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.

Revision #2
Created 17 September 2025 12:26:46 by Hieu Nguyen
Updated 27 October 2025 06:32:19 by Hieu Nguyen