

C?m nang s? d?ng email an toàn, tránh rò r? d? li?u

S? d?ng m?t kh?u an toàn

- Đặt mật khẩu mạnh cho email
- Thay đổi mật khẩu định kỳ
- Không chia sẻ mật khẩu với người khác
- Không đặt trùng với các tài khoản khác

S? d?ng b?o m?t 2 l?p

Với các dịch vụ email phổ biến như Gmail, Outlook... tính năng bảo mật 2 lớp đều được hỗ trợ do đó hãy bật tính năng này để tăng cường bảo mật cho tài khoản của bạn.

Đối với email doanh nghiệp nếu không biết có tính năng này hay không bạn hãy liên hệ với quản trị viên công ty để được hỗ trợ.

S? d?ng email trên thi?t b? / m?ng an toàn

- Chỉ sử dụng trên thiết bị của bạn, tránh đăng nhập trên thiết bị lạ
- Thiết bị sử dụng cần được cài chương trình antivirus, cập nhật phần mềm đầy đủ
- Sử dụng mạng an toàn, nếu có thể hãy dùng VPN

Xem xét các thông báo b?o m?t

Thông thường các dịch vụ email có tính năng thông báo các hoạt động liên quan đến tài khoản qua email dự phòng như thay đổi mật khẩu, đăng nhập từ thiết bị lạ, tuy nhiên nhiều người dùng thường bỏ qua. Hãy tập thói quen xem xét các thông báo này để có thể phát hiện sớm các vấn đề liên quan đến tài khoản email và kịp thời xử lý.

G?i ?úng ??a ch? email ng??i nh?n

Hãy cẩn thận nhập chính xác địa chỉ email người nhận và kiểm tra lại trước khi gửi để đảm bảo email được gửi đến đúng người nhận, tránh rò rỉ thông tin. Nếu bạn là sinh viên và gửi tài liệu học tập cho bạn bè thì nhầm lẫn có thể không sao, nhưng nếu bạn đi làm mà đó là email chứa hợp đồng, bản báo giá của công ty... thì đó vấn đề lớn.

S? d?ng ?úng CC và BCC

- **Cc (Carbon Copy)** được dùng để gửi email cho nhiều người cùng lúc, danh sách những người nhận được nội dung mail cũng được hiển thị công khai với tất cả những người được nhận mail.

- **Bcc (Blind Carbon Copy)** được sử dụng để gửi email cho nhiều người nhận cùng lúc, nhưng họ sẽ không biết được danh sách những người cùng nhận được thư chung với mình.

Việc sử dụng 2 chế độ này không đúng có thể vô tình làm rò rỉ thông tin cụ thể là danh sách email. Đặc biệt nguy hiểm khi làm email marketing.

Mã hóa email

Nếu đó là email riêng tư, có nội dung quan trọng. Người dùng cần bật tính năng mã hóa email nhằm đảm bảo rằng không ai khác có thể đọc được ngoài người nhận. Nguy cơ bị chặn và đọc trái phép được giảm thiểu đáng kể bằng cách mã hóa dữ liệu trong bộ nhớ và trong quá trình truyền đi.

Cẩn thận tránh các email kèm link, hình ảnh kèm

Như hầu hết chúng ta đều biết, một trong những điểm yếu trong bảo mật email thường bắt nguồn từ lỗi của con người. Vì tính tò mò muốn biết tập tin đính kèm là gì hoặc ngại thơ nhiều người dùng đã vô tình nhấp vào các liên kết không an toàn trong email. Ngay cả những người có kinh nghiệm nếu không cẩn thận cũng có thể trở thành nạn nhân của những email lừa đảo tinh vi. Do đó người dùng hãy luôn cảnh giác và cẩn thận không mở bất kỳ tập tin đính kèm nghi ngờ nào cũng như không nhấp vào liên kết từ những người gửi không xác định.

Không sử dụng email công việc cho mục đích cá nhân

Việc cấp phát tài khoản email doanh nghiệp cho nhân viên là không hề hiếm và tài khoản email cũng có thể được dùng để truy cập các hệ thống nội bộ. Tùy vào mỗi doanh nghiệp sẽ có chính sách quy định riêng về việc sử dụng tài khoản. Dù chính sách thế nào, người dùng cũng không nên sử dụng email được cấp để sử dụng cho việc riêng như đăng ký tài khoản trực tuyến, mua hàng... Bởi vì việc này có thể dẫn đến việc email doanh nghiệp cấp bị spam thư rác, mã độc... tệ hơn là bị hack email từ đó là bước đệm để truy cập vào các hệ thống nội bộ gây mất an toàn thông tin. Chưa kể trường hợp người dùng sử dụng mail vào việc riêng rồi nghỉ việc thì những email này sẽ bị thu hồi và sẽ dẫn đến nguy cơ mất truy cập vào các dịch vụ đã liên kết.

Revision #2

Created 17 September 2025 11:21:40 by Hieu Nguyen

Updated 27 October 2025 05:48:31 by Hieu Nguyen