科技期刊钓鱼网站常用技术手段分析及防范措施

■胡国强[1)]　杨彦荣[1)]　马秋明[2)]

收稿日期:2018-05-18
修回日期:2018-08-02

1)西北农林科技大学网络与教育技术中心,陕西省咸阳市杨凌区邰城路 3 号　712100
2)《西北农林科技大学学报(自然科学版)》编辑部,陕西省咸阳市杨凌区邰城路 3 号　712100

摘　要　**【目的】**分析科技期刊钓鱼网站常用技术手段,并提出防范措施。**【方法】**总结科技期刊钓鱼网站屡禁不止的原因,分析钓鱼网站常用的技术手段,从科技期刊、作者、政府相关部门、互联网企业等方面提出防范科技期刊钓鱼网站的具体措施。**【结果】**假冒科技期刊官方网站网址和利用漏洞攻击科技期刊官方网站是科技期刊钓鱼网站常用技术手段。为了遏制钓鱼网站的不法行为,科技期刊编辑部需重视网络安全建设,并努力提升官方网站的可见度;作者应提高防范意识;政府相关部门需提高监管水平;互联网企业应加大防范力度。**【结论】**只要科技期刊、作者、政府相关部门、互联网企业等多方共同采取切实有效的防范措施,定会让钓鱼网站再无可乘之机。

关键词　科技期刊;钓鱼网站;技术手段;防范措施
DOI:10.11946/cjstp.201805180447

随着信息技术在新闻出版领域的广泛应用,大部分科技期刊建立了官方网站。科技期刊网站是期刊宣传自身文化和品牌的重要窗口,也是作者、编辑、审稿专家相互沟通的平台,不仅方便了作者投稿和专家审稿,而且实现了远程采编、在线数字出版、在线办公等功能,极大地提高了编辑的工作效率。网络钓鱼(Phishing)是不法分子利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗的一种犯罪行为,是一直存在的一种网络犯罪手段。科技期刊官方网站在给作者、编辑、读者、审稿专家提供便利的同时,不可避免地受到了网络钓鱼的攻击。科技期刊钓鱼网站是网络钓鱼的形式之一,不法分子利用仿冒期刊网站的统一资源定位符(Uniform Resource Locator,URL)地址以及页面内容,或利用期刊网站服务器程序上的漏洞在站点的某些网页中插入包含危险内容的超文本标记语言(HyperText Markup Language,HTML)代码[1],以此来骗取作者账号信息,更有甚者通过假冒的期刊官方邮件向读者发送“录用通知”,骗取读者高额的版面费。科技期刊钓鱼网站非常多,其疯狂程度令人触目惊心,严重损害了科技期刊和作者的利益。面对层出不穷的科技期刊钓鱼网站,如何利用信息技术保证作者和编辑部的正当权益,维护科技期刊名誉,是值得与此相关的单位和从业人员关注的问题。

目前,已有一些关于防范和打击科技期刊钓鱼网站的研究。例如:汪勤俭等[2-5]对如何防范科技期刊假冒网站进行了讨论,并提出了防范的措施;黄锋等[6]不但提出了具体的防范措施,而且对假冒科技期刊网站的打击策略进行了研究;马爱芳等[7]探究了中文科技期刊非法网站现状,给出了非法期刊网站的防范对策;钮效鹃[8]对学术期刊假冒网站进行了深入调查,认为此现象与百度等搜索引擎的社会责任缺失有着密不可分的关系,并探析了搜索引擎的社会责任。上述研究虽从不同角度对科技期刊钓鱼网站问题进行了讨论,但缺乏对钓鱼网站或假冒网站核心技术的研究,缺乏从技术角度的防范措施。本研究对科技期刊钓鱼网站屡禁不止的原因进行了总结,并分析了其常用的技术手段,然后从科技期刊、作者、网络监控部门、互联网企业等方面给出了具体的防范措施,旨在为打击科技期刊钓鱼网站提供参考。

