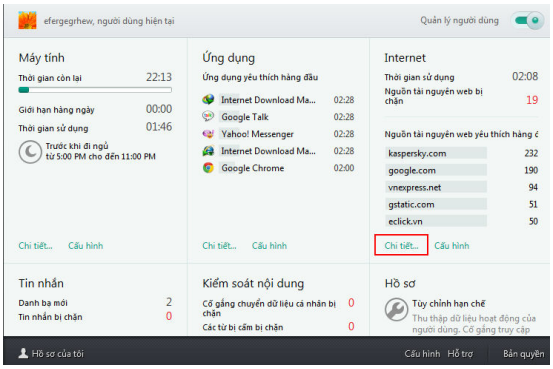
Ngăn không cho tải tập tin nhạc, phim, hình ảnh, ứng dụng, tập tin nén

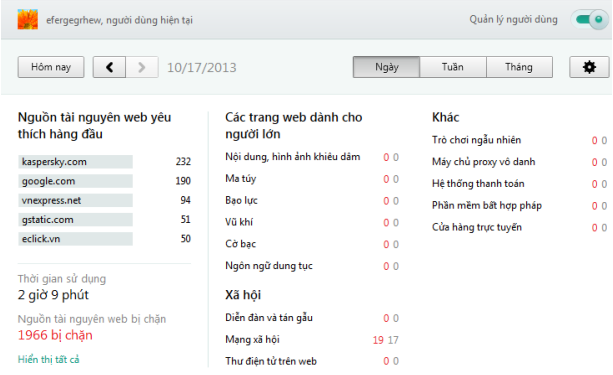
Bạn cũng có thể cấu hình ngăn không cho con bạn tải về các tập tin ứng dụng (định dạng .exe, tập tin nhạc, phim ảnh, hình ảnh, tập tin nén). Bạn vào phần **Internet** để tiến hành cấu hình như hình bên dưới.



Xem báo cáo Quản lý người dùng

Tất cả các sự kiện ngăn chặn của tính năng Kiểm soát người dùng đều được lưu lại trong phần **Báo cáo**. Để xem báo cáo bạn Mở giao diện chính của chương trình Kasperksy > chọn **Hiển thị công cụ bổ sung** > Phần **Quản lý người dùng** > Chọn account đang cấu hình kiểm soát > Chọn **Chi tiết** vào nội dung mà bạn muốn xem báo cáo > Hình dưới cho thấy bạn xem báo cáo về tình hình duyệt Web, bạn có thể xem chi tiết các trang web mà con mình đã truy cập, các ứng dụng mà con mình đã sử dụng, lịch sử truy cập máy tính, internet,…việc xem trong phần Báo cáo có thể giúp bạn quản lý tốt được con cái mình, phát hiện nhanh các vấn đề nguy hiểm có thể xảy ra với con mình và từ đó giúp bạn đề ra các hướng quản lý truy cập internet cho con mình





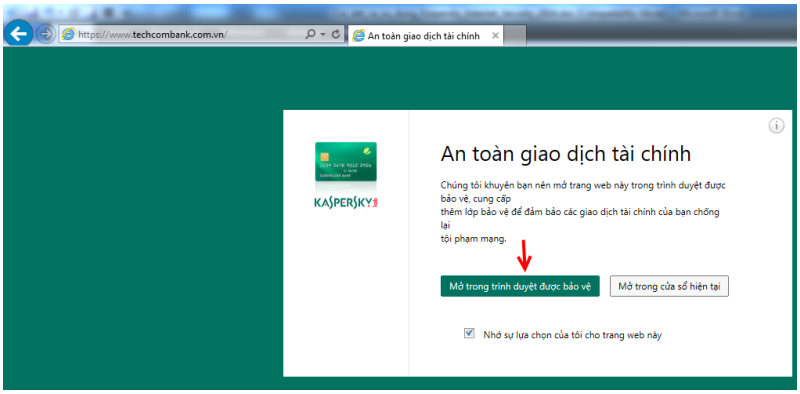
11. Cấu hình tính năng An toàn giao dịch tài chính

