ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

LÊ THỊ THU HƯƠNG

CÁC LỪA ĐẢO TRÊN MẠNG MÁY TÍNH VÀ CÁCH PHÒNG TRÁNH

LUẬN VĂN THẠC SỸ CÔNG NGHỆ THÔNG TIN

HÀ NỘI 2016

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

LÊ THỊ THU HƯƠNG

CÁC LỪA ĐẢO TRÊN MẠNG MÁY TÍNH VÀ CÁCH PHÒNG TRÁNH

Ngành: Công nghệ thông tin
Chuyên ngành: Truyền dữ liệu và Mạng máy tính
Mã số:

LUẬN VĂN THẠC SỸ CÔNG NGHỆ THÔNG TIN

HƯỚNG DẪN KHAO HỌC: PGS. TS Trịnh Nhật Tiến

HÀ NỘI 2016

MỤC LỤC

GIỚI THIỆU

Lừa đảo qua mạng (Social Engineering) được thực hiện chủ yếu dựa trên việc khai thác hành vi và tâm lý của người sử dụng Internet; Và các "lỗ hổng" trong hệ thống an ninh mạng máy tính. Được phân làm 2 nhóm:

1- Cố gắng đánh lừa mọi người gửi tiền trực tiếp cho kẻ lừa đảo (ví dụ: giả bộ gặp trục trặc).

2- Lừa đảo nhằm mục đích ăn cắp thông tin cá nhân và dữ liệu máy tính.

Một trong những hình thức lừa đảo qua mạng khá phổ biến là "phishing – lừa đảo giả dạng". Trong phần nghiên cứu này ta sẽ tập trung nghiên cứu vào hình thức lừa đảo giả dạng "***phishing".***

Chương 1 – LÝ THUYẾT CÁC DẠNG LỪA ĐẢO QUA MẠNG

1.1. KHÁI NIỆM LỪA ĐẢO GIẢ DẠNG

Lừa đảo giả dạng (phishing) là loại hình gian lận (thương mại) trên Internet, một thành phần của "Social Engineering – kỹ nghệ lừa đảo" trên mạng. Nguyên tắc của lừa đảo giả dạng là bằng cách nào đó "lừa" người dùng gửi thông tin nhạy cảm đến kẻ lừa đảo; các thông tin như tên, địa chỉ, mật khẩu, số thẻ tín dụng, mã thẻ ATM, số an sinh xã hội,… . Cách thực hiện chủ yếu là mô phỏng lại giao diện đăng nhập trang web của các website có thật, kẻ lừa đảo sẽ dẫn dụ nạn nhân điền các thông tin vào trang "dỏm" đó rồi truyền tải đến anh ta (thay vì đến server hợp pháp) để thực hiện hành vi đánh cắp thông tin bất hợp pháp mà người sử dụng không hay biết.

1.2. LỊCH SỬ LỪA ĐẢO GIẢ DẠNG

Từ "phishing", ban đầu xuất phát từ sự tương đồng giống với cách mà bọn tội phạm Internet đầu tiên sử dụng e-mail để nhử "lừa đảo-phish" cho mật khẩu và các dữ liệu tài chính từ một biển người sử dụng Internet. Việc sử dụng "ph" trong thuật ngữ là một phần bị mất trong biên niên sử của thời gian, nhưng nhiều khả năng liên kết với các hacker đặt tên phổ biến theo hiệp ước chung như "Phreaks" mà dấu vết để lại cho tin tặc đầu tiên, kẻ mà đã tham gia vào "Phreaking" - hacking hệ thống điện thoại.

Thuật ngữ này được đặt ra trong năm 1996 khoảng thời gian của tin tặc kẻ mà đã ăn cắp tài khoản (account) của America Online (AOL) bằng cách lừa đảo mật khẩu từ việc những người dùng AOL không nghi ngờ. Việc đề cập đến đầu tiên được phổ biến rộng rãi trên Internet về Phishing được đưa ra trong "***Ialt.2600 hacker newsgroup in January 1996"***; Tuy nhiên, nhóm này có thể đã được sử dụng ngay cả trước đó trong các hacker nổi tiếng nhất trên Bản tin "2600".

It used to be that you could make a fake account on AOL so long as you had a credit card generator. However, AOL became smart.

Now they verify every card with a bank after it is typed in.

Does anyone know of a way to get an account other than phishing?
—mk590, "AOL for free?" alt.2600, January 28, 1996

Tạm dịch:

Nó được sử dụng để bạn có thể làm giả một tài khoản trên AOL trong 1 thời gian dài giống như bạn đã có một máy tạo thẻ tín dụng. Tuy nhiên, AOL đã trở nên thông minh hơn. Bây giờ họ xác minh mỗi thẻ với ngân hàng sau khi nó được gõ vào.

Liệu rằng có ai biết cách nào khác để có được một tài khoản khác hơn là lừa đảo (phishing)?

-mk590, "AOL for free?" alt.2600, 28 tháng 1 năm 1996

Đến năm 1996, tài khoản bị hack đã được gọi là "lừa đảo-phish", và đến năm 1997 Phish là giao dịch tích cực giữa các hacker như một hình thức tiền tệ điện tử. Có những trường hợp trong đó những kẻ lừa đảo thường xuyên sẽ thương mại 10 việc làm AOL Phish cho một mảnh phần mềm hack hoặc warez (bị đánh cắp bản quyền các ứng dụng và trò chơi). Các phương tiện truyền thông trích dẫn sớm nhất đề cập đến lừa đảo -phishing đã không được thực hiện cho đến tháng 3 năm 1997:

The scam is called 'phishing' — as in fishing for your password, but spelled differently — said Tatiana Gau, vice president of integrity assurance for the online service.

—Ed Stansel, "Don't get caught by online 'phishers' angling for account information," Florida Times-Union, March 16, 1997

Tạm dịch:

Lừa đảo – scam được gọi là 'lừa đảo -phishing' – được ví như việc câu cá khi lừa đảo để "câu" mật khẩu của bạn, nhưng đánh vần khác nhau - Tatiana Gau - phó chủ tịch của công ty bảo hiểm tính toàn vẹn cho các dịch vụ trực tuyến - nhận định.

-Ed Stansel, "Đừng dính tới phishing online - phishers 'những kẻ lừa đảo' cho thông tin tài khoản ", Florida Times-Union, 16 Tháng 3 năm 1997

Qua thời gian, định nghĩa thế nào là một cuộc tấn công lừa đảo-phishing đã bị mờ đi và phát triển rộng hơn. Mục đích của nhóm Phishing không chỉ với việc có được tài khoản chi tiết của người dùng, mà còn gồm cả quyền truy cập vào dữ liệu cá nhân và tài chính. Ban đầu là lừa người dùng trả lời e-mail để đưa ra các mật khẩu và các thông tin chi tiết thẻ tín dụng, về sau dần dần đã mở rộng sang các trang web giả mạo, cài đặt Trojan horse key-logger và ảnh chụp màn hình, và man-in-the-middle dữ liệu proxy - tất cả các tuyến giao thông qua bất kỳ kênh truyền thông điện tử nào.

Do tỷ lệ thành công cao của những vụ lừa đảo, hiện nay nó được lan rộng thành lừa đảo giả dạng –phishing; lừa đảo-scam cổ điển bao gồm việc sử dụng các Jobsites giả hoặc mời làm việc. Ứng viên bị dụ dỗ với khái niệm làm sẽ có rất nhiều tiền cho công việc nhỏ -chỉ cần tạo một tài khoản ngân hàng mới, lấy tiền đó đã được chuyển vào nó (ít hoa hồng cá nhân của họ) và gửi nó vào như một trật tự tiền tệ quốc tế - kỹ thuật rửa tiền cổ điển.

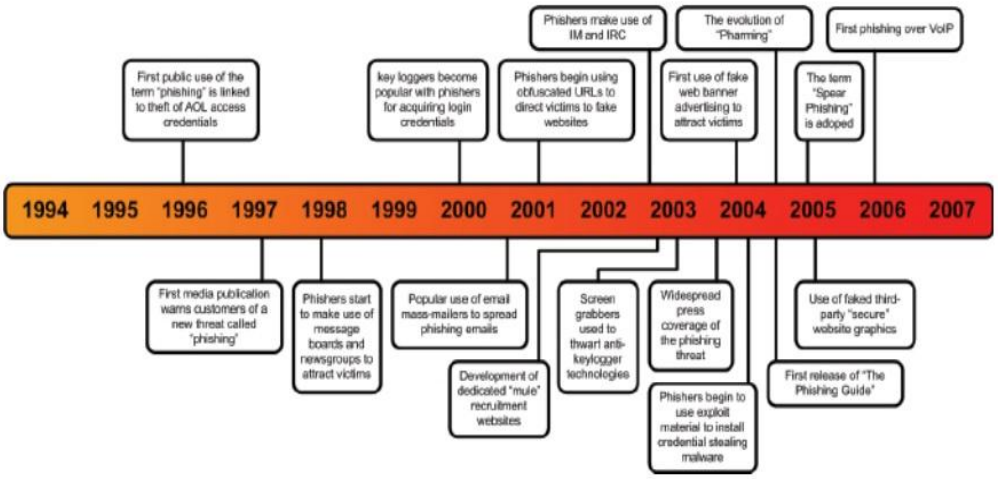


Figure 1: The evolution of "phishing".

1.3. TỔNG HỢP VỀ MỘT SỐ TỔ CHỨC BỊ TẤN CÔNG LỪA ĐẢO GIẢ DẠNG

Thời gian qua, hàng loạt các công ty, hãng công nghệ nổi tiếng trên thế giới trở thành nạn nhân của tin tặc như IMF, Google, Sony, Lockheed Martin, RSA Security, và CitiGroup.

Sau đây là một số thống kê các cuộc tấn công, xâm nhập thành công của tin tặc vào các công ty, hãng công nghệ nổi tiếng thời gian gần đây.

IMF (Quỹ Tiền tệ Quốc tế)

Tin tặc đã tiến hành các cuộc tấn công trước ngày 14/5/2011, khi Strauss-Kahn, cựu Tổng giám đốc IMF bị bắt tại New York. Cuộc tấn công xâm nhập vào máy chủ của Quỹ Tiền tệ Quốc tế (IMF) có thể do các tin tặc, làm việc cho chính phủ nào đó ở nước ngoài, thực hiện. Tin tặc đã đánh cắp số lượng lớn dữ liệu bao gồm email và nhiều tài liệu khác. Các dữ liệu của IMF rất nhạy cảm vì nó chứa rất nhiều thông tin bí mật về tình hình tài chính của nhiều quốc gia trên thế giới và nó có thể ảnh hưởng đến thị trường toàn cầu. Tuy nhiên, hiện vẫn chưa có thông tin rõ ràng về các tài liệu mà tin tặc đã đánh cắp.

CitiGroup

Sau cuộc tấn công vào cổng thông tin điện tử của CitiGroup, tin tặc đã lấy cắp dữ liệu chứa thông tin cá nhân của khoảng 210.000 chủ thẻ CitiGroup. Các thông tin này bao gồm tên chủ thẻ, số tài khoản, thông tin liên lạc như địa chỉ email.

Google

Hôm 1/6/2011, Google cho biết hãng phát hiện các cuộc xâm nhập đánh cắp hàng trăm tài khoản người dùng và mật khẩu Gmail. Trong số các tài khoản bị đánh cắp, có rất nhiều tài khoản của các quan chức chính phủ Mỹ, các quan chức ở khu vực châu Á, các nhà báo…

Google không biết chắc chắn về phương thức tấn công xâm nhập của tin tặc, nhưng hãng cho rằng, có thể tin tặc dùng Phishing. Google nói rằng hệ thống nội bộ của hãng vẫn an toàn và hãng đã thực hiện các biện pháp bảo mật cho các tài khoản đã bị tin tặc đánh cắp.

Lockheed Martin

Lockheed Martin, nhà thầu quốc phòng lớn cho chính phủ Mỹ, cũng là nạn nhân của các cuộc tấn công xâm nhập.

Lockheed Martin cho biết ngay khi phát hiện sự xâm nhập, hãng đã thực hiện các biện pháp bảo vệ dữ liệu và hệ thống. Lockheed Martin nói rằng tin tặc không lấy được bất kỳ dữ liệu nào về khách hàng, các chương trình và thông tin nhân viên. Các báo cáo cho rằng, tin tặc đã sử dụng thẻ bài bảo mật token, được ăn cắp sau cuộc tấn công vào RSA Security, để xâm nhập vào hệ thống của Lockheed Martin.

RSA Security

Tháng 3/2011, EMC thông báo cho người dùng của hãng biết rằng RSA Security, một công ty của hãng, là nạn nhân của "cuộc tấn công xâm nhập cực kỳ tinh vi". EMC cho biết tin tặc đã đánh cắp dữ liệu liên quan đến hệ thống xác thực 2 yếu tố SecurID (SecurID two-factor authentication system) của RSA.

Tại thời điểm đó, EMC tự tin nói rằng dữ liệu mà tin tặc đã đánh cắp sẽ không thể sử dụng để "làm hại bất kỳ ai" đang dùng RSA SecurID. Tuy nhiên, sau đó, EMC tiết lộ tin tặc đã dùng SecurID đánh cắp được để xâm nhập vào hệ thống của Lockheed Martin. "Cuộc tấn công xâm nhập cực kỳ tinh vi" mà EMC tuyên bố trước đó, thực ra là "lỗi" do một nhân viên của RSA Security tải về tập tin Excel nhiễm độc trên email.

Epsilon

Tháng 4/2011, tin tặc xâm nhập vào máy chủ của Epsilon, hãng tiếp thị qua email lớn nhất thế giới, lấy cắp danh bạ: tên, địa chỉ email. Tin tặc đánh cắp cơ sở dữ liệu khách hàng của Epsilon, trong đó có rất nhiều tên tuổi lớn như JPMorgan Chase, Capital One, Marriott Rewards, US Bank, Citigroup, và Walgreens.

Sony

Vụ tấn công mạng nhằm vào hãng Sony Pictures có thể đi vào lịch sử như vụ xâm nhập mạng máy tính lớn nhất năm 2014.

Ngày 24/11/2014, các tin tặc tự xưng là **"Những người bảo vệ hòa bình"** *(Guardians of Peace – GOP)* đã phát động cuộc tấn công vào Sony Pictures Entertainment, lấy cắp nhiều terabyte dữ liệu nhạy cảm. Các thông tin số an sinh xã hội, hộp thư điện tử và tiền lương của các ngôi sao và nhân viên của Sony, cũng như bản sao các bộ phim chưa phát hành đã bị tung lên mạng.

Nhiều người suy đoán Bắc Triều Tiên đứng sau vụ rò rỉ dữ liệu lớn này vì cuộc tấn công xảy ra vài ngày trước sự kiện ra mắt dự kiến của "**The Interview**", bộ phim hài về một vụ ám sát hư cấu của CIA nhằm vào nhà lãnh đạo Triều Tiên Kim Jong-un.

Ngày 19/12/2014, FBI chính thức cáo buộc Bắc Triều Tiên chịu trách nhiệm về cuộc tấn công này, mặc dù Bình Nhưỡng đã nhiều lần bác bỏ sự liên quan đến vụ hack này.

Phim "The Interview" kể từ khi được phát hành đã bị dư luận đánh giá khác nhau, từ khen ngợi cho đến chỉ trích.

Chương 2. CÁC PHƯƠNG PHÁP LỪA ĐẢO GIẢ DẠNG

2.1. NHỮNG YẾU TỐ ĐỂ CUỘC TẤN CÔNG LỪA ĐẢO GIẢ DẠNG THÀNH CÔNG

2.1.1. Sự thiếu hiểu biết

Sự thiếu hiểu biết về hệ thống mạng và máy tính đã giúp cho các hacker khai thác những thông tin nhạy cảm.

Cần hiểu rõ rằng quá trình hoạt động của internet, hoặc ít hơn hiểu về cách thức truy cập một website an toàn. Điển hình nhất cần phải biết đó là việc bấm vào nút Save Password khi truy cập web tại các điểm công cộng sẽ làm tăng nguy cơ bị xâm phạm tài khoản cá nhân. Đặc biệt đối với những người thường xuyên mua bán, thanh toán qua mạng thì cần phải hiểu rõ việc cung cấp credit card là rất quan trọng và biết được khi nào nên cung cấp, khi nào không. Người sử dụng cũng nên tìm hiểu sơ về các giao thức mạng, và phân biệt được giao thức nào là an toàn. Điển hình là người dùng cần phải hiểu đừng bao giờ giao dịch trực tuyến với giao thức truy cập web là **http**, mà phải đảm bảo an toàn với giao thức **https.**

Những cửa sổ cảnh báo của windows về mức độ an toàn của việc truy cập thông tin thường hay bị bỏ qua, lại là nguy cơ chính biến người dùng thành nạn nhân.

Thói quen duyệt email không tốt cũng làm cho người dùng gặp nhiều nguy hiểm. Có một số lời khuyên khi sử dụng email đó là cẩn thận với những email không có địa chỉ người gửi rõ ràng, email không có tiêu đề, hoặc là nội dung có tính kích động trí tò mò.

2.1.2. Nghệ thuật đánh lừa ảo giác

Nghệ thuật của sự đánh lừa ảo giác chính là làm cho nạn nhân không còn phân biệt được đâu là thật đâu là giả. Chắc hẳn bạn cũng biết trò chơi tìm những điểm khác nhau giữa hai tấm hình. Kỹ thuật đánh lừa ảo giác sẽ tạo ra một trang web, hoặc một lá

thư…những thứ mà ngày nào bạn cũng truy cập, nó giống nhau đến mức gần như người ta không thể phát hiện ra sự giả mạo.

Lời khuyên dành cho người sử dụng đó là cẩn thận với những trang web thường truy cập, đặc biệt là những email của ngân hàng, của những người thân của ta mà tự nhiên lại yêu cầu chúng ta cung cấp thông tin cho họ, hãy cảnh giác bởi những trang đó có nguy cơ giả mạo rất cao. Thứ hai là hãy tự ghõ địa chỉ trang web vào trình duyệt, thay vì click vào đường link từ trang web khác. Có nghĩa là hãy tự gõ vào trình duyệt địa chỉ thay vì click vào một liên kết trong email để nó chuyển đến với trang có nội dung giống hệt trang như trang amazone.

2.1.3. Không chú ý đến những chỉ tiêu an toàn

Như đã nói ở trên, những cảnh báo thường bị người dùng bỏ qua, chính điều đó đã tạo điều kiện cho hacker tấn công thành công hơn. Người dùng cũng thường không chú ý đến những chỉ tiêu an toàn. Ví dụ khi bạn truy cập một website thanh toán trực tuyến, bạn phải hiểu những quy định an toàn của website kiểu này, như thông tin về giấy chứng nhận (Cerificate), nhà cung cấp, nội dung, và nhiều quy định khác. Windows thường nhận biết những quy định an toàn này, và nếu không đủ nó sẽ lập tức cảnh báo cho người sử dụng. Tuy nhiên, có một số người dùng cảm thấy phiền phức với những cảnh báo này và đã tắt chức năng này đi, vì thế mà họ dễ dàng trở thành nạn nhân.

Đôi khi, chúng ta cũng nên dành thời gian cho việc đọc tin tức về thế giới hacker để biết được những thủ đoạn lừa lọc mới được phát minh, từ đó có ý thức về sự cảnh giác an toàn hơn.

2.2. NHỮNG PHƯƠNG THỨC CỦA LỪA ĐẢO GIẢ DẠNG

2.2.1. Thư điện tử và thư rác (Email and Spam)

Kỹ thuật tấn công “Phishing” phổ biến nhất là dùng email. Hacker sẽ tiến hành gửi hàng loạt các thư đến những địa chỉ email hợp lệ. Bằng những kỹ thuật và công cụ

khác nhau, hacker tiến hành thu thập địa chỉ email trước. Việc thu thập địa chỉ email hàng loạt không hẳn là bất lợi nếu biết sử dụng đúng cách. Điển hình là chiến lược quảng cáo cần rất nhiều đến sự trợ giúp của hàng loạt địa chỉ email này. Tuy nhiên hacker đã lợi dung việc này để gửi đi những lá thư có nội dung bên ngoài có vẻ hợp lệ. Những nội dung này thường có tính khẩn cấp, đòi hỏi người nhận thư phải cung cấp thông tin ngay lập tức.

Hacker sử dụng giao thức SMTP kèm theo một số kỹ thuật để giả mạo trường "Mail From" khiến cho người nhận không có chút nghi ngờ nào.

Nội dung email được gửi thường sẽ có vài đường link cho bạn liên kết đến một trang web. Như đã trình Ví dụ, hacker sẽ giả email được gửi từ ngân hàng, và yêu cầu người dùng cung cấp thông tin cá nhân để mở lại tài khoản do một sự cố nào đó.bày ở trên, những link này nếu không cẩn thận sẽ cho là link đến một trang web giả mạo do hacker dựng nên.

Dưới đây là một ví dụ về một email giả mạo danh ngân hàng Citibank gửi đến khách hàng.

Mã

```
// ————————————————————————————————————————————————————————————Received: from host70-72.pool80117.interbusiness.it ([80.117.72.70])          by mailserver with SMTP          id <20030929021659s1200646q1e>; Mon, 29 Sep 2003 02:17:00 +0000Received: from sharif.edu [83.104.131.38] by host70-72.pool80117.interbusiness.it (Postfix) with ESMTP id EAC74E21484B for <e-response@securescience.net>; Mon, 29 Sep 2003 11:15:38 +0000Date: Mon, 29 Sep 2003 11:15:38 +0000 From: Verify <verify@citibank.com>Subject: Citibank E-mail Verification: e-response@securescience.net To: E-Response <e-response@securescience.net> References: <F5B12412EAC2131E@securescience.net> In-Reply-To: <F5B12412EAC2131E@securescience.net> Message-ID: <EC2B7431BE0A6F48@citibank.com>Reply-To: Verify <verify@citibank.com> Sender: Verify <verify@citibank.com> MIME-Version: 1.0 Content-Type: text/plain Content-Transfer-Encoding: 8bit
Dear Citibank Member, This email was sent by the Citibank server to verify your e-
```

mailaddress. You must complete this process by clicking on the link below and entering in the small window your Citibank ATM/Debit Card number and PIN that you use on ATM. This is done for your protection -t- becaurse some of our members no longer have access to their email addresses and we must verify it.
To verify your e-mail address and access your bank account, click on the link below. If nothing happens when you click on the link (or if you use AOL)K, copy and paste the link into the address bar of your web browser.
http://www.citibank.com:ac=piUq3027qcHw003nfuJ2@sd96V.pIsEm.NeT/3/?3X6CMW2I2uPOVQW y

———————————— Thank you for using Citibank!

