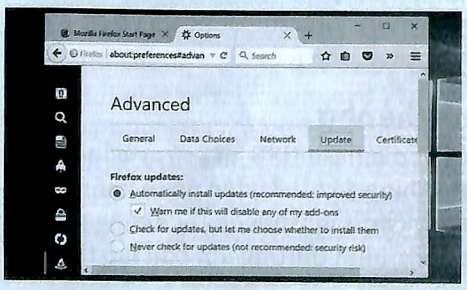
Thiết lập trình duyệt web an toàn hơn để không bị tấn công

Nếu bạn sử dụng một trình duyệt web không được thiết lập đúng cách, thì có thể bị tin tặc (hacker) khai thác các lỗ hổng bảo mật để tấn công vào máy tính của bạn. Từ đó, chúng sẽ lấy cắp những dữ liệu quan trọng, hoặc thậm chí là mã hóa toàn bộ dữ liệu trên máy tính của bạn rồi đưa ra thông báo đóng tiền chuộc dữ liệu. Vậy, một trình duyệt web được thiết lập như thế nào là an toàn?

1. Luôn giữ cho trình duyệt được cập nhật

Dù đang sử dụng trình duyệt web nào, bạn nên đặt vấn đề cập nhật phiên bản mới lên hàng đầu. Việc giữ cho trình duyệt luôn nhận được các cập nhật mới có thể sẽ giúp bạn không trở thành nạn nhân của tin tặc.

Bạn hãy sử dụng những trình duyệt web được nhiều người đánh giá cao. Nếu sử dụng máy tính chạy hệ điều hành Windows, bạn không nên chọn Safari làm trình duyệt mặc định bởi sự hạn chế cập nhật của nó. Bạn không nên sử dụng trình duyệt Internet Explorer phiên bản cũ trong Windows, bởi đây chính là yếu tố mà tin tặc có thể tấn công, do nó không được cập nhật các bản vá lỗi bảo mật.



Hiện nay, đa số người dùng đều chọn trình duyệt web Chrome của Google, hoặc Firefox của Moziila. Nhiều người sử dụng đồng thời 2 trình duyệt web này. Sở dĩ nó được người dùng ưu ái là nhờ được nhà phát triển liên tục tung ra các bản cập nhật. Hơn nữa, Firefox nay đã hỗ trợ người dùng hệ điều hành phiên bản 64bit.

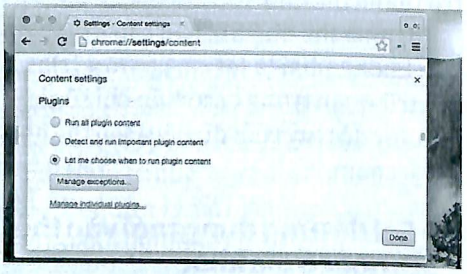
Trong trình duyệt web, bạn hãy kích hoạt tính năng tự động cập nhật và có thể hạn chế người khác sử dụng máy tính của mình để họ không thể tắt tính năng này.

Nếu là một "fan" của Microsoft, bạn hãy thử trải nghiệm trình duyệt web Microsoft Edge trên Windows 10. Hiện tại, trình duyệt này cũng được người dùng trên thế giới đánh giá tích cực.

2. Kích hoạt tính năng "ClicktoPlay"

Nếu muốn việc duyệt web và chơi những trò chơi trên nền web được mượt mà và nhanh hơn, bạn hãy chú ý tới công cụ mở rộng này. Nếu được kích hoạt lên, ClicktoPlay sẽ giúp bạn tải các trang web nhanh hơn và tiêu tốn ít tài nguyên CPU cũng như mức pin sử dụng (đối với laptop).

Ngoài ra, nó còn có những mặt tốt trong việc giữ an toàn cho bạn hơn. Cụ thể, những kẻ tấn công sẽ không thể nào lợi dụng các lỗ hổng trong các plug-in được tích hợp trong trình duyệt của bạn. Vì khi ClicktoPlay được mở, chỉ khi nào có sự đồng ý của bạn thì chúng mới được khởi chạy.