Tính năng An toàn giao dịch tài chính cho phép tự động chạy các trang web internet banking, mua hàng trực tuyến trong một chế độ chạy an toàn. Khi trang web chạy trong chế độ an toàn, phần mềm độc hại và tội phạm mạng không có cách nào có thể lấy đi các thông tin quan trọng bao gồm cả tiền bạc của bạn. Tính năng này mặc định được kích hoạt và hiện tại cơ sở dữ liệu sẵn có đã có nhiều trang web ngân hàng và mua hàng trực tuyến tại Việt Nam. Ngoài ra, bạn có thể thêm bằng tay một trang web chỉ định nào đó

Lưu ý: Để đảm bảo tính năng này chạy đúng cách > bạn phải vào phần quản lý Add-ons của các trình duyệt Internet và cho phép Add-ons: **Sale Money Plugin** (hoặc **An toàn giao dịch tài chính**)

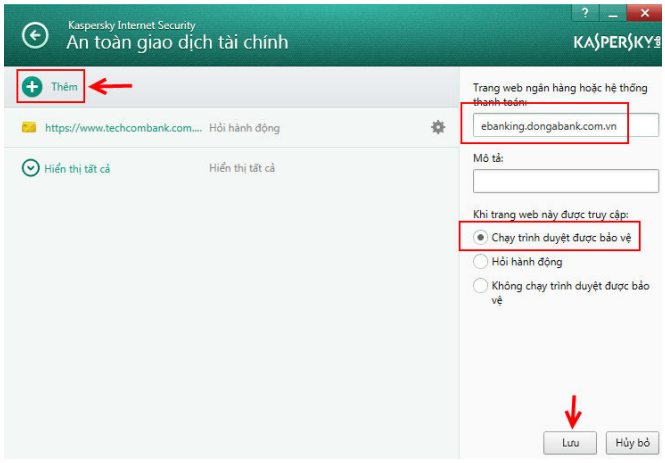
Vd: Khi truy cập trang web internet banking của Vietcombank https://www.techcombank.com.vn > giao diện như hình bên dưới xuất hiện, nếu bạn muốn chạy an toàn trang web này bạn chọn **Mở trong trình duyệt**

được bảo vệ, nếu không muốn chạy an toàn bạn chọn **Mở trong cửa sổ hiện tại** > mặc định Kaspersky sẽ nhớ sự lựa chọn này của bạn cho những lần truy cập sau này (vì dòng **Nhớ sự lựa chọn của tôi cho trang web này** mặc định được chọn) (hình dưới)

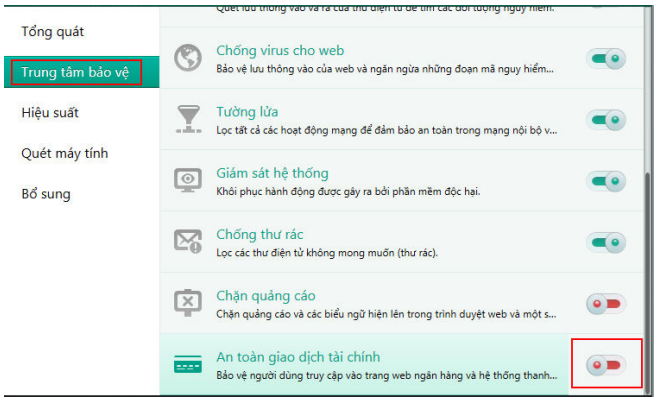


Lúc này, trang web được chạy trong chế độ an toàn (viền xanh lá cây bao quanh trình duyệt web)

Trường hợp bạn có một trang web ngân hàng trực tuyến mà bạn muốn chạy an toàn nhưng trang web này không có sẵn trong cơ sở dữ liệu của chương trình Kaspersky > bạn có thể Thêm vào bằng tay bằng cách > mở giao diện chính của chương trình > chọn **An toàn giao dịch tài chính** > chọn **Thêm** > điền vào trang web (hình dưới)

