Cách s? d?ng email an toàn

- Quy định sử dụng email
- Cẩm nang sử dụng email an toàn, tránh rò rỉ dữ liệu
- Mẹo cho một tài khoản email an toàn
- Phishing là gì, mẹo giúp nhận biết một email lừa đảo
- Tổng hợp 18 loại phishing email phổ biến và thường gặp
- xxx

Quy ??nh s? d?ng email

- Người dùng không được phép sử dụng email đang được lưu trữ tại AEC để lạm dụng gửi **SPAM, QUẢNG CÁO, BULK MAIL, MASS MAIL, BOMB MAIL**, … chúng tôi có quyền tạm ngưng hoặc chấm dứt dịch vụ tùy theo mức độ vi phạm, ảnh hưởng.

  Chúng tôi không chấp nhận đối với bất kỳ hình thức gửi Email Spam nào, cho dù hành vi đó có thể là vô tình do người dùng đang bị Virus lợi dụng điều khiển & khai thác tài nguyên máy tính của người dùng.

- Người dùng phải có trách nhiệm kiểm soát việc gửi Email ra ngoài trên các tài khoản Email của mình. Mọi hậu quả của việc **SPAM, QUẢNG CÁO, BULK MAIL, MASS MAIL, BOMB MAIL**, … gây ra dẫn đến địa chỉ IP bị chặn bởi các tổ chức chống Spam, người dùng sẽ phải chịu trách nhiệm.

  Các tổ chức Blacklist quốc tế có uy tín: Có rất nhiều tổ chức quốc tế về Chống Spam trên thế giới. Tuy nhiên, chúng tôi chỉ đề cập đến 3 tổ chức sau đây thường được các nhà cung cấp dịch vụ chuyên dùng:

  - Spamhaus: http://www.spamhaus.org
  - The Barracuda Reputation Block List: http://www.barracudacentral.org
  - UCE Protect Network: http://www.uceprotect.net
- Người dùng phải hiểu và chấp nhận trình duyệt mail mà chúng tôi cung cấp được cấu hình và triển khai phù hợp với mục đích sử dụng chung. Chúng tôi không hỗ trợ thay đổi trình duyệt mail theo yêu cầu hoặc theo tiêu chí riêng của người dùng.

- Chỉ sử dụng các chức năng có sẵn trên công cụ quản trị Email mà chúng tôi cung cấp. Chúng tôi cố gắng mang đến cho đa số người dùng những tính năng được đánh giá tốt nhất. Do đó, chúng tôi không thể tùy biến theo yêu cầu và tiêu chí của riêng người dùng.

- Bộ lọc chống vi-rút ngăn chặn các khả năng gây nguy hại đến từ tập tin đính kèm đáng ngờ hoặc chứa vi-rút (Ví dụ như tập tin đính kèm có định dạng đuôi: exe, com, iso, jar, vbs, bat, pif, scr, hta, js, cmd, chm, ade, adp, cab, ins, isp, jse, lib, mde, msc, msp, mst, msp, nsh, sct, shb, vxd, wsc, wsf, cpl, jsp, reg, vbe, lnk, dll, dmg, sys, btm, msi, prf, wsh, vb …).

  Nếu người dùng chắc chắn rằng tệp an toàn, người dùng có thể yêu cầu người gửi tải tệp lên đám mây chia sẽ. Sau đó gửi nó dưới dạng tệp đính kèm drive (liên kết có thể chia sẻ).

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 rỏ 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.

C?n th?n tr??c các email l? kèm link, ?ính 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 ngây 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 s? d?ng email công vi?c cho m?c ?ích 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.

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.)

Th?c hành thói quen s? d?ng email t?t

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.

S? d?ng thi?t b? 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 ??ng xu?t

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.

??ng ?? trình duy?t ho?c ?i?n tho?i di ??ng c?a b?n ghi nh? tài kho?n email ho?c m?t kh?u c?a b?n

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.

Phishing là gì, m?o giúp nh?n bi ?t m?t email l?a ??o

Phishing là gì?

Phishing email (email giả mạo) là hình thức tấn công bằng email mà các tin tặc thường dùng. Theo đó, các tin tặc sẽ giả mạo một đơn vị hoặc doanh nghiệp uy tín nào đó để thực hiện các hành vi lừa đảo.

Các nạn nhân tin tưởng và cung cấp tài khoản ngân hàng, tài khoản mạng xã hội,... hoặc nhấp chuột vào các đường dẫn có chứa mã độc sẽ bị đánh cắp thông tin. Không những thế, các tin tặc còn có thể xâm nhập vào hệ thống mạng nội bộ của công ty.

