

Phishing Email là gì? Cách ngăn chặn Phishing Email mới hiệu quả nhất

Video Clip :

Phishing Email là một hình thức lừa đảo qua email đã và đang xảy ra phổ biến ở các doanh nghiệp, gây ra những thiệt hại về tài chính và ảnh hưởng đến uy tín của tổ chức. Vì vậy, để đối phó với Phishing Email, các doanh nghiệp cần nắm rõ các hình thức phishing email và những giải pháp bảo mật hiệu quả để ngăn chặn các mối đe dọa này.

Phishing email là gì?

Phishing Email (Email giả mạo) là một hình thức tấn công Email mà trong đó các hacker tấn công thường giả mạo một doanh nghiệp uy tín nào đó để thực hiện các kế hoạch lừa đảo trong email người dùng. Khiến họ tin tưởng và cung cấp các thông tin tài khoản cá nhân, hoặc click vào các liên kết có chứa mã độc, nhằm xâm nhập vào hệ thống mạng doanh nghiệp.

Các hacker này có thể sẽ tạo ra những nội dung email gần giống với giao diện email của các bên tổ chức uy tín như: ngân hàng, chính phủ,... để lừa đảo người dùng khiến họ tin tưởng rằng đó là email thực sự, người dùng sẽ dễ dàng chia sẻ các thông tin quan trọng và bị tấn công.

Phishing Email được xem là phương pháp tấn công nguy hiểm và phổ biến nhất hiện nay, nó được phát hiện lần đầu tiên vào năm 1987. Nguồn gốc của từ Phishing là sự kết hợp của 2 từ: fishing for information (câu thông tin) và phreaking (trò lừa đảo). Vì có sự tương quan về mặt ý nghĩa giữa việc “câu cá” và “câu thông tin người dùng”, vì thế thuật ngữ Phishing đã ra đời từ đó.

11 Hình thức phishing email

Đây là những hình thức tấn công Phishing Email được các hacker thường xuyên sử dụng vì chúng đạt được những kết quả thành công cao ngoài mong đợi.

1. Phishing Email giả mạo thông báo Email Doanh Nghiệp overload data

Phishing email giả mạo thông báo email doanh nghiệp overload data là một hình thức tấn công phổ biến. Tin tặc giả mạo email của doanh nghiệp và gửi đến người dùng yêu cầu họ cập nhật thông tin tài khoản hoặc bảo mật. Email này thường có liên kết đến trang web giả mạo hoặc tệp đính kèm để cài đặt phần mềm độc hại. Người dùng nên kiểm tra thông tin trước khi thực hiện hành động nào và sử dụng phần mềm bảo mật email để tránh bị tấn công phishing.

Phishing Email giả mạo thông báo Email Doanh Nghiệp overload data

2. Phishing Email giả mạo đặt hàng

Phishing Email giả mạo đặt hàng là hình thức tấn công mạng khi tin tặc giả mạo email từ các doanh nghiệp và yêu cầu người dùng thanh toán cho một đơn đặt hàng hay dịch vụ. Vì các doanh nghiệp thường xuyên nhận được đơn đặt hàng, nên người dùng có thể dễ dàng mở email phishing này mà không nhận ra. Nếu người dùng sử dụng email tên miền doanh nghiệp mà không có hệ thống bảo mật vững chắc, họ sẽ rất dễ rơi vào bẫy của tin tặc.

Phishing Email giả mạo đặt hàng

3. Phishing email giả mạo hóa đơn

Phishing email giả mạo hóa đơn là một hình thức tấn công phổ biến. Tin tặc giả mạo email từ các doanh nghiệp hay tổ chức và yêu cầu thanh toán cho một đơn đặt hàng hoặc dịch vụ. Email thường có đính kèm file PDF hoặc Word giả mạo và liên kết đến trang web giả mạo. Nếu người dùng nhấp vào liên kết hoặc tải xuống tệp đính kèm, phần mềm độc hại sẽ được cài đặt trên máy tính của họ, cho phép tin tặc truy cập vào thông tin cá nhân hoặc lừa đảo họ cung cấp thông tin tài khoản. Để tránh bị lừa đảo, người dùng cần kiểm tra kỹ thông tin và sử dụng phần mềm bảo mật email.

