

M?o cho m?t tài kho?n email an toàn

Địa chỉ email không chỉ là một phương thức liên lạc đơn thuần. Ngày nay, địa chỉ email rất cần thiết cho hầu hết các giao dịch, từ kích hoạt điện thoại thông minh, mua sắm trực tuyến đến thiết lập tài khoản trực tuyến. Tài khoản email của bạn có thể chứa thông tin liên lạc nhạy cảm và quan trọng, và thường được kết nối với các tài khoản quan trọng, chẳng hạn như ngân hàng của bạn. Việc đảm bảo địa chỉ email của bạn an toàn - chỉ bạn mới có quyền truy cập - là rất quan trọng.

Tài liệu hướng dẫn này đưa ra những gợi ý về cách bảo mật địa chỉ email của bạn ở mức cao nhất có thể.

Nên ch?n d?ch v? email nào?

Nếu bạn lo lắng email của mình bị hack (thông qua các cuộc tấn công trung gian), một dịch vụ email được mã hóa đầu cuối có thể là lựa chọn bạn cần. Ví dụ: ProtonMail được mã hóa hoàn toàn và bạn có thể thiết lập để email không còn khả dụng sau một khoảng thời gian nhất định. Các dịch vụ email được mã hóa miễn phí khác bao gồm Tutanota và Mailfence.

Tuy nhiên, hãy lưu ý rằng các dịch vụ này có thể phức tạp hơn một chút so với email truyền thống. Ví dụ: một số dịch vụ email được mã hóa có thể yêu cầu người nhận email cũng sử dụng cùng một dịch vụ email hoặc để đọc email, họ phải nhấp vào liên kết và đọc email trên trình duyệt web. Lưu ý rằng email được mã hóa sẽ không ngăn người khác xem email của bạn nếu họ biết địa chỉ email và mật khẩu của bạn hoặc nếu bạn đang sử dụng thiết bị được giám sát.

Bạn hoàn toàn có thể sử dụng dịch vụ email thương mại phổ biến như Gmail hoặc Yahoo mà vẫn có một tài khoản an toàn. Bảo mật email thường phụ thuộc vào mật khẩu, tính bảo mật của thiết bị được sử dụng để truy cập email, và các thói quen bảo mật và quyền riêng tư email tốt như được đề cập trong phần còn lại của tài liệu này.

Thi?t l?p ??a ch? email

Quyền riêng tư và bảo mật email bắt đầu ngay khi bạn tạo tài khoản email đầu tiên.

- **Sử dụng thông tin không xác định danh tính**

Những người sống sót sau lạm dụng và theo dõi có thể không muốn một địa chỉ email dễ bị nhận dạng. Khi bạn thiết lập địa chỉ email với dịch vụ email thương mại, địa chỉ email của bạn không nhất thiết phải sử dụng thông tin nhận dạng như tên. Bạn có thể sử dụng bất kỳ tên nào làm địa chỉ email, chẳng hạn như brightredstar3@gmail.com .

Trong quá trình thiết lập, nhà cung cấp dịch vụ email sẽ yêu cầu thông tin liên kết với địa chỉ email của bạn, bao gồm tên và ngày sinh. Bạn có thể sử dụng bút danh và ngày sinh giả.

Chỉ cần nhớ bút danh và ngày sinh của bạn trong trường hợp bạn cần thông tin đó để xác minh tài khoản. Một số dịch vụ email cũng yêu cầu giới tính, số điện thoại di động và địa chỉ email phụ. Một số dịch vụ cho phép bạn bỏ qua những câu hỏi này mà không cần nhập bất kỳ thông tin nào; điều này sẽ khác nhau tùy theo dịch vụ email. Ví dụ: Gmail yêu cầu tên, tên người dùng, mật khẩu, ngày sinh và giới tính; tuy nhiên, bạn có thể để trống số điện thoại di động và địa chỉ email hiện tại và tiếp tục. Yahoo Mail yêu cầu tên, địa chỉ email, ngày sinh và số điện thoại di động, trong khi giới tính là tùy chọn. Outlook Mail chỉ yêu cầu tên, địa chỉ email và mật khẩu của bạn.