Tin tặc sẽ tạo ra những email có giao diện và nội dung gần giống với các đơn vị uy tín như ngân hàng, chính phủ... để lừa đảo người dùng. Người dùng tin rằng đó là các email thực sự từ các tổ chức lớn và thực hiện theo yêu cầu trong trong email thì sẽ bị đánh cắp thông tin.

Phishing email là phương pháp tấn công khá nguy hiểm và rộng rãi nhất hiện nay. Nó được phát hiện lần đầu vào năm 1987. Nguồn gốc của phishing là sự kết hợp của câu thông tin (fishing for information) và trò lừa đảo (phreaking). Từ đó, thuật ngữ phishing đã ra đời.

10 m?o giúp nh?n bi?t m?t email l?a ??o

- **Hãy cẩn thận với những tin nhắn được ngụy trang dưới dạng thông báo vận chuyển hoặc thanh toán.**

  Những tin nhắn này thường chứa liên kết đến các trang web chứa phần mềm độc hại. Kiểm các liên kết để kiểm tra xem chúng có an toàn không trước khi nhấp chuột!

- **Hãy cảnh giác với những tin nhắn yêu cầu thông tin cá nhân**

  Hãy cảnh giác với những email yêu cầu thông tin cá nhân như số tài khoản, mạng xã hội và các thông tin cá nhân khác, vì các công ty chính thống sẽ không bao giờ yêu cầu thông tin này qua email.

- **Hãy cẩn thận với những tin nhắn khẩn cấp hoặc đe dọa**

  Hãy cẩn thận với những tin nhắn khẩn cấp hoặc đe dọa cho rằng tài khoản của bạn đã bị tạm ngừng và yêu cầu bạn nhấp vào một liên kết để mở khóa tài khoản.

- **Kiểm tra ngữ pháp hoặc lỗi chính tả kém**

Trong khi các công ty chính thống rất nghiêm khắc với các email mà họ gửi đi, các email lừa đảo thường chứa lỗi chính tả hoặc ngữ pháp kém.

- **Di chuột qua trước khi nhấp chuột**

  Các email lừa đảo thường chứa liên kết đến các trang web chứa phần mềm độc hại. Đừng tin tưởng vào URL bạn nhìn thấy! Luôn di chuyển chuột qua liên kết để xem địa chỉ đích thực của nó. Ngay cả khi liên kết khẳng định chỉ đến một trang web uy tín đã biết trước, nó vẫn an toàn hơn nếu bạn gõ địa chỉ (URL) thủ công vào thanh địa chỉ trình duyệt của bạn.

- **Kiểm tra lời chào**

  Tin nhắn có gửi đến người nhận chung chung, chẳng hạn như “Quý Khách Hàng” hoặc “Ông / Bà”? Nếu vậy, hãy xem xét thật kỹ! Doanh nghiệp chính thống biết và thường sử dụng tên và họ thật của bạn.

- **Kiểm tra chữ ký**

  Ngoài lời chào, các email lừa đảo thường bỏ qua thông tin quan trọng trong chữ ký. Các doanh nghiệp chính thống luôn có thông tin liên hệ chính xác trong chữ ký của họ, vì vậy nếu chữ ký của một tin nhắn có vẻ thiếu hoặc không chính xác, khả năng cao đó là thư rác.

- **Đừng tải xuống các tập tin đính kèm**

  Với sự phổ biến của Ransomware as a Service (Raas), những người gửi thư rác có công cụ dễ dàng để phân phát các tin nhắn thư rác chứa phần mềm độc hại đến hàng ngàn người dùng. Vì lợi nhuận từ ransomware có thể rất cao, ngay cả một lần nhiễm ransomware thành công cũng có thể mang về cho người gửi thư rác số tiền lớn. Nếu có bất kỳ nghi ngờ nào về người gửi tin nhắn hoặc nội dung của một tệp đính kèm nhất là các tập tin có định dạng: .zip, .exe, .scr, hãy đảm bảo an toàn và không tải xuống tệp đính kèm hoặc liên hệ với công ty hợp pháp mà bạn nghi ngờ họ đang bị tổ chức hacker giả mạo để đánh lừa bạn cấp thông tin.

- **Đừng tin tưởng vào địa chỉ Gửi**

  Nhiều email lừa đảo sẽ có một địa chỉ người gửi giả mạo. Chú ý rằng địa chỉ Gửi hiển thị ở hai nơi: Envelope From được sử dụng bởi máy chủ thư để tạo ra các tin nhắn không được gửi đi, trong khi Header From được sử dụng bởi trình duyệt mail để hiển thị thông tin trong trường Gửi. Cả hai tiêu đề này đều có thể được giả mạo.