Phishing email giả mạo hóa đơn

4. Phishing Email giả mạo nâng cấp tài khoản email

Khi tài khoản email của bạn sắp hết hạn và cần gia hạn ngay, hacker sẽ lợi dụng giả danh các nhà cung cấp email đáng tin như Microsoft và Google hoặc giả vờ là bộ phận CNTT của công ty bạn gửi thông báo nâng cấp tài khoản.

Phishing Email giả mạo nâng cấp tài khoản email

Như bạn có thể thấy, không có gì bất thường từ email này. Không có lỗi ngữ pháp, không có yêu cầu phức tạp nào và liên kết hướng đến một trang web “https” an toàn cho người dùng. Một lời khuyên hữu ích là khi được yêu cầu cung cấp thông tin cá nhân, bạn nên di chuột qua đường dẫn để kiểm tra đích đến thực sự của nó, bởi vì văn bản trong email thường không cho thấy được điều này.

5. Phishing Email giả mạo phí trả trước

Phishing Email giả mạo phí trả trước là hình thức lừa đảo phổ biến, trong đó tin tặc giả danh các công ty hoặc tổ chức để gửi email yêu cầu người dùng thanh toán trước cho một sản phẩm hoặc

dịch vụ. Thông thường, email này sẽ chứa tệp đính kèm hoặc liên kết đến một trang web giả mạo, khi người dùng nhấp vào liên kết hoặc tải xuống tệp đính kèm, phần mềm độc hại sẽ được cài đặt trên máy tính của họ, cho phép tin tặc truy cập vào thông tin cá nhân hoặc lừa đảo họ cung cấp thông tin tài khoản.

Để tránh bị lừa đảo, người dùng cần kiểm tra kỹ thông tin trước khi thực hiện bất kỳ hành động nào, nên kiểm tra địa chỉ email của người gửi và kiểm tra tính hợp lệ của nó, và nên sử dụng phần mềm bảo mật email để bảo vệ máy tính khỏi các cuộc tấn công phishing và các cuộc tấn công mạng khác.

Phishing Email giả mạo phí trả trước

6. Phishing Email giả mạo Google tài liệu

Đây là một dạng lừa đảo mới và khá nguy hiểm vì email này có thể xuất hiện dưới tên của một người bạn quen biết. Email này sẽ yêu cầu bạn bấm vào một liên kết để xem một "tài liệu", nhưng thực tế đó là một trang web giống hệt trang đăng nhập Gmail. Khi bạn nhập tài khoản và mật khẩu của mình vào trang web đó, hacker sẽ có thể truy cập vào tài khoản của bạn và lấy cắp thông tin.

Phishing Email giả mạo Google tài liệu

7. Phishing Email giả mạo PayPal

PayPal là một cách thanh toán trực tuyến tiện lợi. Tuy nhiên, những kẻ lừa đảo cũng sử dụng nó để lừa đảo người dùng. Họ sẽ cố gắng lấy thông tin tài khoản của bạn để lấy tiền hoặc chiếm đoạt thông tin thẻ tín dụng của bạn. Vì vậy, bạn cần cẩn trọng khi sử dụng PayPal và không chia sẻ thông tin tài khoản của mình với bất kỳ ai.

Với khoảng 200 triệu người dùng, PayPal là một công cụ cực kỳ sinh lợi cho tội phạm mạng. Cùng với số lượng tài khoản lớn, PayPal mang đến cho những kẻ lừa đảo cơ hội lợi dụng nền tảng được liên kết trực tiếp với thẻ tín dụng hoặc tài khoản ngân hàng của họ.

Phishing Email giả mạo PayPal

Những email này thường bao gồm logo PayPal, cộng với một đoạn chữ in đẹp thuyết phục ở cuối email. Một lần nữa, trò lừa đảo này cố gắng thực thi chế độ hoảng loạn đối với các nạn nhân của nó, thường bằng loại thông báo "Có vấn đề với tài khoản của bạn, vui lòng nhấp vào đây để khắc phục sự cố". Hãy coi chừng, chúng cũng chứa bản in đẹp hợp pháp.