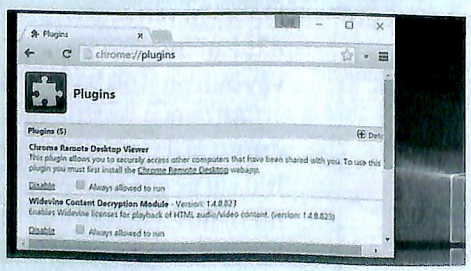


Chẳng hạn, đối với trình duyệt web Google Chrome. Bạn bấm nút menu hình 3 gạch ngang (nằm ở góc trên bên phải cửa sổ trình duyệt web), rồi chọn *Settings*. Trong cửa sổ hiện ra, bạn chọn *Show advanced settings*, rồi mục *Content settings* trong nhóm *Privacy*. Sau đó, bạn kéo thanh trượt để tìm nhóm *Plug-ins*, rồiđánh dấu chọn trước hàng chữ *Let me choose when to run plugin content.*

3. Gỡ bỏ các plug-in không cần thiết

Việc gỡ bỏ các plug-in không cần thiết hoặc không được nhà phát triển cập nhật sẽ giúp trình duyệt web trên máy tính bạn an toàn hơn.

Đơn cử, Java có lẽ plug-in ngày càng có ít website sử dụng hơn so với trước đây. Vì vậy, việc gỡ bỏ nó là yếu tố bạn nên làm. Ngay cả ứng dụng Flash Player cũng sắp bị thay thế bởi HTML5, thì có lẽ việc gỡ bỏ bớt những gì quá cũ sẽ an toàn hơn cho bạn.



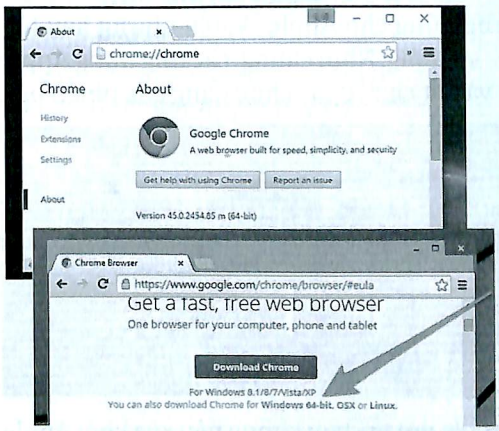
Tuy nhiên, bạn cần lưu ý, có thể một số website chưa ứng dụng công nghệ thiết kế mới. Vì vậy, trước khi gỡ bỏ bất kỳ plug-in nào, bạn hãy nên cân nhắc xem đã thực sự cần thiết hay chưa.

4. Sử dụng trình duyệt web 64bit

Ngày nay giá thành các linh kiện máy tính đã rẻ hơn rất nhiều so với trước đây. Việc sở hữu một máy vi tính có cấu hình tối thiểu 4GB RAM không còn vấn đề quá lớn. Vì vậy, việc chọn dùng hệ điều hành phiên bản 64bit để khai thác triệt để sức mạnh của phần cứng máy tính là cần thiết.

Khi đó, bạn sẽ cài được trình duyệt web phiên bản 64 bit để dùng. Nó được cho là sẽ ngăn ngừa được các nguy cơ tấn công mạng, và phòng chống việc lây lan mã độc tốt hơn.

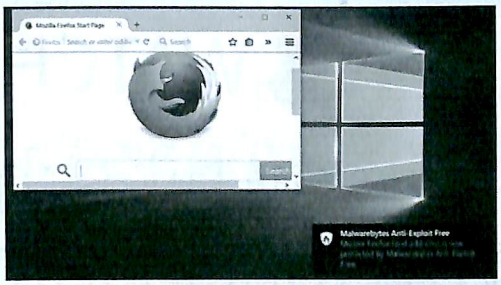
Hiện tại, Google Chrome đã có phiên bản 32bit và 64bit. Truy nhiên, đa phần người dùng đều chọn tải Chrome một cách tùy thích mà không biết ý thế mạnh của từng phiên bản. Để biết, trình duyệt web Chrome trên máy tính của mình là 32 bit hay 64 bit, bạn bấm menu của Chrome rồi chọn *Help> About Google Chrome*.



Nếu muốn dùng đúng phiên bản thích hợp với Windows 64bit đang cài trên máy tính, bạn hãy chọn tải về Chrome 64 bit.