  MDaemon Webmail có tính năng bảo mật tích hợp giúp người dùng nhận dạng những email bị giả mạo. Ví dụ, nhiều trình duyệt mail ẩn địa chỉ Gửi, chỉ hiển thị tên Gửi, điều này có thể dễ dàng bị giả mạo. Trong MDaemon Webmail, địa chỉ Gửi luôn được hiển thị, giúp người dùng có cái nhìn rõ ràng hơn về nguồn gốc của email và giúp họ xác định người gửi

giả mạo.

- **Đừng kích hoạt enable macros**

  Trong khi chúng ta đang nói về ransomware, một điểm vào chung cho nhiễm ransomware là các chức năng trong tài liệu Microsoft Word. Những tài liệu này thường xuất hiện trong các email lừa đảo, nhận định chúng có nội dung quan trọng từ phòng nhân sự, tài chính hoặc một bộ phận quan trọng khác; để lừa người dùng, chúng yêu cầu người dùng kích hoạt macros. Đừng bao giờ tin tưởng vào một email yêu cầu bạn kích hoạt các chức năng trước khi tải xuống một tài liệu Word.

T?ng h?p 18 lo?i phishing email ph? bi?n và th??ng g?p

Để hiểu hơn về khái niệm **phishing email** là gì, bạn cần tìm hiểu các loại phishing email phổ biến. Dưới đây là 18 loại phishing email thường gặp.

1. **Giả mạo thông báo email doanh nghiệp overload data**

   Trong các loại phishing email thì đây là hình thức phổ biến nhất. Sau khi bạn click vào liên kết để nâng cấp dung lượng email (upgrade email quota) thì mã độc sẽ tràn vào hệ thống email của bạn. Toàn bộ mã độc đều đã được cài đặt sẵn.

2. **Giả mạo đặt hàng**

   Hình thức này thường nhắm vào các doanh nghiệp cung cấp các sản phẩm đặt hàng. Những phishing email dạng này sẽ được thiết kế giống như các email đơn hàng thông thường, khiến người dùng dễ dàng mở ra mà không hề đề phòng.

3. **Giả mạo hóa đơn**

   Giả mạo hóa đơn thông qua phishing email cũng là một hình thức thịnh hành. Các tin tặc sẽ giả mạo email của doanh nghiệp hoặc tổ chức với nội dung yêu cầu thanh toán hóa đơn cho một đơn đặt hàng hoặc dịch vụ nào đó.

   Email thường có đính kèm tập tin giả mạo và liên kết trang web giả mạo. Nếu bạn click vào các đường dẫn đó hoặc tải các tập tin về máy thì phần mềm độc hại sẽ tự động được cài đặt trên máy. Để tránh bị lừa đảo qua email, các bạn nên kiểm tra kỹ lưỡng các thông tin và sử dụng phần mềm diệt virus.

4. **Giả mạo nâng cấp tài khoản email**

   Các tin tặc có thể giả danh nhà cung cấp dịch vụ email để gửi thông báo đến tài khoản của bạn. Các email giả danh có thể của Google, Microsoft hoặc là bộ phận công nghệ thông tin của công ty bạn.

   Các email đó không có gì bất thường, từ lỗi ngữ pháp cho đến chính tả. Nội dung email không có gì phức tạp và thường có ít nhất một liên kết hướng đến web “https” an toàn cho người dùng.

   Khi bạn được yêu cầu cung cấp các thông tin cá nhân trong email, bạn nên di chuyển chuột qua đường dẫn để kiểm tra đích đến thực sự của nó. Vì văn bản trong email thường

không thể hiện điều này.

5. **Giả mạo phí trả trước**

   Phishing Email giả mạo phí trả trước là một hình thức lừa đảo phổ biến, trong đó kẻ tấn công giả danh các công ty hoặc tổ chức để gửi email yêu cầu người dùng thanh toán trước cho một sản phẩm nào đó. Email này thường chứa tệp đính kèm hoặc liên kết đến một trang web giả mạo.

   Để tránh bị lừa đảo, người dùng cần lưu ý kiểm tra kỹ thông tin trước khi thực hiện bất kỳ hành động nào. Cụ thể, người dùng nên kiểm tra địa chỉ email của người gửi và xem liệu địa chỉ đó có hợp lệ hay không. Ngoài ra, người dùng cũng nên sử dụng phần mềm bảo mật email để bảo vệ máy tính khỏi các email phishing và các cuộc tấn công mạng khác.