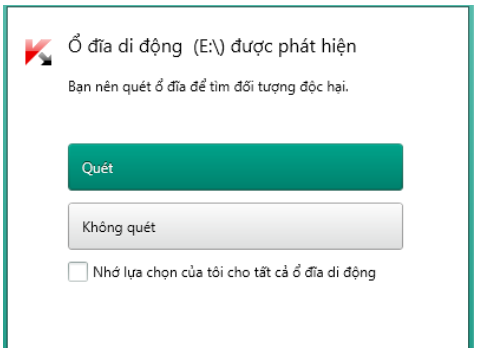


Trường hợp bạn không muốn sử dụng tính năng này, bạn có thể tắt nó đi bằng cách: mở giao diện chính của chương trình > chọn **Cấu hình** > chọn **Trung tâm bảo vệ** > đi đến phần **An toàn giao dịch tài chính** > kéo thanh tắt tính năng

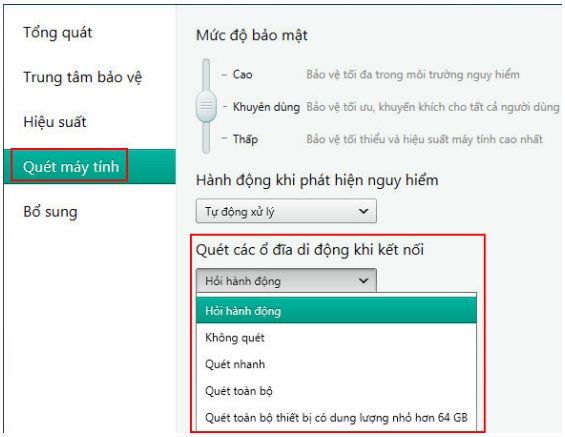


12. Tùy chỉnh quét virus ổ đĩa di động

Mặc định khi bạn gắn USB vào máy tính, một giao diện hiện như hình bên dưới xuất hiện yêu cầu bạn chọn hành động: Quét hoặc không quét ổ đĩa. Bạn có thể chọn vào dòng **Nhớ lựa chọn của tôi cho tất cả các ổ đĩa di động** để nhớ lại hành động này (lần sau sẽ không xuất hiện giao diện này)



Ngoài ra, bạn có thể tùy chỉnh tính năng này bằng cách: Mở giao diện **Cấu hình** của chương trình > Đến phần **Quét máy tính** > Trong phần **Quét các ổ đĩa di động khi kết nối** (hình dưới).



- ✓ Nếu chọn **Không quét**: Khi cắm USB vào máy tính, chương trình sẽ không hiện lên giao diện yêu cầu quét dữ liệu trong USB.

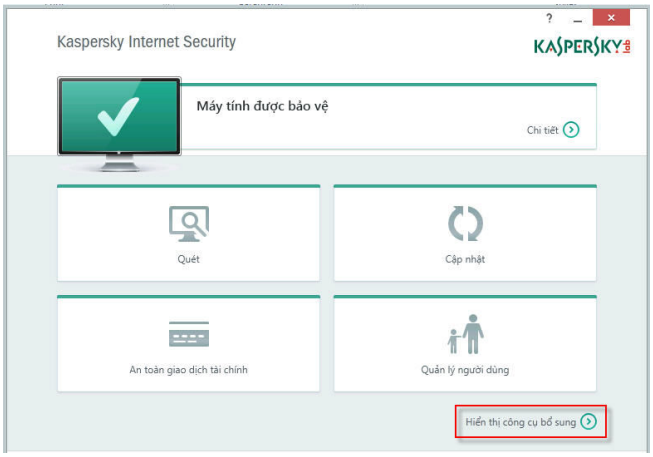
- ✓ Nếu chọn **Hỏi hành động** (đây là tùy chọn mặc định của chương trình): khi cắm USB vào máy tính, một giao diện hỏi hành động sẽ hiện lên (hình trên).
- ✓ Nếu chọn **Quét toàn bộ**: khi cắm USB vào máy tính, Kaspersky sẽ quét toàn bộ dữ liệu của USB
- ✓ Nếu chọn **Quét nhanh**: khi cắm USB vào máy tính, Kaspersky sẽ quét nhanh USB (bỏ qua một số định dạng tập tin).

