Tăng cường khả năng bảo mật cho Google Chrome

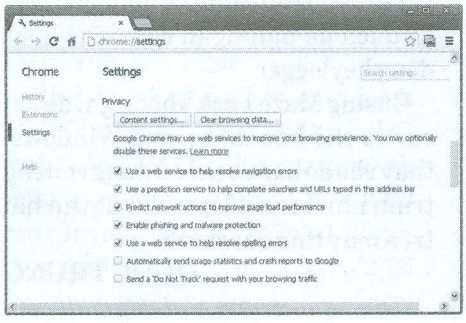
Có khá nhiều tính năng bảo mật hữu ích được tích hợp trong Google Chrome, điển hình là chức năng sandboxing độc đáo, hạn chế các đặc quyền và thậm chí ngăn chặn cả việc cập nhật nền, giúp bảo vệ bạn khỏi tin tặc và các phần mềm độc hại khai thác lỗ hổng của trình duyệt. Tuy nhiên, giống như tất cả các trình duyệt khác, Chrome vẫn không là hoàn hảo và bạn có thể phải thực hiện một số công việc để loại bỏ nguy cơ bị tấn công. Bài viết sau đây giới thiệu cách khắc phục những thiếu sót bảo mật của trình duyệt rất được ưa chuộng này.

• Các tính năng bảo mật trong Chrome

Chrome cung cấp một số tính năng bảo mật giúp bảo vệ trong khi bạn duyệt web. Đáng chú ý nhất là chống lừa đảo, phương án bảo vệ chống phần mềm độc hại và tự động sửa sai chính tả địa chỉ trang web.

Với khả năng chống lừa đảo và bảo vệ khỏi phần mềm độc hại, Chrome hiển thị cảnh báo bất cứ khi nào bạn ghé thăm một trang web được Google xác định là có thể gây nhiễm độc, lây lan phần mềm độc hại hoặc cố gắng ăn cắp thông tin cá nhân của bạn. Trong khi đó, tính năng tự động sửa lỗi URL trên Chrome cung cấp một dịch vụ trực tuyến để sửa các đường dẫn sai chính tả có thể do gõ nhầm phím, giúp bạn tránh truy cập vào các trang web không an toàn.

Để sử dụng các tính năng này, hãy vào cửa sổ *Settings* của Chrome, di chuyển xuống phần *Privacy* (có thể phải bấm *Show advanced settings* để truy cập) và đánh dấu kiểm trước hộp có nhãn *Use a web service to help resolve navigation errors* và *Use a web service to help resolve spelling errors*. Ngoài ra, hãy đánh dấu kiểm trước mục *Enable phishing and malware protection*.

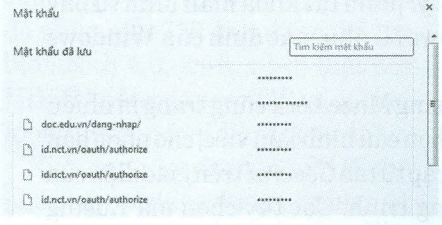


Bạn cũng cần bấm vào tab *Content settings* và xem xét các hạn chế trên một số nội dung. *Ví dụ:* vô hiệu hóa JavaScript (thường được khai thác bởi phần mềm độc hại) và plug-in...

• Bảo vệ mật khẩu đã lưu và các chi tiết thẻ tín dụng

Nếu bạn cho phép Chrome lưu mật khẩu trang web, bất cứ ai sử dụng máy tính của bạn cũng đều có thể dễ dàng truy cập chúng chỉ với một vài thao tác trong cửa sổ Settings.

Để ngăn ngừa việc này, bạn có thể thực hiện một vài thao tác giúp bảo vệ sự riêng tư. Đầu tiên, cần giới hạn không cho những người không tin tưởng sử dụng tài khoản người dùng Windows của bạn, thay vào đó bạn hãy tạo ra một tài khoản khách (không phải là administrator) cho người khác sử dụng hoặc bật tài khoản Guest lên.



Nếu việc tạo ra một tài khoản Windows là khá bất tiện, bạn nên xem xét việc sử dụng một phần mở rộng dành cho Chrome (có thể tìm trong Chrome Web Store tại *https://chrome.google.com/webstore*) như ChromePW, Browser Lock hoặc Secure Profile để bảo vệ mật khẩu Chrome.

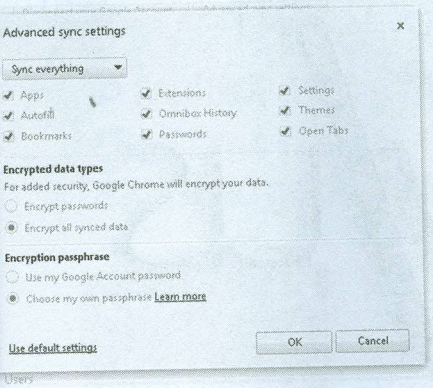
Cách làm này này sẽ buộc người khác phải sử dụng một trình duyệt khác trên hệ thống của bạn như Internet Explorer (không cho phép xem mật khẩu đã lưu), hoặc Firefox (cho phép mã hóa với mật khẩu bảo vệ các mật khẩu đã lưu).

