

## Tổng hợp những phần mềm Anti-Ransomware hiệu quả

Cuộc khủng hoảng tấn công "khủng khiếp" mang tên mã độc WannaCry tới hệ thống an ninh mạng trên toàn thế giới cho thấy việc cài đặt các phần mềm chống mã độc, anti-ransomware là điều vô cùng cần thiết.

Virus, malware, ransomware,... là những mối nguy hiểm luôn có thể tấn công hệ thống máy tính của bạn bất cứ lúc nào. Đặc biệt, những loại biến thể của mã độc ransomware ngày càng nguy hiểm như WannaCry là minh chứng rõ nhất, khi chúng đã làm tê liệt hệ thống máy tính toàn thế giới, đòi tiền chuộc dữ liệu. Vì vậy, để hạn chế khả năng máy tính bị nhiễm virus hoặc bị tấn công bởi các loại mã độc, người dùng cần cài đặt những phần mềm anti-virus, anti-ransomware. Bạn đọc có thể tham khảo một số những phần mềm chống mã độc mà Quản trị mạng giới thiệu dưới đây.

### 1. BitDefender Antivirus Plus 2017:

BitDefender là công cụ phòng chống mã độc tổng tiền và virus mạnh mẽ. Phần mềm xây dựng một hệ thống bảo vệ chặt chẽ, tiên tiến để chống lại mọi loại virus, phần mềm gián điệp hoặc những loại mã độc tổng tiền nhưng không làm ảnh hưởng đến tốc độ làm việc của máy tính.



Thông thường các loại ransomware sẽ tìm kiếm các tệp mở rộng cụ thể, các vị trí file phổ biến khác để tấn công và xâm nhập sâu hơn vào máy tính. Và BitDefender có khả năng ngăn chặn mọi hành động truy cập trái phép vào những thư mục mà người dùng đưa chúng vào vòng bảo vệ, như Documents, Desktop, Pictures, Music và Videos hay các dịch vụ lưu trữ Dropbox và Google Drive.

Ngoài ra, phần mềm này còn kiểm soát mạng WiFi công cộng khi người dùng kết nối, từ đó ngăn chặn mọi nguy cơ tấn công hệ thống từ WiFi.

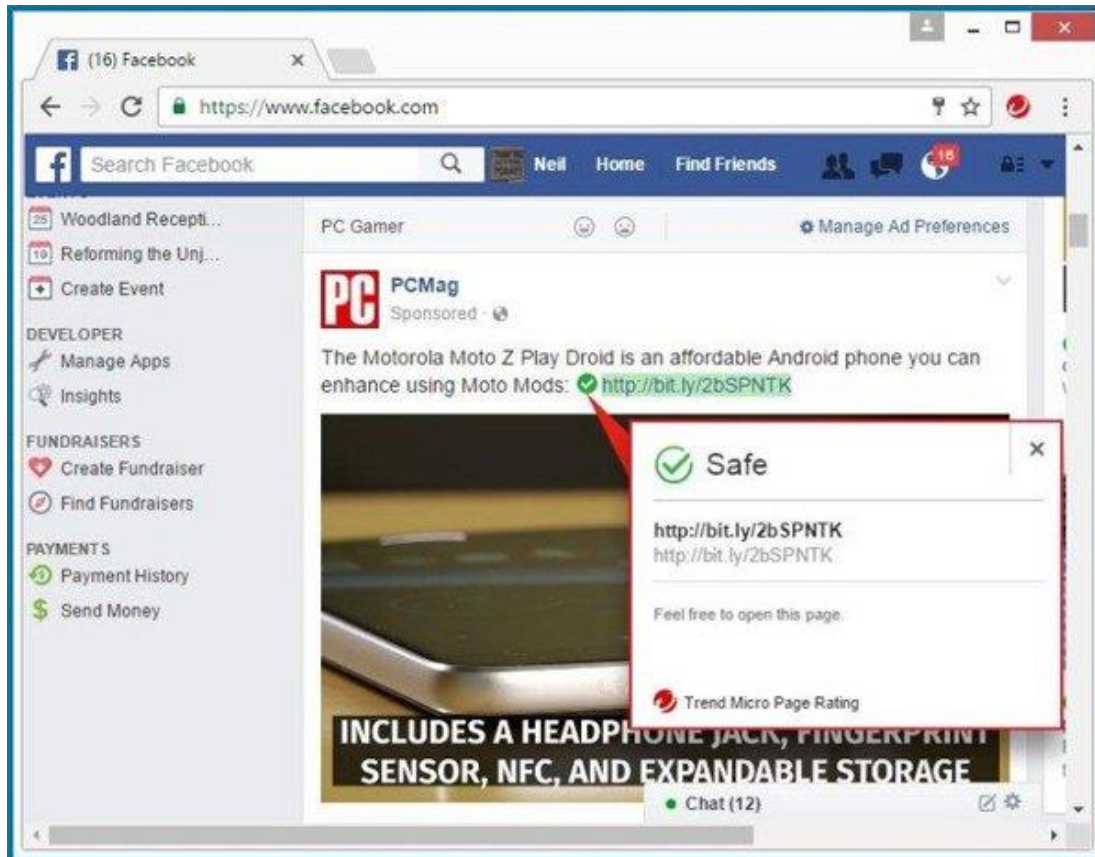
## 2. Trend Micro Antivirus+:

Phần mềm bảo mật này tập trung vào việc ngăn chặn sửa đổi thư mục trái phép, phân tích hành vi, phát hiện mã hóa và cách ly, sao lưu và khôi phục tập tin.



Trend Micro Antivirus sẽ bảo vệ thư mục Documents và các thư mục con mặc định. Ngoài ra, công cụ còn sở hữu hệ thống Smart Protection Network kiểm tra các mạng xã hội như Facebook, Twitter,... kiểm tra các link liên kết. Nếu phát hiện link đó có vấn đề, người dùng sẽ nhận được thông báo.

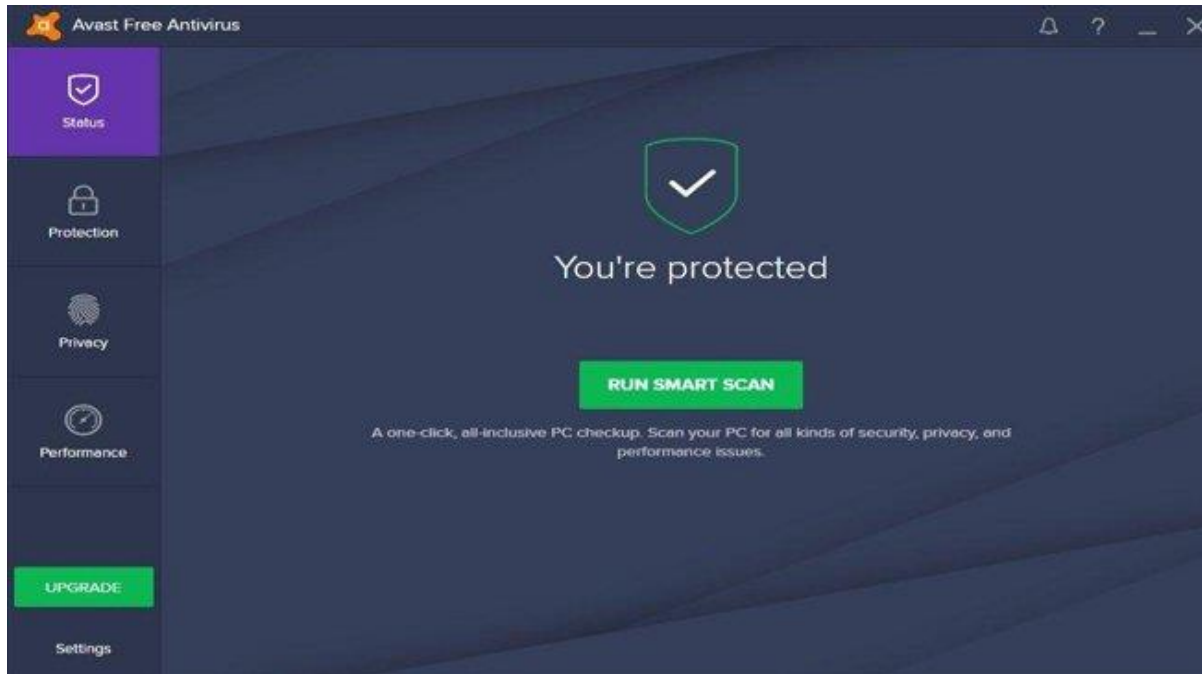
Đặc biệt, phần mềm còn cung cấp thêm lớp bảo mật cho tài khoản Facebook, ngoài việc bạn đã thiết lập bảo mật 2 lớp. Nó sẽ quản lý các cài đặt tài khoản, kiểm soát toàn bộ bạn bè tương tác với tài khoản Facebook.