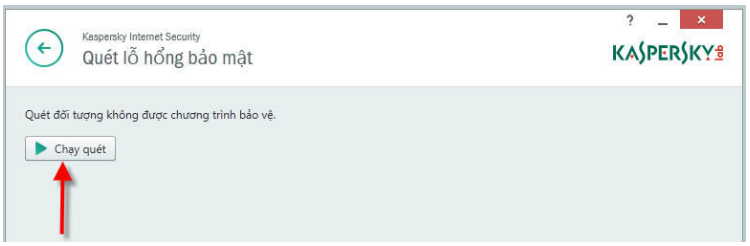
Lưu ý: Dù bạn chọn chế độ Không quét dữ liệu chứa trong USB > Kaspersky vẫn bảo vệ máy tính của bạn trong thời gian thực trước sự tấn công của virus từ USB (khi virus cố gắng lây nhiễm từ USB đến hệ điều hành sẽ bị Kaspersky tiêu diệt).

13. Quét lỗ hổng bảo mật

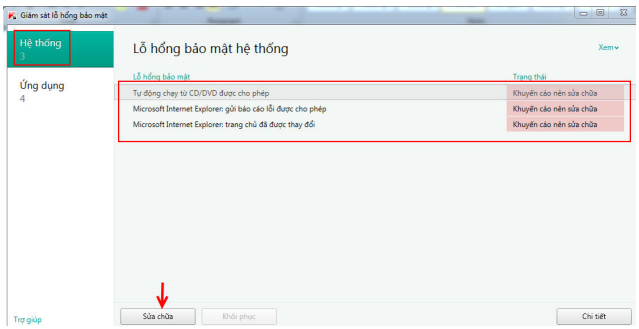
Tính năng quét lỗ hổng bảo mật của Kaspersky giúp quét toàn bộ hệ điều hành và ứng dụng trên máy tính, giúp bạn dò tìm tất cả các lỗi bảo mật hiện có trên máy tính. Lỗ hổng bảo mật là một trong những nguyên nhân chính để virus và hacker khai thác nhằm lây nhiễm, chiếm quyền điều khiển, lấy đi dữ liệu cá nhân quan trọng trên máy tính của bạn. Hạn chế càng ít lỗ hổng bảo mật là một cách phòng chống virus và hacker rất hiệu quả. Sau khi phát hiện lỗ hổng bảo mật, Kaspersky sẽ cung cấp cho bạn khả năng sửa chữa nhanh chóng bằng một cú click hoặc cung cấp đường link để tải về các bản vá lỗi.

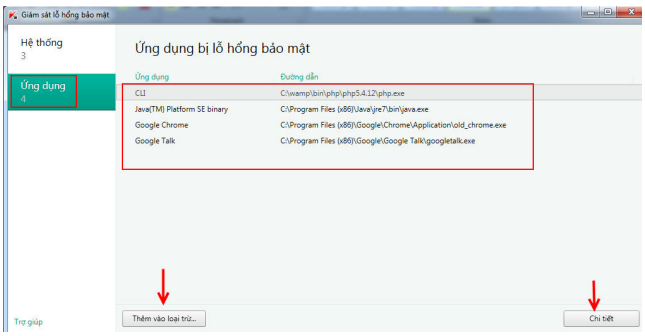
Tiến hành quét lỗ hổng: Mở giao diện chính của chương trình > Chọn **Công cụ** > Tại **Quét lỗ hổng bảo mật** > chọn Chạy quét > sau đó chờ đợi chương trình quét





Sau khi chờ đợt quét xong, bạn chọn **Xóa lỗ hổng bảo mật** > tại **Hệ thống** sẽ hiển thị một số lổ hỏng bảo mật của hệ điều hành đã được Kaspersky phát hiện. Bạn bấm **Sửa chữa** để sửa lỗi, bấm vào **Chi tiết** để đi đến phần mô tả chi tiết về lỗ hổng (hình dưới)