1　科技期刊钓鱼网站屡禁不止的原因

目前,相关部门和从业人员已经对科技期刊钓鱼网站进行了严厉的打击,但这颗危害科研成果发表的毒瘤却屡禁不止,其原因主要表现在以下几方面。

作者简介:胡国强(ORCID:0000-0002-9638-2466),硕士,高级工程师,E-mail:hgq@nwsuaf.edu.cn;杨彦荣,硕士,工程师。
通信作者:马秋明(ORCID:0000-0002-8776-4024),硕士,副编审,E-mail:maqm87092511@163.com。

1.1 科技论文发表供需不平衡为不法分子提供了可乘之机

目前,我国各科教单位对在职人员的考评制度和研究生培养制度均要求发表科技论文,导致在科技期刊上发表学术论文的需求一直很旺盛,而我国科技期刊,特别是高层次的科技期刊数量又相对较少,致使学术论文发表供需严重不平衡,作者在高层次科技期刊发表学术论文较难。这种现状为钓鱼者提供了可乘之机,不法分子利用作者想发论文的心理,通过盗用科技期刊官方网站信息、在期刊官方网站插入包含危险内容的 HTML 代码、仿冒官方网站页面风格、设置跟官方网站相同的栏目等手段对作者进行诈骗,牟取暴利[6]。

1.2 网络监管不到位

网络作为新时代的产物,发展十分迅速。在此过程中政府给予了高度重视,但由于网络监管工作的特殊性及监管主体的复杂性,目前监管中仍存在思想认识不足和管理手段欠缺等问题,导致我国网络监管立法滞后、相关法律法规的效力有限和可操作性较弱、监管技术落后、监管政策失衡等。以上诸多因素导致科技期刊钓鱼网站猖獗,破坏了网络通信环境和谐,严重损害了科技期刊的公信力和作者的切身利益。

1.3 作者的安全意识和法律意识薄弱

通过对周围受骗作者的调查发现,受骗对象大多数是初次投稿、没有投稿经验、缺乏安全意识的研究生作者。作者之所以上当受骗,主要原因是对科技期刊钓鱼网站防范意识太薄弱,直接百度查找期刊网站投稿,缺乏对科技期刊钓鱼网站的甄别能力和应对钓鱼者发起网络攻击的能力。受骗后,大部分作者由于法律意识薄弱,抱着息事宁人的态度而不愿意利用法律维护自己的权益,这反而助长了钓鱼者的气焰,导致科技期刊钓鱼网站越禁越多。

1.4 科技期刊编辑部对网络安全的重视程度不够

科技期刊编辑部对网络空间安全缺乏深度认识,重视程度不够,导致科技期刊官方网站从一开始制作时就未将网络安全放在首位。再者,科技期刊编辑人员受专业限制,缺乏网络安全知识。在此背景下,开发的官方网站和投稿系统本身就存在安全隐患,容易被钓鱼者攻击。为了避免上述情况,许多科技期刊委托其他专业公司(如北京勤云科技发展有限公司)为自己提供投稿平台,如此以来官方网站和投稿系统的安全性就有了一定的保障。但由于编辑部缺乏网络安全人才,官方网站和投稿系统的日常安全维护跟不上,导致官方网站和投稿系统没人管理,这就加大了钓鱼者入侵的风险。

2 科技期刊钓鱼网站常用的技术手段

分析科技期刊钓鱼网站常用的技术手段有助于各方对之加以甄别和防范。通过对一些钓鱼网站的分析,笔者发现科技期刊钓鱼网站所用的技术手段主要有以下几种。

2.1 假冒科技期刊官方网站网址

由于科技期刊钓鱼网站的主要目的是通过假冒科技期刊官方网站,欺骗作者向其钓鱼在线投稿系统、邮箱投稿,通过收取巨额版面费或骗取作者稿件等手段牟利,所以钓鱼者经常使用各种手段伪造科技期刊官方网站 URL,将作者引导至钓鱼网站。这种技术手段主要有以下几种表现形式。

