

Máy tính hiện nay là công cụ không thể thiếu trong cuộc sống hiện đại của chúng ta. Tuy nhiên, với sự phát triển của công nghệ và internet, việc bảo vệ máy tính khỏi hacker và virus là một thách thức phức tạp. Không chỉ gây ra thiệt hại cho máy tính, hacker và virus còn có thể truy cập, chiếm đoạt, và lợi dụng thông tin cá nhân của người dùng mà không được phép.

Để bảo vệ máy tính, người dùng cần phải có hiểu biết về các nguy cơ mà hacker và virus đem lại. Trong bài viết này, Vị Tính Quang Chính xin chia sẻ đến bạn đọc cách để bảo vệ máy vi tính của mình trước nguy cơ đánh cắp dữ liệu hiện nay.

[Cách bảo vệ máy tính khỏi hacker và virus](#)

Có một câu nói vui rằng Để không bị lây nhiễm virus thì ngắt kết nối khỏi mạng, không sử dụng ổ mềm, ổ USB hoặc copy bất kỳ file nào vào máy tính. Nhưng nghiêm túc ra thì điều này có vẻ đúng khi mà hiện nay sự tăng trưởng số lượng virus hàng năm trên thế giới rất lớn.

Không thể khẳng định chắc chắn bảo vệ an toàn 100% cho máy tính trước hiểm họa virus và các phần mềm độc hại, nhưng chúng ta có thể hạn chế đến tối đa có thể và có các biện pháp bảo vệ dữ liệu của mình.

Nguồn: <https://thumuavitinh.com/cach-bao-ve-may-tinh-khoi-hacker-va-virus>



Lướt web thông minh

Nhiều ứng dụng chống mã độc dành cho doanh nghiệp sẽ được tích hợp ngay trên trình duyệt web để giúp chống lại việc lây nhiễm từ các ổ đĩa, hoặc dùng để lọc các cuộc tấn công. Việc làm này nhằm tránh cho người dùng bị đánh cắp thông tin mật khẩu, tài chính hay dữ liệu nhạy cảm.

Người dùng không nên gõ bất kỳ thông tin cá nhân, tài chính hay tài khoản đăng nhập vào các trang web không đáng tin cậy. Đồng thời, không mở trực tiếp các đường dẫn đính kèm email.

Không kích vào các đường dẫn trên email hay trong tài liệu đính kèm

Người dùng không bao giờ được kích vào các file đính kèm email trước khi dùng các ứng dụng chống mã độc dành cho doanh nghiệp để quét. Thay vì kích vào đường dẫn đính kèm email, người dùng nên truy cập vào các trang Web này bằng cách mở trình duyệt và gõ địa chỉ trang đó vào.

Vô hiệu hóa tính năng xem trước hình ảnh trong Outlook

Khi thư điện tử chứa các hình ảnh bị nhiễm virus và ứng dụng Outlook cho phép người dùng xem trước hình ảnh trong đó thì đây là một cách khởi động cho virus lây nhiễm sang hệ thống PC người dùng. Vì vậy, để ngăn chặn việc lây nhiễm tự động, người dùng nên tắt chức năng xem trước hình ảnh trong Outlook.

Đối với các phiên bản mới của ứng dụng Microsoft Outlook sẽ không có chế độ tự động hiển thị hình ảnh. Nhưng nếu người dùng thay đổi các thiết lập bảo mật mặc định thì nên quay lại tắt chức năng này đi. Nếu dùng Outlook 2007, người dùng thực hiện các bước sau để tắt chức năng này: vào Tools | Trust Center, bật Automatic Download và lựa chọn Don't Download Pictures Automatically In HTML E-Mail Messages Or RSS.

[Cần thu mua máy tính cũ giá cao tphcm](#)

Liên hệ ngay [Vi Tính Quang Chính](#)

Sử dụng phần mềm diệt virus

Nhiều người sử dụng máy tính tin tưởng các ứng dụng diệt virus miễn phí có thể bảo vệ thiết bị của họ trước virus hay spyware. Tuy nhiên, các chương trình miễn phí này sẽ không cung cấp một sự bảo vệ đầy đủ cho các nguy cơ đang tăng lên hàng ngày.

Bảo vệ bằng cách trang bị thêm một phần mềm diệt virus có khả năng nhận biết nhiều loại virus máy tính và liên tục cập nhật dữ liệu để phần mềm đó luôn nhận biết được các virus mới.

Vì vậy, người dùng PC nên cài đặt các phần mềm diệt virus dành cho doanh nghiệp và chuyên nghiệp hơn trên máy tính của mình. Các chương trình diệt virus chuyên nghiệp sẽ được cập nhật hàng ngày nhằm chống lại những nguy cơ mới tấn công vào lỗ hổng của các phần mềm và hệ điều hành.

Trên thị trường hiện có rất nhiều phần mềm diệt virus.

Trong nước (Việt Nam): Bkav, CMC.
Của nước ngoài: Avira, Kaspersky, AVG, ESET.
Và phát hành bởi Microsoft: Microsoft Security Essentials.
Khi sử dụng phần mềm diệt virus, người dùng nên chú ý:

Đảm bảo chương trình chống mã độc luôn hoạt động

Các chương trình antivirus và anti-spyware yêu cầu việc cập nhật dữ liệu và đăng ký đều đặn. Nếu không cập nhật, các chương trình chống mã độc sẽ không có khả năng bảo vệ máy tính trước các nguy cơ tấn công mới. Nhiều cuộc tấn công diễn ra chỉ trong thời gian ngắn nhưng có sức lây nhiễm 100-300 nghìn trang web mỗi ngày. Vì vậy, người dùng nên cập nhật thường xuyên cho phần mềm diệt virus và spyware cũng như chú ý đến thời điểm hết hạn đăng ký của phần mềm này.

Thực hiện quét máy tính hàng ngày

Đôi khi, virus và spyware thoát khỏi vòng kiểm soát của phần mềm bảo vệ và lây nhiễm vào thiết bị. Vì vậy, việc quét hệ thống hàng ngày sẽ giúp phát hiện và loại bỏ được mầm lây nhiễm này ra khỏi máy tính.

Xem thêm

[Dịch vụ thu mua máy tính cũ giá cao tại tphcm](#)

<https://boosty.to/vitinhquangchinh/posts/5f901c4a-7467-4090-8330-31de2aa49dd9>