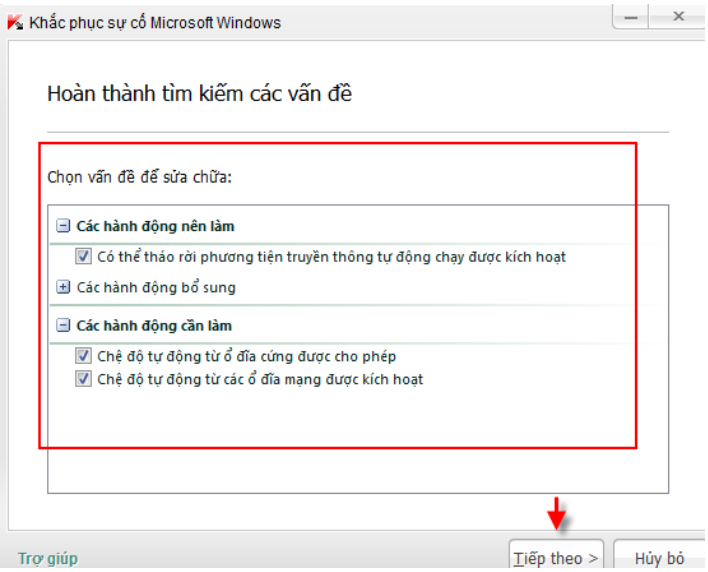


Tại thẻ **Ứng dụng** bạn sẽ thấy được những ứng dụng đang có lỗ hổng bảo mật > bấm vào **Chi tiết** để đi đến phần mô tả chi tiết về lỗ hổng, bao gồm cả đường link tải về bản vá lỗi. Chọn **Thêm vào loại trừ** nếu bạn muốn bỏ qua lỗ hổng này, sau này Kaspersky sẽ không thông báo về lỗ hổng này (hình trên).

14. Sửa lỗi cấu hình hệ điều hành Windows

Trường hợp máy tính của bạn bị nhiễm virus nặng trước khi cài Kaspersky vào máy. Sau khi cài Kaspersky vào và diệt sạch virus, tuy nhiên virus đã thay đổi một số tùy chỉnh của hệ điều hành (không cho hiện tập tin ẩn, truy cập Internet bị chặn,…) làm cho hệ điều hành hoạt động không đúng cách mà bạn không biết cách để khắc phục lỗi. Tính năng Sửa lỗi cấu hình Windows sẽ giúp ích cho bạn trong trường hợp này, giúp bạn khôi phục một số tùy chỉnh của hệ điều hành Windows về mặc định.

Mở giao diện chính của chương trình > Chọn **Công cụ** > Tại phần **Khắc phục sự cố Microsoft Windows** > Chọn **Bắt đầu**. Sau khi thực hiện xong thao tác, bạn sẽ thấy Kaspersky thông báo các hành động cần được sửa chữa > bạn đánh dấu chọn hết (hoặc chỉ chọn các lỗi mà bạn cần sửa) > sau đó bấm **Tiếp theo** để hoàn thành thao tác (hình dưới).



15. Xóa lịch sử hoạt động

Bạn muốn xóa tất cả lịch sử hoạt động của bạn: bao gồm lịch sử truy cập dữ liệu trên máy tính (các tập tin đã mở, các yêu cầu tìm kiếm, các ứng dụng đã chạy,…) cũng như lịch sử truy cập Internet. Mở giao diện chính của chương trình > Chọn **Công cụ** > Chọn **Xóa thông tin cá nhân**. Tại đây, bạn có thể chọn các đối tượng cần xóa.

16. Tinh chỉnh khả năng bảo mật của trình duyệt Internet

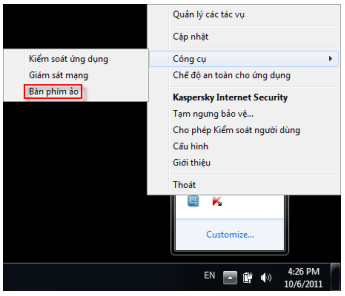
Tính năng này giúp bạn tìm ra lỗi bảo mật của trình duyệt Internet Explorer (IE) cũng như những tùy chỉnh không chính xác của IE. Mở giao diện chính của chương trình -> Chọn **Công cụ** -> Chọn **Cấu hình trình duyệt**. Kaspersky sẽ đưa ra các khuyến cáo mà bạn nên làm để tinh chỉnh trình duyệt IE trở nên bảo mật hơn. Bạn đánh dấu chọn những hành động nên làm để cho chương trình sửa chữa.

