

Quản lý các email của quý vị một cách an toàn (Managing your emails safely)

Địa chỉ email là cánh cổng dẫn quý vị đến thế giới trực tuyến. Nó cho phép quý vị giữ liên lạc với gia đình và bạn bè, cũng như truy cập các dịch vụ như mua sắm trực tuyến và giao dịch ngân hàng. Điều quan trọng là phải giữ tài khoản email của quý vị an toàn nhất có thể được bằng cách sử dụng mật khẩu mạnh và xác thực đa yếu tố.



Các cách truy cập email

Có nhiều cách để truy cập email của quý vị. Quý vị có thể thực hiện điều này qua:

Ứng dụng

- dùng ứng dụng của nhà cung cấp email mà quý vị có thể tải xuống từ App Store cho thiết bị Apple hoặc Play Store cho thiết bị Android
- liên kết tài khoản email của quý vị tới:
 - ứng dụng thư được cài đặt sẵn trên thiết bị thông minh của quý vị
 - ứng dụng Mail hoặc Outlook trên máy tính của quý vị.

Trang mạng

- đăng nhập vào trang mạng của nhà cung cấp email từ trình duyệt trên máy tính hoặc thiết bị thông minh của quý vị.

Nhà cung cấp dịch vụ email

Có rất nhiều nhà cung cấp dịch vụ email cung cấp cả tùy chọn tài khoản email miễn phí và trả phí, bao gồm:

-  **Gmail** của Google
-  **Outlook** của Microsoft
-  **Yahoo Mail** của Yahoo
-  **iCloud** của Apple
-  **ProtonMail** của Proton AG

Truy cập trang mạng Be Connected để biết **[hướng dẫn từng bước](#)** về cách thiết lập và sử dụng Gmail, Outlook và Yahoo.

Mẹo: Quý vị có thể muốn thiết lập một tài khoản email chỉ dành cho giao dịch ngân hàng hoặc chỉ sử dụng cho mua sắm trực tuyến để giúp quản lý email rác.

Quản lý tài khoản email của quý vị

Thiết lập thư mục và nhãn

Thiết lập các thư mục trong hộp thư đến là cách tuyệt vời để sắp xếp tài khoản của quý vị và giúp quý vị dễ dàng tìm thấy các email quan trọng khi cần. Thư mục đôi khi còn được gọi là nhãn, tùy thuộc vào dịch vụ email quý vị sử dụng.

Tổ chức và lưu trữ email của quý vị

Dịch vụ email của quý vị có các tính năng kiểm soát tiện dụng giúp quý vị phân loại email theo nhiều cách khác nhau và giảm thiểu thư rác và thư không mong muốn. Khi có email mới đến và quý vị mở ra để đọc, một số nút điều khiển sẽ xuất hiện ở đầu màn hình. Quý vị có thể nhấp vào các nút điều khiển này để:

- **Xóa:** di chuyển email vào thư mục Bin/Thùng rác
- **Lưu trữ:** di chuyển email vào kho lưu trữ
- **Đánh dấu là chưa đọc:** làm cho email trông như mới một lần nữa
- **Nhãn/Thư mục:** dán nhãn cho email hoặc di chuyển email vào một thư mục.

Quản lý email rác

Dịch vụ email của quý vị sẽ tự động phát hiện và chuyển hướng email rác đã biết, nhưng một số thư rác vẫn có thể lọt vào.

Nếu quý vị xem một email trong hộp thư đến của mình là thư rác hoặc thư không mong muốn, quý vị có thể:

- **Báo cáo thư rác:** thông báo cho nhà cung cấp email rằng email đó là thư rác
- **Chặn email:** ngừng nhận email từ người gửi
- **Hủy đăng ký:** ngừng nhận bản tin hoặc email tiếp thị mà quý vị đã đăng ký.

Nếu quý vị cho rằng mình đã hủy đăng ký nhưng vẫn tiếp tục nhận được email rác không mong muốn, quý vị có thể khiếu nại lên [Cơ quan Truyền thông và Giao tiếp Úc](#).

Mẹo: Để tránh nhận email rác không mong muốn, hãy cẩn thận khi cung cấp thông tin của quý vị cho các cuộc tranh giải và bất kỳ ô nào được chọn trước để nhận email tiếp thị khi quý vị mua sản phẩm hoặc dịch vụ.

Giữ tài khoản email của quý vị an toàn

Cụm mật khẩu

Giữ tài khoản của quý vị an toàn bằng cụm mật khẩu mạnh. Cụm mật khẩu là phiên bản mật khẩu có tính an toàn hơn và bao gồm bốn hoặc nhiều từ ngẫu nhiên.

Hãy thử nghĩ ra một cụm mật khẩu khác nhau cho mỗi tài khoản của quý vị và đừng sử dụng lại bất kỳ mật khẩu cũ nào.

Khi quý vị chọn mật khẩu, hãy đặt mật khẩu:

- **Dài** – có ít nhất 14 ký tự
- **Không thể đoán trước** – sử dụng bốn hoặc nhiều từ ngẫu nhiên với số, ký hiệu, chữ hoa và chữ thường
- **Duy nhất** – không sử dụng lại cụm mật khẩu của quý vị.

Ví dụ: Yellow So Hey Plant > Yell*w-SOheyPl@nt!

Mẹo: Ứng dụng quản lý mật khẩu cũng có thể giúp quý vị tạo và lưu trữ cụm mật khẩu phức tạp, khó đoán hoặc khó bẻ khóa. Quý vị có thể tìm thông tin về [trình quản lý mật khẩu](#) và cách thiết lập chúng trên trang mạng Be Connected.

