Cách phát hiện scam trực tuyến

SCAM là một thuật ngữ tiếng Anh, có nghĩa là lừa đảo. Theo định nghĩa, SCAM được sử dụng để mô tả bất kỳ doanh nghiệp, cá nhân nào kiếm tiền hoặc những "món hời" khác từ những nạn nhân mà không bị nghi ngờ. Trong thế giới Internet, SCAM trực tuyến ngày càng tăng và phát sinh ra nhiều biến thể. Chúng ta sẽ tìm hiểu kỹ hơn trong bài viết này.

"Này anh bạn, chú ý này. Nghe và nhớ giữ bí mật nhé. Tôi có một người bạn ở nước ngoài rất muốn về đây chơi. Anh ta rất giàu nhưng lại gặp khó khăn trong việc vượt qua một loạt các bước thủ tục phức tạp. Chính vì vậy, tôi hy vọng rằng bạn có thể đưa trước cho tôi một vài chục đô la để chúng tôi có thể thúc đẩy nhanh quá trình. Bạn không phải lo đâu. Một khi nào bạn tôi về được đây, anh ta sẽ trả bạn gấp 100 lần số tiền bạn đã ứng trước. Bạn nghĩ thế nào?"

Nếu một ai đó lạ gặp bạn trên phố và nói với bạn điều gì đó tương tự như vậy, bạn nên lờ đi những gì anh ta nói và đi tiếp. Thậm chí, bạn có thể thông báo điều này với công an khu vực. Ai có thể tin một người chúng ta chưa từng gặp? Tuy vậy, scam trực tuyến cũng gần giống như vậy và đã lừa được hàng ngàn người đưa tiền cho chúng theo các cách khác nhau. Dường như, ở cuộc sống đời thường mọi người rất thông minh, nhưng khi trực tuyến thì họ lại rất dễ bị lừa.

Những scam thông thường hay lấy tên như *Nigerian scam* hay *419 scam*. Ngoài ra, còn rất nhiều dạng khác nữa của scam nhưng mục đích chính của chúng là lừa đảo mọi người đưa cho chúng càng nhiều tiền càng tốt, cùng với các thông tin tài

khoản ngân hàng của bạn. Cùng với đó là hàng ngàn các scam trực tuyến khác. Một số thì giống Nigerian scam nhưng một số khác thì lại khác hoàn toàn. Một số thậm chí còn cài đặt chương trình chứa mã độc là malware trên máy tính của bạn và trở thành vấn đề dai dẳng.

Cách tốt nhất để giải quyết scam trực tuyến là tránh xa chúng hoàn toàn. Như vậy, bạn sẽ không phải khôi phục lại những sự cố mà chúng gây ra. Chính vì lý do này, chúng tôi sẽ hướng dẫn bạn các bước để nhận dạng một scam để bạn không trở thành nạn nhân của chúng. Tiếng anh có câu: "*if it sounds too good to be true, it probably is*." (*nếu điều nào đó nghe quá hay, quá tốt đẹp đến nỗi như không thể thành sự thật, điều đó có thể đúng là không có thật*).

Các loại hình scam

Có hàng ngàn cách thức lừa đảo ngày nay, nhưng hầu hết đều hướng đến mục đích là ăn cắp tiền, tài sản hoặc thông tin. Kẻ lừa đảo sẽ sử dụng tất cả các phương pháp lén lút để ăn cắp thông tin cá nhân của bạn. Sau khi đã lấy được những thông tin này, chúng có thể sử dụng danh tính của bạn để thực hiện các hoạt động gian lận như sử dụng thẻ tín dụng hoặc mở tài khoản ngân hàng. Dưới đây là các phương thức scam cũng như lấy cắp thông tin cá nhân phổ biến nhất:

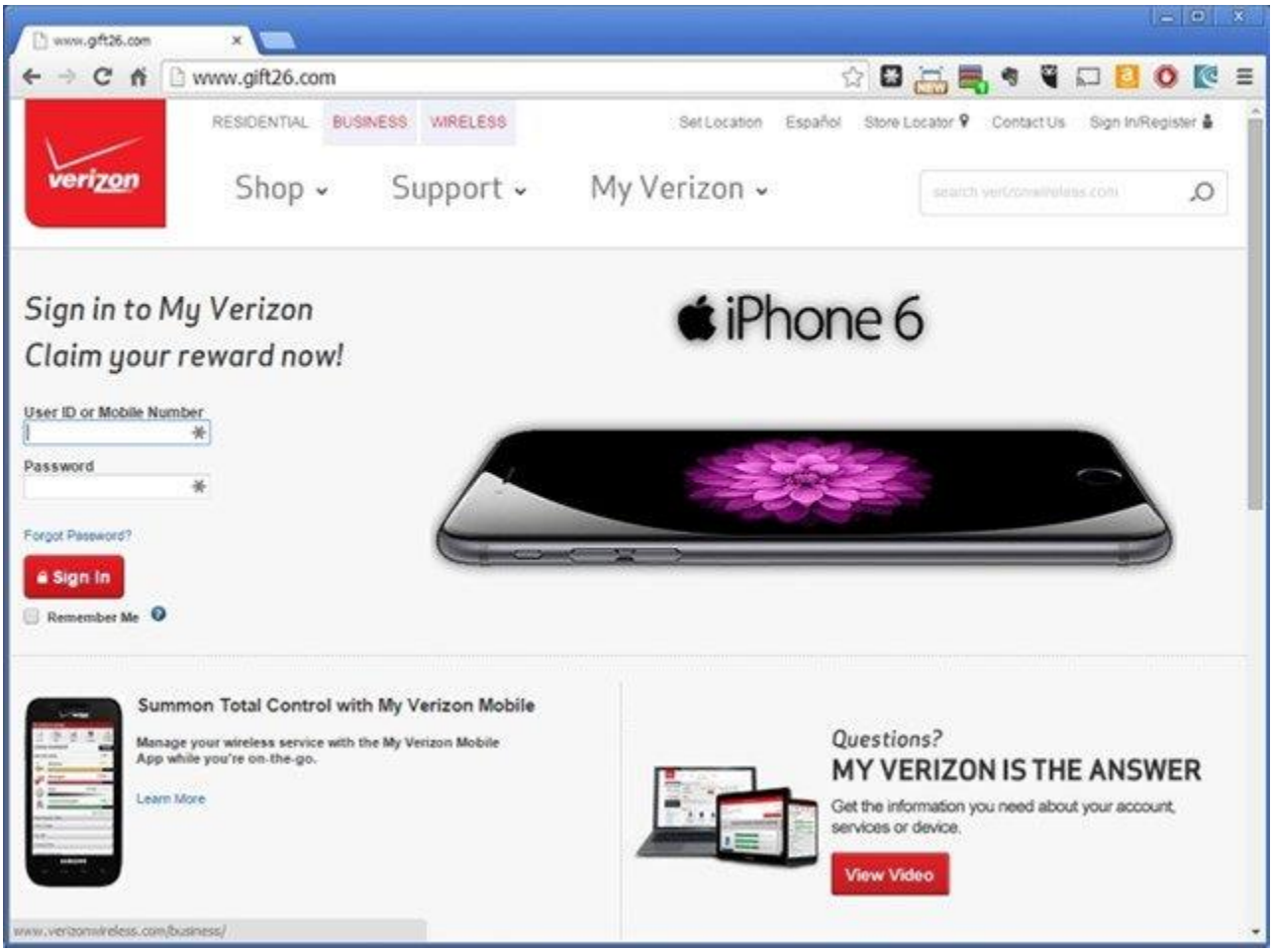
Hack

Hack là phương thức được dùng khi kẻ lừa đảo truy cập vào thông tin cá nhân của bạn bằng cách sử dụng công nghệ để đột nhập vào máy tính, thiết bị di động hoặc hệ thống mạng của bạn và đánh cắp các thông tin đó.

Trộm cắp danh tính

Trộm cắp danh tính là một loại gian lận liên quan đến việc sử dụng danh tính của người khác để ăn cắp tiền hoặc thu được các lợi ích khác.

Lừa đảo giao dịch



Một ví dụ đơn giản của loại hình lừa đảo này là bạn sẽ nhận được e-mail từ một người giả vờ là nhân viên của ngân hàng và cho biết bạn đã bị thấu chi hoặc mua hàng mà trên thực tế bạn không hề thực hiện, và sau đó chúng yêu cầu bạn đăng nhập và xác minh thông tin. Tuy nhiên, liên kết trong e-mail mà những kẻ này gửi tới lại đưa bạn đến một trang web giả mạo. Trang web này sẽ ghi lại các thông tin như tên người dùng và mật khẩu của bạn.