6. **Giả mạo Google docs tài liệu**

   Đây là hình thức lừa đảo còn mới và cực kỳ nguy hiểm. Vì các email này có thể xuất hiện dưới tên người quen của bạn. Nội dung email sẽ yêu cầu bạn click vào liên kết để xem tài liệu đính kèm. Tập tin đính kèm đó là một trang web giống với trang đăng nhập Gmail. Khi bạn nhập tài khoản và mật khẩu của mình vào trang web, các tin tặc sẽ truy cập vào tài khoản và lấy cắp thông tin.

7. **Giả mạo thanh toán PayPal**

   PayPal là ví điện tử và là phương thức thanh toán trực tuyến tiện lợi. Tuy nhiên, tin tặc cũng sử dụng PayPal để lừa đảo người dùng. Chúng sẽ lấy thông tin tài khoản của bạn để lấy tiền hoặc chiếm đoạt tài khoản PayPal của bạn. Do đó, bạn nên cẩn thận khi sử dụng PayPal và không chia sẻ thông tin tài khoản PayPal của mình cho bất cứ ai.

   Với khoảng 200 triệu người dùng, PayPal thường bị tin tặc nhắm tới. Phishing Email dạng này thường có logo PayPal và một đoạn chữ in đẹp thuyết phụ ở cuối email. Trò lừa đảo này có mục đích là cố gắng tạo tâm lý hoảng loạn đến các nạn nhân bằng thông báo “tài khoản của bạn đang gặp vấn đề, vui lòng nhấp vào đây để khắc phục sự cố”. Bạn nên đặc biệt cẩn thận vì rất khó để nhận diện.

8. **Giả mạo tin nhắn lừa đảo từ HR**

   Các email từ phòng nhân sự luôn quan trọng vì họ thường thông báo các thông tin nội bộ cho toàn thể nhân viên. Tuy nhiên, vẫn có phishing email giả mạo phòng nhân sự. Dạng phishing email này thường chứa các tập tin đính kèm hoặc liên kết độc hại. Do đó, bạn nên hỏi trực tiếp người gửi để biết yêu cầu cung cấp thông tin cá nhân có hợp pháp hay không.

9. **Giả mạo cơ quan Nhà Nước**

   Các email được gửi từ cơ quan Nhà Nước thường được các tin tặc giả mạo với giao diện rất

giống. Nội dung email thường mang tính chất cảnh báo thông dụng như quyền truy cập Internet của bạn sẽ bị thu hồi, bạn đã truy cập hoặc tải xuống các tập tin bất hợp pháp,...

10. **Giả mạo lừa đảo thông qua Dropbox**

    Email lừa đảo Dropbox là một hình thức tấn công phishing phổ biến, trong đó kẻ tấn công giả danh Dropbox để gửi email cho người dùng. Email này thường thông báo cho người dùng rằng có một tệp lớn được gửi cho họ và yêu cầu họ nhấp vào một liên kết để tải xuống. Khi người dùng nhấp vào liên kết, họ sẽ được chuyển hướng đến một trang web giả mạo trông giống như trang web của Dropbox.

    Trang web này sẽ yêu cầu cung cấp thông tin cá nhân hoặc thông tin tài khoản, chẳng hạn như tên người dùng, mật khẩu, hoặc số thẻ tín dụng. Một số email lừa đảo Dropbox thậm chí còn có thể truy cập vào tài khoản Dropbox của người dùng mà không cần họ cung cấp bất kỳ thông tin nào.

11. **Mạo danh chi cục thuế**

    Mạo danh chi cục thuế là loại tấn công rất khó chịu và tinh vi vì các tin tặc có thể sử dụng đa dạng các nội dung để thuyết phục bạn tiết lộ thông tin mật nào đó. Một số mẫu nội dung phishing email chi cục thuế có thể là:

    Email chỉ rõ bạn đang sai phạm luật thuế và đang nợ các khoản thanh toán trên hóa đơn trong khi thực tế là bạn không sai gì cả.

    Email thể hiện rằng nó được gửi từ chi cục thuế địa phương hoặc của thành phố và yêu cầu bạn tiết lộ đầy đủ thông tin tài khoản ngân hàng để hoàn lại thuế dư đã đóng trước đó.

    Email giả mạo Chi cục thuế địa phương chỉ ra rõ là bạn đang nợ thuế của năm nào đó.

    Bạn được khuyến khích click vào liên kết nào đó trong nội dung email để được chuyển hướng tới một trang web trông có vẻ hợp pháp. Ở trang đó, bạn phải khai báo các thông tin cá nhân và mật khẩu của mình. Tuy nhiên, bất cứ thông tin đăng nhập nào được nhập vào trong đó sẽ được gửi thẳng đến hacker.