2.1.1 虚假 URL

作者投稿时,鉴别投稿网站的常用方法是检查浏览器地址栏中显示的 URL 地址。钓鱼者为了达到欺骗作者的目的,一般会注册一个跟期刊官方网站很相似的域名。由于大多数浏览器以无衬线字体显示 URL ,因此钓鱼者往往使用相似字符或特殊字符来迷惑作者。比如,浏览器域名显示栏里小写“l”和大写“I”很难被区分,所以钓鱼者就用Iibedit.cn伪造 libedit.cn。还有的钓鱼者将申请域名的一部分插入其中,冒充官方网站真实域名。例如用 libedit-XXXXXXX.cn 冒充 libedit.cn。

2.1.2 URL 隐藏

假冒 URL 的另一种方法利用了 URL 语法中一种较少用到的特性[9]。超文本传输协议(Hyper Text Transfer Protocol,HTTP)规定的 URL 完整格式是“http://username:password@ IP 地址或主机名”,其中 IP 地址或主机名为平时使用的 URL 地址,而 URL 真正起解析作用的网址是从@ 后面开始的。钓鱼者利用这一原理,用“正规期刊网址@ 钓鱼网站网址”的形式欺骗作者。

2.1.3 利用 URL 编码原理伪装 URL

不法分子为了提高钓鱼网站与科技期刊官方网站域名的相似度来更好地迷惑作者,还会利用 URL 编码原理来仿冒真实 URL。例如,钓鱼者仿冒 http://www.xnxbz.net(《西北农林科技大学学报(自然科学版)》的域名)的操作为:先申请 de.cn 域名,然后构造一个 http://www.xnxbz.net.de.cn 子域名,

最后通过 URL 编码技术得到 URL“http://www.xnxbz.net%2e%64%65%%2e63%6e”,利用此伪装 URL 吸引作者访问钓鱼网站。

2.1.4 利用 IP 地址直接指向钓鱼网站

钓鱼者要想达到欺骗作者的目的,就要想方设法把作者引向钓鱼网站。为了掩人耳目,最常用的技术手段就是用 IP 地址直接访问,而不用域名。普通作者很少去核实 IP 地址的具体消息,这就给了钓鱼者可乘之机。比如,钓鱼者可以先做好一个假冒网站,然后将 http://61.150.47.X 这个地址和冒充期刊的信息发布出去,让作者以为此 IP 地址就是想要访问期刊的真实地址,从而引诱作者通过此 IP 地址访问钓鱼网站。

2.1.5 欺骗性超链接

超链接是超级链接的简称,根据使用对象可划分为文本超链接、图像超链接、E-mail 链接、锚点链接、多媒体文件链接、空链接等,超链接的标题可独立于它指向的 URL[9]。钓鱼者利用超链接的这个特性,构建欺骗性超链接来迷惑作者,比如:钓鱼者可在链接标题中显示 http://www.xnxbz.net,然后将指向 URL 改成 http://www.xnxbz.net.de.cn,利用欺骗性超链接误导作者访问这个钓鱼网站。

2.2 利用漏洞攻击科技期刊官方网站

漏洞也称为脆弱性(Vulnerability),是硬件、软件和协议的具体实现或系统安全策略上存在的缺陷[10]。黑客或钓鱼者往往利用 Web 漏洞、浏览器漏洞和服务器漏洞对科技期刊官方网站发起攻击,对期刊主页和投稿信息进行篡改,从而达到欺骗作者的目的。