17. Bảo mật dữ liệu nhập từ bàn phím và Sử dụng bàn phím ảo

Mặc định Kaspersky bảo vệ dữ liệu nhập vào từ bàn phím thật chống lại việc lưu lại thao tác gõ phím của keglogger thông qua tính năng Bảo mật dữ liệu nhập từ bàn phím. Tính năng này mặc định được cho phép, để

tiến hành tùy chỉnh các loại trang web được bảo vệ, bạn mở giao diện **Cấu hình** > chọn **Bổ xung** > chọn **Bảo mật dữ liệu nhập vào** > trong phần **Bảo mật dữ liệu nhập từ bàn phím** chọn **Chỉnh sửa loại** > tại đây bạn sẽ tùy chọn các loại trang web sẽ được bảo mật khi bạn nhập dữ liệu từ bàn phím (hình dưới)

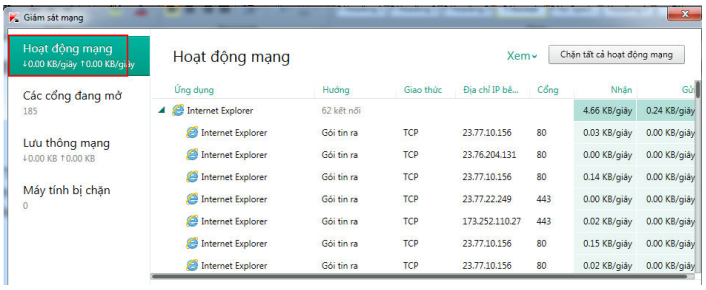
Ngoài ra, tính năng bàn phím ảo hỗ trợ thêm sẽ giúp bạn gia tăng mức bảo mật khi đăng nhập vào địa chỉ email, tài khoản game online, tài khoản ngân hàng vì các chương trình keylogger không thể nào lưu lại các thao tác gõ phím khi bạn sử dụng bàn phím ảo. Nhấn chuột phải vào biểu tượng Kaspersky chọn **Công cụ** > chọn **Bàn phím ảo.**

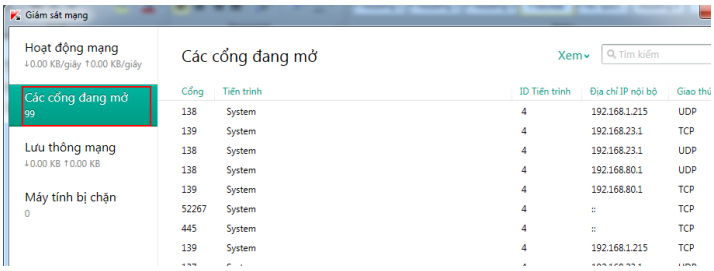


Ngoài cách sử dụng bàn phím ảo ở trên, bạn có thể cấu hình cho Bàn phím ảo xuất hiện trên giao diện các trang web bằng cách vào giao diện **Cấu hình** > chọn **Bổ xung** > chọn **Bảo mật dữ liệu nhập vào** > trong phần **Bàn phím ảo** bạn chọn **Chỉnh sửa loại** > chọn các loại trang web sẽ cho xuất hiện (hình dưới). Ví dụ bên dưới, khi truy cập vào địa chỉ mail yahoo, bạn sẽ thấy xuất hiện biểu tượng bàn phím ảo tại ô nhập ID và Password (hình dưới)

18. Sử dụng công cụ giám sát mạng

Tính năng này giúp bạn giám sát lưu lượng vào và ra máy tính. Rất hữu ích cho bạn để đánh giá tình hình hoạt động của máy tính (có cổng nào lạ đang hoạt động không? có chương trình nào đang kết nối đến địa chỉ lạ không?) Nhấn chuột phải vào biểu tượng Kaspersky chọn **Công cụ** > chọn **Giám sát mạng**.





19. Sử dụng Kaspersky Rescue Disk

Trường hợp máy tính của bạn bị nhiễm virus nặng (virus lây nhiễm sâu vào hệ thống) bạn có thể sử dụng đĩa cứu hộ - Kaspersky Rescue Disk để quét qua toàn bộ máy tính.