Gian lận đấu giá

Kiểu scam này xuất hiện dưới hình thức một người nào đó bán một đồ vật trên các trang web đấu giá trực tuyến như E-bay hoặc Craigslist nhưng chỉ là ảo. Ví dụ: Ai đó có thể yêu cầu bán cho bạn vé cho một buổi hòa nhạc sắp diễn ra thực sự đây không phải là vé chính thức.

Lừa đảo quyên góp

Hình thức lừa đảo này sẽ được tiến hành theo mô-tuýp có một người tuyên bố rằng họ có một đứa trẻ hoặc một người nào đó mà họ biết đang bị bệnh và cần được hỗ trợ tài chính (kiểu lừa đảo này đằng biệt phổi biến trên các trang mạng xã hội ở Việt Nam). Mặc dù trên thực tế cũng có nhiều trường hợp kêu gọi quyên góp là thật cũng có một số lượng đáng báo động những người tạo tài khoản giả mạo trên các trang web với hy vọng lừa đảo, chiếm đoạt tiền của những nhường có lòng hảo tâm.

Catfish (hẹn hò trực tuyến)

Hình thức lừa đảo này được thực hiện theo kịch bản một người tạo lập một hồ sơ trực tuyến giả mạo với ý định lừa dối những người khác. Ví dụ, một người phụ nữ có thể tạo một hồ sơ giả mạo trên một trang web hẹn hò trực tuyến, tạo mối quan hệ với một hoặc nhiều người và sau đó dần dần yêu cầu người khác cho mình tiền hoặc cung cấp thông tin cá nhân. Ở Việt Nam, phương thức scam này đặc biệt phổ biến trong những năm đầu mà game online bùng nổ. Thường là một game thủ sẽ tạo một tài khoản trong game để làm quen và lừa đảo các tài khoản khác.

Lừa đảo qua các cuộc gọi

Ví dụ, có một người tự xưng là nhận viên hỗ trợ kỹ thuật từ một công ty máy tính (như Dell chẳng hạn) gọi điện và thông báo với bạn là họ đã nhận được thông tin rằng máy tính của bạn bị nhiễm virus hoặc đã bị tấn công và họ sẽ cung cấp các kết nối từ xa với máy tính của bạn để khắc phục sự cố rồi từ đó đánh cắp các thông tin trên thiết bị của bạn.