2.2.1 Web 漏洞

Web 漏洞通常是指网站程序上的漏洞,目前最常见的 Web 漏洞有结构化查询语言(Structured Query Language,SQL)注入、跨站脚本攻击(Cross Site Scripting,XSS)、跨目录访问、缓冲区溢出、cookies 修改、HTTP 方法篡改、跨站请求伪造(Cross-Site Request Forgery,CSRF)、回车换行(Carriage-Return Line-Feed,CRLF)注入等。根据安全研究组织开放式 Web 应用程序安全项目(Open Web Application Security Project,OWASP)的统计,XSS 漏洞和注入漏洞(Injection Flaws)(SQL 注入漏洞中最主要的一种)的数量高居榜首。XSS 漏洞的特性就是能够在远程 Web 网页中插入恶意目的网络脚本语言(JavaScript),达到跨域名、跨页面修改网页任意内容的目的[11]。当用户使用浏览器下载这一页面时,嵌在其中的恶意脚本就被执行。Injection Flaws 是通过把 SQL 命令插入到 Web 表单提交、输入域名和页面请求的查询字符串中,最终实现欺骗服务器执行恶意的 SQL 命令[12]。钓鱼者往往利用这两种技术手段,先修改某些科技期刊服务器的数据库或官方网站内容,然后通过官方网站邮箱或官方网站投稿系统给作者发送虚假录用信息,引诱作者向虚假账号汇款,以牟取非法利益。

2.2.2 浏览器漏洞

目前,常用的 Web 浏览器有微软公司的 Internet Explorer 浏览器、网景公司的 Netscape Navigator 浏览器、开放源代码的网页浏览器 Firefox、Opera Software ASA 公司的浏览器 Opera、Sun 公司推出的 HotJava 浏览器等。根据“常见漏洞及风险”(Common Vulnerabilities & Exposures,CVE)组织的公报,浏览器的总漏洞超过 300 个,每个浏览器厂商的产品都有几十个漏洞[13],几乎所有的浏览器都存在漏洞。钓鱼者或黑客利用浏览器漏洞,生成一个科技期刊钓鱼网页,作者有意或无意访问该网页时,特洛伊木马或者其他类型的间谍软件会在作者毫无察觉的情况下安装在作者的电脑中,以窃取作者信息[14]。目前,对浏览器构成潜在威胁的因素主要有浏览器劫持(Browser Hijack)、恶意脚本、非法 ActiveX 控件、恶意 Java 小程序等。以浏览器劫持为例,其通过 BHO、DLL 插件、Hook 技术、Winsock LSP 等载体[8]对作者的浏览器进行攻击,进而直接控制作者浏览器,或者使作者浏览器强行访问某个钓鱼网站,危及作者浏览器安全。

2.2.3 服务器漏洞

服务器最常见的漏洞是邮件身份伪造漏洞,此漏洞只需修改邮件发送的“From”头区域字段,就可以利用匿名邮件伪造任何人的身份发送邮件。钓鱼者经常利用此漏洞冒充期刊电子邮件给作者发送匿名邮件,甚至架设专门制作伪造邮件的网站,不间断地给作者发送各种匿名邮件。虽然大部分邮件服务商对这类匿名邮件提供的反欺诈保护和邮件过滤手段均能检测到“From”区域的伪造内容,但这些检测手段也并不安全,大量恶意软件、钓鱼链接和勒索病毒利用电子邮件进行传播扩散[15]。2017 年 12 月,德国安全研究员 Sabri Haddouche 发现 30 多种邮件客户端中存在漏洞,可以让任意用户伪造身份发送欺诈邮件并绕过反欺诈保护机制(如 DMARC 等)和

多种垃圾邮件过滤器,Sabri Haddouche 把这些邮件客户端漏洞集统称为 MailSploit,目前它主要影响 Apple Mail(mac OS、iOS 和 watch OS)、Mozilla Thunderbird、部分 Microsoft 客户端、Yahoo Mail、ProtonMail 等。

3 具体防范措施

科技期刊钓鱼网站猖獗,扰乱了科研学术风气,损害了期刊和作者利益。因此,打击科技期刊钓鱼网站势在必行。笔者认为,科技期刊、作者、政府相关部门、互联网企业等多方共同采取防范措施,以遏制科技期刊钓鱼网站的不法行为。