C————————————
This automatic email sent to: e-response@securescience.net Do not reply to this email.
R_CODE: ulG1115mkdC54cbJT469
// ————————————————————————————

Nếu quan sát kỹ, chúng ta sẽ thấy một số điểm "thú vị" của email này: Về nội dung thu: Rõ là câu cú, ngữ pháp lộn xộn, có cả những từ sai chính tả, ví dụ: becaurse, this automatic,… Và ai cũng rõ là điều này rất khó xảy ra đối với một ngân hàng vì các email đều được "chuẩn hóa" thành những biểu mẫu thống nhất nên chuyện "bị sai" cần phải được xem lại.

Email trên có chứa những ký tự hash-busters – là những ký tự đặc biệt để vượt qua các chương trình lọc thư rác (spam) – dựa vào kỹ thuật hash-based spam nhưu "-t-" , "K" ở phần chính thư và "y", "C" ở cuối thư. Người nhận khác nhau sẽ nhận những spam với những hash-busters khác nhau. Mà một email thật, có nguồn gốc rõ ràng thì đâu cần phải dùng đến các "tiểu xảo" đó.

Phần tiêu đề (header) của email không phải xuất phát từ mail server của Citibank. Thay vì mang 2-a.citicorp.com (mail server chính của Citybank ở Los Angeles) thì nó lại đến từ Italia với địa chỉ host70-72.pool80117.interbusiness.it (80.117.72.70) vốn không thuộc quyền kiểm soát của CityBank. Lưu ý, mặc định Yahoo Mail hay các POP Mail Client không bật tính năng xem header, các bạn nên bật vì sẽ có nhiều điều hữu ích.

Tiếp theo với liên kết ở dưới:

http://www.citibank.com:ac=piUq3027qcHw0…CMW2I2uPOV QW

Nhìn thoáng quá thì có vẻ là xuất phát từ Citibank, nhưng thực tế bạn hãy xem đoạn phía sau chữ @. Đó mới là địa chỉ thật và "sd96V.pIsEm.Net" là một địa chỉ giả từ Mạc Tu Khoa, Nga – hoàn toàn chẳng có liên quan gì đến Citibank.

Kẻ tấn công đã lợi dụng lỗ hổng của trình duyệt web để thực thi liên kết giả.

2.2.2. Phát tán dựa trên các trang mạng (Web-based Delivery)

Một kỹ thuật tiếp theo của Phishing là dựa vào việc phát tán các website lừa đảo. Bạn thường thấy các website dạng như kiếm tiền online. Chúng yêu cầu bạn cung cấp các thông tin tài khoản ngân hàng để tiến hành trả tiền công. Bạn không ngần ngại gì khi đang chờ đợi số tiền công hậu hĩnh. Kết cuộc tiền công không thấy mà tiền trong tài khoản cũng không còn.

Một hình thức khác là khiêu khích sự tò mò của người dùng. Bằng cách chèn vào trang web những biển hiệu (banner) hoặc những dòng chữ (text) quảng cáo có ý khiêu khích sự tò mò của người dùng. Ví dụ như những hình ảnh khiêu dâm, những nội dung đang nóng. Kết quả sau khi click vào đó thì máy tính của bạn có thể bị nhiễm một loại virus malware nào đó, virus này sẽ phục vụ cho một cộng tấn công khác.

2.2.3. Mạng lưới trò chuyện trực tuyến và tin nhắn khẩn (Irc and Instant Messaging)

"Chat" là thuật ngữ quá quen thuộc với mọi người, hay còn gọi là trò chuyện trực tuyến. Nó rất hữu ích trong giao tiếp. Tuy nhiên, những kẻ lừa đảo đã bắt đầu lợi dụng vào việc "chat chit" này để tiến hành các hành động lừa đảo. Bằng những kỹ thuật tấn công, những kẻ lừa đảo tiến hành gửi tin nhắn tức thì đến hàng loạt người dùng. Những nội dung được gửi thường có liên quan đến hàng loạt người dùng, và cũng lợi dụng vào trí tò mò của mọi người.

Vì tính không nhất quán của việc trò chuyện trực tuyến (online), những người trò chuyện online thường không thấy mặt nhau nên không thể biết người đang nói chuyện với mình có tin cậy hay không. Kỹ thuật tinh vi của kiểu lừa đảo này là giả dạng nick chat.

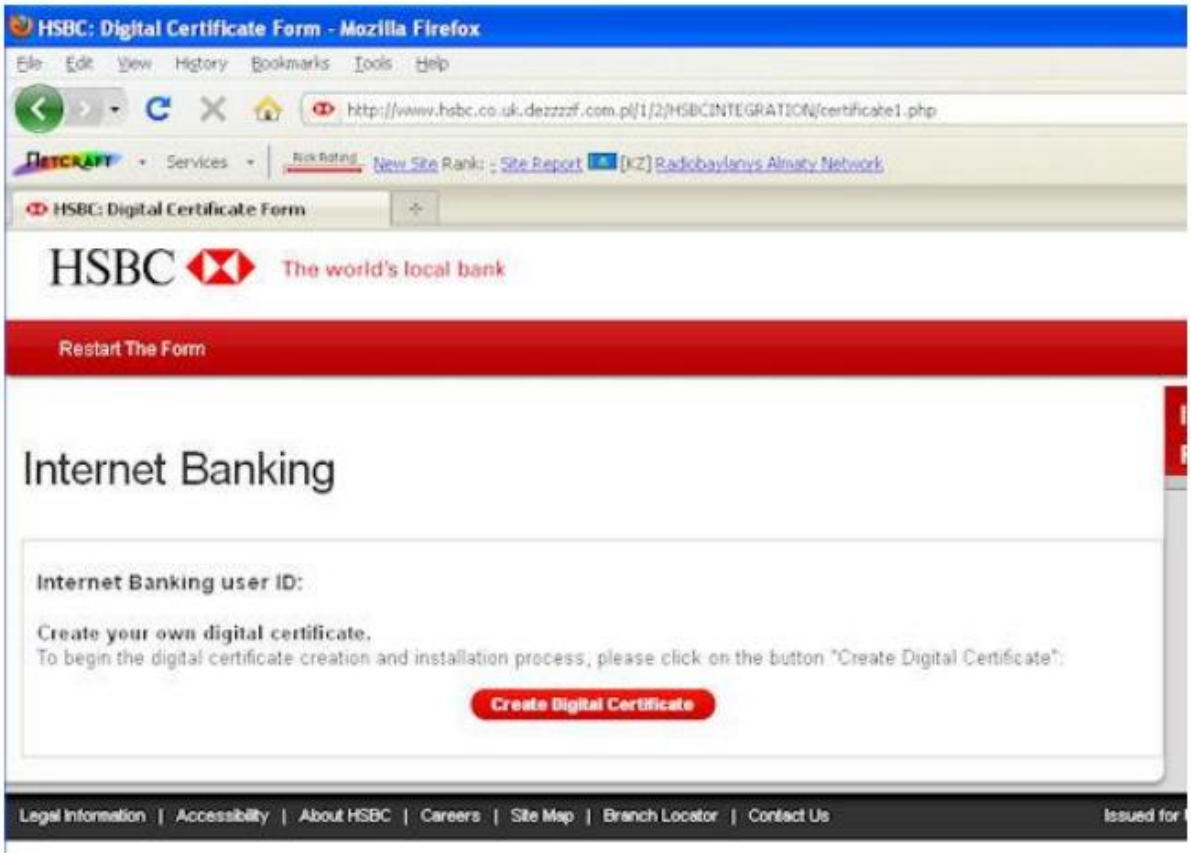
Bằng cách giả một nick chat của người quen để tiến hành trò chuyện và yêu cầu cung cấp thông tin hoặc lừa đảo làm một việc gì đó. Gần đây ở Việt Nam nở rộ tình trang lừa đảo này. Nhiều người dùng chat với bạn bè người thân của mình, và họ được nhờ vả việc nạp tiền điện thoại di động. Nạn nhân vì thấy "nick" đang "chat" là của người quen nên không chút ngần ngại nào trong việc được nhờ vả này.

2.2.4. Các máy tính bị nhiễm phần mềm gián điệp (Trojaned Hosts)

Như đã nói ở phần trước, lừa đảo không những chỉ nhắm đến những thông tin cá nhân của nạn nhân, mà còn nhiều hình thứ khác. Một kiểu lừa đảo khác là lừa cho nạn nhân cài vào máy tính của mình một phần mềm gián điệp. Phần mềm gián điệp (trojan, keylog) này sẽ phục vụ cho một mục đích tấn công khác.

Điển hình của công việc này là nạn nhân bị nhiễm trojan và trở thành một máy tính con trong một cuộc tấn công tổng thể trên diện rộng.

Dưới đây là hình minh họa việc giả mạo một trang web của ngân hàng để cài trojan Zeus vào máy tính nạn nhân.



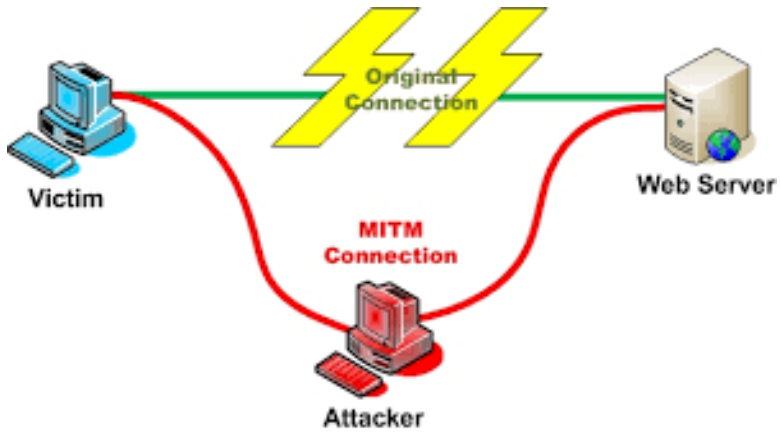
Một trang web lừa đảo, nhấp vào nút "Create Digital Certificate" sẽ tải về các trojan Zeus đến máy tính của nạn nhân.

2.3. CÁC KIỂU LỪA ĐẢO GIẢ DẠNG

Dựa vào những phương thức trên, những kẻ lừa đảo bắt đầu tiến hành quá trình lừa đảo. Căn cứ theo cách thức hoạt động, người ta phân loại những cuộc tấn công lừa đảo ra thành các loại sau.

2.3.1. Tấn công MITM

Ở kỹ thuật này, máy tính của kẻ tấn công được xem như là máy tính trung gian giữa máy tính của người dùng và website thật. Những kẻ tấn công dựng lên một máy tính trung gian để nhận dữ liệu của người dùng và chuyển nó cho website thật. Hoặc nhận dữ liệu của website thật rồi chuyển cho người dùng. Dữ liệu khi chuyển qua lại sẽ được lưu trữ lại tại máy tính của kẻ tấn công.



Tấn công MITM (Main-in-the-Middle)

Thoạt nghe mô tả này chúng ta nghĩ ngay đến chức năng của Proxy Server. Đúng vậy, là do proxy chính là những nơi không tin cậy cho lắm khi chúng ta truy cập web thông qua nó. Những kẽ tấn công sẽ dựng lên một Proxy Server với lời mời gọi sử dụng được tung ra internet. Vì lý do gì đó (để giả IP trong quá trình mua bán hàng qua mạng) người dùng sẽ tìm đến Proxy Server này để nhờ giúp đỡ trong việc truy cập web. Và thế là vô tình người dùng trở thành con mồi cho bọn hacker.

Những kẽ tấn công ngoài việc dựng lên Proxy Server giả rồi dụ con mồi đến còn nghĩ đến việc tấn công vào các Proxy Server thật này để lấy dữ liệu. Bằng những kỹ thuật tấn công khác nhau, hacker xâm nhập hệ thống lưu trữ của Proxy để lấy dữ liệu, phân tích và có được những thứ mà chúng cần.

Một cách khác để tấn công trong kỹ thuật này, là tìm cách làm lệch đường đi của gói dữ liệu. Thay vì phải chuyển gói tin đến cho Web-server, thì đằng này là chuyển đến máy tính của hacker trước, rồi sau đó máy tính của hacker sẽ thực hiện công việc chuyển gói tin đi tiếp. Để làm điều này, hacker có thể sử dụng kỹ thuật DNS Cache Poisoning – là kỹ thuật làm lệch đường đi của gói dữ liệu bằng cách làm sai kết quả phân giải địa chỉ của DNS.

Một điểm cần lưu ý rằng, kỹ thuật tấn công này không phân biệt giao thức web là HTTP hay HTTPS.

2.3.2. Các cuộc tấn công gây rối URL (URL Obfuscation Attacks)

URL thường được sử dụng trong thanh địa chỉ của trình duyệt để truy cập vào một trang web cụ thể. Làm rối URL (URL Obfuscation) là làm ẩn hoặc giả mạo URL xuất hiện trên các thanh địa chỉ một cách hợp pháp. Ví dụ địa chỉ http://204.13.144.2/Citibanj có thể xuất hiện là địa chỉ hợp pháp cho ngân hành Citibank, tuy nhiên thực tế thì không. Phương pháp tấn công làm rối URL sử dụng để làm cho cuộc tấn công và lừa đảo trực tuyến trở nên hợp pháp hơn. Một trang web xem qua thì hợp pháp với hình ảnh, tên tuổi của công ty, nhưng những liên kết trong đó sẽ dẫn đến những trang web của hacker.

Việc giả mạo có thể nhắm đến những người dụng bất cẩn. Ví dụ bạn vào trang với địa chỉ là http://ebay.com và thực hiện giao dịch bình thường. Tuy nhiên, bạn đã vào trang giả mạo của hacker, vì trang web của ebay là https://ebay.com Khác biệt là ở chổ giao thức http và https.

2.3.3. Tấn công XSS (Cross-Site Scripting Attacks)

Cross-Site Scripting (XSS) là một trong những kỹ thuật tấn công phổ biến nhất hiện nay, đồng thời nó cũng là một trong những vấn đề bảo mật quan trọng đối với các nhà phát triển web và cả những người sử dụng web. Bất kì một website nào cho phép người sử dụng đăng thông tin mà không có sự kiểm tra chặt chẽ các đoạn mã nguy hiểm thì đều có thể tiềm ẩn các lỗi XSS.

Cross-Site Scripting hay còn được gọi tắt là XSS (thay vì gọi tắt là CSS là để tránh nhầm lẫn với CSS-Cascading Style Sheet của HTML) là một kĩ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP …). Các hacker sẽ chèn những đoạn script độc hại (thông thường là javascript hoặc HTML) vào website và sẽ

được thực thi ở phía người dùng (trong trình duyệt của người dùng). Đối với XSS, người bị tấn công là người dùng chứ không phải website, hacker có thể dùng XSS để gửi những đoạn script độc hại tới một người dùng bất kỳ, và trình duyệt của người dùng sẽ thực thi những đoạn script đó và gửi về cho hacker những thông tin của người dùng thông qua email hoặc server do hacker định sẵn từ trước.

Phụ thuộc vào mục đích của hacker, những đoạn Javascript được chèn vào để lấy những thông tin như:

+ **Cookie**: hacker có thể lấy được cookie của người dùng và dùng những thông tin trong cookie để giả mạo phiên truy cập hoặc lấy những thông tin nhạy cảm khác được lưu trong cookie.

+ **Keylogging:** hacker có thể ghi lại những thao tác gõ phím của người dùng bằng cách sử dụng sự kiện *addEventListener* trong Javascript và gửi tất cả những thao tác gõ phím đó về cho hắn để thực hiện những mục đích như đánh cắp các thông tin nhạy cảm, lấy mật khẩu truy cập website hoặc mã số thẻ tín dụng…

+ **Phishing**: hacker có thể thay đổi giao diện của website bằng cách thay đổi cấu trúc HTML trong trang web để đánh lừa người dùng. Hacker có thể tạo ra những dạng đăng nhập giả nhằm lừa người dùng đăng nhập vào để đánh cắp mật khẩu.

2.3.4. Tấn công ẩn (Hidden Attacks)

Attacker sử dụng các ngôn ngữ lập trình HTML, DHTML, hoặc ngôn ngữ dạng script khác để chèn vào trình duyệt của người dùng. Hoặc sử dụng các ký tự đặc biệt để đánh lừa người dùng. Những phương thức thường được attacker sử dụng là làm ẩn các frame. Các Frame sẽ được attacker làm ẩn đi trên trình duyệt của người dùng, qua đó attacker có thể chèn vào những đoạn mã độc. Một cách khác để tấn công là ghi đè nội dung trang web hoặc thay đổi hình ảnh trên trang web. Qua những nội dung bị thay đổi này, attaker sẽ chèn những đoạn mã độc hại vào đó.

Chương 3. PHƯƠNG PHÁP PHÒNG TRÁNH LỪA ĐẢO GIẢ DẠNG

Như đã trình bày trong Chương II, những kẻ lừa đảo giả dạng (phisher) có một số lượng lớn các phương pháp riêng của chúng - hậu quả là không có giải pháp riêng có khả năng chống lại mọi hướng tấn công khác nhau. Tuy nhiên, vẫn có thể ngăn chặn các cuộc tấn công lừa đảo hiện nay và trong tương lai bằng cách sử dụng một hỗn hợp kỹ thuật và công nghệ bảo mật, bảo toàn thông tin.

Để bảo vệ tốt nhất, những kỹ thuật và công nghệ bảo mật thông tin phải được được triển khai tại ba lớp hợp lý:

1. Client-side - bao gồm máy tính của người dùng.

2. Server-side - bao gồm các 'Internet kinh doanh có khả năng nhìn thấy các hệ thống và các ứng dụng tùy chỉnh.

3. Enterprise- Mức doanh nghiệp - công nghệ được phân phối và các dịch vụ quản lý bên thứ 3.

Phần này sẽ mô tả chi tiết về các cơ chế quốc phòng khác nhau tại mỗi lớp hợp lý.

3.1. PHÍA MÁY TRẠM

Phía máy trạm (client) nên được xem như là đại diện hàng đầu về an ninh (anti-phishing). Do tính chất phân bổ tự nhiên của máy tính cá nhân và trình độ kỹ năng và nhận thức khách hàng rất khác nhau, nên an ninh phía khách hàng thường nghèo hơn nhiều so với việc triển khai quản lý máy trạm của công ty. Tuy nhiên, vẫn có nhiều giải pháp hiện thời được sử dụng trong cả gia đình và môi trường doanh nghiệp.

Ở phía khách hàng, khả năng bảo vệ chống lại lừa đảo có thể được tạo nên với:

• Các công nghệ bảo vệ máy tính để bàn.

• Sử dụng các thiết lập/cài đặt truyền thông phù hợp.

• Giải pháp giám sát mức độ ứng dụng người dùng.

• Khả năng khóa các trình duyệt.

• Chữ ký số và xác thực đối với email.

• Các nhận thức an ninh chung của khách hàng.

3.1.1. Các doanh nghiệp bảo vệ máy tính để bàn

Hầu hết người dùng của hệ thống máy tính để bàn đã quen thuộc với phần mềm bảo vệ cài đặt cục bộ, là cách thường thấy trong các hình thức của một giải pháp chống virus phổ biến. Lý tưởng nhất, hệ thống máy tính để bàn nên được cấu hình để sử dụng bảo vệ nhiều doanh nghiệp máy tính để bàn (ngay cả khi tính năng này sao lại bất kỳ dịch vụ bảo vệ nào trong phạm vi công ty), và có khả năng thực hiện các dịch vụ sau:

• Bảo vệ phòng chống Virus cục bộ (Anti-Virus)

• Tường lửa cá nhân

• IDS cá nhân

• Phòng chống thư rác (Anti-Spam) đối với từng cá nhân.

• Phát hiện Spyware

Nhiều nhà cung cấp phần mềm bảo vệ máy tính để bàn (như Symantec, McAfee, Microsoft, vv) hiện nay cung cấp các giải pháp có khả năng hoàn thành một hoặc nhiều hơn các chức năng. Đặc biệt để lừa đảo hướng (vector) tấn công, thì các giải pháp này nên được cung cấp các chức năng sau đây:

• Khả năng phát hiện và ngăn chặn "on the fly" cố gắng để cài đặt phần mềm độc hại (như ngựa Trojan, key-logger, màn hình grabber và tạo backdoors) thông qua file đính kèm e-mail, file downloads, HTML động và nội dung kịch bản.

• Khả năng xác định/nhận dạng các kỹ thuật gửi thư rác phổ biến và các tin nhắn vi phạm kiểm duyệt trong 40 ngày.

• Khả năng tải xuống bản phòng chống virus (anti-virus) mới nhất và khả năng chống chữ ký rác –spam và gán chúng vào các phần mềm bảo vệ có tính ngăn chặn. Với sự đa dạng về các kỹ thuật gửi thư rác (spam), quá trình này nên được sắp xếp như một hoạt động hàng ngày.

• Khả năng phát hiện và ngăn chặn trái phép kết nối từ phần mềm cài đặt hoặc các quá trình hoạt động. Ví dụ, nếu máy chủ của khách hàng trước đó đã bị xâm nhập, các giải pháp bảo vệ phải có khả năng truy vấn tính xác thực của các kết nối ràng buộc với bên ngoài (out-bound) và kiểm tra điều này với người sử dụng.

• Khả năng phát hiện bất thường trong hồ sơ lưu lượng mạng (cả inbound và outbound) và biện pháp đối phó thích hợp đầu tiên. Ví dụ, phát hiện một kết nối HTTP--inbound đã được thực hiện và lưu lượng SSL-outbound cho thấy có sự bắt đầu xâm nhập không chính đáng vào một cổng nào đó trên hệ thống.

• Khả năng để ngăn chặn: các kết nối gửi đến bị mất kết nối (unassociated) hay cổng mạng bị hạn chế và các dịch vụ.