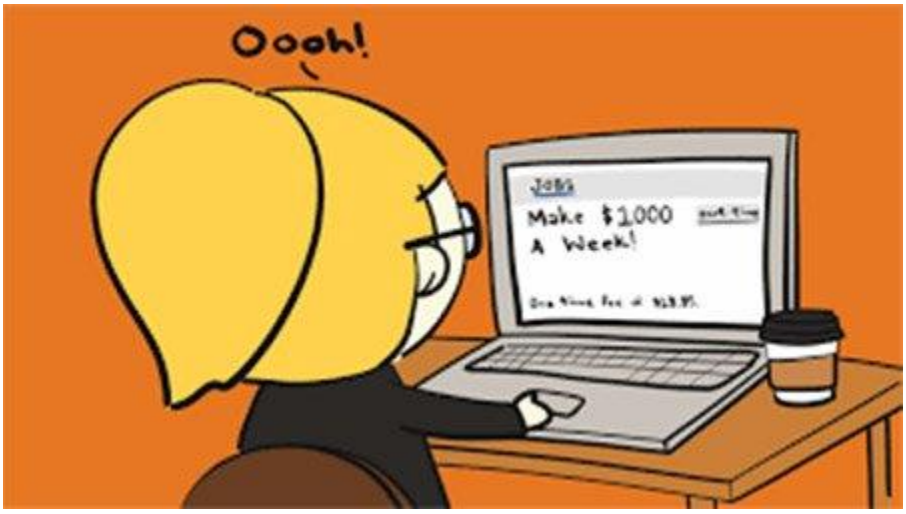
Lừa đảo 419

Lừa đảo 419 hay còn được gọi là lừa đảo Nigeria. Trò lừa này đánh vào lòng tham, hám lợi và sự cả tin của người khác. Danh xưng 419 là lấy từ điều luật chống gian lận của Nigeria. Người ta gọi những kẻ lừa đảo này là 419-er và trò lừa này là kỹ nghệ 419. Những tay lừa đảo này thường gửi email tự xưng mình là kế toán trưởng của một công ty hay là nhân viên một ngân hàng, đề nghị hợp tác với bạn trong những thương vụ có lợi nhuận lớn và yêu cầu thông tin về tài khoản ngân hàng để gửi tiền vào tài khoản của bạn. Nhưng trên thực tế, những thông tin ngân hàng này được sử dụng để chống lại chủ sở hữu hoặc tiền gửi sẽ không được gửi vào tài khoản của bạn.

Lừa đảo đầu tư

Nếu bạn đang tìm kiếm một phương thức nhanh chóng để kiếm tiền, làm giàu thì hãy cẩn thận, những kẻ lừa đảo đã tạo ra rất nhiều kịch bản theo kiểu cơ hội kiếm tiền dễ dàng để săn đón sự nhiệt tình và khao khát làm giàu của bạn từ đó khiến cho bạn “tiền mất tật mạng”.

Lừa đảo việc làm và thu nhập



Hình thức lừa đảo thông qua việc làm sẽ lừa bạn chuyển tiền cho kẻ gian thông qua việc chúng sẽ cung cấp cho bạn những cách thức "được bảo đảm" để kiếm tiền

nhanh chóng hoặc một công việc “việc nhẹ lương cao”. Hình thức lừa đảo này cũng đặc biệt phổ biến ở Việt Nam.

Chiến thuật của Scam Internet

Hầu hết các scam thường bám lấy những đức tính căn bản của con người trong cuộc sống. Rất nhiều điều không phải là thổi phồng. Chúng bao gồm những đặc điểm như nỗi sợ hãy, tính kiêu căng tự phụ và tính tham lam. Nghệ thuật lừa đảo đã tận dụng những đặc điểm này từ hàng trăm năm nay, dựa trên lòng tham của con người và bạn có thể thuyết phục họ vui là buồn và lạnh là nóng.

Điều này cũng có nghĩa là hầu hết những scam trực tuyến có rất ít dấu hiệu. nếu bạn nhận một tin nhắn hoặc lời mời truy cập một trang web cho rằng bạn sẽ rơi vào tình trạng nguy hiểm nếu không tải một số ứng dụng, đây chỉnh là dấu hiệu của một scam. Những thông báo như thế này thường dựa vào nỗi sợ hãi của con người. Tất nhiên, bạn không hề muốn máy tính của mình bị nhiễm virut. Nhưng, những ứng dụng này thường là virut ẩn danh hay một loại nào đó của malware. Hãy cảnh giác cao độ với những thông báo đáng nghi như thế và nhớ tìm hiểu kĩ về bất kì một ứng dụng nào trước khi tải và cài đặt nó.

Hầu hết trong chúng ta không nghĩ rằng mình có tính tự đắc. Tuy nhiên, hãy thử tưởng tượng rằng bạn đang trên mạng xã hội và nhận được một thông báo có chứa đường link, cho rằng “You won't believe how great you look in this video!” (Bạn không thể tưởng tượng rằng bạn trông tuyệt vời thế nào trong video này đâu!). Hầu hết chúng ta sẽ truy cập đường link đó ngay lập tức để xem đoạn video, nhất là khi chúng ta lo rằng nó trông rất hài hước. Có rất nhiều người và tổ chức trên mạng xã hội, bạn không thể biết được ai đó sẽ bị xem.

Những “nghệ nhân” scam nắm bắt được tâm lý mọi người rằng họ rất lo lắn về những tấm hình của mình trên mạng. Đó chính là lý do tại sao chúng sử dụng những thông báo kiểu như thế trên để lừa mọi người truy cập những video giả mạo. Trong nhiều trường hợp, có nhiều video xuất hiện cùng với một cửa sổ pop-up. Cửa sổ này thông báo rằng người dùng không có đúng chương trình chạy video cho đoạn video này và yêu cầu người dùng tải và cài đặt một phần mềm, sau đó video sẽ được hiển thị. Tuy nhiên, chương trình này sẽ hiển thị là malware giả mạo sau đó.

