Advances in Psychology 心理学进展, 2021, 11(4), 968-977
Published Online April 2021 in Hans. http://www.hanspub.org/journal/ap
https://doi.org/10.12677/ap.2021.114109

Hans汉斯

网络钓鱼的影响因素：心理学的视角

葛　燕[1,2]，崔馨月[1,2]，瞿炜娜[1,2]

[1]中国科学院行为科学重点实验室(中国科学院心理研究所)，北京
[2]中国科学院大学心理系，北京
Email: quwn@psych.ac.cn

收稿日期：2021年3月26日；录用日期：2021年4月16日；发布日期：2021年4月25日

摘　要

网络钓鱼是指通过计算机技术并利用人类心理弱点对终端用户进行攻击的行为，研究网络钓鱼的影响因素可以提高网络安全水平，降低网络钓鱼伤害。本文以心理学的视角，从个体、情境和系统三个方面对网络钓鱼的影响因素进行梳理总结，并探讨了各影响因素联结的动态过程。在个体因素方面，先天特质会影响网络钓鱼易感性，但后天学习和积累的知识经验能降低被钓鱼的风险；在情境方面，身份伪装和特殊情境设定能够利用用户的心理弱点，直接影响用户回复钓鱼邮件的行为；在系统方面，系统反馈影响人对系统安全的信任，进而影响网络钓鱼风险。未来的研究可从三个方面展开：一是探讨和细化个人特质对整体网络钓鱼易感性的综合影响，建立易感者模型；二是量化邮件特征在用户动态决策过程的作用；三是结合个体特质、情境因素和系统特征，建立基于三者结合关系模型的防护体系。

关键词

网络钓鱼，人格特质，情境因素，系统特征

Influencing Factors of Phishing: A Psychological Perspective

Yan Ge[1,2], Xinyue Cui[1,2], Weina Qu[1,2]

[1]Key Laboratory of Behavioral Science, Institute of Psychology, Chinese Academy of Sciences, Beijing
[2]Deptmentof Psychology, University of Chinese Academy of Sciences, Beijing
Email: quwn@psych.ac.cn

Received: Mar. 26th, 2021; accepted: Apr. 16th, 2021; published: Apr. 25th, 2021

Abstract

Phishing refers to the behavior of attacking end-users through computer technology and taking

文章引用: 葛燕, 崔馨月, 瞿炜娜(2021). 网络钓鱼的影响因素: 心理学的视角. *心理学进展, 11(4),* 968-977.
DOI: 10.12677/ap.2021.114109

advantage of human psychological weaknesses. Investigating what shapes phishing susceptibility can improve the level of network security and reduce the damage of phishing. From the perspective of psychology, this paper summarized the influential factors of phishing from three levels: the individual level, the email level and the system level. Meanwhile the dynamic processes of the link of those factors are also explored. At the individual level, people with high score in some specific individual are easier to be attached by phishing, but acquired knowledge and accumulated experience can reduce the risk of getting phished. At the email level, identity camouflage and context setting can make use of users' psychological weaknesses, and thus directly affect the possibility to respond to phishing email. At the system level, system features affect users' trust in automation security and reliability, which in turn affects phishing risk. Future research could be focused on three aspects: first, to refine the comprehensive influence of different personalities on overall phishing susceptibility and to establish the susceptibility model; second, to qualify the influence of email characteristics on users' the dynamic decision-making process; third, to establish a protective system based on the comprehensive impact of individual traits, email characteristics and system features.

Keywords

Phishing, Personality Traits, Email Characteristics, System Features

1. 引言

网络钓鱼(phishing)是指利用计算机技术和人的心理弱点针对用户私密信息和金融账号进行盗取的犯罪行为(Aaron, 2019)。“phishing”在1996年首度被使用，它是“fishing”和“homophone”的结合体，因为最初攻击者是通过电话作案，所以用“Ph”取代“F”，意为放线“钓”到目标信息。随着互联网发展，网络钓鱼攻击手段日益丰富，由最初引诱用户输入密码转变为多种形式，如勒索软件、Java 静默窃取等。传播途径也逐渐多样可通过搜索引擎、邮件、短信等方式传播(顾威，2017)，但是邮件攻击依然是目前的主要攻击方式和载体(杨明，2012)。网络钓鱼的研究得到了世界范围内研究者广泛关注，但是大多数研究围绕不断发展的技术因素展开，而忽视了处于核心地位的被攻击者的心理因素。因此，本文从心理学视角出发，以邮件钓鱼作为切入点，从个体、情境和系统三个方面论述网络钓鱼的影响因素，并对未来研究发展趋势加以展望，希望为后续研究提供方向并为改善网络安全提出建议。

2. 网络钓鱼的影响因素

从人的角度看，网络钓鱼影响因素主要包括三个方面：一是什么样的人容易被钓鱼？也就是说受害者具有什么样的特征，这方面主要涉及人本身的个性特征和知识经验等。二是什么样的邮件容易钓鱼？也就是邮件的情境特征如何影响了人对邮件的判断，这主要涉及人的信息加工过程。三是什么样的系统可以降低钓鱼伤害？也就是什么样的系统可以帮助人们更好地识别钓鱼邮件，这方面涉及人机协作问题。因此，我们将从个体、情境和系统三个方面对网络钓鱼的影响因素分别进行阐述。