3.1 科技期刊应加强网络安全建设

作者之所以会误入科技期刊钓鱼网站,一个重要的原因是不容易找到期刊官方网站。科技期刊作为钓鱼网站侵害的主体,应主动作为,利用自己的资源,采取多种途径提高官方网站网址、邮箱和编辑部电话的可见度。如汪勤俭等[2]建议,科技期刊可在每篇论文中标注网址、在中国知网等数据库期刊信息中标注期刊网址,加大宣传力度,扩大期刊及其网站的知名度;在期刊官方网站的显著位置刊登反钓鱼网站声明等;还可以利用微信平台扩大网站网址可见度。另外,对于那些尚未建立官方网站的科技期刊,应尽快建立自己的官方网站,不要让假冒期刊的钓鱼网站再危害作者,损坏期刊和作者的合法权益。科技期刊应动员作者、读者和编辑积极参与钓鱼网站的打击活动,一旦发现有假冒自己期刊的钓鱼网站应立刻向中国互联网违法和不良信息举报中心(http://www.12377.cn/)、网络违法犯罪举报网站(http://www.cyberpolice.cn/wfjb/)、中国反钓鱼网站联盟(http://www.apac.cn/)等机构举报,切实维护自身合法权益。

习近平总书记指出,网络安全是事业发展的前提。科技期刊编辑部应充分重视科技期刊网络安全,在投稿平台选择或建设时应将系统安全作为第一选择因素。科技期刊编辑部应安排有网络安全知识的编辑或聘请相关的网络安全工程师定期对投稿平台进行维护,以保障投稿平台安全;应定期对编辑开展网络安全培训,培养编辑的网络安全意识,筑牢网络安全防线,从根本上抵御钓鱼攻击。科技期刊编辑部还可以向搜索引擎运营商申请官方网站认证,以便作者查询。

3.2 作者应增强安全防范意识

作者通过网络进行投稿时,应增强安全防范意识。首先,应确保自己使用计算机的安全,在计算机上一定要安装防火墙和杀毒软件,并实时更新,启用防火墙的自动拦截功能,自动过滤网络钓鱼网站;设置系统登录口令,尽可能使用复杂密码;及时更新系统补丁和应用程序,并留意网络中的陷阱。其次,应保证自己电子邮箱的安全性,避免在网吧、游戏厅等安全性不确定的计算机中登录自己的电子邮箱;不要随意点击浏览器中的陌生链接,关闭电子邮件客户端的自动脚本功能。再次,作者要养成良好的投稿习惯,当首次向自己不熟悉的期刊投稿时,一定要采用多种途径核实通过搜索引擎获得的投稿网站、邮箱的真实性。最后,作者应该明白,大多数正规科技期刊的审稿周期为 1~2 月,且收款账户名多是单位名称,若投稿后 3~5 天就收到要求向私人账户汇版面费的“录用通知”,则应对该“录用通知”的真实性进行核查,切不可被突如其来的“好事”所蒙蔽而上当受骗。

3.3 政府相关部门应齐抓共管

目前,科技期刊钓鱼网站泛滥跟监管部门监控不严有很大关系。笔者认为,应加大监管力度,制定严格的法规,从严处理钓鱼者的犯罪行为,发动作者、期刊编辑和科技期刊网站承包企业监督举报,共同保障互联网的网络空间安全。监管部门应依靠先进的信息技术对科技期刊官方网站进行科学监管。例如,张义等[3]提出在.cn 域名下设置新闻出版广电领域统一的二级域名,即在国家顶级域名下设置出版传媒领域专属的二级类别域名,以方便作者鉴别。教育部和科技部可联合建立专门的科技期刊查询网站,并将其大力宣传、推广到各科教单位和研究生培养单位,为作者提供一个获取科技期刊正确信息的官方平台。