8. Phishing Email tin nhắn lừa đảo từ HR

Tất cả chúng ta (hy vọng) tin tưởng vào đội ngũ nhân sự của mình, đặc biệt là khi nhận được những email cực kỳ quan trọng liên quan đến các cập nhật cá nhân hoặc toàn công ty. Vấn đề là, tội phạm mạng biết chúng ta đặt niềm tin nhiều như thế nào vào các đồng nghiệp nhân sự của mình.

Phishing Email tin nhắn lừa đảo từ HR

Lừa đảo qua email nhân sự thường chứa tệp đính kèm hoặc liên kết độc hại mà sau khi được nhấp vào, sẽ cài đặt phần mềm độc hại vào máy tính hoặc thiết bị của bạn. Khuyến khích đồng nghiệp hỏi trực tiếp người gửi nhân sự xem yêu cầu cung cấp thông tin cá nhân có hợp pháp hay không trước khi nhấn gửi.

9. Phishing Email lừa đảo Dropbox

Cùng một câu chuyện cũ về việc khuyến khích người dùng nhấp vào một liên kết, nhưng một nền tảng hoàn toàn mới để sử dụng. Dropbox, nền tảng lưu trữ và chia sẻ trực tuyến, đã trở nên phổ biến rộng rãi trong những năm gần đây - và các bản sao gian lận của nó cũng vậy.

Phishing Email lừa đảo Dropbox

Email lừa đảo Dropbox thường hoạt động bằng cách thông báo cho người dùng rằng 'tệp' đã được gửi qua email cho họ quá lớn và cần được mở bằng cách "nhấp chuột vào liên kết này" nhanh chóng. Có lẽ bạn đã đoán được rằng một trang đích Dropbox giả mạo đang chờ... và bạn đã đúng. Những gì bạn có thể không đoán được là trang này thực sự có thể nằm trong chính Dropbox - kiên nhẫn chờ đợi để thu thập thông tin chi tiết của bạn.

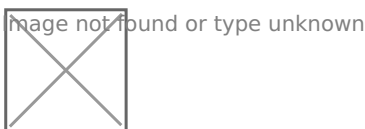
10. Phishing Email lừa đảo thuế hội đồng

Lừa đảo thuế hội đồng là một cuộc tấn công đặc biệt khó chịu, vì nó có thể sử dụng nhiều thông điệp thông minh thuyết phục bạn tiết lộ thông tin chi tiết của mình.

Phishing Email lừa đảo thuế hội đồng

Từ trang web của Chính phủ Vương quốc Anh, dưới đây là một số ví dụ khác về nội dung của một email lừa đảo về thuế:

- Nó khẳng định rằng bạn đang ở sai phạm vi Thuế Hội đồng và bị nợ các khoản thanh toán trên hóa đơn Thuế Hội đồng của bạn, trong khi thực tế là phạm vi của bạn đúng;
- Nó nói rằng họ đến từ hội đồng địa phương hoặc Cơ quan Văn phòng Định giá (VOA) và yêu cầu chi tiết ngân hàng của bạn để họ có thể hoàn lại tiền;
- Tuyên bố rằng VOA tính phí bạn để phản đối mức thuế Hội đồng của bạn;
- Tuyên bố rằng theo luật, người nộp thuế phải được đại diện bởi một đại lý để thách thức ban nhạc của họ.



Người dùng cuối được khuyến khích nhấp vào liên kết bên trong email để được chuyển hướng đến một trang hợp pháp (ví dụ: Microsoft), nơi họ có thể nhanh chóng cập nhật mật khẩu của mình. Tuy nhiên, bất kỳ thông tin đăng nhập nào được nhập vào trang này sẽ được gửi thẳng đến bọn tội phạm mạng.

11. Phishing Email giả mạo thông báo hoạt động bất thường

Khi nhận được email hoặc văn bản thông báo rằng đã có “hoạt động đáng ngờ trên tài khoản của bạn”, chuông cảnh báo bắt đầu đổ chuông hết tốc lực. Đó là lý do tại sao trò lừa đảo này rất hiệu quả đối với những kẻ lừa đảo, vì nạn nhân không chỉ phải đối mặt với tình trạng cấp bách và hoảng sợ - họ còn phải đối mặt với sự bối rối.