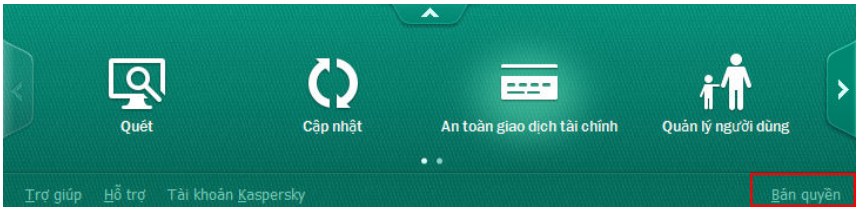
- ✓ Cách 1: Mặc định đĩa bản quyền Kaspersky có chứa sẵn Kaspersky Rescue Disk. Bạn bỏ đĩa vào máy tính > khởi động lại hệ điều hành > vào Safe Mode để cho máy tính khởi động từ ổ đĩa CD/DVD > sau khi máy tính khởi động từ đĩa cứu hộ bạn chọn Scan để quét toàn bộ máy tính
- ✓ Cách 2: Truy cập http://rescuedisk.kaspersky-labs.com/rescuedisk/updatable/kav_rescue_10.iso để tải về đĩa Kaspersky Rescue Disk > đây là một tập tin ISO, sau khi tải về bạn tiến hành ghi tập tin ISO ra đĩa CD
- ✓ Cách 3: Mở giao diện chính của chương trình chọn **Công cụ** -> **Tạo Kaspersky Rescue Disk** -> thực hiện theo các hướng dẫn dễ hiểu để tạo Kaspersky Rescue Disk.

20. Bật tính năng hỗ trợ trò chơi

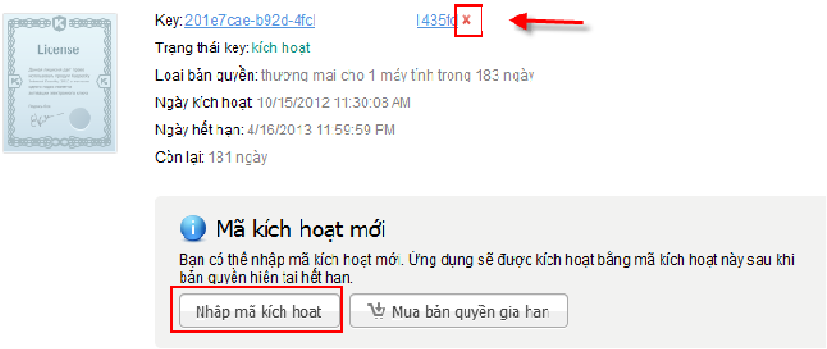
Khi bạn bật chế độ này thì chương trình Kaspersky sẽ không tiến hành cập nhật, không hiện giao diện yêu cầu xử lý khi phát hiện virus (Kaspersky sẽ tự động xử lý mã độc), không chạy các tác vụ quét theo lịch. Chế độ này sẽ giúp cho các game thủ yên tâm khi chơi game mà không sợ bị chương trình Kaspersky làm phiền. Vào giao diện cấu hình của chương trình > qua thẻ **Hiệu xuất** > chọn **Sử dụng Chế độ trò chơi** (như hình bên dưới).

21. Quản lý bản quyền - Kích hoạt bản quyền mới (trường hợp mua gia hạn)

Để xem và quản lý bản quyền hiện tại, bạn vào giao diện chính của chương trình > chọn **Bản quyền** như hình dưới.



Giao diện Quản lý bản quyền xuất hiện như hình dưới.