• Khả năng xác định cài đặt Spyware phổ biến và khả năng ngăn chặn cài đặt của phần mềm hoặc ngăn chặn thông tin liên lạc ra bên ngoài vào những trang web giám sát, Spyware.

• Tự động chặn việc giao hàng ra nước ngoài khi có các thông tin nhạy cảm với bên bị nghi ngờ có chứa thành phần độc hại. Bao gồm các thông tin nhạy cảm như chi

tiết tài chính bí mật và các thông tin liên lạc. Ngay cả khi khách hàng không thể xác định bằng trực quan, thì các trang web thực sự sẽ nhận được các thông tin nhạy cảm, một số sẽ loại ra khỏi hệ thống bằng các giải pháp phần mềm tương ứng.

Ưu điểm

- Nâng cao nhận thức và nâng cao cảnh giác phòng thủ mang tính nội bộ.

- Cài đặt cục bộ đối với các doanh nghiệp mong muốn bảo vệ các máy tính cá nhân đang trở nên dễ dàng hơn, và hầu hết khách hàng dần dần đã có những đánh giá cao về giá trị của các phần mềm chống virus.

- Đây là một quá trình đơn giản nhằm mở rộng phạm vi hướng tới các doanh nghiệp có chế độ bảo vệ khách hàng khác nhau và nắm được các khách hàng có nhu cầu sử dụng dịch vụ (buy-in).

- Có sự kết hợp bảo vệ chéo (protection Overlapping).

- Sử dụng một loạt các doanh nghiệp có chế độ bảo vệ máy tính cá nhân từ các nhà sản xuất phần mềm khác nhau có xu hướng tạo nên hiệu ứng bảo vệ chéo trong quá trình bảo vệ tổng thể. Điều này có nghĩa là một lỗi nào đó trong sản phẩm hay một lỗi an ninh trong một sản phẩm có thể được phát hiện và được bảo vệ để chống lại lừa đảo giả dạng bằng những cách khác nhau.

- Bảo vệ chuyên sâu (Defense-in-Depth).

- Tính chất độc lập tự nhiên của các doanh nghiệp có đặt chế độ bảo vệ máy tính cá nhân đồng nghĩa với việc chúng không ảnh hưởng (hoặc là bị ảnh hưởng bởi) các chức năng bảo mật của các tổ chức dịch vụ mở rộng khác - qua đó góp phần vào kế hoạch bảo vệ chuyên sâu (Defense-in-depth) của tổ chức.

Nhược điểm

- Chi phí đặt mua cao (purchasing price).

- Chi phí của doanh nghiệp bảo vệ máy tính cá nhân không phải là một sự đầu tư đáng kể cho nhiều khách hàng. Nếu các giải pháp của nhiều nhà cung cấp được yêu cầu cung cấp bảo hiểm đối với tất cả các hướng tấn công, như vậy sẽ có một phép nhân đáng kể về chi phí tài chính mà chỉ dùng cho phạm vi bảo mật nhỏ được thêm vào.

- Cần gia hạn thuê bao (Subscription Renewals).

- Đa số các doanh nghiệp bảo vệ máy tính để bàn hiện nay dựa trên các khoản thanh toán thuê bao hàng tháng hoặc hàng năm để giữ người dùng hiện thời. Trừ khi có thông báo phù hợp đưa ra, những gia hạn có thể không diễn ra và sự bảo vệ sẽ bị hủy trong ngày.

- Phức tạp và yêu cầu khả năng về quản lý.

- Đối với môi trường doanh nghiệp, "thuốc" bảo vệ máy tính cá nhân có thể phức tạp khi triển khai và quản lý - đặc biệt là ở cấp độ doanh nghiệp. Do vậy các giải pháp này đòi hỏi phải liên tục triển khai các bản cập nhật (đôi khi theo một lịch trình hàng ngày), có thể cần có một yêu cầu về một khoản đầu tư của người có quyền lực nào đó (man-power) được thêm vào.

3.1.2. Độ nhạy của thư điện tử (E-mail)

Nhiều trong số những người sử dụng thư điện tử của doanh nghiệp và khách hàng sử dụng để truy cập tài nguyên Internet cung cấp mức độ ngày càng tăng về chức năng và sự giả mạo. Trong khi một số các chức năng này có thể được yêu cầu cho các ứng dụng và các hệ thống doanh nghiệp phức bị gỉa mạo- sử dụng các công nghệ này thường chỉ áp dụng cho hệ thống giữa các công ty. Hầu hết các chức năng này không cần thiết để sử dụng hằng ngày - đặc biệt đối với dịch vụ thông tin liên lạc Internet.

Chức năng này được nhúng một các không cần thiết (thường được để mặc định) được khai thác bởi các cuộc tấn công lừa đảo (cùng với sự tăng lên về xác suất của các loại tấn công khác nhau). Nói chung, các ứng dụng phổ biến nhất cho phép người dùng tắt chức năng nguy hiểm nhất.

3.1.2.1. HTML dựa trên thư điện tử

Nhiều vụ tấn công thành công là do chức năng HTML dựa trên e-mail, đặc biệt là khả năng xáo trộn những điểm đến thật của các link - liên kết, khả năng nhúng vào các phần trong kịch bản (scripting) và các biện giả tự động của các yếu tố đa phương tiện được nhúng (hoặc liên kết) vào đó. Chức năng HTML phải được vô hiệu hóa bởi tất cả các ứng dụng trong e-mail của khách hàng, những email mà có khả năng chấp nhận hoặc gửi e-mail qua Internet. Thay vào đó, việc giải thích bằng đại diện văn bản e-mail nên được sử dụng, và lý tưởng nhất là phông chữ được chọn phải được cố định, ví dụ như chỉ dùng phông "Courier".

E-mail sau đó sẽ được đưa ra trong văn bản gốc, ngăn chặn các hướng tấn công phổ biến nhất. Tuy nhiên, người sử dụng nên được chuẩn bị để nhận được một số email có những lối văn cầu kỳ (gobbledy-gook) có thể do vấn đề định dạng văn bản và cả các vấn đề về mã hóa trong HTML. Một số khách hàng hay dùng e-mail thường sẽ tự động loại bỏ các mã HTML. Trong khi những kháng cáo về hình ảnh trong e-mail nhận được có thể được hướng dẫn, thì vấn đề về an ninh sẽ được cải thiện đáng kể.

3.1.2.2. Chặn tin đính kèm (attachment Blocking)

Các ứng dụng E-mail có khả năng ngăn chặn các file đính kèm "nguy hiểm" và ngăn chặn người dùng khỏi việc thực hiện nhanh hoặc xem nội dung đính kèm nên được sử dụng bất cứ khi nào có thể.

Một số ứng dụng e-mail phổ biến (như Microsoft Outlook) duy trì một danh sách các định dạng tập tin đính kèm "nguy hiểm", và ngăn chặn người dùng mở chúng.

Trong khi các ứng dụng khác buộc người sử dụng lưu các tập tin ở một nơi nào đó khác trước khi họ có thể truy cập nó.

Một cách lý tưởng, người dùng sẽ không thể truy cập trực tiếp file đính kèm trong e-mail từ bên trong ứng dụng e-mail. Điều này áp dụng cho tất cả các loại tập tin đính kèm (bao gồm tài liệu Microsoft Word, tập tin đa phương tiện và các tập tin nhị phân) giống như nhiều của các định dạng tập tin (files) có thể chứa mã độc hại có khả năng ảnh hưởng đến các ứng dụng dựng hình (rendering) liên quan (ví dụ như trước đây: lỗ hổng trong máy nghe nhạc RealPlayer.RM). Ngoài ra, bằng cách tiết kiệm các tập tin địa phương, các giải pháp chống virus địa phương có thể tốt hơn để kiểm tra file virus hay nội dung độc hại khác.

3.1.2.3. Ưu điểm

- Vượt qua sự làm rắc rối hóa HTML (HTML Obfuscation): Buộc tất cả tất cả các email (inbound e-mail) sang định dạng văn bản chỉ là đủ để vượt qua những tiêu chuẩn dựa trên các kỹ thuật làm rối HTML.

- Vượt qua virus đính kèm (Overcoming attached viruses): Bằng cách ngăn chặn file đính kèm, hoặc buộc nội dung được lưu ở nơi khác, điều đó gây khó khăn hơn cho các cuộc tấn công tự động để thực hiện và cung cấp thêm cho các sản phẩm có tiềm năng chống virus các tiêu chuẩn để phát hiện nội dung độc hại.

3.1.2.4. Nhược điểm

- Dễ đọc: Hình dựng của HTML dựa trên e-mail thường có nghĩa là các yếu tố mã HTML code khiến cho tin nhắn (messager) trở nên khó đọc và khó để hiểu được.

- Giới hạn tin nhắn: Những người dùng thường cảm thấy khó khăn để gộp các file đính kèm (như đồ họa) trong TEXT-chỉ có e-mail đã được sử dụng để kéo và thả chúng và nhúng các hình ảnh vào HTML hay các biên tập Microsoft: Word, e-mail.

- Chặn lựa chọn hợp lý (Onerous Blocking): Chức năng lọc mặc định của file đính kèm "nguy hiểm" thường cho kết quả trong sự cố gắng của những người sử dụng kỹ thuật để vượt qua những hạn chế trong môi trường thương mại được sử dụng cho nội dung được gắn hoặc nhận nội dung có thể thực thi.

3.1.3. Khả năng của trình duyệt

Các trình duyệt web phổ biến có thể được sử dụng giống như sự bảo vệ chống lại các cuộc tấn công giả dạng (phishing) - nếu nó được cấu hình đảm bảo an toàn. Tương tự như các vấn đề với các ứng dụng e-mail, các trình duyệt web cũng cung cấp chức năng mở rộng mà từ đó có thể bị lạm dụng (thường ở một mức độ cao hơn so với e-mail của khách hàng). Đối với hầu hết người dùng, có lẽ trình duyệt web của họ là ứng dụng kỹ thuật tinh vi nhất mà họ sử dụng.

Các trình duyệt web phổ biến nhất cung cấp một mảng tuyệt vời của chức năng – ví như việc phục vụ "đồ ăn" cho tất cả người sử dụng trong tất cả các môi trường - mà họ vô tình cung cấp lỗ hổng bảo mật cái mà phơi bày sự toàn vẹn của các hệ thống máy chủ để từ đó dễ dàng bị tấn công (gần như sự xuất hiện này được đưa ra theo chu kỳ hàng tuần, một lỗ hổng mới sẽ được phát hiện và nó có thể được khai thác từ xa thông qua một trình duyệt web công cộng khác). Phần lớn sự tinh tế được dành để trở thành một kệ đỡ đối với tất cả các ngành nghề, và không một cá nhân nào có thể yêu cầu được sử dụng của tất cả các chức năng này.

Khách hàng và các doanh nghiệp phải thực hiện một động thái để sử dụng một trình duyệt web đó là "tương thích/dành riêng" cho các nhiệm vụ chính. Đặc biệt, nếu mục đích của các trình duyệt web chỉ là duyệt các dịch vụ web Internet, thì một trình duyệt bị làm giả sẽ không được yêu cầu.

Để giúp ngăn ngừa nhiều hướng tấn công lừa đảo, người dùng trình duyệt web nên:

• Vô hiệu hoá tất cả các chức năng cửa sổ pop-up.

• Hỗ trợ Java runtime Disable.

• Hỗ trợ Vô hiệu hoá ActiveX.

• Vô hiệu hoá tất cả các chức năng đa phương tiện và tự động (auto-play) cho các tính năng mở rộng.

• Ngăn chặn việc lưu trữ các tập tin cookie không an toàn.

• Đảm bảo rằng bất kỳ một công việc tải về (download) về máy nào đều không thể được tự động chạy từ trình duyệt, và phải được thay thế khi được tải về vào một thư mục để kiểm tra phòng chống virus (anti-virus).

3.1.3.1. Loại bỏ trình duyệt IE (Microsoft Internet Explorer)

Trình duyệt web của Microsoft là Internet Explorer, là trình duyệt web có sẵn phức tạp nhất. Do đó nó có một hồ sơ theo dõi rất dài việc phát hiện lỗ hổng và khai thác chúng từ xa. Đối với trình duyệt web đặc trưng, có ít hơn 5% các chức năng tích hợp được sử dụng. Trong thực tế, nhiều "tính năng" có sẵn trong trình duyệt đã được thêm vào để bảo vệ chống lại những sai sót từ trước và chống lại các hướng tấn công. Thật không may, mỗi tính năng mới được gắn vào trong một máy chủ đều làm tăng thêm các vấn đề an ninh và tăng thêm sự phức tạp.

Trong khi một số các chức năng nguy hiểm nhất có thể được vô hiệu hóa hoặc được tắt bằng cách sử dụng tùy chọn cấu hình khác nhau, khách hàng và người dùng doanh nghiệp được khuyến khích sử dụng một trình duyệt web mà có thể áp dụng cho hầu hết các tác vụ trong tầm tay (trong khả năng của chúng) -(ví dụ như trình duyệt được coi là một trung tâm đa phương tiện, một mail-client, một nền tảng trò chuyện hoặc một nền tảng phân phối ứng dụng biên dịch).

Có một số nhà cung cấp thường tặng kèm các trình duyệt web, thường khi đó nó sẽ an toàn hơn đối với một số hướng tấn công- bao gồm cả lừa đảo giả dạng (phishing).

Với một mặc định cài đặt trình duyệt web là một trong những nơi an toàn nhất, nhưng nó vẫn có thể được quản lý bởi một công ty môi trường nào đó và có thể được mở rộng thông qua việc chọn lọc các tính năng đính kèm "module add-on".

3.1.3.2. Gắn kèm các công cụ chống lừa đảo giả dạng (Anti-Phishing Plug-ins)

Ngày nay, ngày càng tăng số lượng các nhà sản xuất phần mềm chuyên dụng chống lừa đảo giả dạng (phishing) cung cấp trình duyệt plug-ins. Thông thường, các plug-ins được thêm vào thanh công cụ (toolbar) của trình duyệt và cung cấp một cơ sở giám sát hoạt động. Những thanh công cụ thường được gọi là "điện thoại nhà" cho mỗi URL, xác minh những máy chủ hiện tại và lập danh sách các vụ lừa đảo giả dạng.

Phải lưu ý rằng có nhiều trong số các trình duyệt plug-ins chỉ hỗ trợ trình duyệt của Microsoft cụ thể là trình duyệt Internet Explorer. (IEE).

3.1.3.3. Ưu điểm

- Cải tiến bảo mật được thực hiện tức thì, nhanh chóng.

- Chuyển dần từ một trình duyệt web phức tạp thành trình duyệt với chức năng được giảm nhẹ tức thì.

- Khả năng chống lại các lỗ hổng bảo mật phổ biến nhất và lỗ hổng trong Internet Explorer.

- Tốc độ: Trình duyệt web ít phức tạp thường truy cập và xem chất liệu dựa trên web nhanh hơn.

3.1.3.4. Nhược điểm

- Mất các chức năng được mở rộng.

- Đối với môi trường doanh nghiệp, sự mất mát của một số chức năng được mở rộng có thể đòi hỏi các ứng dụng chuyên dụng thay vì trình duyệt web tích hợp các thành phần.

- Việc đưa ra các ứng dụng web phức tạp.

- Việc loại bỏ một số chức năng phức tạp (đặc biệt một số ngôn ngữ client-side scripting) có thể khiến cho các ứng dụng web không đưa được ra nội dung trang một cách chính xác.

- Phản hồi của Plug-ins: Các công cụ plug-ins phòng chống lừa đảo giả dạng hiện tại chỉ có tác dụng như sự duy trì danh sách các nhà cung cấp đã được quản lý và được bết đến với lừa đảo giả mạo (scams) và giả mạo trang web (sites). Plug-ins thường chỉ có tác dụng đối với những công cụ đã được biết đến, được phân phối rộng rãi, và các cuộc tấn công lừa đảo.

3.1.4. Sử dụng chữ ký số trong thư điện tử

Có thể nên sử dụng các hệ thống mật mã khóa công cộng để làm chữ ký kỹ thuật số trong e-mail. Việc ký này có thể được sử dụng để xác minh tính toàn vẹn của nội dung tin nhắn - từ đó xác định xem nội liệu dung tin nhắn có bị thay đổi trong quá trình gửi hay không. Một tin nhắn đã được ký có thể được gán cho một người dùng (hoặc tổ chức) cụ thể khóa công khai.

Hầu như tất cả các ứng dụng client e-mail phổ biến hỗ trợ việc ký kết và xác minh các thông điệp e-mail đã ký kết. Người ta khuyến cáo người sử dụng là:

• Tạo một cặp khóa công khai cá nhân hoặc cặp khóa bí mật cá nhân.

• Tải lên khóa công khai của họ để tôn trọng các máy chủ quản lý chủ chốt như vậy thì những người khác, những người mà có thể nhận được e-mail của họ có thể xác minh tính toàn vẹn của tin nhắn.

• Kích hoạt tính năng, để theo mặc định, các chữ ký tự động của e-mail.

• Kiểm tra tất cả các chữ ký trên email nhận được và hãy cẩn thận với tin nhắn không có chữ hoặc tin nhắn không hợp lệ - trường hợp lý tưởng là xác minh một cách lý tưởng nguồn gốc thực sự của e-mail.

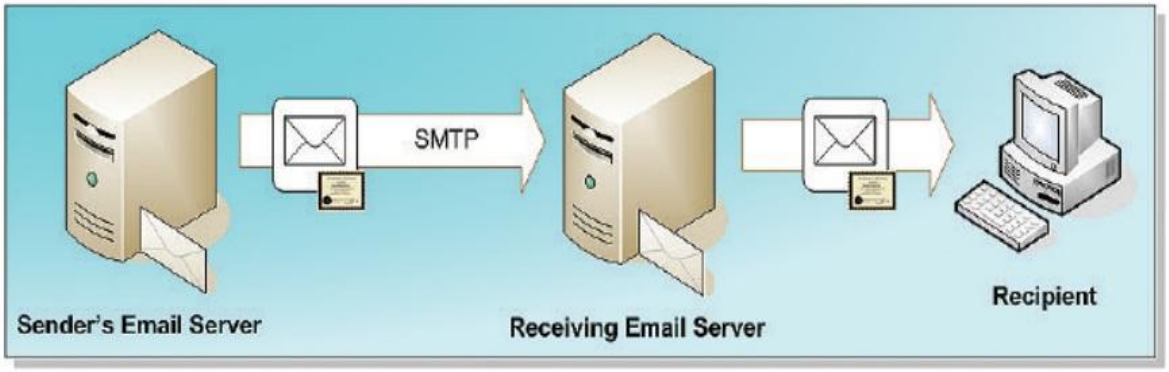


Figure 16: Digitally signed e-mail – recipient validation of authenticity

Một chữ ký trong tin nhắn về bản chất là một giá trị băm cái mà sử dụng các khía cạnh của khóa bí mật của người gửi tin gồm có: độ dài của tin nhắn, ngày và thời gian. Người nhận e-mail sử dụng khóa công khai kết hợp với các địa chỉ email của người gửi để xác minh giá trị băm này. Các nội dung của e-mail không nên được thay đổi bởi bất kỳ máy chủ mail trung gian nào.

Nói chung, điều quan trọng cần phải lưu ý rằng, không có hạn chế về việc tạo ra một cặp khóa công khai/ khóa bí mật nào cho bất kỳ địa chỉ e-mail nào, một người có thể chọn và sau đó tải lên các khóa công khai đến một máy chủ quản lý chủ chốt Internet. Vì vậy, nó vẫn còn có khả năng để cho một kẻ lừa đảo (phisher) gửi đi một e-mail với một địa chỉ giả mạo và chữ ký số đó với một chìa khóa mà chúng sở hữu.

3.1.4.1. S/MIME và PGP

Hiện nay có hai phương pháp phổ biến để cung cấp chữ ký điện tử. Đó là S / MIME và PGP (bao gồm PGP / MIME và OpenPGP với tiêu chuẩn mới hơn). Hầu hết

các ứng dụng mail Internet đối với các nhà cung cấp các sản phẩm lớn có khả năng sử dụng và hiểu S / MIME, PGP / MIME và OpenPGP đều sử dụng chữ ký số trong thư điện tử (e-mail).

Mặc dù họ cung cấp các dịch vụ tương tự cho người sử dụng e-mail, nhưng hai phương pháp có định dạng rất khác nhau. Quan trọng hơn là người sử dụng và doanh nghiệp đều có được các dạng khác nhau đối với các chứng chỉ khác nhau của họ. Điều này có nghĩa là người dùng sẽ chỉ sử dụng một giao thức không giao tiếp với những người sử dụng khác, mà họ cũng không thể chia sẻ chúng để xác thực.

3.1.4.2. Những điểm chính cho S/MIME và PGP:

• S/MIME ban đầu được phát triển bởi công ty RSA Data Security; Đó là dựa trên các dữ liệu định dạng PKCS # 7 cho các tin nhắn, và các định dạng X.509v3 cho việc cấp chứng chỉ. PKCS # 7 được dựa vào n các ASN.1, định dạng DER cho dữ liệu.

• PGP / MIME được dựa trên PGP, được phát triển bởi nhiều cá nhân, một số người hiện nay đã gia nhập với nhau như tập đoàn PGP. Các định dạng tin nhắn và giấy chứng nhận đã được tạo ra từ đầu và sử dụng mã hóa nhị phân đơn giản. OpenPGP cũng dựa trên PGP.

• S/MIME, PGP / MIME, và OpenPGP MIME sử dụng để cấu trúc tin nhắn. Họ tin cậy vào multipart/MIME đã được ký, loại mà được mô tả trong RFC 1847 để chuyển thông điệp ký qua Internet.

3.1.4.3. Ưu điểm

1) Tiêu chuẩn kinh doanh

Kể từ khi S/MIME trở thành một tiêu chuẩn kinh doanh, nó đã được tích hợp vào hầu hết các tiêu chuẩn e-mail của khách hàng. Vì vậy nó có thể làm việc mà không có các yêu cầu phần cứng và yêu cầu phần mềm bổ sung.

2) Đồng nhất đường mòn kiểm toán (audit Trail)

Những kẻ lừa đảo giả dạng (phisher) sử dụng chữ ký số trong e-mail của chúng phải đăng ký khóa công khai của chúng với cơ quan chính quyền có thẩm quyền. Quá trình đăng ký có thể cung cấp một đường mòn kiểm toán mạnh hơn khi truy tố những kẻ lừa đảo giả dạng.