Tính xác thực đa yếu tố

Bật xác thực đa yếu tố cho tài khoản của quý vị luôn là một ý tưởng hay. Tính xác thực đa yếu tố (còn gọi là xác thực 2 bước) gia tăng thêm một tầng bảo mật cho tài khoản của quý vị. Điều này có nghĩa là khi quý vị đăng nhập vào tài khoản bằng mật khẩu, quý vị có thể được yêu cầu thực hiện thêm một bước để xác nhận đó là quý vị – như nhập mã số từ tin nhắn văn bản hoặc sử dụng nhận dạng khuôn mặt.

Sử dụng bảo mật dành cho thiết bị

Sử dụng phần mềm bảo mật trên máy tính là một trong những cách đơn giản nhất để bảo vệ tài khoản và thiết bị của quý vị. Việc bảo mật máy tính tốt là bao gồm cài đặt phần mềm chống gián điệp, chống vi-rút và phần mềm tường lửa có uy tín. Quý vị cũng nên cập nhật các công cụ và ứng dụng bảo mật trực tuyến của mình bằng cách bật tính năng cập nhật tự động.

Sử dụng kết nối an toàn

Khi quý vị cần truy cập tài khoản, gửi thông tin nhạy cảm hoặc nhập mật khẩu, hãy kết nối với một kết nối mạng đáng tin cậy, chẳng hạn như ở nhà, tại nơi làm việc hoặc sử dụng dữ liệu di động của riêng quý vị nếu có. Wi-Fi công cộng không an toàn bằng Wi-Fi tại nhà hoặc nơi làm việc của quý vị.

Tùy chọn khôi phục tài khoản

Đảm bảo quý vị thiết lập số điện thoại khôi phục hoặc địa chỉ email thay thế cho tất cả tài khoản email của mình. Nếu quý vị mất quyền truy cập vào tài khoản hoặc tài khoản bị xâm phạm, quý vị có thể đặt lại mật khẩu bằng cách khôi phục.

Email lừa đảo

Các email lừa đảo được thiết kế trông giống như chúng được gửi từ các tổ chức hợp pháp mà quý vị biết. Chúng có thể trông giống thật khi sử dụng logo và địa chỉ email tương tự như tổ chức mà chúng đang mạo danh. Các email lừa đảo có thể xuất hiện từ ngân hàng, nhà cung cấp dịch vụ internet, cơ quan chính phủ, nhà bán lẻ hoặc thậm chí là kẻ lừa đảo giả danh bạn bè hoặc người trong gia đình của quý vị. Bằng cách giả danh người mà quý vị tin tưởng, kẻ lừa đảo lợi dụng cảm giác cấp bách để lừa quý vị trả tiền hoặc cung cấp thông tin cá nhân, chẳng hạn như mật khẩu quan trọng, thông tin thẻ tín dụng hoặc thông tin ngân hàng.

Những loại lừa đảo này được gọi là lừa đảo mạo danh hoặc email lừa đảo.

Mẹo để tránh email lừa đảo

- Hãy cảnh giác với các dấu hiệu của email lừa đảo. Email lừa đảo có thể:
 - có cảm giác cấp bách hoặc sử dụng chiến thuật đe dọa, yêu cầu thanh toán hoặc yêu cầu quý vị xác nhận thông tin cá nhân
 - sử dụng lời chào chung chung như 'Kính gửi khách hàng', 'Kính gửi người dùng' hoặc không có lời chào nào cả
 - yêu cầu quý vị nhấp vào liên kết hoặc tải xuống tập tin mà có thể dẫn quý vị đến trang mạng giả mạo hoặc chứa vi-rút hoặc phần mềm độc hại.
- Luôn kiểm tra xem địa chỉ email của người gửi có hợp lệ không và liên hệ trực tiếp với tổ chức bằng cách tra cứu trang mạng chính thức và số điện thoại của họ.
- Không bao giờ đăng nhập vào tài khoản trực tuyến hoặc xác minh thông tin chi tiết thông qua liên kết trong email hoặc nhấp vào liên kết hoặc mở tập tin đính kèm trong email từ người gửi không biết hoặc đáng ngờ.
- Xóa các email đáng ngờ hoặc có khả năng là lừa đảo, sử dụng tùy chọn 'báo cáo thư rác' để phân loại đó là email không mong muốn.

Mẹo: Nếu quý vị không biết chắc về email, hãy trao đổi với bạn bè hoặc thành viên gia đình đáng tin cậy và liên hệ với tổ chức bằng số điện thoại trên trang mạng của họ.

Truy cập trang mạng Be Connected để xem miễn phí [những hướng dẫn về các trò lừa đảo mạo danh](#) do Scamwatch phát triển.

Hãy dành thời gian để khám phá Be Connected

Be Connected là một trang mạng toàn diện với các nguồn tài liệu miễn phí được thiết kế riêng để hỗ trợ người Úc lớn tuổi kết nối trực tuyến an toàn và điều hướng thế giới kỹ thuật số một cách tự tin. Trang mạng này cũng hữu ích cho các gia đình và tổ chức cộng đồng muốn giúp những thành viên lớn tuổi trong cộng đồng tiếp cận mọi lợi ích của Internet.



Hãy truy cập beconnected.esafety.gov.au



Chương trình này được Ủy hội eSafety biên soạn như một phần của sáng kiến Be Connected.