5. Sử dụng các chương trình chống khai khác lỗ hổng

Nếu máy tính của bạn có cài phần mềm diệt virus thì chí ít chúng cũng sẽ bảo vệ bạn khi lướt web, hay nhận email. Tuy nhiên, điều này vẫn chưa đủ, bởiviệc khai thác lỗ hổng để tấn công người dùng thông qua các thông báo đăng nhập rất hay xảy ra. Do đó, bạn nên sử dụng thêm các công cụ chống khai thác lỗ hổng khác để chúng phân tích và ngăn chặn các hành vi bất thường, những trang web có yêu cầu lạ đối với người dùng.

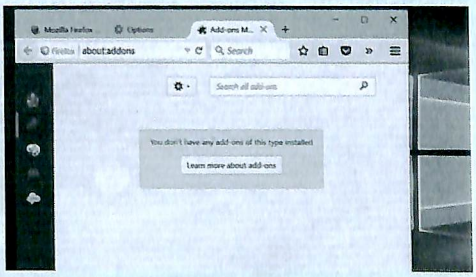


Hiện nay có 2 lựa chọn khá tốt, đó là Microsoft's EMET và Malwarebytes Anti-Exploit. Điểm cộng cho cả hai chương trình này là chúng đều miễn phí và tương thích với đa số trình duyệt web thông dụng.

Việc sử dụng chúng cũng không quá khó. Tuy nhiên, theo đa số người dùng thì Malwarebytes Anti-Exploit dễ sử dụng hơn so với Microsoft's EMET cả về tính năng cũng như giao diện.

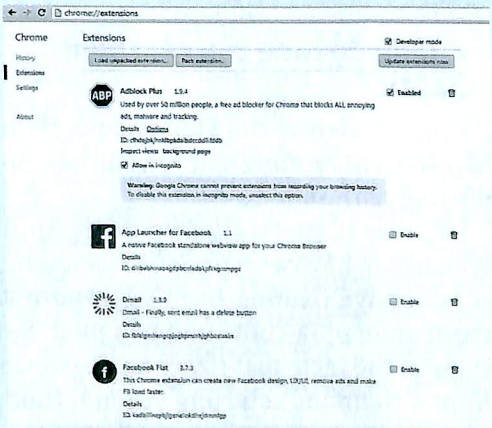
6. Thận trọng với các phần mở rộng cho trình duyệt web

Việc ra đời của các extensions (phần mở rộng tiện ích) thực sự là điều tuyệt vời cho người dùng máy tính. Bạn chỉ cần tải một tập tin dung lượng vài KB và cài đặt chúng vào trình duyệt web thông qua một số cú bấm chuột đơn giản là sử dụng được. Hiện nay, kho extension khá đa dạng, trong đó có tiện ích giúp bạn tùy biến trang web hiển thị, hay tối ưu những thao tác thường dùng khi lướt web. Đơn cử, có những extension sẽ giúp bạn chặn các pop-up quảng cáo khi vào các trang web.



Tuy vậy, cũng có không ít extension giả mạo, lừa đảo người dùng cài đặt. Nguy hiểm nhẹ thì chúng sẽ chạy quảng cáo ngầm trong máy tính của bạn. Nguy hiểm hơn thì chúng sẽ cài các malware hay rookit vào máy tính, từ đó khai thác dữ liệu quan trọng trên máy tính. Nặng nhất là chúng sẽ đánh cắp lịch sử duyệt web của bạn, hay các tài khoản cá nhân mà người dùng thường có thói quen cho phép trình duyệt web ghi nhớ để thuận tiện đăng nhập cho những lần sau.

Do vậy, rất khó để đưa ra lời khuyên extension nào là tốt, extension nào là độc hại không nên dùng. Điều này xuất phát từ sự cẩn thận của người dùng và thói quen của họ. Tốt nhất, hạn hãy chế sử dụng những phần mở rộng, chỉ sử dụng những extension thật cần thiết, không nên cài đặt quá nhiềuextension ít khi dùng đến.



Ngoài ra, trước khi cài một extension, bạn hãy tham khảo những đánh giá từ những trang web uy tín.

Hiện nay, bạn hãy cẩn thận với những phần mềm, hay trang web yêu cầu bạn sử dụng công cụ tải về của họ để lấy (download tiếp) phần mềm bạn đang cần, bởi hơn 90% trong số đó đều có chèn các phần mềm quảng cáo, lừa đảo.

VÕ TÌNH THƯƠNG *votinhthuong9@gmail.com*