3) Mối quan hệ tin cậy

Hợp pháp kinh doanh e-mail có thể được xác định tốt hơn bởi khách hàng, do đó tạo ra một sự tin tưởng lớn hơn trong mối quan hệ với khách hàng của họ.

3.1.4.4. Nhược điểm

1) Web dựa trên hỗ trợ E-mail

Không phải tất cả các khách hàng đều dựa trên web mail hỗ trợ S / MIME (ví dụ như: Hotmail, AOL, Yahoo! Mail, Outlook Web Access cho Exchange 5.5).

2) Tên miền gây hiểu lầm

Khách hàng vẫn phải kiểm tra chặt chẽ các địa chỉ gửi (From:), địa chỉ cho các tên miền có thể sai (ví dụ như support@mybánk.com thay vì support@mybank.com).

3) Kiểm tra truy hồi

Người nhận có thể không kiểm tra tình trạng thu hồi chứng chỉ.

3.1.5. Cảnh giác của khách hàng

Khách hàng có thể mất một số bước để tránh trở thành nạn nhân của vụ tấn công lừa đảo trực tuyến, những bước mà liên quan đến việc kiểm tra nội dung được trình bày cho họ và đặt câu hỏi về tính xác thực của nó.

Cảnh giác chung (ngoài những gì đã được trình bày trong phần trên) thì cần chú ý:

• Nếu bạn nhận được một e-mail cảnh báo cho bạn, với rất ít hoặc không có thông báo, rằng một tài khoản của bạn sẽ bị khóa, trừ khi bạn xác nhận lại thông tin thanh toán, đừng trả lời hoặc nhấp vào liên kết trong e-mail. Thay vào đó, liên hệ với các công ty được trích dẫn trong các e-mail bằng cách sử dụng một số điện thoại hoặc địa chỉ trang web mà bạn biết là chính hãng.

• Không bao giờ trả lời các e-mail HTML với các hình thức nhúng. Bất kỳ thông tin gửi qua e-mail (thậm chí nếu nó là hợp pháp) sẽ được gửi văn bản rõ ràng và có thể được nhìn thấy dễ dàng.

• Tránh thông tin cá nhân và thông tin tài chính gửi trong thư điện tử. Trước khi trình thông tin tài chính thông qua một trang web, hãy tìm kiếm "khóa -lock" biểu tượng trên thanh trạng thái của trình duyệt. Nó sẽ báo hiệu rằng liệu thông tin của bạn được an toàn trong suốt truyền dẫn hay không.

• Đối với các trang web được nhận định là an toàn, hãy xem xét các chứng chỉ SSL đã được nhận và đảm bảo rằng nó đã được phát hành bởi một cơ quan chứng nhận đáng tin cậy. Thông tin về giấy chứng nhận SSL có thể thu được bằng cách kích đúp chuột vào "khóa-lock" biểu tượng ở dưới cùng của trình duyệt, hoặc bằng cách nhấn phải chuột vào một trang web và chọn “properties”.

• Kiểm tra thẻ tín dụng và báo cáo tài khoản ngân hàng ngay sau khi bạn nhận được chúng để xác định xem liệu có bất kỳ khoản phí trái phép nào không. Nếu sự xác nhận của bạn trễ hơn một vài ngày, hãy gọi tới công ty thẻ tín dụng hoặc ngân hàng của bạn để xác nhận địa chỉ và số dư tài khoản thanh toán của bạn.

3.1.5.1. Rửa tiền (Scams Job)

Với những thành công của trò gian lận lừa đảo (phishing scam) trong thu thập thông tin tài chính cá nhân từ các nạn nhân của chúng, những kẻ lừa đảo (phisher) đã phát triển theo dõi lừa đảo nhằm chuyển giao một cách an toàn các khoản tiền bị đánh

cắp. Phương pháp này ngày càng được những kẻ lừa đảo sử dụng đến mức trở lên phổ biến là do chúng lợi dụng qua quá trình lừa đảo những việc làm giả (take job scam).

3.1.5.2. Cách mà trò gian lận việc làm giả thực hiện

• Những kẻ lừa đảo khai thác một số tài khoản ngân hàng theo hướng tấn công chuẩn của lừa đảo giả dạng.

• Sau đó, vấn đề chúng gặp phải là không lấy được tiền vì hầu hết các ngân hàng Internet không cho phép chuyển trực tiếp vào tài khoản ở nước ngoài.

• Một cách thông thường để tránh những hạn chế này là thông qua việc lừa đảo. Những kẻ lừa đảo cung cấp những "công việc" thông qua thư rác e-mail, quảng cáo về việc một làm giả nào đó trên các trang web việc làm chính thông hay gửi tin đồng loạt các thư rác (spam) tức thời.

• Một khi họ đã tuyển dụng một được một người (lúc này được coi là con la – mule), thì ngay sau đó người này sẽ được hướng dẫn để tạo một tài khoản ngân hàng mới với các ngân hàng đã được khai thác (hoặc đang được họ sử dụng như là một khách hàng), ngân hàng mà những kẻ lừa đảo đã khai thác các tài khoản trước đó. Những kẻ lừa đảo sau đó loại bỏ tiền từ tài khoản khai thác được và đưa vào tài khoản của “con la”.

• Các con la sẽ được giải thích rằng đây là một khoản thanh toán mà cần phải được chuyển giao và được yêu cầu rút tiền, rồi trừ "hoa hồng" của họ, và đường dây này thường thông qua các dịch vụ như Western Union tới một nước châu Âu hoặc châu Á.

• Lúc này những kẻ lừa đảo đã có được phần lớn số tiền từ các tài khoản khai thác ban đầu và khi tiền được theo dõi bởi các ngân hàng hay công an, con la còn lại có trách nhiệm với nó.

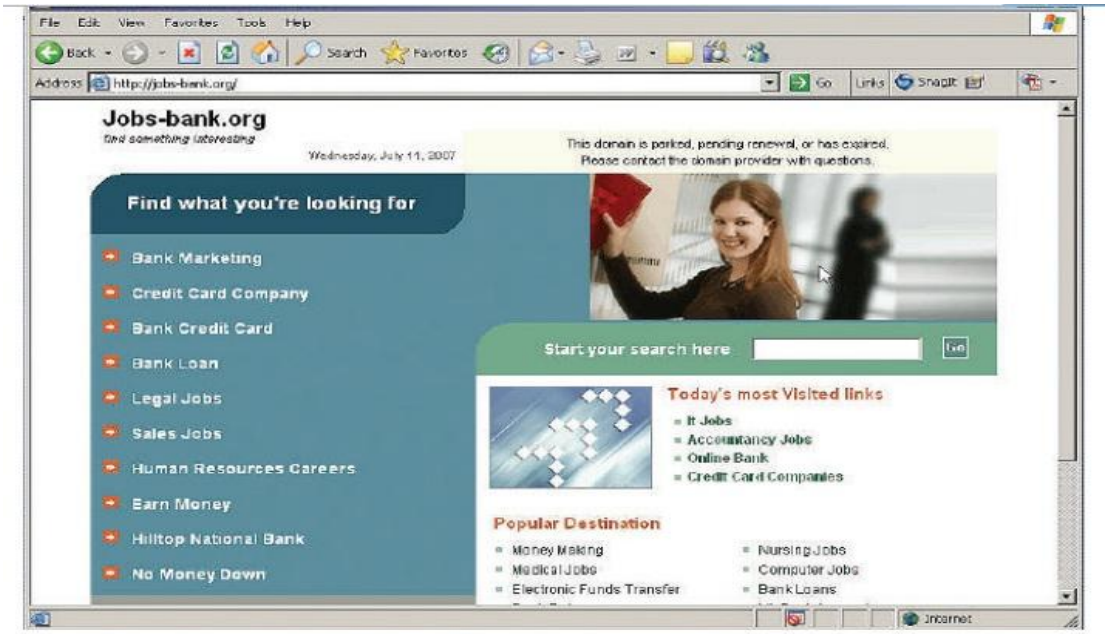


Figure 17: A typical fake recruitment page and supporting site for attracting "mules"

3.1.5.3. Ưu điểm

Giá cả: Bằng cách luôn nhận thức được chiều hướng tấn công lừa đảo giả dạng phổ biến và sự hiểu biết làm thế nào để ứng phó lại chúng, khách hàng có thể có những hành động với mức chi phí hợp lý nhất để tự bảo vệ mình.

3.1.5.4. Nhược điểm

1) Thông tin quá tải

Với rất nhiều phương hướng tấn công và các bước tương ứng mà phải được thực hiện để xác định các mối đe dọa, khách hàng thường quá tải với quá trình phát hiện cần thiết. Điều này có thể dẫn đến khách hàng không tin tưởng hoặc sử dụng bất kỳ phương pháp truyền thông điện tử nào.

2) Thay đổi chiến trường (Battlefield)

Những kẻ lừa đảo đang không ngừng phát triển các kỹ thuật lừa đảo mới để gây nhầm lẫn cho khách hàng và che giấu bản chất thật sự của thông điệp. Điều này làm cho ngày càng khó khăn hơn để xác định các cuộc tấn công.

3.2. PHÍA MÁY CHỦ

Bằng cách thực hiện các kỹ thuật chống lừa đảo giả dạng (anti-phishing) thông minh vào bảo mật ứng dụng web của tổ chức, phát triển các quy trình nội bộ để chống lại các hướng tấn công lừa đảo giả dạng và hướng dẫn khách hàng – điều này có thể đóng một vai trò hữu ích trong việc bảo vệ khách hàng khỏi bị tấn công trong tương lai. Bằng cách thực hiện công việc này từ phía máy chủ, các tổ chức có thể thực hiện các bước lớn hơn trong việc giúp đỡ để bảo vệ chống lại những gì luôn luôn là mối đe dọa phức tạp và xảo quyệt.

Ở phía máy chủ, bảo vệ chống lại lừa đảo có thể được tạo nên bởi:

• Nâng cao nhận thức của khách hàng.

• Cung cấp thông tin để có thể xác nhận về thông báo chính thức.

• Đảm bảo rằng các ứng dụng web Internet được an toàn để phát triển và không bao gồm các hướng tấn công dễ dàng được khai thác.

• Sử dụng hệ thống xác thực mạnh mẽ dựa vào thẻ bài token.

• Duy trì hệ thống đặt tên đơn giản và dễ hiểu.

3.2.1. Nhận thức của khách hàng

Điều quan trọng là tổ chức liên tục thông báo cho khách hàng và người sử dụng ứng dụng khác của các mối nguy hiểm từ các cuộc tấn công lừa đảo giả dạng và những hành động phòng ngừa có sẵn. Đặc biệt, thông tin phải có thể thấy được về cách mà tổ chức giao tiếp an toàn với khách hàng của họ. Ví dụ, một bài viết tương tự như sau đây sẽ giúp khách hàng xác định lừa đảo e-mail được gửi trong tên của tổ chức.

"MyBank will never initiate a request for sensitive information from you via e-mail (i.e., Social Security Number, Personal ID, Password, PIN or account number). If you receive an e-mail that requests this type of sensitive information, you should be suspicious of it. We strongly suggest that you do not share your Personal ID, Password, PIN or account number with anyone, under any circumstances.

If you suspect that you have received a fraudulent e-mail, or wish to validate an official e-mail from MyBank, please visit our antiphishing page http://mybank.com/antiphishing.aspx"

Tạm dịch:

"MyBank sẽ không bao giờ bắt đầu một yêu cầu thông tin nhạy cảm từ bạn qua e-mail (ví dụ, số an sinh xã hội, ID cá nhân, mật khẩu, PIN hoặc số tài khoản). Nếu bạn nhận được một e-mail yêu cầu loại thông tin nhạy cảm, bạn nên cảnh giác với nó. Chúng tôi đề nghị rằng bạn không chia sẻ ID cá nhân của bạn, mật khẩu, mã PIN hoặc số tài khoản với bất kỳ ai, trong bất kỳ trường hợp nào.

Nếu bạn nghi ngờ rằng bạn đã nhận được một e-mail lừa đảo, hoặc muốn xác nhận một e-mail chính thức từ MyBank, vui lòng truy cập trang http://mybank.com/antiphishing.aspxantiphishing của chúng tôi "

Các bước quan trọng trong việc giúp đỡ để đảm bảo nhận thức khách hàng và tiếp tục cảnh báo:

• Nhắc nhở khách hàng liên tục. Việc này có thể thực hiện được với các thông báo nhỏ trên trang đăng nhập quan trọng về cách mà tổ chức giao tiếp với khách hàng của họ. Khách hàng truy cập vào trang nên được nhắc nhở để suy nghĩ về tính hợp pháp của các e-mail (hoặc thông tin liên lạc khác) cái mà lái họ truy cập vào trang.

• Cung cấp một phương pháp dễ dàng cho khách hàng để thông báo lừa đảo giả mạo, hoặc những email gian lận khác có thể được gửi trong tên của tổ chức. Điều này

thực hiện được bằng cách cung cấp các liên kết rõ ràng trên các trang được xác thực và giúp đỡ để khách hàng báo cáo bất kỳ khả năng nào có thể là lừa đảo giả mạo và cũng cung cấp lời khuyên trong việc xác nhận một sự giả mạo. Quan trọng hơn, các tổ chức phải đầu tư đủ nguồn lực để xem lại các bản đệ trình và có khả năng làm việc với các cơ quan thực thi pháp luật và các ISP để ngăn chặn cuộc tấn công được tiến hành.

• Cung cấp lời khuyên về cách làm thế nào để xác minh tính toàn vẹn của các trang web mà họ đang sử dụng. Điều này bao gồm việc làm thế nào để:

- Kiểm tra các thiết lập bảo mật của trình duyệt web của họ.

- Kiểm tra kết nối của họ để an toàn khi qua SSL.

- Xem lại các "ổ khóa - padlock" và chữ ký chứng nhận của trang.

- Giải mã dòng URL trong trình duyệt của họ.

• Xây dựng chính sách truyền thông của công ty và thực thi chúng. Tạo chính sách của công ty đối với nội dung e-mail để hợp pháp e-mail đảm bảo không thể bị nhầm lẫn với các cuộc tấn công lừa đảo. Đảm bảo rằng các cơ quan có khả năng giao tiếp với khách hàng hiểu rõ các chính sách và thực hiện các bước để thực thi chúng (chẳng hạn như phạm vi mà hệ thống đang kiểm tra nội dung, được xem xét lại bởi đội QA, vv).

• Để có hiệu quả, tổ chức phải đảm bảo rằng họ đang gửi một thông điệp rõ ràng, ngắn gọn và phù hợp cho khách hàng của họ. Ví dụ, không đăng thông báo tuyên bố "không bao giờ nhắc người sử dụng điền vào định dạng trong một e-mail nào đó" một ngày và sau đó gửi một yêu cầu e-mail để thanh toán hóa đơn trực tuyến ngày hôm sau, trong đó bao gồm một mẫu đăng nhập trong e-mail.

• Phản ứng nhanh chóng và rõ ràng về các âm mưu đã được xác định là lừa đảo. Điều quan trọng khách hàng hiểu rằng mối đe dọa này là có thật, và tổ chức đang làm

việc để bảo vệ họ chống lại cuộc tấn công. Tuy nhiên, các tổ chức phải chú ý không để tràn ngập quá nhiều thông tin với khách hàng.

3.2.1.1. Ưu điểm

1) Chi phí thấp

Trong số tất cả các kỹ thuật chống lừa đảo giả dạng (anti-phishing), thì kỹ thuật nào đảm bảo các khách hàng nhận thức được những mối đe dọa và có thể có hành động tự phòng ngừa thì chứng tỏ rằng kỹ thuật đó được đầu tư xứng đáng.

2) Yêu cầu về kỹ thuật thấp

Bằng cách cung cấp một giải pháp công nghệ thấp nhưng lại đạt đến trình độ đe dọa cao, khách hàng có thể để tin tưởng hơn rằng mối liên hệ của họ với tổ chức được đảm bảo an toàn.

3.2.1.2. Nhược điểm

1) Yêu cầu tính nhất quán cao

Chăm sóc khách hàng phải luôn được thực hiện để đảm bảo rằng thông tin liên lạc được thực hiện một cách nhất quán. Một quyết định sai lầm có thể làm suy yếu nhiều công việc.

2) Thông tin dễ quá tải hệ thống

Cần phải cẩn thận để không làm quá tải thông tin đến với khách hàng và làm cho họ sợ hãi trong việc sử dụng các nguồn tài nguyên trực tuyến của tổ chức.

3.2.2. Giá trị truyền thông mang tính nội bộ

Bước này có thể được thực hiện bởi một tổ chức để giúp xác nhận thông tin liên lạc của khách hàng chính thức và cung cấp một phương tiện để xác định liệu có khả năng là các cuộc tấn công lừa đảo. Gắn kết chặt chẽ với các vấn đề về nhận thức của

khách hàng đã được thảo luận, có một số kỹ thuật mà tổ chức có thể áp dụng để thông tin liên lạc chính thức, tuy nhiên việc chăm sóc khách hàng phải được thực hiện để chỉ sử dụng các kỹ thuật thích hợp với khả năng của từng khách hàng và giá trị mang tính thương mại đối với từng đối tượng khách hàng.

3.2.2.1. Thư điện tử cá nhân

E-mail gửi đến khách hàng nên được cá nhân hóa cho từng đối tượng người nhận. Việc cá nhân hóa này có thể dao động từ việc sử dụng tên của khách hàng, hoặc tham khảo một số phần khác của thông tin được chia sẻ duy nhất giữa khách hàng với tổ chức hay doanh nghiệp. Một số ví dụ như:

• Nội dung thư thường có: "Dear Mr Smith" thay vì "Dear Sir," hay "khách hàng tiềm năng của chúng tôi (Our valued customer)"

• Chủ tài khoản thẻ tín dụng "**** **** ** 32 6722" (đảm bảo rằng chỉ có các phần của thông tin bí mật được sử dụng)

• Tham khảo các liên hệ cá nhân khởi xướng như "quản lý tài khoản của bạn bà Mrs Jane Doe ..."

Các tổ chức phải đảm bảo rằng chúng không bị rò rỉ bất kỳ chi tiết bí mật nào của khách hàng (chẳng hạn như các chi tiết đầy đủ về địa chỉ, mật khẩu, thông tin tài khoản cá nhân, vv) trong thông tin liên lạc của họ.

3.2.2.2. Tham khảo thông báo trước đó (Previous Message Referral)

Có thể tham khảo một mẫu e-mail đã được gửi đến khách hàng - do đó cần thực hiện việc thiết lập sự tin tưởng trong truyền tin. Điều này có thể đạt được thông qua các phương tiện khác nhau. Các phương pháp phổ biến nhất là:

• Tham khảo các thông tin rõ ràng về các chủ đề và ngày gửi của e-mail trước.

• Định kỳ gửi các e-mail nhắc nhở.

Trong các phương pháp tham khảo, phương pháp dựa vào e-mail có tính khả thi hơn cả, nhưng chúng lại rất khó khăn đối với nhiều khách hàng trong việc xác nhận được email. Ở đây có sự đảm bảo rằng khách hàng vẫn giữ lại quyền truy cập vào một e-mail trước đó để xác minh trình tự - và đây là cách đặc biệt để biết liệu tổ chức có gửi cho khách hàng một số lượng lớn e-mail hoặc tin nhắn quảng cáo thường xuyên không.

3.2.2.3. Các cổng thông tin xác thực ứng dụng trang mạng (Web Application Validation Portals)

Một phương pháp thành công của việc cung cấp sự bảo đảm cho khách hàng về tính xác thực của thông tin liên lạc đó là cung cấp một cổng thông tin trên trang web của công ty, và sau đó cung cấp khả năng xác định một cuộc tấn công lừa đảo mới. Các cổng thông tin web tồn tại để cho phép khách hàng sao chép / dán nội dung tin nhắn nhận được của họ vào một hình thức tương tác, và cho các ứng dụng để hiển thị rõ tính xác thực của thông điệp.

Nếu thông báo thất bại khi kiểm tra tính xác thực, thì các tin nhắn sẽ tự động được xác nhận bởi tổ chức, và được đánh giá xem các tin nhắn có chứa yếu tố của một cuộc tấn công lừa đảo nguy hiểm nào không.

Tương tự như vậy, Cần được cung cấp một giao diện mà trong đó khách hàng có thể sao chép hay dán các URL nghi ngờ mà họ đã nhận được. Các ứng dụng sau đó xác nhận liệu rằng đây có phải là một URL hợp pháp liên quan đến tổ chức không.

3.2.2.4. Hình ảnh hay âm thanh cá nhân trong thư điện tử

Có thể nhúng các dữ liệu hình ảnh hay âm thanh cá nhân trong một e-mail. Tài liệu này sẽ được cung cấp bởi các khách hàng trước đây, hoặc có chứa tương đương với một bí mật chia sẻ. Tuy nhiên, phương pháp này không được khuyến khích vì nó có thể đưa ra kết quả không có hiệu quả thông qua việc thực hiện các non-HTML hoặc tập tin đính kèm e-mail ở phía khách hàng.

3.2.2.5. Ưu điểm

Hiệu quả: Quá trình đơn giản của cá nhân hoá thông tin liên lạc làm cho nó dễ dàng hơn nhiều đối với khách hàng trong việc xác định thông tin chính thức từ các email spam. Làm cho quá trình chứng thực nguồn tin nhanh hơn và hiệu quả hơn.

3.2.2.6. Nhược điểm

1) Tài nguyên bổ sung

Tổ chức thường phải mở rộng dịch vụ xác nhận trực tuyến của họ việc này sẽ đòi hỏi nguồn lực bổ sung - cả về phát triển và quản lý diễn ra ngày-qua-ngày.

2) Nhận thức của khách hàng

Khách hàng có thể không sử dụng hoặc không nhận thức được tầm quan trọng của những hành động tự bảo vệ mang tính cá nhân.

3.2.3. Bảo mật ứng dụng trang mạng đối với khách hàng

Các tổ chức liên tục đánh giá thấp khả năng chống lừa đảo của các ứng dụng web tùy chỉnh của họ. Bằng cách áp dụng các chức năng kiểm tra nội dung mạnh và thực hiện một vài "cá nhân hóa" các phần bổ sung an ninh, nhiều hướng tấn công lừa đảo phổ biến có thể được gỡ bỏ.

