Hướng dẫn bảo mật Gmail toàn diện

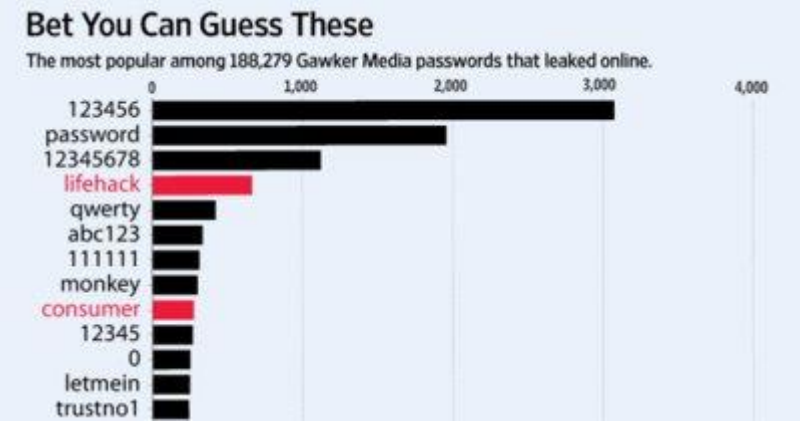
Mỗi khi người sử dụng đăng nhập vào tài khoản ngân hàng, quỹ bảo hiểm, thẻ tín dụng, mua hàng trực tuyến... tất cả những hệ thống trên đều có điểm chung là gì? Đó là yêu cầu người dùng khai báo địa chỉ email. Trên thực tế, rất nhiều người chỉ sử dụng 1 địa chỉ email duy nhất đối với tất cả các tài khoản như trên. Do vậy sẽ rất nguy hiểm nếu họ để mất tài khoản hoặc tin tặc đột nhập và lấy cắp thành công những dữ liệu cá nhân. Email được dùng phổ biến nhất hiện nay là Gmail.

Sau hàng loạt vụ đánh cắp dữ liệu cá nhân, bị hack tài khoản Gmail xảy ra vừa qua cộng với tình trạng an ninh mạng ngày càng trở nên phức tạp thì việc làm thế nào để bảo mật Gmail tốt nhất thực sự là vấn đề nên được bạn lưu tâm. Hãy tưởng tượng một ngày bạn tỉnh dậy, mở máy check mail như bình thường, nhưng bạn bị out ra khỏi tất cả Gmail trên máy tính, điện thoại và không thể đăng nhập tài khoản Gmailcủa mình nữa. Bi kịch hơn, email đó liên kết với tài khoản ngân hàng, Facebook, là công cụ giao tiếp trong công việc, với khách hàng. Chắc hẳn bạn sẽ muốn nổi điên lên và chửi bới kẻ đã hack Gmail của mình một cách thậm tệ. Nhưng trước khi định làm thế, hãy tự hỏi xem mình đã đối xử với một công cụ quan trọng như thế đúng mức chưa? Đã làm mọi cách để bảo vệ nó chưa? Hãy tự bảo vệ mình trước khi bị hacker, kẻ xấu sờ gáy nhé.

Trong bài viết dưới đây, chúng tôi sẽ trình bày một số thao tác cơ bản để bạn có thể tự bảo vệ tài khoản Gmail an toàn trước những mối nguy hiểm luôn luôn "rình rập" bên ngoài.