### 3. Avast Free Antivirus 2017:

Avast Free Antivirus là cái tên quá quen thuộc trong lĩnh vực bảo mật, anti-virus cho máy tính. Mặc dù, phần mềm này tuy không có khả năng chống ransomware mạnh mẽ như các phần mềm trên, nhưng vẫn có thể đảm bảo sự an toàn chặt chẽ cho hệ thống.

Avast Free Antivirus sẽ tiến hành quét hệ thống, phát hiện những loại phần mềm độc hại gây rủi ro, chặn URL độc hại, theo dõi các hành vi ứng dụng để chắc chắn rằng những ứng dụng đó không bị xâm phạm đột ngột.



#### **4. Malwarebytes Anti-Ransomware Beta:**

Cũng như Avast Free Antivirus, Malwarebytes là thương hiệu tin cậy để bảo mật hệ thống. Phần mềm sẽ chạy ở chế độ nền, không ảnh hưởng đến hiệu suất của máy tính, tiến hành kiểm soát hệ thống từ đó phát hiện các loại ransomware dễ dàng.

Malwarebytes Anti-Ransomware có thể nhận biết và ngăn chặn nhiều chủng loại ransomware như CryptoWall4, CryptoLocker, Tesla và CTB-Locker. Ngoài ra, dung lượng của phần mềm tương đối nhẹ không chiếm quá nhiều tài nguyên của máy tính, như những chương trình anti-ransomware khác.



## 5. Kaspersky Anti-Ransomware Tool for Business:

Đây là phần mềm phát hiện và phòng chống mã độc dành cho các doanh nghiệp và máy tính cá nhân. Kaspersky Anti-Ransomware chủ yếu bảo vệ máy tính khỏi lỗ hổng trong giao thức chia sẻ dữ liệu SMB, giao thức mà WannaCry, EternalRocks lợi dụng để tấn công máy tính.