Bảo mật ứng dụng web dựa trên cung cấp các phương pháp đầu tư mang lại nhiều lợi nhuận lớn nhất (bang for the buck) là phương pháp bảo vệ khách hàng chống lại các cuộc tấn công lừa đảo.

Mối quan tâm an ninh chính xoay quanh các lỗ hổng (có tính chất chồng chéo) ngày càng trở nên tinh vi. Những lỗ hổng chồng chéo nhau thường vượt ra khỏi các chiến lược bảo vệ khách khác do các mối quan hệ tin cậy vốn có giữa khách hàng và chủ sở hữu trang web - dẫn đến các cuộc tấn công thành công (và không thể phát hiện).

3.2.3.1. Xác thực nội dung

Một trong những lỗ hổng bảo mật phổ biến nhất trong các ứng dụng web dựa trên tùy chỉnh liên quan đến quy trình xác nhận đầu vào kém (hoặc không tồn tại).

Các nguyên tắc quan trọng để thực hiện thành công quá trình xác nhận nội dung bao gồm:

• Không bao giờ thực sự tin tưởng dữ liệu được gửi từ một người dùng hoặc các thành phần ứng dụng khác.

• Không bao giờ thực hiện gửi lại dữ liệu trực tiếp cho người dùng một ứng dụng mà không “khử trùng” nó trước tiên.

• Luôn luôn “khử trùng” dữ liệu trước khi “chế biến” hoặc lưu trữ nó.

• Đảm bảo rằng tất cả các đặc tính nguy hiểm (tức là đặc tính có thể được giải thích bởi các tiến trình ứng dụng trình duyệt khách hàng duyệt hoặc tiến trình ứng dụng nền) ví như tạo thành một ngôn ngữ thực thi được thay thế bằng phiên bản HTML thích hợp an toàn của chúng. Ví dụ, ít hơn so với đặc tính "<" có một ý nghĩa đặc biệt trong HTML - như vậy là cần được trả lại cho người sử dụng như **&lt**.

• Đảm bảo rằng tất cả các dữ liệu được “khử trùng” bằng cách giải mã cơ chế mã hóa thông thường (chẳng hạn như % 2E, % C0% AE, % u002E, %% 35% 63) trở lại với đăc tính gốc của chúng. Một lần nữa, nếu đặc tính này "không an toàn", nó phải được kết xuất trong các định dạng tương đương HTML. Lưu ý rằng tiến trình giải mã này có thể thực thi.

3.2.3.2. Xử lý phiên (Session handling)

Bản chất phi trạng thái của truyền thông HTTP và HTTPS đòi hỏi phải áp dụng đúng các quy trình xử lý phiên. Nhiều ứng dụng tùy chỉnh thực hiện các tùy chỉnh thói quen quản lý mà có khả năng dễ bị tấn công để tấn công các phiên tấn được cài sẵn.

Để vượt qua một cuộc tấn công theo phiên đặt trước, các nhà phát triển phải đảm bảo các chức năng ứng dụng của họ tuân thủ theo cách sau đây:

• Không bao giờ chấp nhận thông tin phiên trong URL.

• Đảm bảo rằng nhân SessionID có giới hạn thời gian hết hạn và họ được kiểm tra trước khi sử dụng với mỗi yêu cầu của khách hàng.

• Các ứng dụng phải có khả năng thu hồi hoạt động của SessionID và không tái chế cùng SessionID trong một khoảng thời gian dài.

• Bất kỳ cố gắng nào để gửi một SessionID không hợp lệ (tức là một trong đó đã hết hạn, bị thu hồi, mở rộng vượt ra ngoài cuộc sống tuyệt đối của nó, hoặc không bao giờ được phát hành) thì kết quả trong một chuyển hướng phía máy chủ đến trang đăng nhập và được cấp một SessionID mới.

• Không bao giờ giữ một SessionID mà ban đầu được cung cấp qua HTTP sau khi khách hàng đã đăng nhập trên một kết nối an toàn (tức là HTTPS). Sau khi xác thực, khách hàng luôn luôn cần được phát một SessionID mới.

3.2.3.3. Năng lực URL

Đối với các ứng dụng dựa trên web mà thấy nó cần thiết phải sử dụng client-side chuyển hướng đến các địa điểm trang khác hoặc máy chủ/host khác, thì việc đặc biệt chăm sóc/quan tâm phải được thực hiện trong chứng nhận có đủ khả năng về bản chất/đặc tính của liên kết trước. Những nhà Phát triển ứng dụng cần phải nhận thức được các kỹ thuật thảo luận trong phần 2 của bài viết này.

Thực hành tốt nhất đối với năng lực của URL là:

• Không chuyển hướng tham khảo URL hoặc đường dẫn tập tin thay thế trực tiếp trong trình duyệt; Ví dụ như:

http://mybank.com/redirect.aspx ? URL=secure.mybank.com.

• Luôn luôn duy trì một giá trị đã được phê duyệt, danh sách các URL chuyển hướng. Ví dụ, quản lý danh sách phía máy chủ của URL liên kết với một tham số chỉ số. Khi một khách hàng đi theo một liên kết, họ sẽ tham khảo chỉ số này, và các trang chuyển hướng trở về sẽ chứa các URL được quản lý đầy đủ.

• Không bao giờ cho phép khách hàng cung cấp các URL của riêng họ.

• Không bao giờ cho phép địa chỉ IP được sử dụng trong thông tin URL. Luôn luôn sử dụng tên miền đầy đủ, hoặc ít nhất cũng tiến hành tra cứu tên ngược trên địa chỉ IP và xác minh rằng nó nằm với một miền ứng dụng đáng tin cậy.

3.2.3.4. Các quy trình thẩm định

Đối với những mưu đồ lừa đảo, mục tiêu chính của cuộc tấn công là để nắm bắt thông tin xác thực của khách hàng. Để làm như vậy, những kẻ tấn công phải có khả năng giám sát tất cả các thông tin được nộp trong giai đoạn đăng nhập ứng dụng. Các tổ chức có thể sử dụng nhiều phương pháp để làm cho quá trình này khó khăn hơn đối với những kẻ lừa đảo.

Phát triển ứng dụng nên xem lại các chỉ dẫn toàn diện để xác thực tùy chỉnh HTML để ngăn chặn được hầu hết các hình thức tấn công có thể. Tuy nhiên, liên quan một cách đặc biệt đến sự bảo vệ chống lại các cuộc tấn công lừa đảo, các nhà phát triển nên:

• Đảm bảo rằng tối thiểu một quá trình đăng nhập có hai giai đoạn được sử dụng. Những khách hàng đầu tiên được trình bày với một màn hình đăng nhập mà họ phải trình bày chi tiết tài khoản mà thường ít an toàn (tức là có một xác suất cao mà khách hàng có thể sử dụng những chi tiết trên các trang web khác - chẳng hạn như tên đăng nhập của họ và số thẻ tín dụng). Sau khi đi qua trang này thành công, họ được dẫn đến với một trang thứ hai cái mà đòi hỏi hai hay độc nhất mẩu thông tin xác thực trước khi họ có thể thực thi các ứng dụng thích hợp.

• Sử dụng các quy trình chống khóa-đăng nhập (key-logging) ví như lựa chọn các phần đặc biệt của một mật khẩu hay cụm mật khẩu lấy từ các hộp danh sách thả xuống (drop-down) rất được khuyến khích.

• Cố gắng sử dụng nội dung cá nhân (kết hợp với nhận thức của khách hàng) để xác định các trang web giả mạo. Ví dụ, khi một khách hàng ban đầu tạo ra tài khoản trực tuyến của họ, họ sẽ có thể lựa chọn hoặc tải lên hình ảnh cá nhân của họ. Đồ họa cá nhân này sẽ luôn luôn được trình bày cho họ trong giai đoạn thứ hai của quá trình xác thực và trên bất kỳ trang xác thực nào. Đồ họa này có thể được sử dụng như một kỹ thuật Watermark với tính xác thực để chống lại nội dung giả mạo.

• Không làm cho quá trình xác thực quá phức tạp. Hãy hiểu rằng khách hàng bị mất khả năng hoạt động (disabled customers) có thể gặp khó khăn với một số chức năng ví như các hộp kéo - thả (drop-down boxes).

3.2.3.5. Quy định ảnh (Image Regulation)

Khi nhiều cuộc tấn công lừa đảo dựa vào việc lưu trữ một bản sao của trang web được nhắm đến trên một hệ thống điều khiển của kẻ lừa đảo, thì sẽ có những con đường tiềm năng cho các tổ chức để tự động xác định một trang web giả mạo.

Tuỳ thuộc vào việc các phisher đã phản ánh toàn bộ trang web (bao gồm các trang và đồ họa liên quan) hoặc chỉ được lưu trữ một trang HTML đã sửa (mà đồ họa tham chiếu đặt trên các máy chủ, tổ chức thực), nó có thể làm gián đoạn hoặc xác định tính duy nhất nguồn gốc cuộc tấn công.

Hai phương pháp có sẵn để phát triển ứng dụng đó là:

• Chu kỳ hình ảnh: Mỗi trang ứng dụng hợp pháp tham chiếu các hình ảnh đồ họa cấu thành bởi một tên duy nhất. Mỗi giờ, tên của những hình ảnh được thay đổi và yêu cầu trang phải tham khảo các tên hình ảnh mới. Vì thế bất kỳ bản sao (copy) hết hạn nào của trang đó mà tạo ra bản tham chiếu đến những hình ảnh được lưu trữ tập

trung sẽ trở nên lỗi thời một cách nhanh chóng. Nếu một hình ảnh hết hạn được yêu cầu (say 2+ hours old) thì một hình ảnh khác được cung cấp - có lẽ việc đề nghị rằng các khách hàng đăng nhập lại để tới các trang web chính thống (chẳng hạn như "Cảnh báo: Image Expired – hình ảnh đã hết hạn").

• Các hình ảnh phiên – giới hạn (Session – bound): Nghiên cứu sâu hơn về nguyên lý chu kỳ hình ảnh, có thể tham khảo tất cả các hình ảnh với một tên có các SessionID hiện tại của người dùng. Do đó, một khi một trang web giả mạo đã được phát hiện (thậm chí nếu các phisher đang sử dụng đồ họa được lưu trữ tại địa phương), thì tổ chức có thể xem lại nhật ký của họ trong một nỗ lực để tìm ra nguồn gốc xuất xứ của các trang web sao chép. Điều này đặc biệt hữu ích cho các trang web giả mạo, các trang mà cũng sử dụng nội dung yêu cầu truy cập xác thực và chỉ có thể đạt được bởi một phisher thực sự sử dụng một tài khoản thực ở vị trí đầu tiên.

Ngoài ra, tổ chức có thể sử dụng công nghệ **watermarking** trong suốt - transpareng hoặc vô hình- invisible và nhúng thông tin phiên-session vào đồ họa riêng của mình. Tuy nhiên, quá trình này sẽ phải chịu các chi phí hiệu suất cao ở phía máy chủ.

3.2.3.6. Ưu điểm

1) Tính mạnh mẽ

Bằng cách bổ sung an ninh thích hợp để phát triển các ứng dụng tùy chỉnh web, tổ chức thấy rằng không phải chỉ là những ứng dụng của họ có khả năng tốt hơn để chống các cuộc tấn công lừa đảo, mà còn vững mạnh tổng thể trong việc chống lại các cuộc tấn công tinh vi hơn khác đã đạt được.

2) Hiệu quả về mặt chi phí

Bằng cách sửa chữa các vấn đề bảo mật trong ứng dụng, số lượng các cuộc tấn công theo hướng có sẵn cho một phisher giảm đi đáng kể. Như vậy đảm bảo ứng dụng

cơ bản chứng minh sự phòng thủ chống lại các mối đe dọa hiện tại và tương lai mang lại hiệu quả về mặt chi phí.

3) Độc lập đối với khách hàng

Cải tiến an ninh với các ứng dụng phía máy chủ thường không liên quan đến những thay đổi về kinh nghiệm của khách hàng. Vì vậy những thay đổi có thể được tiến hành độc lập với cấu hình client-side của khách hàng.

3.2.3.7. Nhược điểm

1) Cần các yêu cầu phát triển kỹ năng

Thực hiện những bổ sung an ninh cần yêu cầu phát triển kỹ năng với một số kinh nghiệm trong việc thực hiện đảm bảo an ninh. Những nguồn tài nguyên này thường khá khó khăn để có được chúng.

2) Phải được thử nghiệm

Các tổ chức phải đảm bảo rằng tất cả các tính năng bảo mật mới (cùng với bất kỳ sửa đổi ứng dụng tiêu chuẩn nào) đều được kiểm tra kỹ lưỡng về góc độ an ninh trước khi đi vào thực tế (hoặc càng sớm càng tốt sau khi được đưa ra sử dụng chính thức).

3) Chi phí quản lý hiệu suất

Nguồn lực xử lý mở rộng bình thường được yêu cầu để thực hiện các cơ chế bảo mật. Do đó hiệu suất ứng dụng có thể bị ảnh hưởng xấu.

3.2.4. Xác thực dựa trên thẻ bài mạnh (Strong Token)

Có một số phương pháp xác thực là làm cho việc sử dụng các hệ thống bên ngoài tạo ra các mật khẩu sử dụng 1 lần hoặc tạo ra các mật khẩu dựa trên thời gian. Các hệ thống này, thường được gọi là hệ thống xác thực dựa trên thẻ bài token, có thể dựa trên các thiết bị vật lý (như khóa (key)-bỏ túi nhỏ gọn hay máy tính) hoặc phần

mềm. Mục đích là tạo ra mật khẩu mạnh (chỉ sử dụng một lần: one - time) cái mà không thể được sử dụng lặp đi lặp lại để xâm nhập vào một ứng dụng.

Khách hàng của các ứng dụng dựa trên web hợp pháp có thể sử dụng một thẻ vật lý giống như một thẻ thông minh hoặc máy tính để cung cấp một mật khẩu cho 1 lượt sử dụng hoặc mật khẩu sử dụng trong một khoảng thời gian nhất định (time-dependant).

Figure 18: Strong token-based authentication

Do chi phí lắp đặt và chi phí bảo dưỡng cao, nên giải pháp này là phù hợp nhất với các ứng dụng web giao dịch giá trị cao cái mà gần như không yêu cầu số lượng lớn người sử dụng.

Như với bất kỳ quá trình xác thực nào, các tổ chức phải có sự cân bằng giữa những chi tiết cá nhân hoặc bí mật được tối thiểu cần thiết để xác thực tính duy nhất của một khách hàng, và làm thế nào những thông tin này hoặc được công khai hoặc có thể được sử dụng bởi khách hàng để truy cập vào web của một tổ chức khác dựa trên các ứng dụng. Bằng cách làm giảm khả năng của các chi tiết xác thực được chia sẻ giữa nhiều tổ chức, sẽ có rất ít cơ hội cho kẻ tấn công để có thể đánh cắp thông tin nhận dạng người dùng.

3.2.4.1. Ưu điểm

1) Sự phụ thuộc thời gian

Các mật khẩu phụ thuộc thời gian, vì vậy, trừ khi các phisher có thể truy xuất và sử dụng thông tin này trong giới hạn thời gian định trước, nếu không sau đó mật khẩu sẽ hết hạn và trở nên vô dụng.

2) Truy cập thẻ bài (token) vật lý

Một phisher phải truy cập vật lý đến các mã thông báo để mạo danh người dùng và thực hiện các hành vi trộm cắp.

3) Tạo cảm giác tin tưởng

Người dùng có xu hướng tin tưởng hệ thống xác thực dựa trên token cho các giao dịch tiền tệ.

4) Chống gian lận

Việc nhân đôi thẻ token vật lý đòi hỏi sự tinh tế hơn nhiều, ngay cả khi các nạn nhân cung cấp số PIN cá nhân của mình mà được gắn liền với token.

3.2.4.2. Nhược điểm

1) Đào tạo người sử dụng

Người sử dụng phải được cung cấp các hướng dẫn về cách sử dụng các mã thông báo vật lý trong một khuôn khổ phụ thuộc vào thời gian.

2) Các chi phí cho thẻ bài (token)

Thẻ vật lý thường tốn kém để sản xuất và phân phối đến người dùng. Mỗi thẻ vật lý có thể có giá trong khoảng từ 7 $ đến 70 $, cùng với các chi phí phân phối (như bưu phí) được đi cùng.

3) Thời gian thiết lập

Việc tạo tài khoản và phân phối thẻ thường sẽ đòi hỏi cần một số ngày trước khi người dùng có khả năng truy cập vào các ứng dụng web.

4) Chi phí quản lý cao

Quản lý hệ thống thẻ token yêu cầu nhiều nỗ lực hơn và tiếp cận lớn hơn với các nguồn lực nội bộ.

5) Các vấn đề bị chia nhỏ

Một khách hàng có thể cần phải mang theo nhiều thẻ, mỗi thẻ cho mỗi dịch vụ mà họ đã đăng ký.

3.2.5. Máy chủ và những hiệp ước liên kết

Số lượng lớn các cuộc tấn công lừa đảo tận dụng sự nhầm lẫn bị gây ra bởi tổ chức sử dụng tên phức tạp với các dịch vụ lưu trữ-host và các URL không thể đọc được (chẳng hạn như các tên miền đầy đủ). Hầu hết khách hàng đều không hiểu về kỹ thuật và dễ dàng bị choáng ngợp với những thông tin dài và phức tạp được trình bày trong các URLs "theo sau các liên kết này".

Bất cứ ở đâu cũng có thể xảy ra các cuộc tấn công lừa đảo này, nên các tổ chức cần phải:

• Luôn luôn sử dụng domain có cùng nguồn gốc. Ví dụ như:

http://www.mybank.com/**ebank** thay cho http://www.**mybank-ebank**.com
http://www.mybank.com/**UK** thay cho http://**uk**.mybank.com
https://**secure**.mybank.com thay cho https://www.**secure-mybank**.com

- Tự động chuyển hướng các tên domain được đăng ký trong khu vực hoặc trong các khu vực khác tới các domain chính của công ty. Ví dụ như:

http://www.mybank.**co.uk** chuyển hướng tới http://www.mybank.com/**UK**

https://secure.mybank.**com.au** chuyển hướng tới https://secure.mybank.com/**AU**

http://www.**mybank-investor.de** chuyển hướng tới http://www.mybank.com/**DE/Investor**

- Sử dụng các tên máy chủ-host mà đại diện cho tính chất ứng dụng dựa trên web. Ví dụ như:

  https://secure.mybank.com thay cho **https://www**.mybank.com

  http://**invest**.mybank.com thay cho http://www.**InvestorAtMyBank**.com

- Luôn luôn sử dụng URL đơn giản nhất hay các máy chủ có thể lưu trữ tên. Ví dụ như:

  https://secure.mybank.com thay cho **https:**//www.mybank.com/**secureinvestor**

  http://**news**.mybank.com/**UK** thay cho http://**www**.mybank.**co.uk/onlinebanking/changes/news**

- Sử dụng sự chuyển đổi địa chỉ và công nghệ cân bằng tải để tránh sử dụng của các máy chủ được đánh số. Ví dụ như:

  http://**www**.mybank.com thay cho http://**www3**.mybank.com

- Không bao giờ giữ thông tin về phiên giao dịch trong 1 dạng URL. Ví dụ, không được làm như sau:

  http://www.mybank.com/ebanking/transfers/doit.aspx?**funds=34000&agent=kelly02&sessionid=898939289834**

Thay vào đó, hãy giữ các URL càng sạch càng tốt và quản lý các thông tin mở rộng thông qua các kỹ thuật quản lý phiên phía máy chủ phù hợp (được ưu tiên), hoặc giữ các dữ liệu trong lĩnh vực ẩn của các tài liệu HTML và chỉ sử dụng các lệnh HTTP POST (ít được ưa thích).

3.2.5.1. Ưu điểm

1) Dễ áp dụng

Việc áp dụng một quy ước đặt tên mạnh mẽ và đơn giản cho máy chủ và đặt tên URL là một quá trình đơn giản. Nó có thể được áp dụng một cách nhanh chóng.

2) Xác định hữu hình

Một quy ước đặt tên đơn giản để dễ dàng hơn cho khách hàng phát hiện các đường dẫn (link) lừa đảo và hiểu được đích đến trang của chúng.

3) Dễ dàng để giải thích

Các tổ chức có thể giải thích khá đơn giản về quy ước đặt tên của họ, và đưa ra lời khuyên có ý nghĩa trong việc xác định và báo cáo các liên kết độc hại.

3.2.5.2. Nhược điểm

Sửa đổi ứng dụng: Một số các ứng dụng phức tạp với các tên máy chủ được mã hóa cứng có thể được yêu cầu cập nhật.

3.3. PHÍA DOANH NGHIỆP

Doanh nghiệp và các ISP có thể thực hiện các bước ở cấp độ doanh nghiệp để bảo vệ chống lại lừa đảo giả mạo từ đó bảo vệ các khách hàng của họ và người sử dụng nội bộ. Những giải pháp bảo mật doanh nghiệp hoạt động kết hợp với phía khách hàng và các cơ chế bảo mật phía máy chủ, sẽ cung cấp đáng kể phòng thủ theo chiều sâu chống lừa đảo và vô số những mối đe dọa hiện tại khác.

Các bước quan trọng để chống lừa đảo bảo mật cho doanh nghiệp bao gồm:

• Tự động xác nhận việc gửi các địa chỉ máy chủ e-mail.

• Chữ ký số trong các dịch vụ e-mail.

• Giám sát các lĩnh vực của công ty và thông báo đăng ký "tương tự".

• Quản lý độc quyền bảo vệ theo phạm vi hoặc tại các cổng-gateway.

• Các dịch vụ do bên thứ ba quản lý.

3.3.1. Xác thực phía máy chủ gửi thư điện tử

Nhiều phương pháp đã được đề xuất để xác thực việc gửi e-mail của máy chủ. Về bản chất, máy chủ gửi mail của người gửi được xác nhận (chẳng hạn như độ phân giải ngược của thông tin tên miền đến một địa chỉ IP cụ thể hoặc một phạm vi cụ thể) của máy chủ nhận mail. Nếu địa chỉ IP của người gửi không phải là một địa chỉ được uỷ quyền cho các miền e-mail, e-mail sẽ bị loại bỏ bằng máy chủ nhận mail.

