Cách nhận biết và tránh lừa đảo mạo danh

Những kẻ lừa đảo sử dụng email hoặc tin nhắn văn bản để lừa bạn cung cấp thông tin cá nhân. Nhưng có một số điều bạn có thể thực hiện để bảo vệ bản thân.

Cách nhận biết lừa đảo mạo danh

Những kẻ lừa đảo sử dụng email hoặc tin nhắn văn bản để lừa bạn cung cấp thông tin cá nhân. Chúng có thể thử đánh cắp mật khẩu, số tài khoản hoặc số An sinh xã hội của bạn. Nếu lấy được thông tin này thì chúng có thể truy cập email, tài khoản ngân hàng hoặc các tài khoản khác của bạn. Những kẻ lừa đảo khởi động hàng ngàn cuộc tấn công mạo danh như vậy mỗi ngày - và chúng thường thành công. Trung tâm Khiếu nại Tội phạm Internet của FBI báo cáo đã có 57 triệu USD bị mất trong các cuộc lừa đảo mạo danh trong một năm.
Những kẻ lừa đảo thường xuyên cập nhật chiến thuật, nhưng có một số dấu hiệu sẽ giúp bạn nhận biết email hoặc tin nhắn văn bản mạo danh.

Email và tin nhắn văn bản mạo danh thường trông rất giống email hoặc tin nhắn từ một công ty mà bạn biết hoặc tin tưởng. Email hoặc tin nhắn đó có thể giống như được gửi từ ngân hàng, công ty thẻ tín dụng, trang mạng xã hội, trang web hoặc ứng dụng thanh toán trực tuyến hoặc cửa hàng trực tuyến.
Email và tin nhắn văn bản mạo danh thường kể một câu chuyện để lừa bạn nhấp vào liên kết hoặc mở tệp đính kèm. Chúng có thể

- nói rằng chúng nhận thấy một số hoạt động hoặc hành vi đăng nhập đáng ngờ
- tuyên bố rằng tài khoản hoặc thông tin thanh toán của bạn có vấn đề
- nói rằng bạn phải xác nhận một số thông tin cá nhân
- bao gồm hóa đơn giả
- muốn bạn nhấp vào một liên kết để thanh toán
- nói rằng bạn đủ điều kiện đăng ký hoàn tiền với chính phủ
- cung cấp phiếu mua hàng miễn phí

Đây là một ví dụ thực tế về một email mạo danh.

Hãy tưởng tượng bạn nhận được email này trong hộp thư đến. **Bạn có nhận thấy dấu hiệu lừa đảo không?** Hãy cùng tìm hiểu.

- Email này trông giống như được gửi từ một công ty mà bạn có thể biết và tin tưởng: Netflix. Thậm chí còn sử dụng biểu trưng và tiêu đề thư của Netflix.
- Nội dung email cho biết tài khoản của bạn đang bị treo do vấn đề thanh toán.
- Email có lời chào chung chung "Bạn thân mến". Nếu bạn có tài khoản với doanh nghiệp này thì có lẽ họ sẽ không sử dụng một lời chào chung chung như vậy.
- Email mời bạn nhấp vào liên kết để cập nhật thông tin thanh toán của bạn.

Mặc dù thoạt nhìn email này có thể giống như thật, nhưng không phải vậy. Những kẻ lừa đảo gửi những email này hoàn toàn không có liên hệ với các công ty mà chúng mạo danh. Email mạo danh có thể gây ra hậu quả thực sự đối với những người cung cấp thông tin cho kẻ lừa đảo. Và có thể gây tổn hại uy tín của các công ty mà chúng mạo danh.

Cách bảo vệ bản thân trước những cuộc tấn công mạo danh

Bộ lọc thư rác cho email của bạn có thể loại bỏ nhiều email lừa đảo ra khỏi hộp thư đến. Nhưng những kẻ lừa đảo luôn tìm cách vượt qua các bộ lọc thư rác, vì vậy, thêm các lớp bảo vệ bổ sung là một lựa chọn tốt. Dưới đây là bốn bước bạn có thể thực hiện ngay để bảo vệ bản thân khỏi các cuộc tấn công mạo danh.