Một lựa chọn khác là để lưu trữ an toàn dữ liệu nhạy cảm là sử dụng trình quản lý mật khẩu của bên thứ ba. Một số công cụ của bên thứ ba giúp quản lý mật khẩu, cho phép đồng bộ hóa mật khẩu của bạn trên các trình duyệt khác nhau, có thể hữu ích nếu bạn chuyển sang một máy tính khác. KeePass tại địa chỉ *http://keepass.info/* và Xmarks tại địa chỉ *http://www.xmarks.com/* là 2 công cụ quản lý mật khẩu rất hữu ích.

• Bảo mật dữ liệu đồng bộ

Chrome có thể đồng bộ hóa các thiết lập và dữ liệu lưu (bao gồm cả mật khẩu, nhưng không ghi chi tiết thẻ tín dụng) trên nhiều máy tính và các thiết bị đã cài đặt Chrome, nhưng điều này có thể tạo ra một lỗ hổng bảo mật. Theo mặc định, Chrome yêu cầu bạn nhập mật khẩu tài khoản Google của mình để thiết lập một máy tính hoặc thiết bị mới khi cần đồng bộ dữ liệu duyệt web. Vì vậy, nếu mật khẩu tài khoản Google của bạn bị tấn công, một kẻ xâm nhập có thể truy cập vào danh sách của tất cả các mật khẩu, trừ khi bạn thiết lập một mật khẩu tùy chỉnh hoạt động đồng bộ hóa mật khẩu.

Sau khi đã thiết lập một mật khẩu đồng bộ hóa, đầu tiên bạn phải đăng nhập với mật khẩu tài khoản Google và sau đó nhập vào cụm từ mật khẩu để thiết lập đồng bộ với các thiết bị mới, nhờ đó, bạn được cung cấp thêm một lớp bảo mật mở rộng quan trọng. Để sử dụng thiết lập này, hãy mở mục *Settings*,



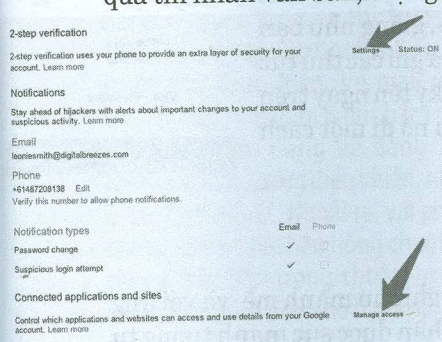
bấm *Advanced sync settings* và chọn *Choose my own passphrase*.

Không những vậy, tại đây bạn cũng có thể bật khả năng mã hóa cho tất cả dữ liệu đồng bộ hóa thay vì chỉ với một mật khẩu duy nhất.

● Bảo mật tài khoản Google của bạn

Google cung cấp một số tính năng bảo mật để giúp người sử dụng kiểm soát tốt hơn và bảo vệ tài khoản của mình, đặc biệt quan trọng nếu bạn có sử dụng tính năng đồng bộ hóa của Chrome.

Tại trang bảo mật tài khoản của Google ở địa chỉ *https://www.google.com/settings/security*, bạn có thể thực hiện hoạt động xác minh 2 bước của Google. Sau khi đã thực hiện điều này, bạn sẽ phải nhập một mã đặc biệt được cung cấp thông qua tin nhắn văn bản, cuộc gọi thoại hoặc ứng dụng Google khi đăng nhập vào Google từ một máy tính hoặc thiết bị di động mới, qua đó đảm bảo bạn là người duy nhất có khả năng đăng nhập. Khi đăng nhập vào ứng dụng mà không có mã xác minh (như tính năng đồng bộ hóa của Chrome), bạn sẽ phải đăng nhập vào tài khoản Google của mình, truy cập thiết lập xác minh 2 bước và tạo ra một mật khẩu ứng dụng cụ thể.



Ngoài ra, tại trang thiết lập bảo mật tài khoản Google, bạn cũng có thể bật thông báo email hoặc điện thoại để thay đổi mật khẩu và kiểm tra hoạt động đăng nhập đáng ngờ. Bằng cách này, bạn có thể biết ngay nếu có ai đó cố gắng thay đổi mật khẩu hoặc cố gắng lén lút đăng nhập vào tài khoản của mình.

Bạn cũng nên xem xét tùy chọn phục hồi trong trường hợp quên mật khẩu, rất có thể xảy ra trong tương lai. Cuối cùng, bạn cần xem xét ứng dụng, các trang web ủy quyền và loại bỏ những dịch vụ mà bạn không sử dụng nữa.

● Cài đặt phần mở rộng để bổ sung khả năng bảo vệ

Bên cạnh những tính năng bảo mật được cung cấp bởi Google và Chrome, bạn cũng có thể sử dụng những phần mở rộng khác nhau để thêm các chức năng bảo mật tốt hơn. Phần mở rộng Web of Trust (WOT) tại địa chỉ *http://tinyurl.com/8w7revu* sẽ cảnh báo bạn về các trang web nguy hiểm, trong khi Adblock tại địa chỉ *http://tinyurl.com/yddouf2* có thể loại bỏ các quảng cáo gây phiền nhiễu, có thể dẫn đến phần mềm độc hại hoặc các trang web lừa đảo. View Thru tại địa chỉ *http://tinyurl.com/295foct* cho phép bạn nhìn thấy điểm đến của các URL rút ngắn, còn KB SSL Enforcer tại địa chỉ *http://tinyurl.com/39b3zu8* giúp tận dụng giao thức mã hóa HTTPS/SSL trên các trang web có hỗ trợ.

PHƯƠNG THU