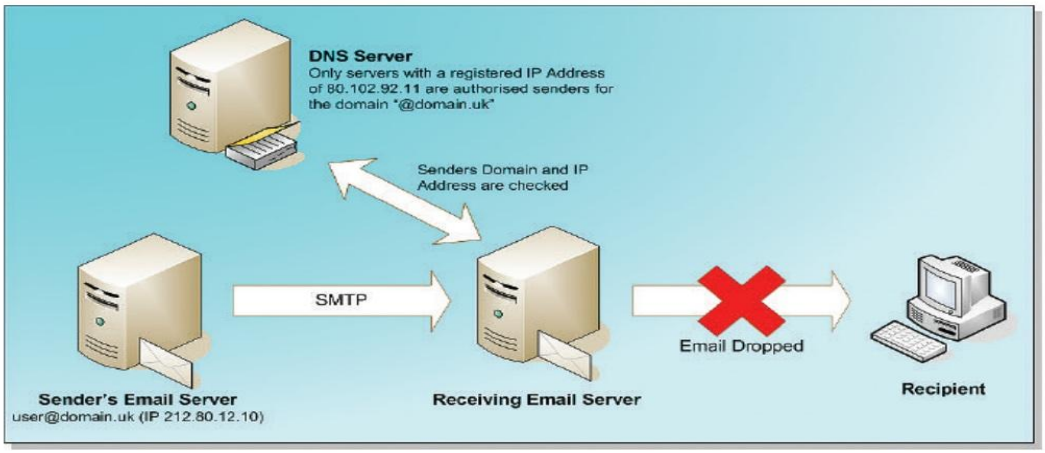


Figure 19: Mail server authentication – DNS querying of MX records

Ngoài ra, thông qua việc sử dụng SMTP an toàn, vận chuyển e-mail có thể được thực hiện qua một liên kết SSL/TLS đã được mã hóa. Khi bộ gửi email của các máy chủ mail kết nối tới máy chủ mail người nhận, thì giấy chứng nhận được trao đổi trước khi một liên kết được mã hóa được thành lập. Việc xác thực các chứng chỉ có thể được sử dụng để nhận diện một người gửi tin cậy. Việc "mất tích" chứng chỉ không hợp lệ hay bị thu hồi sẽ ngăn chặn một kết nối an toàn xảy ra và không cho phép cung cấp e-mail.

Nếu được yêu cầu, thì việc kiểm tra bổ sung với các máy chủ DNS có thể được sử dụng để đảm bảo rằng các máy chủ mail chỉ được ủy quyền có thể gửi e-mail trên các kết nối SMTP an toàn.

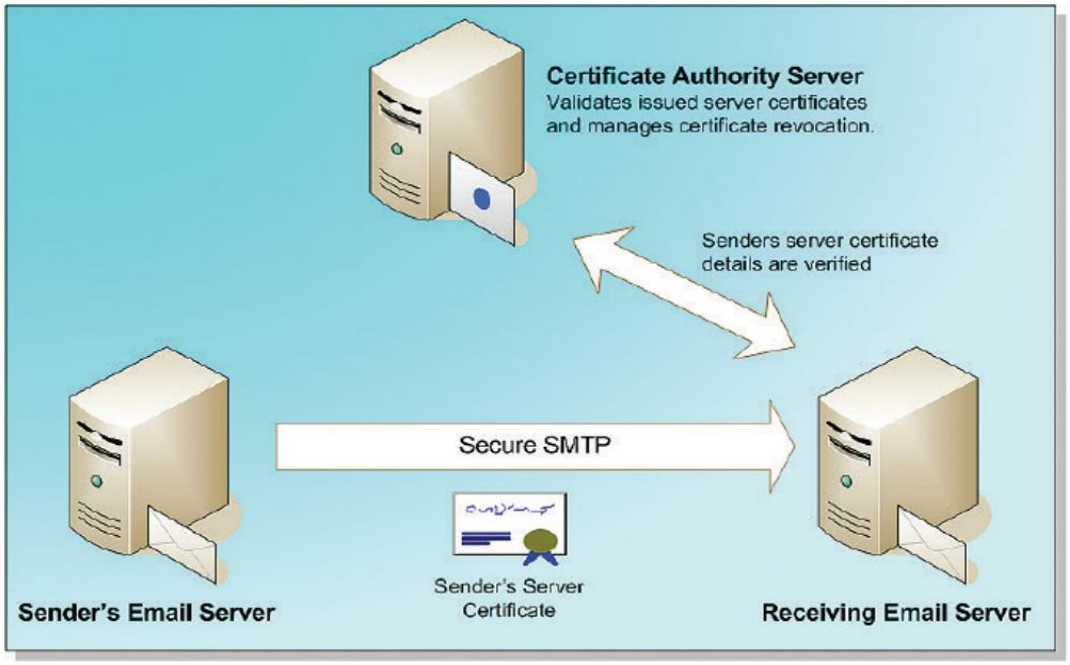


Figure 20: Mail server authentication – server certificates

Mục đích của việc xác nhận địa chỉ máy chủ gửi là để giúp cắt giảm khối lượng thư rác (spam), và đẩy nhanh việc tiếp nhận e-mail được biết đến từ một nguồn "tốt". Tuy nhiên, cả hai hệ thống có thể được khắc phục với cấu hình máy chủ nghèo, đặc biệt là nếu các máy chủ gửi có thể hoạt động như một tác nhân rơle mở. Điều quan trọng cần lưu ý là an toàn SMTP không thường được triển khai. Tuy nhiên, xác nhận e-mail server là có ích trong thông tin liên lạc nội bộ công ty khi được kết hợp với các nguyên tắc máy chủ mail, những máy mà khóa hay không thừa nhận inbound e-mail, mà sử dụng "From": địa chỉ mà chỉ có thể đến từ những người dùng nội bộ.

3.3.1.1. Ưu điểm

1) Cấu hình dễ dàng

Việc cập nhật các máy chủ DNS với các bản ghi MX có liên quan cho mỗi máy chủ mail là cần thiết cho độ phân giải ngược của máy chủ mail hợp lệ trong giới hạn miền.

2) Phòng ngừa giấu tên

Các máy chủ gửi được xác nhận/xác thực trước khi e-mail được chấp nhận bởi các máy chủ nhận. Do đó, máy chủ gửi của những kẻ lừa đảo không thể ẩn danh được.

3) Nhận dạng thư điện tử của doanh nghiệp

Sự xác thực (validation) của máy chủ gửi thư có thể được sử dụng để xác định e-mail doanh nghiệp hợp pháp, do đó làm giảm e-mail được nhận định là spam.

3.3.1.2. Nhược điểm

1) Dễ dàng giả mạo địa chỉ bên gửi email

Vì địa chỉ SMTP gửi bình thường không thể nhìn thấy người nhận e-mail, nên nó vẫn còn có thể giả mạo từ phía bên gửi email.

2) Chuyển tiếp thư điện tử (E-mail Forwarding)

Hoặc không có phương pháp cho phép các quá trình chuyển tiếp e-mail. Việc xác thực của server gửi e-mail phụ thuộc trực tiếp vào những kết nối bộ nhận bên gửi.

3) Dịch vụ E-mail của bên thứ ba

Các nhà cung cấp dịch vụ e-mail của bên thứ ba (như MessageLabs) hành động như giao nhận e-mail.

4) Phân phối SMTP an toàn

SMTP an toàn qua SSL/TLS là các giao thức không phổ biến, hoặc cũng không phải là việc thực hiện của các kiến trúc chứng nhận hỗ trợ cho các máy chủ mail.

3.3.2. Thư điện tử sử dụng chữ ký số (Digitally Signed E-mail)

Các doanh nghiệp có thể cấu hình máy chủ nhận e-mail của họ để tự động xác nhận bằng chữ ký số e-mail trước khi chuyển đến người nhận. Quá trình này có thể chứng minh được sự hiệu quả hơn cho một tổ chức, và các bước tự động có thể được thực hiện để cảnh báo cho người nhận không hợp lệ hoặc các e-mail không sử dụng chữ ký (hay không được đánh dấu).

Ngoài ra, các máy chủ e-mail doanh nghiệp có thể được cấu hình để các e-mail gửi đi luôn được ký. Bằng cách làm như vậy, một giấy chứng nhận kỹ thuật số duy nhất "của công ty" có thể được sử dụng và khách hàng đã nhận được những chữ ký e-mail có thể tự tin rằng tin nhắn nhận được của họ là hợp pháp.

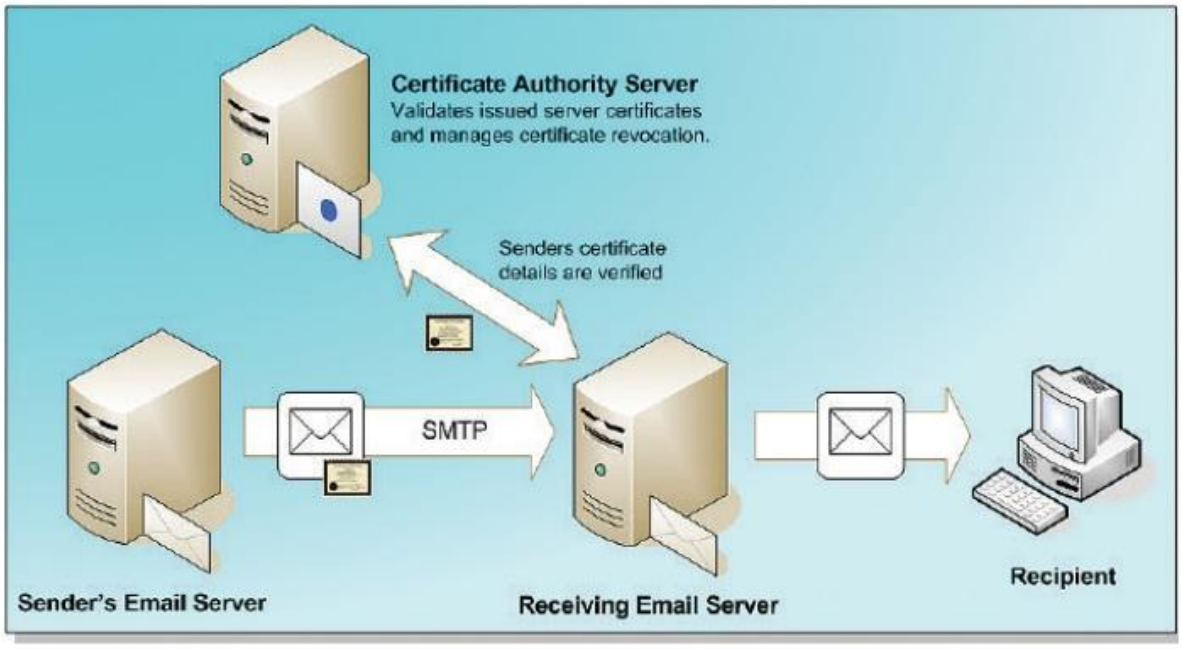


Figure 21: Digitally signed e-mail – receiving mail server validation of authenticity

3.3.3. Giám sát miền

Điều quan trọng là tổ chức một cách cẩn thận theo dõi việc đăng ký tên miền Internet liên quan đến tổ chức của họ. Các công ty nên được giám sát liên tục việc đăng

ký tên miền và hệ thống tên miền cho các tên miền xâm phạm tên thương hiệu của họ, và có thể được sử dụng để tung ra các trang web giả mạo để đánh lừa khách hàng. Có hai lĩnh vực quan tâm:

1. Các hạn sử dụng và ra hạn mới đối với các tên miền (domains) của công ty hiện có.

2. Việc đăng ký các tên miền có tên tương tự nhau.

3.3.3.1. Tên miền hết hạn và gia hạn mới

Có rất nhiều cơ quan cho phép đăng ký tên miền trước đây thuộc sở hữu của một tổ chức mà chưa được gia hạn. Bởi vì nhiều tổ chức sở hữu nhiều tên miền, nên việc chăm sóc tốt phải được thực hiện để quản lý các khoản thanh toán gia hạn nếu họ muốn giữ lại nó. Nếu không đăng ký lại tên miền một cách kịp thời sẽ dẫn đến sự mất mát của các dịch vụ hoặc các tên miền (domains) có thể bị mua bởi một bên thứ ba (ví dụ: miền tra cứu tên không còn liên kết đến một địa chỉ IP).

3.3.3.2. Đăng ký tên miền có tên tương tự nhau

Đó là một quá trình đơn giản cho một người nào đó đăng ký một tên miền thông qua bất kỳ tổ chức đăng ký tên miền nào, ở bất cứ nơi nào trên thế giới. Do đó, có nhiều tuyến đường và cơ hội cho các bên thứ ba để đăng ký tên miền đó có thể xâm phạm nhãn hiệu của một tổ chức hoặc sử dụng để lừa khách hàng tin rằng họ đã đạt đến một máy chủ hợp pháp.

Ví dụ, giả sử tên của tổ chức là "Global Widgets" và trang web bình thường của họ là www.globalwidgets.com , các tổ chức cần giữ một con mắt thận trọng kiểm tra:

• Tên có dấu nối - www.global-widgets.com

• Cụ thể quốc gia - www.globalwidgets.com.au

• Khả năng hợp pháp - www.secure-globalwidgets.com

• Từ ngữ bị sáo trộn - www.widgetglobal.com

• Tên host dài- www.global.widgets.com

• Khó phát âm khác - www.globalwidget.com hay www.globallwidgets.com

• Trường hợp bị xáo trộn không rõ ràng - www.giobaiwidgets.com (www.gIobaIwidgets.com)

Hiện nay có các dịch vụ thương mại có sẵn mà giúp các tổ chức giám sát các dịch vụ tên miền và cảnh báo khi có khả năng đe dọa tên miền mới được đăng ký. Tương tự như vậy, các dịch vụ cảnh báo tồn tại mà sẽ quan sát phòng hacking-chat phổ biến và diễn đàn gửi bài cho các cuộc thảo luận về lừa đảo và lừa đảo giả mạo khác.

3.3.4. Các dịch vụ cổng (Gateway services)

Các vành đai mạng doanh nghiệp là một nơi lý tưởng cho việc thêm các dịch vụ bảo vệ cửa ngõ mà có thể giám sát và kiểm soát cả thông tin liên lạc trong và ngoài nước. Những dịch vụ này có thể được sử dụng để xác định nội dung lừa đảo giả dạng độc hại; cho dù nó nằm trong e-mail hoặc trong các luồng truyền thông khác. Các dịch vụ cổng cấp doanh nghiệp điển hình bao gồm:

• Cổng Anti-Virus Scanning : được sử dụng để phát hiện virus, mã độc hại và các file đính nhị phân có chứa phần mềm Trojan horse.

• Cổng Anti-Spam Filtering: kiểm tra dựa trên quy tắc của nội dung e-mail cho các cụm từ quan trọng (như Viagra) và lời nói xấu, thường được sử dụng để nhận dạng thư rác phổ biến, nhưng cũng có khả năng ngăn chặn nhiều hình thức tấn công lừa đảo được thiết kế để tìm kiếm như thư rác thông thường.

• Cổng Content Filtering: Sự kiểm duyệt với nhiều loại phương pháp thông tin liên lạc đối với các nội dung xấu hoặc các yêu cầu (như e-mail, IM, AOL, HTTP,

FTP). Bảo vệ đơn giản với người dùng truy cập các trang web nổi tiếng xấu hay nổi tiếng nguy hiểm.

• Các dịch vụ Proxy: Việc quản lý nối tiếp của giao thức Internet và kiểm soát trên các kiểu truyền thông ra ngoài. Bảo vệ chống lại các cuộc tấn công trong nước thông qua việc sử dụng các địa chỉ mạng. Bảo vệ tốt chống rò rỉ thông tin chung của cấu hình mạng nội bộ.

3.3.4.1. Ưu điểm

1) Cập nhật hiệu quả

Sẽ là dễ dàng hơn, và nhanh hơn, cho một cơ quan lớn trong việc cập nhật một số lượng tương đối nhỏ của bộ quét cổng hơn là để đảm bảo rằng tất cả các bộ quét máy tính để bàn được cập nhật. Bộ quét virus máy tính để bàn tự động cập nhật sự giúp đỡ, nhưng vẫn còn hơi chậm hơn so với các bản cập nhật gateway.

2) Sự độc lập ISP

Cổng lọc nội dung là rất hiệu quả trong việc ngăn chặn truy cập vào các trang web lừa đảo được biết đến hoặc nội dung được biết đến, mà không cần chờ đợi cho một ISP để loại bỏ các trang web vi phạm lừa đảo.

3) Chế độ bảo vệ được ưu tiên trước tiên

Mã độc hại có thể bị chặn ngay từ khi mới xâm nhập vào mạng.

3.3.4.2. Nhược điểm

1) Những hạn chế về lưu lượng

Một số dạng của lưu lượng mạng không thể bị quét.

2) Các thay đổi Firewall

Triển khai một số cổng có thể yêu cầu cấu hình thủ công các tường lửa và các thiết bị cổng khác để thực hiện các quy tắc chặn.

3) Sự bảo vệ người sử dụng chuyển vùng

Người sử dụng chuyển vùng ví như nhân viên bán hàng điện thoại di động không được bảo vệ bởi các cổng dịch vụ.

3.3.5. Các dịch vụ quản lý

Trong khi các hệ thống phòng thủ vành đai cung cấp một sự bảo vệ tốt chống lại nhiều hướng tấn công lừa đảo phổ biến, những kẻ lừa đảo (cùng với bộ máy gửi thư rác) không ngừng phát triển các phương pháp được thiết kế để vượt qua các tác nhân bảo vệ. Các dịch vụ quản lý trong các lĩnh vực chống thư spam và chống lừa đảo giả dạng cung cấp cải tiến rất có giá trị trong công tác bảo vệ an ninh. Điều này phần lớn nằm trong khả năng của chúng nhằm phân tích các tin nhắn dạng e-mail được gửi đi trên mức độ toàn cầu, và xác định các chủ đề chung giữa e-mail độc hại. Ví dụ, một tổ chỉ có thể nhận được năm hay sáu e-mail ngụy trang lừa đảo một cách cẩn thận với nội dung chỉ thay đổi nhỏ - không đủ để kích hoạt một phản ứng chống thư spam - trong khi các nhà cung cấp dịch vụ quản lý đã phát hiện hàng ngàn các e-mail với cùng một kiểu mẫu, những email này kích hoạt chương trình chống spam và chống phishing. Khi giao dịch với phishing và spam, khối lượng e-mail là một thành phần quan trọng trong việc xác định các hoạt động độc hại.

3.3.5.1. Giám sát hoạt động của trang mạng

Các nhà cung cấp dịch vụ quản lý có thể triển khai dựa trên các chương trình tổng quan để theo dõi các URL và các nội dung web từ các trang web từ xa, tích cực tìm kiếm cho tất cả các trường hợp có logo, nhãn hiệu hàng hoá, hoặc nội dung web độc đáo của một tổ chức. Cuộc điều tra tổ chức đăng ký thuê bao cung cấp một "danh sách trắng" người có thẩm quyền về logo, nhãn hiệu, và nội dung trang web duy nhất cho các nhà

cung cấp dịch vụ. Khi các chương trình phát triển bị triển khai trái phép hoặc các logo đại diện, thương hiệu, hoặc nội dung web khác so với nhà cung cấp đưa ra, thì những hoạt động khắc phục hậu quả có thể được thực hiện ngay từ phía người sử dụng.

3.3.5.2. Ưu điểm

1) Dễ sử dụng

Kể từ khi dịch vụ này được cung cấp bởi thành phần bên ngoài, thì có rất ít các yêu cầu nội bộ trong việc thiết lập và cấu hình dịch vụ.

2) Tầm nhìn rộng hơn

Các nhà cung cấp dịch vụ quản lý đã xem xét sau khi nhiều tổ chức trên toàn cầu có khả năng hiển thị tuyệt vời về các mối đe dọa hiện tại và có thể dễ dàng xác định các mối đe dọa; Thông thường nhờ đó sẽ giảm xuống dưới ngưỡng kích hoạt tiêu chuẩn.

3) Sự can thiệp kịp thời

Các lệnh hợp pháp có thể được tạo ra như là kết quả của việc giám sát hoạt động mang tính nội dung, và xác định sử dụng không hợp ngay cả khi không có các email lừa đảo đã được phát hiện.

3.3.5.3. Nhược điểm

1) Tốn kém

Đối với các tổ chức lớn, việc gia công phần mềm bảo vệ các nhà cung cấp dịch vụ quản lý có thể tốn kém. Đối với các tổ chức nhỏ hơn, thì chi phí có thể ít hơn so với việc họ tự chạy các dịch vụ với các nguồn tài nguyên được dành riêng.

2) Quản lý xác thực lỗi

Các bước phải được thực hiện để quản lý xác thực lỗi (failse positive) và các thủ tục kiểm dịch - đòi hỏi nguồn lực nội bộ để giám sát và quản lý quá trình này.

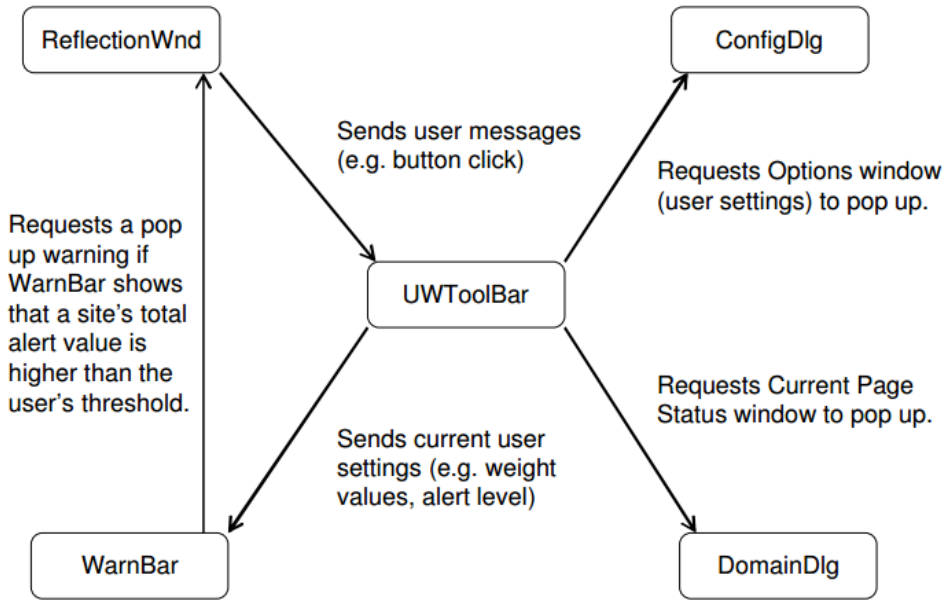
Chương 4. ỨNG DỤNG PHÒNG TRÁNH TRONG TRÌNH DUYỆT

4.1. SPOOFGUARD

Là một phần bổ sung (plug-in) tương thích với Internet Explorer. SpoofGuard đặt một "đèn cảnh báo" tại thanh công cụ (toolbar) của trình duyệt web, và chuyển màu từ xanh sang vàng hoặc đỏ nếu bạn truy cập vào một trang web phishing. Nếu bạn cố gắng cung cấp thông tin, SpoofGuard sẽ cứu dữ liệu và cảnh báo bạn. Mức độ cảnh báo cao hay thấp có thể được điều chỉnh qua các thông số.

