# 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.

---

Revision #2
Created 17 September 2025 16:32:48 by Hieu Nguyen
Updated 27 October 2025 06:44:08 by Hieu Nguyen