1. Sử dụng mật khẩu Gmail đủ an toàn

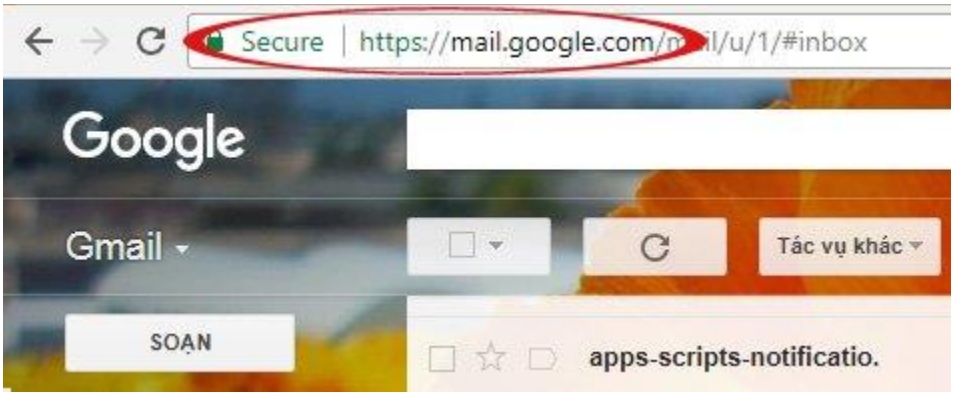
Đây là yếu tố đầu tiên quyết định đến sự an toàn của tài khoản đối với mỗi người dùng. Và cũng thật bất ngờ khi rất rất nhiều người đã, đang và vẫn sử dụng chuỗi **123456** là mật khẩu của họ, tiếp theo sau là **password**.



Thoạt nghe thì có vẻ đơn giản, nhưng chính những số liệu thực tế như trên đã chỉ ra rằng, mọi người vẫn "làm ngơ" và không coi trọng mức độ an toàn của tài khoản họ đang sử dụng. Làm thế nào để đặt mật khẩu an toàn?

2. Luôn luôn kiểm tra đường dẫn URL khi đăng nhập Gmail

Bên cạnh đó, nạn lừa đảo qua hình thức **Fishing** – là khi tin tặc khéo léo "dụ dỗ" người dùng vào những trang quen thuộc và yêu cầu họ cung cấp địa chỉ email, mật khẩu cũng như các thông tin cá nhân khác. Quy luật ở đây là không nên truy cập vào những đường dẫn lạ được gửi tới hòm thư email của bạn, luôn kiểm tra đường dẫn URL thực sự trên thanh Address để chắc chắn rằng đó là domain chính thức của Gmail:



Địa chỉ của Gmail chính xác phải là https://mail.google.com như hình

3. Thường xuyên kiểm tra Gmail để phát hiện những hành động bất thường

Khoảng hơn 1 năm trước, Google đã cung cấp thêm tính năng cảnh báo về những hành động khác lạ trong tài khoản đến người dùng. Do vậy, các bạn có thể kiểm tra các thao tác xảy ra gần đây nhất, chức năng này sẽ hiển thị đầy đủ tác vụ trong 10

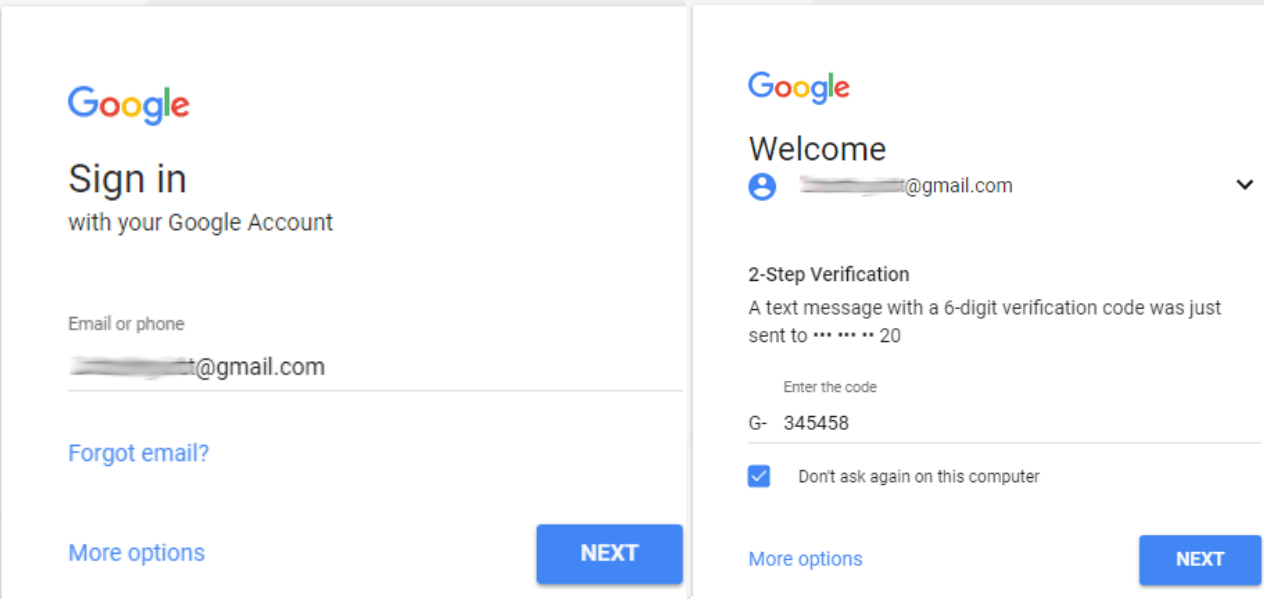
lần đăng nhập mới nhất. Và dựa vào vị trí địa lý, địa chỉ IP cũng như thời gian truy cập, người sử dùng sẽ biết được chuyện gì đang xảy ra.