2.1. 个体因素

早期钓鱼研究表明在面临网络欺诈时，一些用户会更容易泄露信息并且反复上当，所以学者们探讨

是否存在“受害者人格”。研究中涉及的个体差异因素包括：人格(Halevi, Lewis, & Memon, 2013)、知识经验(Downs, Holbrook, & Cranor, 2007)、信任倾向(Alseadoon, Othman, & Chan, 2015)、风险倾向(Moody, Galletta, & Dunn, 2017)和风险感知(Wright, Chakraborty, Basoglu, & Marett, 2010)、认知加工方式(Vishwanath, 2015)等。

2.1.1. 人格

大五人格是网络钓鱼研究中常用的人格特征，五大因素与网络钓鱼风险存在不同程度的相关。宜人性和开放性可以正向预测用户的钓鱼易感性。宜人性得分高的被试有更多的网络被骗经历，辨别钓鱼邮件的能力更差(Modic & Lea, 2011)。开放性得分高的被试会花费更多时间来回复钓鱼邮件(Alseadoon et al., 2015)，开放性较高的女性被试更多地点击钓鱼邮件链接，但在男性被试身上未发现相关结果(Halevi et al., 2013)。而外倾性、责任心和神经质在预测网络钓鱼易感性上存在不一致的结果。外倾性得分高的被试在社交媒体中更多地发布帖子和更新照片(Halevi et al., 2013)，更多地回复钓鱼邮件(Alseadoon et al., 2015)，但是却报告了更少的受骗经历(Modic & Lea, 2011)。责任心和神经质得分高的被试在邮件分类任务中表现更好(Welk et al., 2015)，但他们也会更多地点击钓鱼邮件。Weirich 等人(2001)认为责任心高的个体会服从权威遵守规则，降低回复不合理要求的可能。同时，责任心高的个体会反复检查邮件，查阅频率的增加会提高点击钓鱼链接的概率(Vishwanath, 2015)，情绪不稳定性的个体由于较冲动而导致识别钓鱼邮件的能力较差(Weirich & Sasse, 2001)。人格特质对于用户甄别钓鱼邮件能力的影响可能与用户的知识经验或其他环境因素存在交互作用，因此，研究者也针对这些因素展开了研究。

2.1.2. 知识经验

网络钓鱼研究中涉及到的知识经验包括：计算机技术知识、网络安全知识、网络经验、网络欺诈知识和经验等。Downs 等人(2007)发现知道网络钓鱼定义的被试网络钓鱼风险显著降低，他们更少点击钓鱼链接，进入钓鱼网站或输入私密信息。在另一个研究中，研究者向被试发送钓鱼邮件，邮件知识经验丰富的被试更少回复钓鱼邮件，作者认为邮件知识经验会帮助用户调整区分合法邮件和钓鱼邮件的标准，让用户观察到邮件中矛盾线索从而降低网络钓鱼风险(Alseadoon et al., 2015)。Vishwanath 等人(2015)发现知识经验还会影响对邮件内容的注意和评估，进而影响被试的决策。现实生活中，很多受害者因为安全意识低，不了解网络欺诈而落入陷阱。知识经验会帮助用户理解安全警告进而更好的规避潜在风险，因此增加知识经验可以作为降低网络钓鱼风险的重要干预手段。

2.1.3. 信任

在电子商务的情境中，信任倾向是指基于他人行为所感受到的信心与保证，愿意接受可能受到伤害的一种心理状态(Gefen, Karahanna, & Straub, 2003)。容易相信他人的个体面临更大的攻击风险，这点在许多研究中得到证实(Wang, Herath, Chen, Vishwanath, & Rao, 2012)。Welk 等人(2015)研究结果表明容易相信他人所说的话并认为他人是好的意图的被试总体分类精度更低，更难分辨出钓鱼邮件。但是，信任对网络钓鱼风险的影响会受到其他条件的影响，例如知识经验和邮件本身的可信程度等。

2.1.4. 风险感知

风险感知是个体对于外界各种客观风险的感受和认识,并强调由于对风险的直观判断和主观感受可能引发相应的风险决策行为。Moody 等人(2017)发现对于财务安全更加谨慎的被试更少点击钓鱼链接，认为网络安全风险较小的被试回复钓鱼邮件的概率更高。Wright 等人(2014)测量了风险感知对欺诈检测行为的影响，但没有发现风险感知与欺诈检测行为的相关关系，作者认为可能由于量表条目太少或者对网络欺诈的风险感知受到其他变量，例如知识经验的影响。