3.4 互联网企业应切实担当起自己应尽的社会责任

2016 年 4 月 9 日,习近平总书记在《在网络安全和信息化工作座谈会上的讲话》中明确指出,互联网企业不应只以赚钱为目的,还应承担相应的社会责任,坚持经济效益和社会效益的统一;互联网企业应积极参与网络钓鱼网站的防范,鼓励反网络钓鱼技术的研发与成果转换,并进行技术推广。目前,国内许多学者针对钓鱼网站监测和识别技术进行了研究,并取得了一定成果。钓鱼网站检测技术主要有改进的 TrustRank 算法[16]、特征选择与集成学习[17]、模糊关联分类[18]、敏感特征[19]、基于贝叶斯[20]和支持向量机启发式[21]、深度学习[22]等。钓

鱼网站识别技术主要有基于 URL 文本特征及链接关系[23]、融合多源网络评估数据及 URL 特征[24]等。互联网企业应加大科技成果转换与推广力度,尽快将以上技术应用于实际,为净化网络空间贡献自己的力量。科技期刊网站平台承包商作为互联网企业的一分子,在开发投稿平台时,应尽量采用新技术,以减少投稿平台漏洞;投稿平台建立好后,平台服务商应定期对其进行漏洞扫描,防患于未然。

4 总结

打击科技期刊钓鱼网站刻不容缓,本研究先分析了科技期刊钓鱼网站屡禁不止的原因,然后研究了其常用的技术手段,最后从科技期刊、作者、政府相关部门和互联网企业的角度分别给出了具体防范策略。本研究仅对当前钓鱼者常用的技术手段进行了分析,随着信息技术的发展,钓鱼者是否会利用其他技术手段进行犯罪活动值得跟踪研究。比如,现在不少科技期刊建立了自己的作者 QQ 群、微信群和微信公众号,钓鱼者是否会通过攻击这些即时通讯软件而对作者进行诈骗,这应该引起高度关注。打击科技论文发表过程中的钓鱼犯罪行为任重而道远,不可能一蹴而就,但笔者相信,只要科技期刊编辑部重视网络安全并努力提升官方网站的可见度、作者提高防范意识、政府相关部门提高监管水平、互联网企业加大防范技术投入,定会让钓鱼网站再无可乘之机。