- **Sử dụng mật khẩu mà không ai khác biết**

Đối với hầu hết mọi người, tính bảo mật của tài khoản email phụ thuộc vào việc liệu có ai khác biết địa chỉ email và mật khẩu của họ hay không. Đừng sử dụng mật khẩu mà người khác có thể đoán được hoặc mật khẩu mà bạn cũng dùng cho các tài khoản khác. Hãy tạo một mật khẩu duy nhất mà bạn có thể nhớ mà không cần phải ghi lại, có thể là một cụm từ dài hoặc bao gồm chữ cái, số và ký tự.

- **Sử dụng Xác minh hai bước**

Nếu bạn có địa chỉ email thứ hai hoặc số điện thoại di động bảo mật (tức là không ai khác có thể truy cập vào đó), bạn có thể thiết lập xác minh hai bước. Nếu ai đó cố gắng đăng nhập vào tài khoản email của bạn từ một thiết bị hoặc vị trí khác, dịch vụ email sẽ gửi mã đến email hoặc số điện thoại di động thứ hai. Mã này sẽ được yêu cầu để đăng nhập vào tài khoản email, bên cạnh mật khẩu. Nếu bạn (hoặc người đang cố gắng đăng nhập vào tài khoản email của bạn) không có quyền truy cập vào email hoặc số điện thoại di động phụ đó để xem mã, bạn sẽ không thể đăng nhập vào tài khoản của mình.

Điều này chỉ hữu ích nếu bạn có email hoặc số điện thoại di động phụ mà không ai khác có thể truy cập.

Nếu người khác có quyền truy cập vào email/số điện thoại di động đó, họ có thể đăng nhập vào tài khoản của bạn ngay cả khi đã bật xác minh hai bước, hoặc họ có thể nhận được thông báo khi bạn cố gắng đăng nhập vào tài khoản từ một vị trí hoặc thiết bị mới. Tùy thuộc vào tình huống, bạn có thể không nên bật xác minh hai bước cho đến khi bạn bảo mật email và số điện thoại di động phụ trước.

Nếu bạn không cung cấp email hoặc số điện thoại di động phụ, dịch vụ email có thể thỉnh thoảng yêu cầu bạn cung cấp email hoặc số điện thoại di động phụ khi bạn đăng nhập vào tài khoản email sau này. Trong hầu hết các trường hợp, bạn có thể bỏ qua những yêu cầu này và nhấn tiếp tục hoặc OK mà không cần nhập bất kỳ thông tin nào. Email và số điện thoại di động phụ có thể là một bước bảo mật rất hữu ích – nhưng chỉ khi nó hiệu quả với bạn. Nếu bạn không có email hoặc số điện thoại di động phụ, hoặc email hoặc số điện thoại di động của bạn đã bị người khác xâm phạm, việc nhập thông tin này sẽ không giúp tài khoản của bạn an toàn hơn.

Hãy đảm bảo tài khoản email phụ và số điện thoại di động của bạn an toàn trước khi sử dụng.

- **Xem lại thông báo bảo mật**

Một số dịch vụ email sẽ thông báo cho bạn về bất kỳ sự kiện bảo mật nào trong tài khoản của bạn – chẳng hạn như thay đổi mật khẩu, đăng nhập từ một vị trí hoặc thiết bị khác hoặc thay đổi bất kỳ cài đặt bảo mật nào khác.

Thông báo bảo mật có thể được gửi đến địa chỉ email phụ của bạn. Tương tự như vấn đề với xác minh hai bước, nếu người khác có quyền truy cập vào địa chỉ email phụ đó, họ sẽ biết bất cứ khi nào bạn thực hiện bất kỳ thay đổi bảo mật nào cho tài khoản của mình. Bạn có thể chọn giới hạn số lượng thông báo nhận được hoặc thay đổi địa chỉ email phụ thành một địa chỉ an toàn hơn. (Bạn thường có thể tìm thấy thông báo bảo mật trong phần Cài đặt Bảo mật của tài khoản email.)