Bốn bước để bảo vệ bản thân khỏi lừa đảo mạo danh

1. Bảo vệ máy tính của bạn bằng cách sử dụng phần mềm bảo mật. Thiết lập cập nhật tự động cho phần mềm để phần mềm có thể xử lý các mối đe dọa bảo mật mới.
2. Bảo vệ điện thoại di động của bạn bằng cách thiết lập cập nhật tự động phần mềm. Những bản cập nhật này có thể giúp bảo vệ bạn trước những mối đe dọa bảo mật.
3. Bảo vệ tài khoản của bạn bằng cách sử dụng xác thực đa yếu tố. Một số tài khoản cung cấp bảo mật bổ sung bằng cách yêu cầu hai thông tin trở lên khi đăng nhập vào tài khoản của bạn. Phương thức này được gọi là xác thực đa yếu tố. Thông tin bổ sung bạn cần để đăng nhập vào tài khoản thuộc hai loại:

- Thông tin gì đó mà bạn có — chẳng hạn như mật mã bạn nhận được qua tin nhắn văn bản hoặc ứng dụng xác thực.
- Dữ liệu gì đó của bạn — chẳng hạn như quét vân tay, võng mạc hoặc khuôn mặt của bạn.

Xác thực đa yếu tố khiến những kẻ lừa đảo khó đăng nhập vào tài khoản của bạn hơn nếu chúng lấy được tên người dùng và mật khẩu của bạn.

4. Bảo vệ dữ liệu của bạn bằng cách sao lưu. Sao lưu dữ liệu của bạn và đảm bảo các bản sao lưu đó không được kết nối với mạng ở nhà của bạn. Bạn có thể sao chép các tệp tin trên máy tính vào ổ cứng gắn ngoài hoặc bộ nhớ đám mây. Đồng thời, bạn cũng nên sao lưu dữ liệu trên điện thoại.

Bạn nên làm gì nếu nghi ngờ về tấn công mạo danh

Nếu bạn nhận được email hoặc tin nhắn văn bản yêu cầu nhấp vào liên kết hoặc mở tệp đính kèm, hãy trả lời câu hỏi sau: **Tôi có tài khoản ở công ty này không hoặc tôi có biết người liên hệ này không?**
Nếu câu trả lời là "Không" thì đó có thể là lừa đảo mạo danh. Quay lại và xem xét lời khuyên trong phần Cách nhận biết lừa đảo mạo danh và tìm kiếm các dấu hiệu lừa đảo mạo danh. Nếu nhận thấy các dấu hiệu đó, báo cáo, rồi xóa tin nhắn đó.
Nếu câu trả lời là "Có", hãy liên hệ với công ty đó bằng số điện thoại hoặc trang web mà bạn biết là thật. Không phải bằng thông tin trong email. Tệp đính kèm và liên kết có thể chứa phần mềm độc hại.

Bạn nên làm gì nếu đã phản hồi một email mạo danh

Nếu bạn nghĩ rằng một kẻ lừa đảo đã lấy được thông tin của bạn, chẳng hạn như Số An sinh xã hội, thẻ tín dụng hoặc tài khoản ngân hàng, hãy truy cập IdentityTheft.gov. Trong trang này, bạn sẽ thấy các bước cụ thể cần thực hiện tùy theo thông tin bạn bị đánh cắp.
Nếu bạn nghĩ rằng mình đã nhấp vào liên kết hoặc mở một tệp đính kèm tải xuống phần mềm độc hại, hãy cập nhật phần mềm bảo mật của máy tính. Sau đó quét máy tính.

Cách báo cáo hành vi mạo danh

Hãy báo cáo nếu bạn nhận được email hoặc tin nhắn văn bản mạo danh. Thông tin bạn cung cấp có thể giúp chống lại những kẻ lừa đảo.

Bước 1. Nếu bạn nhận được email mạo danh, hãy chuyển tiếp đến Nhóm công tác chống mạo danh theo địa chỉ reportphishing@apwg.org. Nếu bạn nhận được tin nhắn văn bản mạo danh, hãy chuyển tiếp đến SPAM (7726).
Bước 2. Báo cáo cuộc tấn công mạo danh cho FTC tại FTC.gov/complaint.

Gắn thẻ: an ninh mạng, mạo danh, lừa đảo

Tháng 5/2019