参考文献

[1] 网络商城安全解决方案行业标准建议[EB/OL]. (2016-08-15)[2018-04-05]. https://wenku.baidu.com/view/9daed4d2dd36a32d72758101.html.
[2] 汪勤俭,冷怀明,吴培红,等. 关于科技期刊防范假冒网站的思考[J]. 编辑学报,2016,28(2):167-169.
[3] 张义,陈怡平. 科技期刊假冒网站应对措施[J]. 科技与出版,2016(7):35-38.
[4] 王艳军. 学术期刊面对期刊假冒网站侵权的四大举措[J]. 科技与出版,2016(8):118-121.
[5] 黄仲一,郭雨梅,朱雪莲. 科技期刊假冒网站问题分析及应对策略[J]. 编辑学报,2016,28(1):50-52.
[6] 黄锋,黄雅意,辛亮. 科技期刊假冒网站的防范和打击策略研究[J]. 中国科技期刊研究,2016,27(7):739-743.
[7] 马爱芳,王宝英. 中文科技期刊非法网站现状及其对策研究[J]. 中国科技期刊研究,2016,27(4):401-408.
[8] 钮效鹍. 学术期刊假冒网站调查——兼谈百度等搜索引擎的社会责任[J]. 出版发行研究,2016(8):36-38.
[9] 邱远兴. 浅谈钓鱼攻击的技术及对策[J]. 网络与信息,2011,25(12):56-57.
[10] 徐玲. WebFuzz 的 Web 软件漏洞测试[J]. 软件导刊(教育技术),2012,11(8):84-85.
[11] 司响,杜彦辉,李秋锐. 网络钓鱼常用技术手段分析及防范措施[J]. 信息网络安全,2010(6):15-18.
[12] 龚少卿. 浅谈 SQL Server 2000 的入侵和安全管理策略[J]. 科协论坛,2011(2):36-37.
[13] 北斗教育. Web 浏览器漏洞被一览无遗?[EB/OL]. [2018-07-28]. http://22336757.blog.hexun.com/89618330_d.html.
[14] 宋建栋. Web 浏览器安全防御系统设计及实现[D]. 上海:上海交通大学,2008.
[15] MailSploit:30 多种邮件客户端存在电邮身份伪造漏洞[EB/OL]. [2018-04-09]. http://www.freebuf.com/news/156501.html.
[16] 韩浩,刘博文,林果园. 基于改进的 TrustRank 算法的钓鱼网站检测[J]. 电信科学,2018,34(3):86-94.
[17] 周传华,柳智才,丁敬安,等. 基于特征选择与集成学习的钓鱼网站检测方法[J]. 计算机应用研究,2019(4):1-7.
[18] 傅成乐. 基于模糊关联分类的钓鱼网站检测方法研究[D]. 大连:东北师范大学,2016.
[19] 宋明秋,曹晓芸. 基于敏感特征的网络钓鱼网站检测方法[J]. 大连理工大学学报,2013,53(6):903-907.
[20] 顾晓清,王洪元,倪彤光,等. 基于贝叶斯和支持向量机的钓鱼网站检测方法[J]. 计算机工程与应用,2015,51(4):87-90.
[21] 张昭. 基于启发式的钓鱼网站检测技术的研究与实现[D]. 哈尔滨:哈尔滨工业大学,2017.
[22] 许珑于. 基于深度学习的钓鱼网站检测技术的研究[D]. 成都:电子科技大学,2017.
[23] 赵蹲宇,张兆心. 基于 URL 文本特征及链接关系的钓鱼网站识别算法[J]. 高技术通讯,2017,27(8):708-717.
[24] 胡忠义,王超群,吴江. 融合多源网络评估数据及 URL 特征的钓鱼网站识别技术研究[J]. 数据分析与知识发现,2017(6):47-55.

作者贡献声明:

胡国强:确定论文选题,构思论文,撰写并修订论文;
杨彦荣:修改论文;
马秋明:确定论文选题,构思论文,撰写和修订论文。

Analysis on technological means frequently used by phishing websites of scientific journals and the corresponding preventive measures

HU Guoqiang[1)], **YANG Yanrong**[1)], **MA Qiuming**[2)]

1) Network & Education Technology Center, Northwest A&F University, 3 Taicheng Road, Yangling District, Xianyang 712100, China
2) Editorial Office of *Journal of Northwest A&F University* (*Natural Science Edition*), 3 Taicheng Road, Yangling District, Xianyang 712100, China

Abstract: [**Purposes**] This paper aims to analyze the technological means frequently used by phishing websites of scientific journals, and propose the preventive measures for the phishing websites. [**Methods**] We summarized the reasons for the repeated emergence of phishing websites of scientific journals, analyzed the frequently-used technical means of phishing websites, and proposed the specific measures to prevent phishing websites from scientific journals, authors, relevant government departments, and internet companies. [**Findings**] Passing off the official websites of scientific journals and attacking the official websites of scientific journals by use of loophole are two technological means frequently used by phishing websites of scientific journals. Therefore, in order to curb the illegal behaviors of phishing websites, the editorial office of scientific journals should attach great importance to the construction of network security, and strive to improve the visibility of websites. Besides, the authors should raise awareness of prevention, and relevant government departments should uplift the level of supervision. Furthermore, internet companies should increase their prevention efforts as well. [**Conclusions**] As long as effective preventive measures are taken jointly by scientific journals, authors, relevant government departments, and internet companies, there will be no chance left for phishing websites.
Keywords: Scientific journal; Phishing website; Technological means; Preventive measure

(本文责编:刘晶晶)