Thực hành thói quen sử dụng email tốt

Ngoài việc sử dụng mật khẩu mạnh và các tính năng bảo mật (ví dụ: xác minh hai bước) mà dịch vụ email cung cấp, việc thực hành các thói quen bảo mật và quyền riêng tư email tốt là rất quan trọng để đảm bảo không ai khác có thể đăng nhập vào tài khoản email của bạn hoặc đọc email của bạn.

Sử dụng thiết bị an toàn

Cố gắng không đăng nhập vào tài khoản của bạn trên các thiết bị (ví dụ: điện thoại di động, máy tính bảng, máy tính) mà kẻ gian có quyền truy cập hoặc đang theo dõi. Tùy thuộc vào cách thiết bị được theo dõi, người theo dõi có thể nhìn thấy địa chỉ email và mật khẩu của bạn nếu bạn đăng nhập trên thiết bị đó.

Luôn đăng xuất

Bất cứ khi nào bạn đăng nhập vào tài khoản email, dù trên thiết bị của bạn hay của người khác, hãy luôn đăng xuất. Đừng chỉ đóng trình duyệt web, ứng dụng hoặc tắt thiết bị, vì điều đó sẽ không đăng xuất bạn. Nếu bạn không đăng xuất, bất kỳ ai sử dụng thiết bị sau bạn đều có thể thấy tài khoản email của bạn. Ngay cả trên thiết bị của bạn, việc đăng xuất cũng rất hữu ích trong trường hợp ai đó nhặt được điện thoại, máy tính hoặc bạn làm mất chúng.

Nếu bạn kiểm tra email trên điện thoại di động thông qua ứng dụng email hoặc trên máy tính/máy tính xách tay thông qua chương trình email, bạn có thể không dễ dàng đăng xuất. Trong trường hợp này, bạn có một vài lựa chọn. Đặt mật mã hoặc mật khẩu trên thiết bị sẽ giúp hạn chế quyền truy cập này. Trong một số trường hợp, bạn thậm chí có thể muốn xóa tài khoản email khỏi ứng dụng hoặc chương trình email của mình. Một số người làm điều này khi họ đang đi du lịch hoặc lo ngại rằng ai đó không đáng tin cậy có thể truy cập vào thiết bị của họ. Bạn luôn có thể kiểm tra email qua trình duyệt web hoặc cấu hình ứng dụng hoặc chương trình email để truy cập email sau khi bạn chắc chắn rằng điện thoại hoặc máy tính của mình được bảo mật.

Ứng dụng trình duyệt hoặc tiện ích di động có thể ghi nhớ tài khoản email hoặc mật khẩu của bạn

Một số dịch vụ email (đặc biệt là Gmail) có tùy chọn cho phép trình duyệt web ghi nhớ tài khoản của bạn trừ khi bạn yêu cầu. Lần tới khi bạn (hoặc bất kỳ ai khác) mở trang đăng nhập email, địa

chỉ email của bạn sẽ được liệt kê và người khác chỉ cần nhập mật khẩu. Đừng cho phép trình duyệt web ghi nhớ tài khoản email của bạn, đặc biệt là trên các thiết bị không phải của bạn. Yêu cầu cấp quyền này thường sẽ hiển thị dưới dạng "Bạn có tin tưởng trình duyệt này không?". Hãy chọn "không".

Một số trình duyệt web và điện thoại di động sẽ hỏi bạn muốn lưu mật khẩu email hay "ghi nhớ tôi". Trong trường hợp này, ứng dụng sẽ ghi nhớ cả tài khoản email và mật khẩu của bạn. Nếu bạn lo ngại người khác có thể truy cập vào thiết bị của mình, đừng cho phép họ lưu mật khẩu. Điều này có thể thuận tiện cho một số tài khoản ít nhạy cảm hơn, chẳng hạn như thông tin đăng nhập Netflix, nhưng bạn muốn tài khoản email của mình được bảo mật.