Phishing Email giả mạo thông báo hoạt động bất thường

Đây chỉ là một ví dụ về nguồn gốc của lừa đảo hoạt động bất thường. Bất kỳ ứng dụng, trang web hoặc nền tảng nào - cho dù đó là ngân hàng hay thậm chí là tài khoản Instagram của bạn - đều có thể bị kẻ tấn công sử dụng cho kỹ thuật gây hại này.

Những cách để đối phó với Phishing Email trong môi trường doanh nghiệp

Để đối phó với Phishing Email trong môi trường doanh nghiệp, có thể áp dụng những cách sau:

1. Nâng cao ý thức và đào tạo nhân viên: Cung cấp đào tạo và hướng dẫn cho nhân viên cách phát hiện và tránh các email lừa đảo. Tạo một môi trường làm việc an toàn, khuyến khích nhân viên báo cáo những hành vi nghi ngờ.
2. Sử dụng các phần mềm bảo mật chuyên dụng: Sử dụng các [giải pháp bảo mật email](#) doanh nghiệp hiệu quả như phân tích nội dung email, kiểm tra độ tin cậy của email, tạo chữ ký số và mã hóa email.
3. Thiết lập các chính sách bảo mật chặt chẽ: Các chính sách bảo mật email nghiêm ngặt như yêu cầu sử dụng mật khẩu mạnh, thực hiện các kiểm tra định kỳ và đảm bảo các thiết bị có cập nhật bảo mật mới nhất.
4. Sử dụng các dịch vụ chuyên nghiệp: Các công ty bảo mật và các nhà cung cấp dịch vụ email chuyên nghiệp cung cấp các giải pháp bảo mật email doanh nghiệp hiệu quả.

Với các giải pháp này, các doanh nghiệp có thể đối phó với Phishing Email một cách hiệu quả và đảm bảo an toàn cho thông tin của mình.

EG-Platform - Hệ thống lọc Phishing Email được Gartner

chứng nhận bảo mật

EG-Platform – Hệ thống lọc Phishing Email được Gartner chứng nhận bảo mật

Mail Gateway [EG-Platform](#) được thiết kế để ngăn chặn các cuộc tấn công qua email, đặc biệt là Phishing Email. Các đặc điểm nổi trội của giải pháp bảo mật này bao gồm:

1. Hệ thống quản lý và phân tích email: EG-Platform sử dụng các công nghệ phân tích và đánh giá email để phát hiện và ngăn chặn các email lừa đảo.
2. Cơ chế lọc thông minh: EG-Platform có khả năng lọc và xác định các email độc hại, đồng thời phân loại và đánh giá độ tin cậy của email để người dùng có thể xác định độ an toàn của email một cách dễ dàng.
3. Kiểm tra định kỳ và phân tích nội dung: EG-Platform kiểm tra định kỳ nội dung email, đảm bảo rằng các email không chứa các mối đe dọa độc hại.
4. Đảm bảo tính riêng tư: EG-Platform giúp bảo vệ tính riêng tư của người dùng bằng cách mã hóa các email để tránh bị đánh cắp thông tin.

Đặc biệt, điểm nổi bật nhất của giải pháp [Mail Gateway](#) này là khả năng chặn các email lừa đảo (phishing email) bằng các công nghệ tiên tiến như phân tích hành vi người dùng, phân tích nội dung và phát hiện mã độc. Điều này giúp cho doanh nghiệp có thể ngăn chặn được những cuộc tấn công mạng thông qua email một cách hiệu quả và nhanh chóng.

Tóm lại, mail gateway EG-Platform của VNENetwork có nhiều đặc điểm nổi trội để ngăn chặn phishing email, bảo vệ tính riêng tư và đảm bảo an toàn cho người dùng khi sử dụng email trong môi trường doanh nghiệp. Nếu bạn quan tâm đến việc bảo vệ email cho doanh nghiệp của mình, hãy để lại lời nhắn hoặc liên hệ ngay với chúng tôi qua hotline (028) 7306 8789 để được hỗ trợ sớm nhất.

Revision #3

Created 19 December 2022 01:59:55 by Quản trị

Updated 9 June 2023 02:56:17 by Quản trị