4.1.1. Kiến trúc của SpoofGuard

SpoofGuard được viết bằng Visual C ++, sử dụng cả Windows Template Library (WTL) 7.0 và Microsoft Foundation Class Library (MFC). Hai lớp cửa sổ Spoof Guard thực hiện giao diện CWindowImpl để xác định sự xuất hiện và tương tác của người dùng thanh công cụ. Sự tương tác giữa các phân hệ chính, mô tả dưới đây, được thể hiện trong hình dưới:



SpoofGuard architecture

Các phân hệ trên chính là các hàm được lập trình tạo nên chương trình SpoofGuard, với vai trò cụ thể sau:

+ Warner: Đây là một thành phần COM, được cài vào thanh công cụ SpoofGuard. Tất cả các đánh giá trang web và kiểm tra bài dữ liệu được thực hiện ở đây.

+ ReflectionWnd: lớp CWindowImpl này thực hiện cửa sổ trong suốt, cái mà ở trên đầu trang của các thanh công cụ và phản ánh thông điệp sử dụng (ví dụ như cú click chuột) để UWToolBar. WarnBar yêu cầu ReflectionWnd bật lên một thông điệp cảnh báo khi người dùng cố gắng để gửi thông tin nhạy cảm tới một máy chủ đáng ngờ.

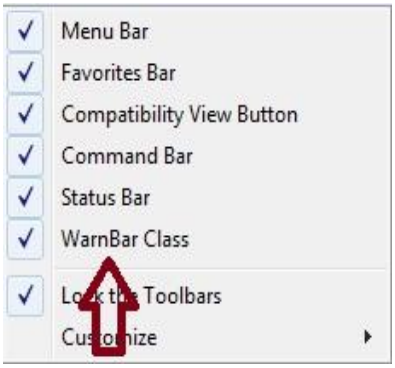
+ UWToolBar: lớp CWindowImpl này định nghĩa sự xuất hiện của thanh công cụ. UWToolBar lưu trữ những cài đặt người dùng (ví dụ kiểm tra chỉ số, ngưỡng, .v.v..) trong thời gian chạy. WarnBar yêu cầu UWToolBar cho các thiết lập để xác định màu đèn giao thông và các thông điệp cảnh báo xuất hiện trong hộp thoại trạng thái trang hiện hành (Current Page Status). Cài đặt người dùng được lưu trữ trong registry khi SpoofGuard đóng.

+ ConfigDlg mở ra một cửa sổ tùy chọn khi người dùng nhấp chuột vào nút Options. ToolBar cập nhật các thiết lập người dùng dựa trên các kết quả mà ConfigDlg trả về khi cửa sổ chấm dứt.

+ DomainDLG mở cửa sổ trang Trạng thái hiện khi người dùng nhấp chuột vào biểu tượng đèn giao thông. Nó chứa đựng những thông điệp cảnh báo cụ thể vào trang hiện tại.

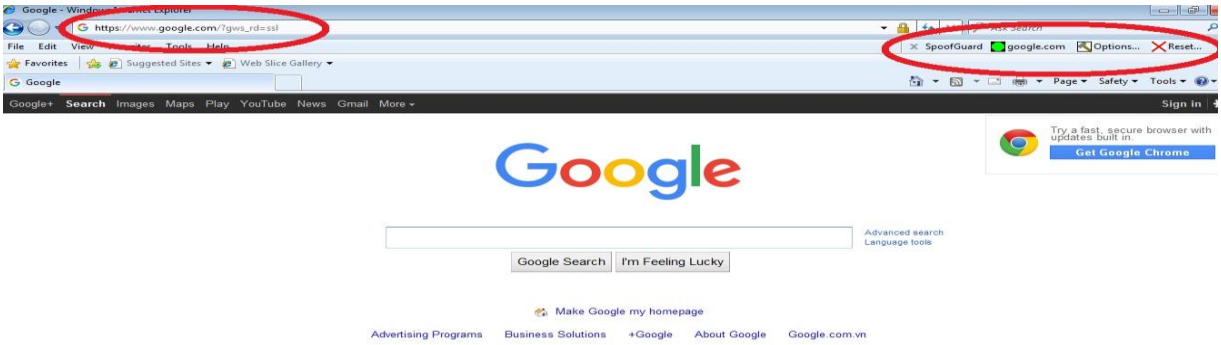
4.1.2. Cài đặt

Tải phần mềm SpoofGuard về tại link: https://crypto.stanford.edu/SpoofGuard/ Chạy file cài đặt, khởi động lại trình duyệt, trong cửa sổ trình duyệt, tại thanh công cụ, nhấn chuột phải rồi chọn WarnBar Class.



4.1.3. Giao diện

Thanh công cụ SpoofGuard có 3 nút: Settings (nơi người dùng thiết lập các thông số) , Status (hiển thị miền website mà bạn truy cập) và Reset (xóa mọi dữ liệu mà SpoofGuard thu thập được, nhưng không xóa History của Internet Explorer).

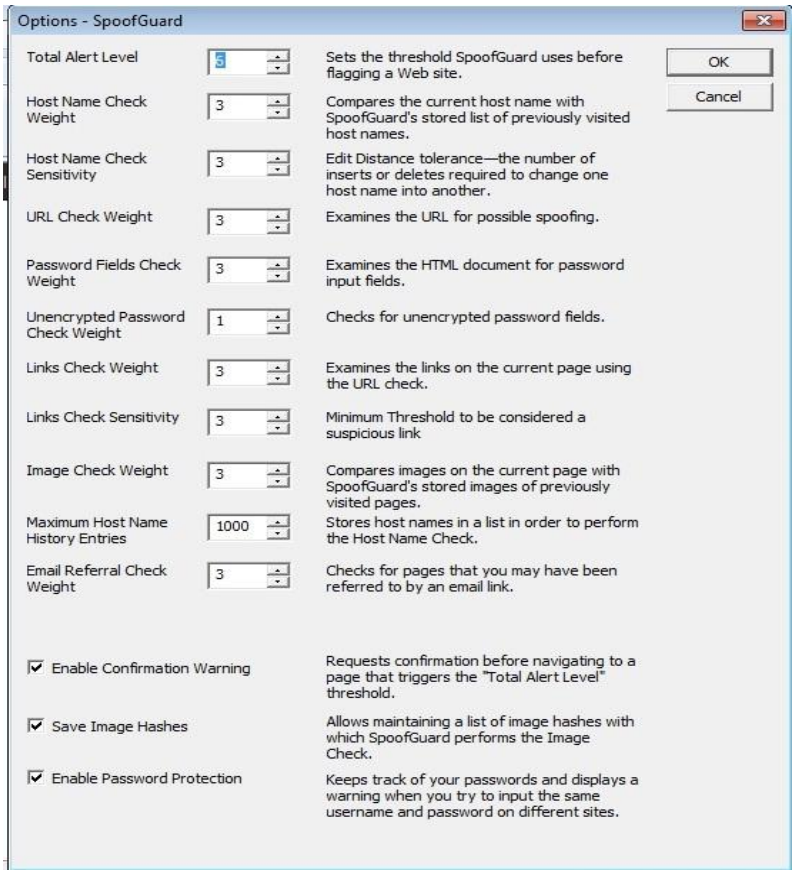


4.1.4. Nguyên lý hoạt động

Khi người dùng truy cập vào một trang web, SpoofGuard sẽ đưa ra 5 kiểm tra (check) trong 2 vòng (round): Domain Name Check, URL check, Email Check, Password Field check và Image check. Mức độ kiểm tra của mỗi check được thể hiện thông qua 1 con số gọi là weight do người dùng thiết lập (có thể thiết lập weight cho mỗi check để cho check này có giá trị lớn hơn check kia). Kết quả của mỗi check sẽ được cộng lại với nhau.

Nếu website có vấn đề, check sẽ trả về kết quả là activated. Người dùng cũng cần phải định mức giá trị giới hạn trong mục Total Alert Level, để một website sẽ bị đánh dấu là web phishing, đèn đỏ của Spoof Guard sẽ hiện lên để cảnh báo rằng đây là một website nguy hiểm.

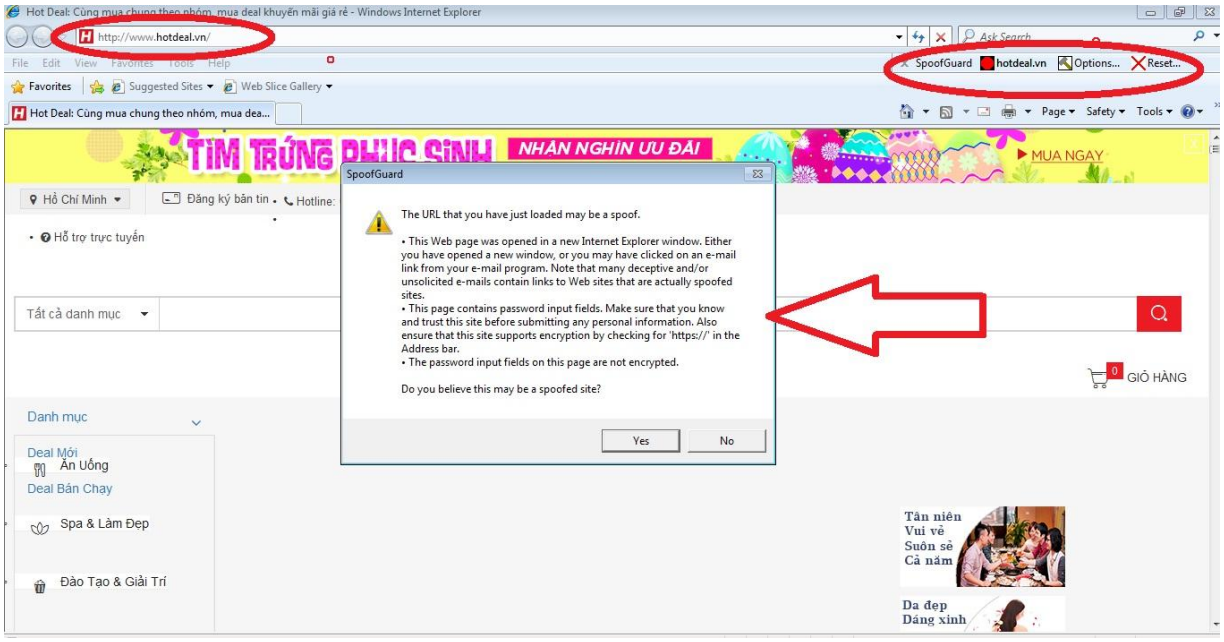
Vòng kiểm tra đầu tiên xuất hiện khi bạn vừa truy cập và một website mới. Tại thời điểm này, trình duyệt chỉ có được thông tin duy nhất là tên miền và URL của website đó. Cho nên, 2 kiểm tra đầu tiên tại vòng 1 là Domain Name check và URL check. Nếu kết quả của 2 check này đủ để đánh dấu website là phishing, bạn sẽ nhận được ngay một cảnh báo trước khi trình duyệt hiển thị nội dung website đó. Nếu không, các kiểm tra khác ở vòng 2 sẽ thực hiện tiếp.



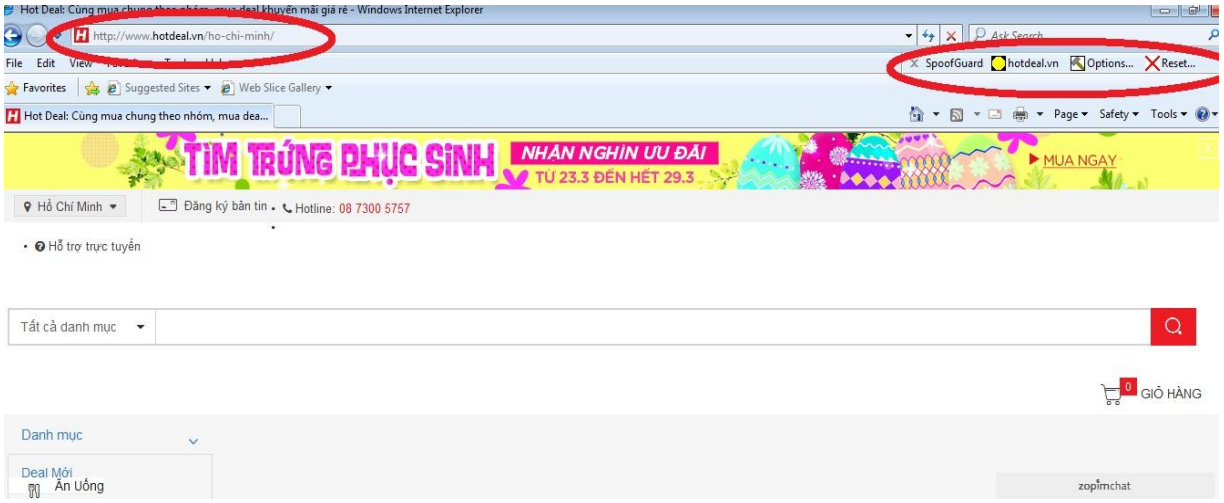
Như vậy, mỗi check dựa vào tiêu chuẩn gì để trả về kết quả là activated? Các cách thức kiểm tra này do người viết chương trình quy định và hiện thực, ở đây chỉ giới thiệu một số tiêu chuẩn đơn giản.

Domain Name Check: bằng cách so sánh tên miền của website mà bạn đang truy cập vào với tên miền của các website bị đánh dấu gần nhất đã được lưu trong history của trình duyệt; URL check: kiểm tra xem trong URL có chứa các user name khả nghi hoặc có chứa các giao thức truy cập lạ khác với các chuẩn hay không (http, https, ftp, gopher,

socks); Password Field check: kiểm tra xem trong nội dung website có những vùng nào cho người dùng nhập password mà không được mã hóa hay không v.v…



Thử nghiệm chương trình với 1 trang web quảng cáo bán hàng- lần đăng nhập đầu tiên



Cùng trang web trên sẽ có đèn cảnh báo màu vàng với lần đăng nhập tiếp theo (sau khi chọn "yes") và lọc bỏ các dữ liệu bị nghi ngờ phishing trong trang web

4.1.5. Ưu điểm và nhược điểm

4.1.5.1. Ưu điểm

+ Công cụ chống lừa đảo SpoofGuard giúp vá một số điểm yếu về bảo mật của phần lớn các trang web hiện tại.

+ Thông tin cảnh báo của SpoofGuard giúp người dùng tự xác định được cả những mối nguy hiểm tiềm tàng (nếu có) của Website.

+ Các kỹ thuật chống lừa đảo được thực hiện và thử nghiệm trong SpoofGuard được thiết kế để phát hiện các cuộc tấn công lừa đảo Web mà không cần bất kỳ sự hợp tác từ các trang web có khả năng bị giả mạo hoặc đã bị giả mạo.

4.1.5.2. Nhược điểm

+ Chỉ áp dụng được với trình duyệt Internet Explorer (IE).

+ Công cụ sử dụng thuật toán MD5 kết hợp với thuật toán SHA-1, thuật toán mà hiện nay đã được phát hiện ra nhiều lỗ hổng, do đó kỹ thuật này không thể chống lại một số dạng giả mạo nguy hiểm.

+ Trong một số trường hợp check sum không thể tin tưởng được (ví dụ, nếu nó được lấy từ 1 lệnh như tập tin đã tải về), trong trường hợp đó SpoofGuard chỉ có chức năm kiểm tra lỗi. Do đó nó áp dụng phù hợp cho phía Client, thông thường với các chuyên gia (hay phía Server) sẽ không cần dùng đến ứng dụng này.

4.2. TRANG WEB KIỂM TRA LỪA ĐẢO GIẢ DẠNG PHISH TANK

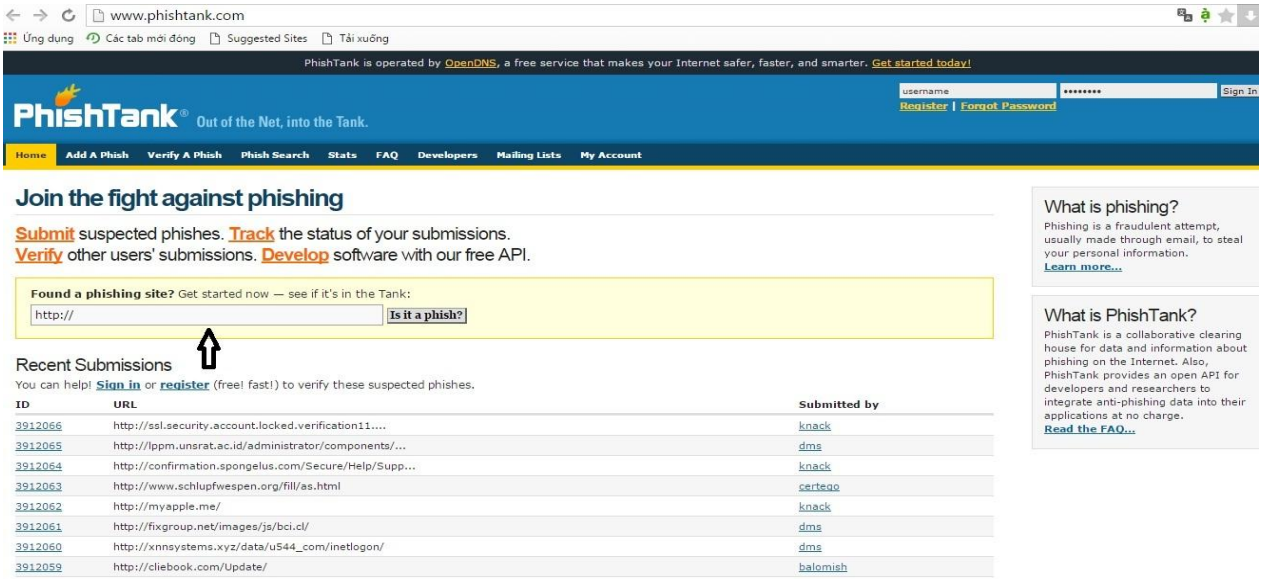
4.2.1. Cơ bản về Phish Tank

PhishTank là một website miễn phí cho mọi người có thể kiểm tra, theo dõi và chia sẻ dữ liệu về phishing. PhishTank được điều hành bởi OpenDNS, một công ty

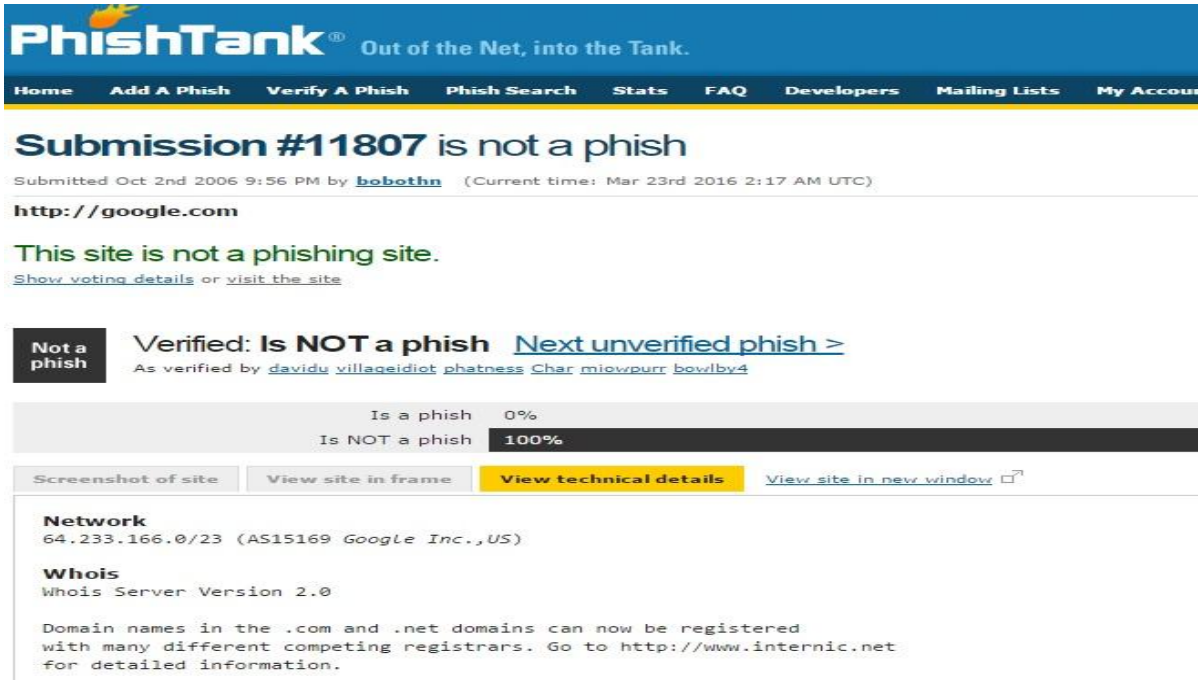
thành lập năm 2005 nhằm cải thiện Internet an toàn hơn, nhanh hơn, và DNS thông minh hơn. PhishTank là một trang web và dịch vụ web (API-Application Programming Interface - Giao diện lập trình ứng dụng) với mục đích nhận thông tin về các trang web lừa đảo. Nó không phải là một phần của phần mềm, và nó không chạy trên máy tính của bạn. PhishTank không xác nhận bất kỳ phần mềm bảo mật đặc trưng nào, nhưng nó lại đưa ra bất cứ điều gì đó giúp bảo vệ người dùng trực tuyến.