Không nh?p vào liên k?t t? nh?ng cá nhân không xác ??nh ho?c ?áng ng?

Để bảo mật hơn cho tài khoản và thiết bị của bạn, đừng nhấp vào liên kết từ những cá nhân không xác định hoặc đáng ngờ hoặc cung cấp thông tin cá nhân qua email hoặc liên kết email.

Không g?i thông tin cá nhân qua email

Nếu ai đó (kể cả ngân hàng hoặc công ty tiện ích của bạn) yêu cầu cung cấp thông tin cá nhân (như mật khẩu, thông tin thẻ tín dụng và thông tin ngân hàng) qua email, đừng gửi email lại kèm thông tin đó. Thay vào đó, hãy tìm số điện thoại của công ty và gọi lại cho họ kèm theo thông tin đó.

Hãy th?n tr?ng khi cung c?p ??a ch? email c?a b?n

Vì địa chỉ email là thứ mọi người sử dụng để liên lạc với bạn nên bạn sẽ cần cung cấp chúng cho mọi người.

Tuy nhiên, bạn có thể không muốn cung cấp địa chỉ email của mình cho bất kỳ ai yêu cầu, đặc biệt là cho các cửa hàng hoặc khi thiết lập các tài khoản trực tuyến không quan trọng. Dưới đây là một số cách để cung cấp địa chỉ email mà không cần phải cung cấp địa chỉ email chính của bạn.

- Bạn có thể tạo một tài khoản email rác khi bạn phải cung cấp địa chỉ email nhưng không thực sự muốn nhận email từ họ. Tài khoản email này dành riêng cho thư rác và không nên được thiết lập để nhận thông tin quan trọng như sao kê ngân hàng hoặc kết nối với các tài khoản quan trọng, chẳng hạn như dịch vụ điện thoại di động.
- Một số dịch vụ email cho phép bạn tạo tài khoản email ngắn hạn. Những địa chỉ email này có thời hạn sử dụng từ 10 phút đến 24 giờ, vì vậy chúng rất tạm thời. Khi bạn cung cấp địa chỉ email đó, email sẽ được gửi đến trang web của dịch vụ email cụ thể đó, nơi bạn có thể kiểm tra email đã gửi. Điều này hữu ích khi bạn cần cung cấp địa chỉ email để "xác nhận" việc đăng ký, nhưng bạn không muốn cung cấp địa chỉ email thực của mình. Lưu ý rằng một số dịch vụ email tạm thời không có quyền riêng tư, nghĩa là bất kỳ ai biết địa chỉ email giả đều có thể xem tất cả email được gửi đến địa chỉ email giả đó (ví dụ về các dịch vụ email tạm thời công khai: Mailinator hoặc Maildrop). Các dịch vụ email tạm thời khác bao gồm Guerrilla Mail hoặc 10-Minute Mail.
- Một giải pháp lâu dài hơn để bảo vệ địa chỉ email của bạn là một dịch vụ như Abine Blur. Abine Blur là một tiện ích mở rộng trình duyệt web dành cho máy tính để bàn và thiết bị di động, hoạt động như một dịch vụ chuyển tiếp. Tiện ích này "làm mờ" thông tin thực của

bạn để người nhận nhận được một địa chỉ email ẩn danh, chứ không phải địa chỉ email thực tế của bạn. Khi họ trả lời, Abine Blur sẽ chuyển tiếp thư trả lời đến địa chỉ email thực tế của bạn. Về phía bạn, bạn vẫn gửi email qua lại như bình thường, nhưng về phía người nhận, họ chỉ thấy địa chỉ email ẩn danh.

Revision #2

Created 17 September 2025 11:34:28 by Hieu Nguyen

Updated 27 October 2025 06:15:41 by Hieu Nguyen