Một số malware có thể gây một số khó khăn nếu bạn cài đặt chúng trên máy tính của mình. Ứng dụng khó phím có thể sao chép mọi thông tin bạn gõ trên bàn phím và gửi ngay thông tin về cho "nghệ nhân" scam. Những người này sẽ lọc bỏ những thông tin bạn gõ trên phím và dễ dàng tìm ra thông tin cá nhân như tên người dùng cũng nwh mật khẩu mà bạn truy cập một trang web nào đó, bao gồm tài khoản ngân hàng hay một trang mua sắm trực tuyến nào đó. Một số khác có thể truy cập trực tiếp vào máy tính của bạn với cracker – một hacker malicious. Cracker này có thể kiểm soát máy tính của bạn mà bạn không để ý tới.

Đâu là một scam?

Không phải tất cả scam lừa mọi người dựa vào lòng tham hoặc tính tự đắc của họ. Một số còn dựa vào lòng vị tha của con người. Scam từ thiện rất phổ biến trên Internet. Vì vậy, bạn nên tìm hiểu kĩ về bất kì lời yêu cầu làm từ thiện nào trước khi quyên góp tiền.

Trong số những chiến thuật scam sử dụng để "săn mồi", lòng tham thường là chiến thuật hay được sử dụng nhất. Những scam này thường hứa hẹn trả một lượng tiền lớn nếu nạn nhân chịu đầu tư một khoản tiền nhỏ. Điều này có nghĩa là lấy một thứ gì đó mà không mất gì cả. Rất nhiều "nghệ nhân" scam sử dụng email để săn mồi. Chúng sẽ gửi hàng tram, thậm chí hàng triệu email tới những nạn nhân tiềm năng. Nếu như thành công chỉ với một phần nhỏ trong số những email mà chúng gửi đi, số tiền lừa được cũng rất lớn.

Khi nhận được một lời mời trên mạng, hãy dành chút thời gian để phân tích nó. Một chút thời gian để suy nghĩ nhưng lại có thể giữ lại tiền cho bạn. Không nên tin vào những đường dẫn hoặc những chứng nhận được gửi kèm theo lời mời. Ngoài ra, hãy tự tìm kiếm thông tin để xác nhận lời mời này có đáng tin cậy hay không. Một số lời mời rất thành thật, trong khi một số khác lại cố gắng thu hút bạn vào scam pyramid scheme (scam theo hình kim tự tháp) hay scam pump-and-dump (lừa đảo chứng khoán qua email).

Một số dấu hiệu dễ phát hiện của scam lừa đảo:

- • Một thông báo yêu cầu bạn phải hành động ngay: "You must act now!"
- • Một lời hứa kiếm được lợi nhuận cao trong một khoảng thời gian ngắn
- • Sử dụng nhiều thuật ngữ và biệt ngữ
- • Khẳng định là thông tin mật hoặc một lời thổ lộ tâm tình

Những “nghệ nhân” scam sẽ cố gắng dùng bất kì điều gì để thuyết phục bạn đưa tiền cho chúng. Gần đây, một số scam thậm chí còn tự xưng là đại diện của chính phủ Mỹ. Chúng gửi tin nhắn tới những nạn nhân tiềm năng với một lời mời đóng góp cho gói kích cầu kinh tế giúp vượt qua giai đoan khủng hoảng kinh tế.

Một số nạn nhân tiềm năng đã quay lại để lừa lại những “nghệ nhân” scam. Một trang web có tên 419 Eater đã thuyết phục mọi người đã bị scam tham gia chống lại scam - scambaiting. Trang web này định nghĩa scambaiting là thu hút những “nghệ nhân”scam khiến chúng mất thời gian và công sức. Một số còn thuyết phục chúng đi một chặng đường dài. Thế mới biết rằng những “nghệ nhân” scam cũng tham lam không kém gì nạn nhân của chúng.

Luôn luôn cẩn thận, không nên tin bất kì thứ gì bạn đọc và hãy nhớ nghĩ thật kĩ trước khi kích vào bất kì thứ gì. Như vậy, bạn mới có thể tránh được mưu mẹo của những kẻ lừa đảo.