Đối với những người dùng, sau khi hoàn thành việc đăng ký PhishTank miễn phí và sử dụng giao diện lập trình ứng dụng (API) để lập trình gửi thông tin hoặc yêu cầu thông tin từ PhishTank, những thông tin được thêm vào sẽ được ghi lại, trong đó có các tên màn hình ("User ID"), chìa khóa API, hành động, các thông số, và các địa chỉ IP được sử dụng để thực hiện yêu cầu. Sử dụng API là không có giới hạn, và nó là miễn phí, nhưng PhishTank có thể sử dụng dữ liệu này để xác định quá mức các nguồn tài nguyên PhishTank qua API. PhishTank cũng có thể trưng cầu ý kiến phản hồi từ người sử dụng API thông qua địa chỉ email đã đăng ký của họ về cách mà API được sử dụng, và làm thế nào nó có thể được cải thiện.

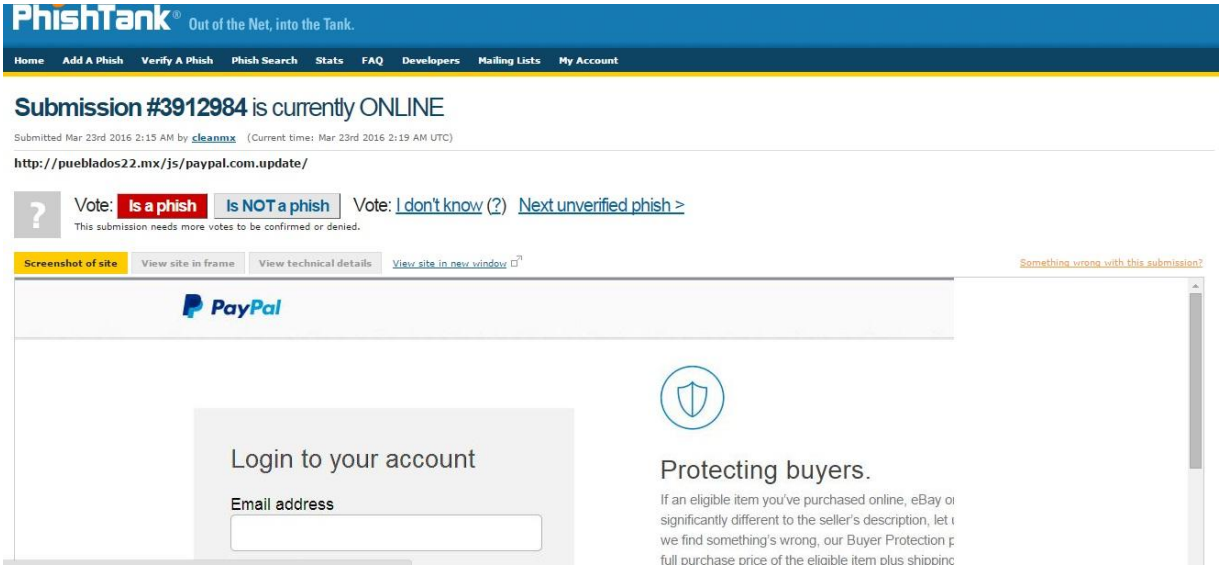
Truy cập vào địa chỉ http://www.phishtank.com/ để có thể sử dụng trang web này.



Sau khi nhập địa chỉ trang web muốn kiểm tra vào, sẽ đưa ra kết quả dự đoán chi tiết; Dưới đây là một số ví dụ minh họa:



Kết quả khi kiểm tra trang web http://google.com



Kết quả là "phishing" khi kiểm tra trang web lạ,
với địa chỉ là: http://pueblados22.mx/js/paypal.com.update

Đối tác của PhishTank gồm các tổ chức lớn là: Yahoo Mail, McAfee, nhóm chống Phishing APWG, Carnegie Mellon, Stbernard, Mozilla, Kaspersky, Fire trust, WOT, Finra, Surbl, Opera, Careerbuilder.com , Sitetruth, Avira. Các tổ chức này sử dụng dữ liệu đệ trình và được xác nhận qua PhishTank.

4.2.2. Ưu điểm

+ Giao diện thân thiện, đơn giản, dễ sử dụng.

+ Thông tin về Phishing được cập nhật nhanh chóng vì ngoài khả việc kiểm tra, thì bất kỳ người dùng nào cũng có thể đề xuất một trang web nghi ngờ là Phishing giúp cảnh báo những người sau.

4.2.3. Nhược điểm

+ Chỉ có khả năng phòng Phishing, không có khả năng chống Phishing.

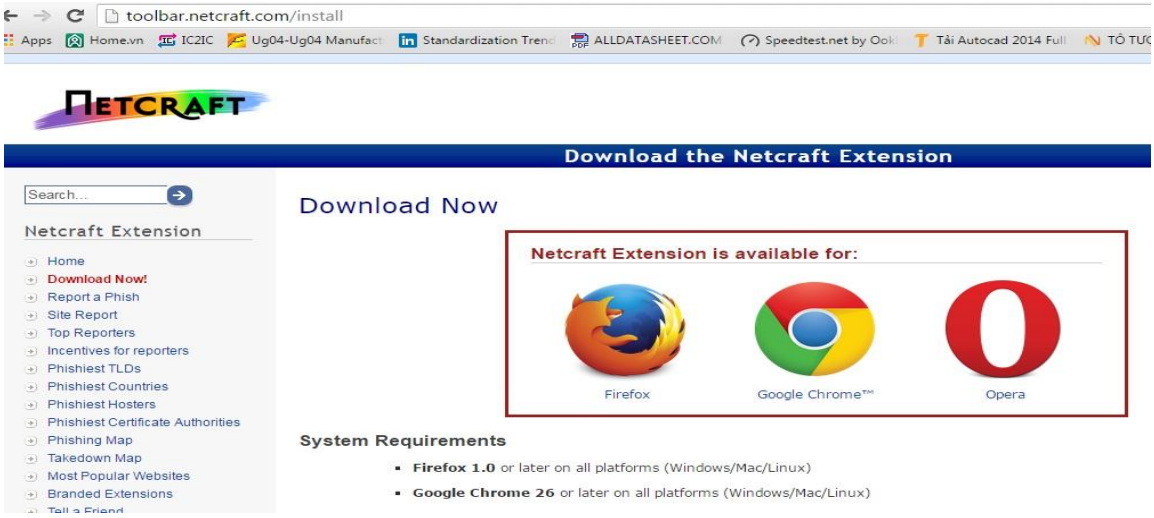
4.3. NETCRAFT

Netcraft là công ty đã khảo sát Internet từ 1995 và thu thập biến thiên của Internet trong vòng gần 20 năm qua. Đây là một công ty của Anh Quốc và có độ tin cậy rất cao. Extension Netcraft dựa vào những thông tin từ người dùng thông báo những trang web độc hại và được Netcraft thử nghiệm và xác thực trước khi hình thành bộ luật cản. Theo Netcraft, cho đến tháng Tám năm 2014, Netcraft đã phát hiện và block 9.9 triệu trang web phishing (một phương thức lừa đảo trên mạng).

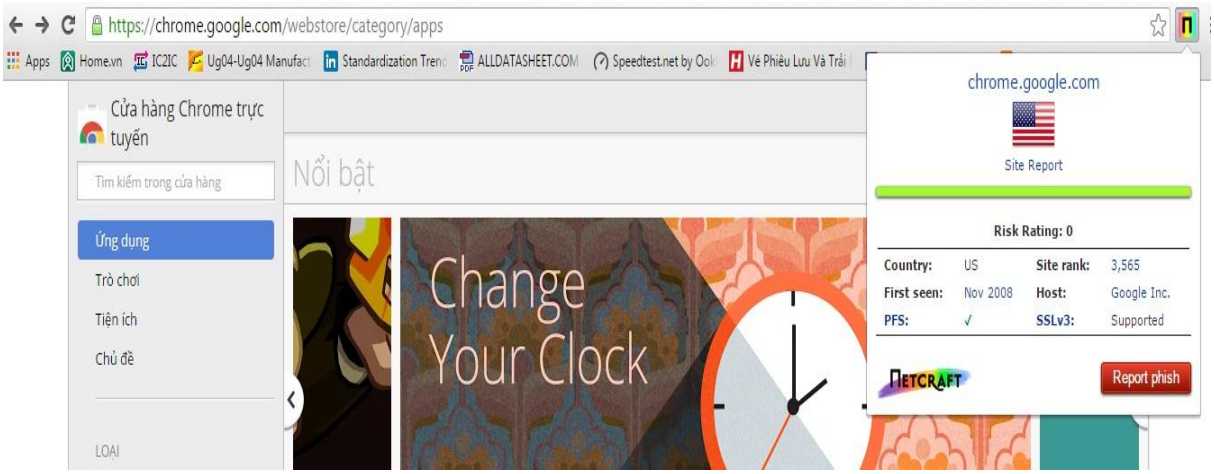
Thử nghiệm cho thấy gần như tuyệt đối các trang đen tối dùng để phishing đều bị block. Có một số trang phishing mới không được block, có lẽ do chưa bị thông báo và chưa được cập nhật trong cơ sở dữ liệu của Netcraft. Extension này gọn nhẹ và hầu như không có ảnh hưởng gì đến hiệu suất và vận tốc duyệt web.

4.3.1. Cài đặt

Tải phần mềm Netcraft về tại link: http://toolbar.netcraft.com/install chọn trình duyệt muốn cài đặt (ở đây ta minh họa với trình duyệt Google Chrome). Hình minh họa:



Tiếp tục cài đặt theo hướng dẫn ta, khi cài đặt add-on được hoàn thành sẽ thấy biểu tượng Netcraft bên góc phải trên cùng của trình duyệt:



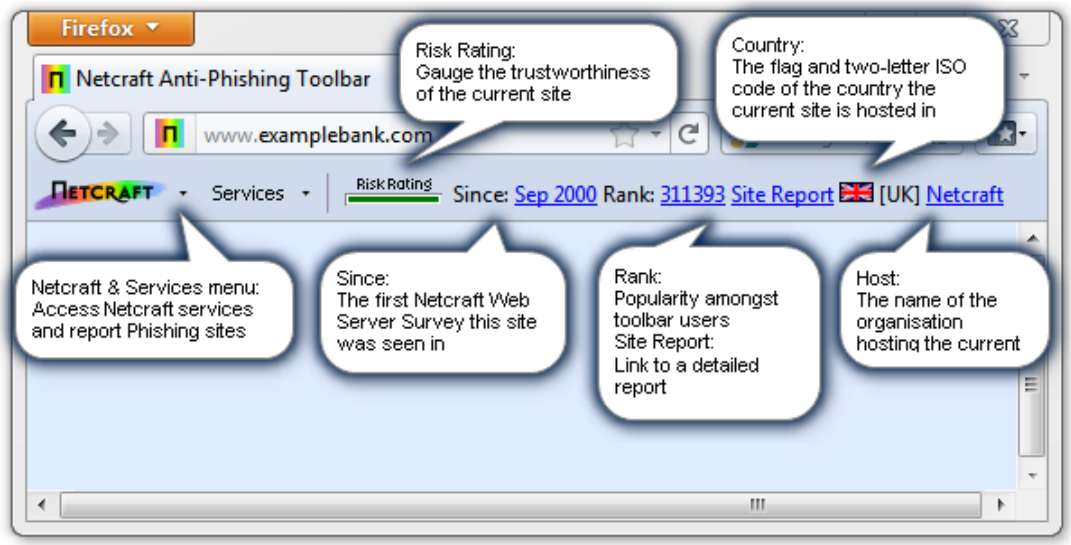
4.3.2. Nguyên lý hoạt động

Netcraft là add-on sử dụng để giải quyết cùng vấn đề về phishing. Netcraft Toolbar cài đặt một thanh công cụ để hiển thị mức độ rủi ro (Risk rating), hạng của site (rank) và cung cấp một liên kết báo cáo (Site Report- báo cáo này cung cấp cho bạn

các thông tin mà Netcraft thu thập được về site). Cũng trên công cụ này, thanh bar là một menu sổ xuống, với menu này bạn có thể báo cáo một site.

Tính năng quan trọng nhất của công cụ này đối với người dùng là xếp hạng rủi ro (Risk Rating). Thanh bar này sẽ có màu xanh (nếu site có mức rủi ro thấp) hoặc đỏ (nếu site có mức rủi ro cao). Có một số hệ số đi kèm với việc tính toán độ rủi ro. Hệ số chính là tuổi đời của site.

Để dễ hiểu ở đây ta đưa ra hình ảnh giải thích chi về tính năng của Netcraft được lấy từ trang chủ của nhà cung cấp (http://toolbar.netcraft.com)



Giải thích tính năng của Netcraft trong Firefox (với Google Chrome cũng tương tự)

4.3.3. Ưu điểm và nhược điểm

4.3.3.1. Ưu điểm

+ Giao diện đơn giản, dễ hiểu và dễ sử dụng.

+ Cung cấp chi tiết các thông tin của trang Web (như: mức độ rủi ro (Risk Rating), tuổi đời của site, mức độ phổ biết của Site (rank), tên của host hiện tại đang được đặt, từ đó giúp người dùng có lựa chọn đúng đắn về tính toàn vẹn của trang Web.

4.3.3.2. Nhược điểm

+ Để có được thông tin đầy đủ về trang web, người dùng phải qua truy cập vào trang web, do đó không có hiệu quả với những trang có chứa mã độc hại hay gắn kèm virus.

+ Không có tác dụng với những site không được cập nhật (ví dụ site do người dùng mới tự tạo ra).

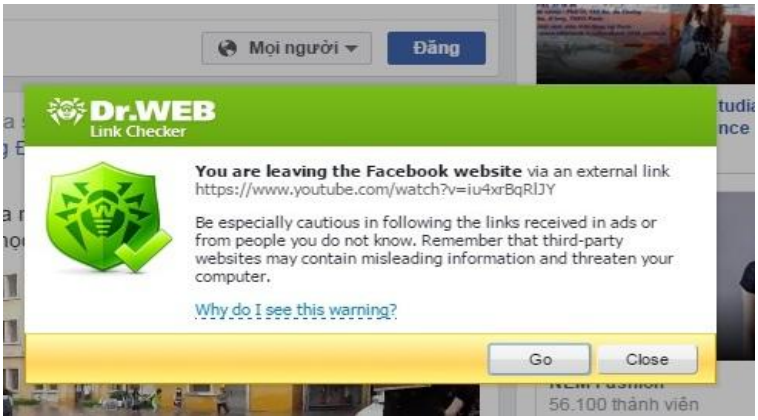
4.4. DR.WEB ANTI-VIRUS LINK CHECKER

4.4.1. Cơ bản về Dr.Web Anti-Virus Link Checker

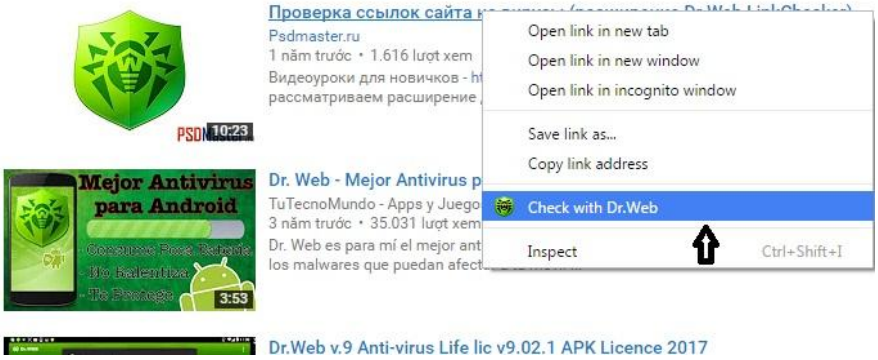
Dr.Web Anti-Virus Link Checker là một phần mở rộng cho trình duyệt web (hỗ trợ cả Chrome, Firefox, IE, Safari và Opera) và cả trình quản lí email Thunderbird. Sử dụng trình quét virus trực tuyến của Dr. Web, Dr.Web Anti-Virus Link Checker có thể phát hiện tất cả các file không an toàn trong trang web. Add-on này cũng có chức năng tự động quét tất cả các đường link trên các mạng xã hội như Facebook, Vk.com hay Google+. Dịch vụ này xuất hiện từ năm 2003 và được cập nhật theo định kỳ.

Cài đặt tương tự như đối với ứng dụng Netcraft đã trình bày ở trên.

Ví dụ 1: Cảnh báo khi vào 1 trang web thứ 3, ở đây lấy ví dụ là từ trang facebook, trang thứ 3 là 1 link được giới thiệu từ đó, khi nhấn chuột vào đường link đó, lập tức Dr.Web sẽ hiện ra cảnh báo để nhắc nhở người dùng như hình dưới.



Ví dụ 2: Kiểm tra xem đường dẫn nào đó có mối nguy hiểm gì không:



Click chuột phải vào Link cần kiểm tra, chọn "Check with Dr.Web"

Sau khi Dr.Web quét sẽ hiện ra kết quả: như ví dụ trên là 1 trang Web an toàn "Clean"

4.4.2. Ưu điểm

+ Dễ sử dụng, dung lượng chương trình nhỏ (hơn 100Mb) nên không ảnh hưởng đến hiệu năng của máy tính.

+ Giao diện đơn giản, luôn cảnh báo người dùng kịp thời nhưng không gây khó khăn cho việc sử dụng. Do đó khả năng phòng và chống Phishing cao.

4.4.3. Nhược điểm

+ Thông tin Phishing do nhà cung cấp cập nhật theo định kỳ, do đó sẽ không có tác dụng đối với các mối đe dọa mới.

4.5. TỔNG KẾT CHƯƠNG

Trong phần nghiên cứu này, tôi đã đưa ra một số phương pháp để phòng và chống Phishing. Tuy nhiên thực tế, đối mặt với Phishing có lẽ là vấn đề nan giải nhất, chúng ta không thể diệt nó, và cũng chưa có phương pháp nào để diệt nó. Trong phần này tôi đề xuất nên kết hợp nhiều phương pháp với nhau để đạt hiệu quả phòng chống Phishing tốt nhất:

+ Trước khi đăng nhập nên sử dụng công cụ Phish Tank để kiểm tra xem đây có phải trang web lừa đảo không?

+ Khi đã xác nhận được đây không phải là trang web lừa đảo, sử dụng công cụ Dr.Web để kiểm tra xem có chứa virus hay phần mềm độc hại gì không;

+ Sử dụng Netcraft để xác thực những thông tin về trang Web nhằm đảo bảo độ tin cậy cao hơn đối với người sử dụng.

+ Trường hợp sử dụng trình duyệt là IE thì thay vì dùng Netcraft ta sử dụng công cụ SpoofGuard để xem các thông tin và các cảnh báo về khả năng Phishing của trang WEB.

KẾT LUẬN

Luận văn với đề tài "Lừa đảo qua mạng và cách phòng tránh" có các kết quả chính như sau:

1/. Tìm hiểu nghiên cứu về lừa đảo trên mạng máy tính.

2/. Thử nghiệm ứng dụng phòng tránh lừa đảo trong trình duyệt Web.

Việc ý thức được vấn nạn lừa đảo giả dạng (phishing) trên thế giới cũng như tại Việt nam là rất quan trọng. Việt Nam nổi tiếng thế giới với việc ăn cắp phần mềm có bản quyền thì không có lý gì mà "phishing" khi có điều kiện sẽ không phát triển. Để phòng chống lại kiểu tấn công này, không có cách nào hiệu quả bằng cách giáo dục cho những người dùng máy tính những thủ đoạn lừa đảo của kẻ tấn công, lừa đảo để họ tự biết cảnh giác.

BẢNG CHỮ VIẾT TẮT, TỪ CHUYÊN MÔN BẰNG TIẾNG ANH

Attacker		Kẻ tấn công
Client		Máy trạm/ máy khách
Enterprise		Doanh nghiệp
Hacker		Chỉ những người (nhóm người) có hành động thâm nhập với mục đích phá hoại hoặc vi phạm pháp luật nhằm phục vụ những mục đích xấu xa của mình
IRC	Internet Relay Chat	Mạng trò chuyện trực tuyến
MITM	Main-In-The-Middle Attacks	
Online		Trực tuyến
Phisher		Kẻ lừa đảo
Phishing		Lừa đảo giả dạng
Phishing scam		Lừa đảo giả mạo
Proxy Server		Máy chủ ảo: đóng vai trò cài đặt các chức năng trung gian giữa người dùng trạm và Internet
URL	Uniform Resource Locator	Định vị tài nguyên
Server		Máy chủ
Spam		Thư rác (trong hộp thư điện tử)
Watermarking		Là một kỹ thuật ẩn giấu thông tin đặc biệt nhằm đưa các dấu hiệu vào ảnh số

TÀI LIỆU THAM KHẢO

Tài liệu tiếng việt

[1] Nguyễn Khắc Cửu, "Bảo mật nhóm hệ thống viễn thông", đề tài luận văn thạc sỹ, Học Viện Công Nghệ Bưu Chính Viễn Thông.

[2] Nguyễn Minh Đức – Chuyên gia về Big Data, hiện đang làm việc tại Ban Công Nghệ tập đoàn FPT, bài báo "Phishing là gì? Và cách để bạn bảo vệ mình", http://securitydaily.net/phishing-la-gi-va-cach-de-ban-bao-ve-minh/ .

[3] Bài báo "Tấn công giả mạo" trên trang wikipedia, https://vi.wikipedia.org/wiki/T%E1%BA%A5n_c%C3%B4ng_gi%E1%BA%A3_m%E1%BA%A1o .

Tài liệu tiếng anh

[1] Christopher Hadnagy, "Social Engineering: The Art of Human hacking", Published by Wiley Publishing, Inc.

[2] Markus Jakobsson, "Modeling and Preventin Phishing Attacks", School of Informatics Indiana University at Bloomington Bloomington, IN 47408.

[3] Gunter Ollmann, "The Phishing Guide: Understanding and Preventing phishing attacks", Directer of Security Strategy IBM Internet Security Systems.

[4] The Anti-phishing working group, http://www.antiphishing.org