12. **Giả mạo thông báo tài khoản bị xâm nhập**

    Khi bạn nhận được email hoặc văn bản thông báo tài khoản của bạn đang có hoạt động đáng ngờ, đó là lúc chuông cảnh báo bắt đầu. Chiêu trò này vẫn còn rất hiệu quả với người dùng email vì các nạn nhân không chỉ hoảng sợ mà còn bối rối không biết phải làm gì.

Phishing email thông báo tài khoản bị xâm nhập chỉ là một ví dụ điển hình về hình thức lừa đảo. Bất cứ ứng dụng hoặc trang web nào của cá nhân hoặc tổ chức đều có thể bị tội phạm mạng sử dụng chiêu trò này.

13. **Giả mạo gửi thông báo rút tiền**

    Nội dung của phishing email này có một số đường link và biểu mẫu yêu cầu bạn điền đầy đủ thông tin để xác minh quyền sở hữu tài khoản. Bạn sẽ bị mắc bẫy của các tội phạm mạng nếu vội vàng điền thông tin vào.

14. **Giả mạo thông tin trúng thưởng**

    Hãy cẩn thận khi nhận được email thông báo trúng thưởng. Đây có thể là một email lừa đảo nhằm đánh cắp thông tin cá nhân của bạn.

    Những email lừa đảo trúng thưởng thường có nội dung rất hấp dẫn, khiến người nhận dễ dàng bị kích thích lòng tham. Email thường thông báo rằng bạn đã trúng một giải thưởng lớn, chẳng hạn như ô tô, tiền mặt, hoặc chuyến du lịch. Để nhận giải, bạn chỉ cần nhấp vào một liên kết và cung cấp thông tin cá nhân, chẳng hạn như tên, địa chỉ, số điện thoại, hoặc thông tin tài khoản ngân hàng.

    Nếu bạn nhận được email trúng thưởng, hãy cẩn thận trước khi nhấp vào bất kỳ liên kết nào hoặc cung cấp bất kỳ thông tin nào. Hãy kiểm tra kỹ địa chỉ email của người gửi và xem liệu địa chỉ đó có hợp lệ hay không. Bạn cũng có thể tìm kiếm thông tin về giải thưởng trên trang web chính thức của công ty hoặc tổ chức đã tổ chức giải thưởng.

15. **Giả mạo làm nạn nhân**

    Giả mạo là nạn nhân cũng là hình thức phổ biến trong phishing email. Các tin tặc sẽ giả dạng đặt hàng của doanh nghiệp nhưng không nhận được bất cứ sản phẩm hoặc không có phản hồi.

    Trong nội dung email, chúng còn thể hiện cảnh báo rằng nếu bạn không đưa ra lời giải thích thỏa đáng, chúng sẽ kiện lên chính quyền địa phương. Thậm chí, chúng còn để liên kết để bạn phản hồi lại. Tài khoản của doanh nghiệp sẽ bị mất khi bạn đăng nhập vào đường dẫn đó.

16. **Giả mạo checkup**

    Một ngày, bạn nhận được email thông báo rằng hệ thống email doanh nghiệp đang tiến hành kiểm tra hệ thống. Để xác minh quyền sở hữu với email mà bạn đang được cấp phát sử dụng, bạn phải điền vào biểu mẫu theo yêu cầu. Nếu bạn làm theo những yêu cầu trong email này, bạn sẽ cung cấp toàn bộ thông tin đăng nhập tài khoản email của mình cho kẻ lừa đảo.

17. **Giả mạo làm người quen cũ**

    Hãy cẩn thận với những email có tên giống với một người bạn hoặc đồng nghiệp cũ, nội dung yêu cầu vay tiền trong tình thế cấp bách và hứa sẽ trả lại ngay sau đó. Để chắc chắn rằng bạn không bị lừa đảo, hãy liên hệ trực tiếp với người có liên quan trong mối quan hệ này để xác minh.

18. **Giả mạo thông báo quá hạn thanh toán**

    Nếu bạn đang sử dụng email tên miền doanh nghiệp và nhận được email thông báo về một dịch vụ đã quá hạn thanh toán, yêu cầu bạn đăng nhập vào hệ thống nhanh nhất để lưu trữ lại dữ liệu quan trọng, hãy cẩn thận. Kẻ lừa đảo có thể đang lợi dụng sự lo lắng của bạn để đánh cắp thông tin đăng nhập.

XXX

xxx