Computer Science and Application 计算机科学与应用, 2017, 7(2), 146-149
Published Online February 2017 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2017.72018

Hans汉斯

Hazards and Characteristic Analysis of Phishing Emails

Haiyan Gu

Jiangsu Police Institute, Nanjing Jiangsu
Email: guhaiyan@jspi.cn

Received: Feb. 3rd, 2017; accepted: Feb. 25th, 2017; published: Feb. 28th, 2017

Abstract

Phishing brings more and more security threats on the Internet. Phishing email is an important means of phishing. This paper introduces the concept of phishing emails, analyzes the main hazards of phishing emails, and deeply analyzes the characteristics and implementation steps of it. A reference has been set up for Internet users to distinguish phishing messages.

Keywords

Phishing Email, Hazards, Practical Procedure, Mail Feature

钓鱼邮件的危害及其特征解析

顾海艳

江苏警官学院，江苏 南京
Email: guhaiyan@jspi.cn

收稿日期：2017年2月3日；录用日期：2017年2月25日；发布日期：2017年2月28日

摘 要

网络钓鱼对互联网的安全威胁越来越大，钓鱼邮件则是实施网络钓鱼的重要手段。该文在介绍钓鱼邮件的概念、剖析钓鱼邮件主要危害的基础上，深入分析了钓鱼邮件的特征及其实施步骤，可给网络用户鉴别钓鱼邮件提供参考。

关键词

钓鱼邮件，危害，实施步骤，邮件特征

文章引用: 顾海艳. 钓鱼邮件的危害及其特征解析[J]. 计算机科学与应用, 2017, 7(2): 146-149.
https://doi.org/10.12677/csa.2017.72018

1. 引言

随着互联网的快速发展，新的网络攻击形式-“网络钓鱼”呈现逐年上升的趋势，利用网络钓鱼进行欺骗的行为越来越猖獗，对互联网的安全威胁越来越大。根据非盈利组织 Anti-Phish 工作组报告，网络钓鱼攻击正以每月 50%的速度增加，一般情况下，约有 5%的人会上当受骗。钓鱼网站严重地影响了在线金融服务和电子商务的发展，危害公众的利益。同时，使网络上人与人之间的互信关系变得越来越脆弱，动摇了互联网世界的信任体系。因此，网络钓鱼已经成为互联网世界的一大公害[1]。

网络钓鱼，最常见的欺骗方式就是设计钓鱼网站，引诱网络用户进入以假乱真的网站而导致自身的用户名、密码等重要数据的泄露，进而遭受重大损失。钓鱼网站的欺骗性很强，用户不细心、不谨慎就很容易上当受骗。而引诱用户进入钓鱼网站的主要手段就是采用钓鱼邮件进行诱导。

2. 钓鱼邮件的概念及危害分析

2.1. 基本概念

“钓鱼邮件”是一种网络欺诈邮件，这类邮件中带有非法链接，可将用户引导至仿冒的某些真实网站的网页，或真实网站的被插入了危险的 HTML 代码的网页(攻击者利用服务器程序上的某些漏洞来实现)，以此来骗取用户银行或信用卡账号、邮箱账号、密码等属于个人的隐私信息[2]。

网络攻击者通过广泛推送钓鱼邮件，实现窃取用户重要信息的主要目的。2014 年，卡巴斯基实验室的垃圾邮件分析师曾指出：虚假的银行提示信息是最常见的恶意邮件或钓鱼攻击类型。攻击者精心设计钓鱼邮件内容，在其中添加较多的官方资源链接和虚假组织的服务链接。通过在邮件中添加合法连接，骗取用户的信任，同时也能成功通过垃圾邮件过滤器的筛选。

2.2. 钓鱼邮件的危害

钓鱼邮件通过隐含的恶意链接，窃取用户重要个人信息，可能造成直接经济损失、带来间接经济危害甚至政治危害。

2.2.1. 直接经济危害

钓鱼邮件的主要目的是要劫财。钓鱼邮件往往暗藏着两重侵害方式：一是用户没有发现邮件中链接的假网银、假网站，输入了个人账户和密码等信息，导致信息泄露造成经济损失；二是用户即便识破了假网银、假网站，没有输入自己的网银账号和密码，虽然本次的直接损失可以避免，但还是可能被攻击者的后招所伤，因为通常这些假网站中都暗藏了事先植入的木马程序或间谍程序。若用户的电脑防御能力较弱，只要点开了虚假网站的界面，电脑就会被植入木马或间谍程序。以后，用户只要在该机上使用此网银就会被这些恶意程序监控到，并以数据包的形式传到不法分子预先设定的邮箱里，从而给网络用户造成重大经济损失。

2.2.2. 间接经济危害

钓鱼邮件除了可能导致上述直接经济危害外，还可能导致用户邮箱被黑客侵入从而造成很多其他间接经济危害。

1) 损坏邮箱中联系人的资料。入侵者会收集所有邮件中的用户资料，更严重的是修改邮箱的密码，用户将永远失去这个邮箱的使用权。若是商业用户邮箱被盗窃，则可能造成更大经济损失。

2) 入侵者掌握用户邮箱后，可以根据需要申请一个与用户类似的名字和一个类似的邮件地址。如果恰好遇到有用户要打款，入侵者就可以把自己的帐户发给用户的客户，或者在成功拦截发往该邮箱的邮件后，把用户帐户替换为入侵者的账户，这样客户的相应款项就会打入到入侵者的帐户。