Kaspersky Anti-Ransomware Tool for Business KASPERSKY

Protection against ransomware is on

GET PREMIUM PROTECTION

Global Kaspersky Security Network in the last 24 hours

Number of threats neutralized: updating

Number of users connected to Kaspersky Security Network: updating

Global Kaspersky Security Network statistics

Whitelisted objects: updating

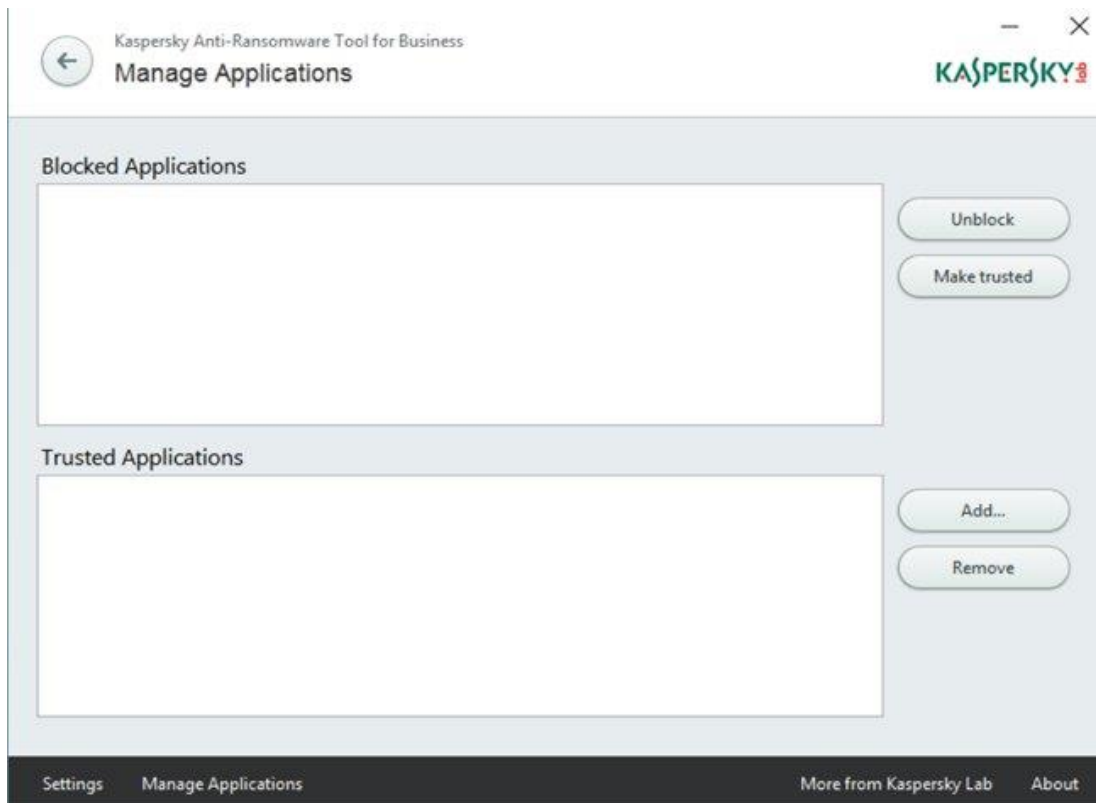
Blacklisted objects: updating

Objects categorized: updating

Kaspersky Security Network is a global, real-time cloud-based threat knowledge database operated by Kaspersky Lab.

Settings Manage Applications More from Kaspersky Lab About

Sau khi cài đặt trên máy tính, công cụ sẽ chạy nền trên hệ thống và giám sát mọi hành vi trên máy tính, phát hiện những loại ransomware độc hại. Ngoài ra, phần mềm còn có tính năng quản lý những chương trình cài đặt độc hại, giúp người dùng dễ dàng thêm hoặc loại bỏ các chương trình được xếp vào diện an toàn trên máy tính hay không.



## 6. Cybereason RansomFree:

Công cụ chống mã độc RansomFree đến từ Cybereason sở hữu giao diện đơn giản, với tính năng chính là phát hiện và bảo vệ máy tính khỏi những đợt tấn công của mã độc tống tiền.

Đặc biệt, phần mềm sẽ tạo ra những tập tin môi ở những vị trí mà ransomware thường xuyên tiến hành mã hóa. Từ đó, RansomFree sẽ dựa vào những tập tin này để phát hiện những hành vi bất thường, ngăn chặn ransomware ngay sau đó trước khi nó tiến hành tiếp công đoạn mã hóa.

The screenshot shows a dark-themed notification window from cybereason.com. At the top left is the cybereason logo, and at the top right is the website URL. The main heading reads "Ransomware activity has been detected!" with a shield icon containing a padlock. Below this, a message states: "c:\python27\python.exe (started on Thursday, Dec 15 at 4:04 PM) might be attempting to maliciously encrypt files on your hard drive and has been suspended." A sub-message follows: "If you recognize it as familiar and safe, click 'No'. If you are unsure, click 'Yes', to avoid the encryption of valuable files (e.g. documents, photos, videos, etc.)". A link "View affected files" with a right-pointing arrow is provided. The next section is titled "Stop & clean the threat?" and includes a note: "RansomFree will remember your selection for this threat. To clear selection history, right-click the tray icon and choose 'Clear history'". Two buttons are shown: a grey "No Let it run" button with a red 'X' icon, and a blue "Yes Stop & clean the threat" button with a white checkmark icon. At the bottom, there are three links: "Ransomware Blog", "Contact us", and "Q&A".

Trên đây là một số những phần mềm anti-ransomware hiệu quả, có tính năng bảo mật máy tính mạnh mẽ. Tuy có những cơ chế hoạt động và sở hữu các tính năng khác nhau, nhưng các chương trình này sẽ đều tập trung vào việc ngăn chặn những loại virus gây hại, các loại mã độc tổng tiền nguy hiểm như WannaCry hay EternalRocks.

Hy vọng bài viết trên hữu ích với bạn!