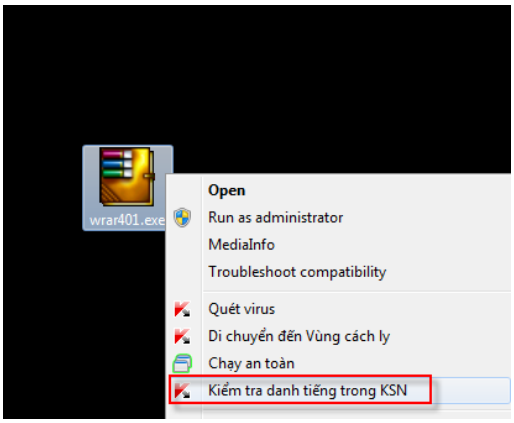


Tại đây, bạn có thể xem được thông tin ngày hết hạn của bản quyền. Nếu muốn xóa bản quyền hiện tại, bạn nhấn chuột vào biểu tượng **X**. Nếu muốn kích hoạt bản quyền mới > chọn **Nhập mã kích hoạt**.

22. Công nghệ điện toán đám mây KSN – Kiểm tra danh tiếng chương trình, tập tin cài đặt

Mạng bảo mật Kaspersky Network Security (KSN) là một công nghệ điện toán đám mây, cung cấp các thông tin cập nhật về tập tin, phần mềm và các mối nguy hiểm. Sử dụng dữ liệu từ mạng KSN để tăng tốc độ phản ứng với các mối đe dọa mới nhất, giảm nguy cơ nhận diện sai. Khi tham gia vào mạng KSN, thông tin về virus, phần mềm cài đặt trên máy tính, tập tin tải về,… sẽ tự động được gửi đến Kaspersky Lab. Mạng bảo mật này không thu thập và xử lý bất kỳ thông tin cá nhân riêng tư nào của người dùng. Mặc định khi cài đặt, có tùy chỉnh yêu cầu bạn cho ý kiến về việc có gia nhập mạng KSN hay không? Ngoài ra, nếu bạn không muốn gia nhập mạng KSN nữa, bạn có thể vào giao diện cấu hình của chương trình > chọn thẻ **Bổ xung** > chon **Phản hồi** > chọn **Vô hiệu**

Trường hợp bạn muốn kiểm tra danh tiếng, độ tin cậy của một phần mềm đã cài đặt trên máy tính hay một tập tin cài đặt của một phần mềm nào đó mà bạn vừa tải về từ Internet. Bạn chỉ cần nhấn chuột phải tập tin cài đặt hay shortcut của chương trình (hoặc tập tin chạy của chương trình) và chọn **Kiểm tra danh tiếng trong KSN**. Ngay lập tức, thông tin chi tiết của chương trình trên mạng KSN sẽ được hiển thị. Bạn sẽ biết được rằng chương trình đó có tin cậy hay không? số lượng người sử dụng có nhiều hay không?,..



IV. Thông tin hỗ trợ

Nâng cấp lên phiên bản mới miễn phí: Trong gian bản quyền còn hạn sử dụng, khách hàng được phép nâng cấp miễn phí lên phiên bản mới. Bạn có thể theo dõi về các phiên bản mới của Kaspersky Lab tại: www.kaspersky.vn. Bản quyền hiện tại sẽ vẫn dùng được để kích hoạt cho phiên bản mới.

Lưu ý: Bạn giữ thẻ bản quyền cẩn thận để dành kích hoạt trong trường hợp cài đặt lại Windows và Kaspersky.

Hỗ trợ kỹ thuật: Trong thời gian bản quyền còn hạn sử dụng, khách hàng được hỗ trợ kỹ thuật miễn phí. Kaspersky Việt Nam hỗ trợ đa kênh từ 8h sáng đến 22h đêm hàng ngày (kể cả thứ bảy và chủ nhật). Khi gặp bất cứ sự cố nào trong lúc sử dụng phần mềm, vui lòng liên hệ đến:

- ✓ Support qua điện thoại: Tổng đài 19001787
- ✓ Support qua email: support@kaspersky.vn
- ✓ Support qua Chát: Truy cập www.kaspersky.vn để chát với các nick hỗ trợ kỹ thuật
- ✓ Support qua diễn đàn: http://forum.kaspersky.vn

Lưu ý: Để được hỗ trợ nhanh chóng và đơn giản nhất, bạn vui lòng chụp ảnh màn hình thông báo lỗi, kèm một mô tả chi tiết về lỗi gặp phải và gửi đến email support@kaspersky.vn