Để xem được, bạn kéo chuột xuống cuối cùng màn hình, nhấp vào **Chi tiết/Details** như hình dưới:

Các hoạt động Gmail gần đây sẽ được liệt kê, nếu thấy những hoạt động bất thường hãy chọn **Đăng xuất khỏi tất cả các phiên web khác** và đổi mật khẩu ngay lập tức.

4. Kích hoạt tính năng bảo mật nâng cao của Gmail

Với chức năng này, tài khoản của người dùng Gmail sẽ được bảo vệ chắc chắn hơn rất nhiều bằng cách xác thực thêm 1 lần nữa sau khi nhập mật khẩu. Điểm đặc biệt ở đây là chuỗi ký tự xác thực được thay đổi ngẫu nhiên theo thời gian (được gửi về thiết bị di động qua số điện thoại đăng ký), do vậy bạn có thể yên tâm tuyệt đối một khi đã kích hoạt chức năng này.



5. Giám sát các địa chỉ người nhận hoặc gửi đáng ngờ

Google đã từng phát hiện được hàng trăm địa chỉ email của các quan chức cao cấp từ Trung Quốc, Hàn Quốc và chủ yếu là Mỹ đã bị xâm nhập và bí mật chuyển tiếp nội dung ra bên ngoài. Do vậy, các bạn hãy kiểm tra lại tài khoản xem có bị tự động chuyển tiếp mail đến địa chỉ nào khác không, bằng cách nhấp vào biểu tượng bánh xe ở góc bên phải, chọn **Cài đặt** > **Chuyển tiếp và POP/IMAP** (**Settings** > **Forwarding and POP/IMAP**):

Nếu trong mục **Chuyển tiếp** của bạn hiện ra như trên hình nghĩa là email của bạn không bị chuyển tiếp đến bất kỳ địa chỉ nào cả.

6. Luôn đảm bảo mức độ an toàn của máy tính cá nhân

Nếu đã thực hiện đầy đủ những bước trên thì vẫn chưa đủ, vì tài khoản của bạn vẫn có thể bị "nhòm ngó" nếu máy tính sử dụng không được trang bị những phương án bảo mật thực sự cần thiết. Cụ thể, đó là những thao tác đơn giản nhất trong quá trình sử dụng, quản lý file và thư mục cá nhân, sử dụng những chương trình diệt virus có uy tín và hiệu quả như: Avira Premium Security Suite, BitDefender Total Security 2010, PC Tools Spyware Doctor with Antivirus 2010, Kaspersky Internet Security 2011...

7. Cảnh giác với liên kết và file được đính kèm trong Gmail

Khi nhận được email từ người lạ, có đính kèm file, liên kết, bạn cần hết sức thận trọng khi nhấp vào liên kết, tải file đính kèm về máy. Bạn còn nhớ WannaCry đã bị lây lan như thế nào? Và rất nhiều vụ bị hack Gmail khác nữa? Hãy cẩn thận! Nếu cảm thấy nghi ngờ tốt nhất bạn nên xóa email đó thay vì nhấp chuột vào bất cứ phần nào trong email. Thậm chí khi email được gửi từ địa chỉ có trong danh bạ mà chứa những link lạ, hoặc tên file đính kèm lạ, bạn nên hỏi lại người gửi xem có phải họ gửi không và vẫn cần thận trọng với những link, file đó.