3) 入侵者还可利用买家贪图便宜的人性弱点，通过被盗用户的名义与用户的客户进行联系来诈骗。例如，入侵者可以把相关产品价格报得适当的低，引诱买家支付一定的预付款，通过这种方式可以在短时间内给很多客户造成重大损失，也给邮箱用户带来更重大的信誉损失。

2.2.3. 政治危害

钓鱼邮件的诈骗方法不会仅拘泥于一种，除了会造成上述经济损失外，也可能造成严重政治危机。

一个典型的案例就是美国的“邮件门”事件。2016 年 7 月 22 日，就在美国司法部宣布不指控希拉里的两周之后，阿桑奇领导下的“维基解密”公布了希拉里方民主党委员会内部约 2 万封的绝密邮件，所有邮件中主要讨论的是如何把希拉里推上总统宝座。这些邮件的公布，让美国民众意识到民主党内部的协作阴谋，从而引起公众更大的质疑：被希拉里团队删掉的另外 3 万封、不能给外人看的邮件可能含有更多可怕的内幕。

在此关键时刻，希拉里竞选团队中最重要的成员，竞选经理 John Podesta 点开了一封黑客发给他的钓鱼邮件，从而泄露了他个人邮箱密码，导致其邮箱被黑客翻遍。黑客把获得的邮件交给了“维基解密”。从 2016 年 10 月开始，“维基解密”逐渐公布 Podesta 的这些邮件。

由此导致美国大选的风云突变，最终特朗普以微弱优势获得选举胜利。可以说，钓鱼邮件在改变 2016 年美国大选结果中起到了至关重要的作用。

上述案例说明，如果国家公职人员、特别是敏感岗位的工作人员，在日常工作、生活中不注意个人邮箱的安全问题，不小心点击了钓鱼邮件中的相关链接，将可能给国家安全带来极大危害。

3. 钓鱼邮件的实施步骤及其特征分析

3.1. 实施步骤分析

钓鱼邮件是一种针对人性弱点的攻击手段，它经常会以别人容易接受的手段来进行“钓鱼”，其实施通常有如下步骤，如图 1 所示。其中关键的第一步就是钓鱼邮件的设计。

钓鱼邮件表面上看和正常邮件没有太大区别，内容和正常业务往来的邮件类似。但这类邮件内容通常很能吸引眼球，特别有真实感或诱惑力，易受到用户重视。寄发的目标通常是攻击者通过各种途径获取的相关用户。

用户阅读邮件后，如果没有仔细甄别，则可能根据钓鱼邮件的提示填写相关信息进行回复或点击相关链接登录钓鱼网站，从而导致个人重要信息的泄露。

3.2. 特征分析

通过对钓鱼邮件的实施过程、传播方式、钓鱼邮件实例进行分析，再结合垃圾邮件过滤器中垃圾邮件具有的若干特征进行分析，可归纳出钓鱼邮件具有如下主要特征[3] [4] [5]：

1) 含有 HTML 语言描述的内容；

2) 所有链接域名至少有一个属于被保护列表中的对象；

3) 链接中含有诱惑性关键字，如“点击此处”等类似文字；

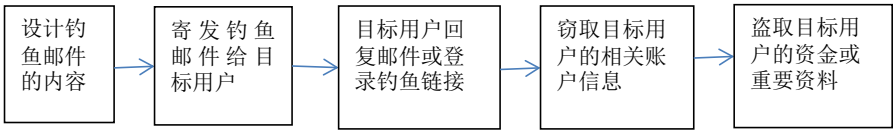

Figure 1. Implementation process diagram of phishing emails
图 1. 钓鱼邮件的实施过程图示

4) 邮件中多次出现的域名与链接登录的域名不相同；

5) 邮件中登录链接的域名与发件人邮箱域名不相同；

6) 发件人邮箱或收件人邮箱通常都是使用 HOTMAIL、YAOHOO 等免费邮箱，不使用单位邮箱(如国内的 gov.cn,edu.cn 等)；

7) 邮件来源通常都是国外的 IP 地址；

8) 链接中有的域名注册时间往往小于 2 个月；

9) 链接中多次使用 HTTP 协议，改变链接导向；

10) 链接域名与网页展开的字符串不一致。例如在链接yhd.com中，这个链接网页上显示 yhd，但是实际链接指向的是域名为 yhd1.com 的网站。

掌握钓鱼邮件的上述特点，有利于邮件服务器进行钓鱼邮件的自动识别、筛选，提高网站的安全性。

4. 结束语

总之，电子邮件在给人们的工作、生活等方方面面带来极大方便的同时，也带来了多种安全风险。为此，一方面，需要网络用户学习掌握钓鱼邮件特征，及时识别钓鱼邮件，避免上当受骗；另一方面，需要对钓鱼邮件的实施方法和相关特征进行跟踪研究，进而给出自动筛选钓鱼邮件的新规则，并研究提出相关技术方法，以便有效防范网络钓鱼攻击，确保网络用户的上网安全。

参考文献 (References)

[1] Barraclough, P.A. (2013) Intelligent Phishing Detection and Protection Scheme for Online Transactions. *Expert Systems with Applications*, **40**, 4697-4706.

[2] 钓鱼网站[EB/OL]. http://baike.baidu.com/, 2016-12.

[3] 彭富明. 基于文本特征分析的钓鱼邮件检测[J]. 南京邮电大学学报(自然科学版), 2012(5): 140-145.

[4] 李玉峰. 中文垃圾邮件过滤邮件服务器的实现[J]. 微计算机信息, 2012(3): 176-178.

[5] 张玉清, 等. 在线社交网络中异常帐号检测方法研究[J]. 计算机学报, 2015(10): 2011-2027.