2.1.5. 认知加工方式

在认知加工方式理论中，系统启发式模型(Heuristic-Systematic Model，简称 HSM)将认知加工方式分为系统式和启发式。系统式加工是通过详细审查信息论据和线索，评估信息质量做出决定的方式；启发式加工则是以简单线索作为参考，没有进行大量逻辑推理做出决定的方式。启发式受“最小认知努力原则”指导，倾向于减少认知资源投入并缩短决策时间(Griffin, Neuwirth, Giese, & Dunwoody, 2002)。Vishwanath (2015)发现与启发式加工的被试相比，系统式加工的被试更少回复钓鱼邮件。进一步的研究发现系统式加工的被试会更多审查邮件来源的真实性，对比推理邮件信息，进而做出更谨慎的判断(Vishwanath, Harrison, & Ng, 2018)。可见，认知加工方式是影响网络钓鱼风险的重要因素，系统式加工的个体会进行深度加工和根源思考，从而去对比信息中的矛盾，拥有更好的鉴别表现。

综上所述，个体差异是影响网络钓鱼风险的重要因素。知识经验、人格、风险感知、认知加工方式等均已被证明对处理钓鱼信息的行为有影响。值得注意的是，这些因素并非独立地影响网络钓鱼，但目前很少有研究综合考虑因素的交互作用。因此有必要针对各个因素展开系列研究，确定个体特质如何影响用户对邮件的判断，研究成果可用于为不同的人群定制网络使用建议帮助规避安全风险。

2.2. 情境因素

除了个体差异以外，邮件内容和设置也是影响网络钓鱼的重要因素。钓鱼者利用人的心理弱点精心设置一种情境，通过恐吓、恭维、引诱欺骗等手段实施诱骗(吴少华，胡勇，2014)。情境设置操纵的常见方式包括：伪装发件人身份(Jagatic, Johnson, Jakobsson, & Menczer, 2007)、添加收件人相关信息(Flores, Holm, Nohlberg, & Ekstedt, 2014)、设置紧急状况(Vishwanath et al., 2011)等。

2.2.1. 发件人身份伪装

操纵发件人熟悉度体现为伪装成知名企业、朋友、高亮发件人等。Jagatic 等人(2007)发现被试更多点击来自朋友的邮件链接。作者认为被试会更信任熟悉的人发送的邮件，遵从邮件要求落入陷阱。Holm 等人(2014)分别以经理和安全中心的名义提示被试升级软件，结果发现用经理名义发送钓鱼邮件使回复概率增加了 22.1%。但是也有研究发现不一致的结果，Wright 等人(2014)发现来自班主任的和普通的钓鱼邮件成功概率没有显著差别。在防护方面的研究发现提高对发件人的关注也可以降低钓鱼邮件的成功率。Nicholson 等(2017)高亮邮件中发件人姓名、邮箱地址与时间，提示被试邮件的矛盾，结果表明添加高亮的钓鱼邮件成功率更低。可见，发件人身份是影响网络钓鱼的重要因素，但发件人熟悉度、权威性等在钓鱼邮件中的作用有待进一步的研究。

链接形式也是影响钓鱼成功的因素之一。钓鱼邮件中链接包括数字链接(像：103.45.3.79)和文字链接(像：www.Tabao.com)，文字链接比数字链接提供更多信息，增加钓鱼邮件权威，提高成功率。Moody 等人(2017)发现文字链接的钓鱼邮件成功率显著高于数字链接钓鱼邮件的成功率。其他像图标式链接由于看不到具体链接更具有迷惑性，但目前相关研究很少。

2.2.2. 收件人相关信息

添加收件人相关信息表现为直呼收件人姓名、添加收件人公司信息、订单信息、账号信息等。添加收件人相关信息可以提供卷入感，促使被试回应邮件要求。Holm 等人(2014)发现当添加收件人姓名、所在组织名称等相关信息后，用户回复邮件概率增加了 22.1%。Bullee 等人(2017)发现鱼叉式钓鱼(直呼被试姓名)比传统钓鱼邮件(模糊称呼)成功率提高了 1.693 倍。Wright 等人(2014)的研究也发现和没有直呼用户名字的邮件相比，直呼用户名字的钓鱼邮件成功率提高了 2.6 倍，作者认为添加用户名字等信息可以促使用户用类似于启发式的方法快速做出决策。

2.2.3. 诱导因素

犯罪者经常在邮件中添加可诱发情绪反应时的刺激来攻击用户心理弱点(Vishwanath et al., 2011)。设置时间紧迫性和利益诱惑是两种比较常见的方式。

操纵时间紧迫性体现为添加紧急信息，像时间截止信息或紧急线索等。Wright 等人(2014)发现要求立即回应的邮件比控制条件下邮件成功率高 3.19 倍。Wang 等人(2012)认为对紧急线索的注意会影响对邮件的加工，时间紧迫性会给用户压力，使用户转换决策策略，减少深度思考并且产生迎合的需要。时间紧迫线索会激发出强烈的情绪反应，比如恐惧、兴奋等；在时间紧迫的情况下，人们考虑较少的线索从而做出次优决策(Dambacher & Hübner, 2015)。

设置和利益相关的线索会让用户兴奋，吸引用户的注意，影响用户对信息的真实性的判断(Vishwanath et al., 2011)。Goel 等人(2017)向被试发送八种钓鱼邮件，结果显示与志愿者报名和领取杀毒软件相比，被试更多查看点击领取礼品卡和 ipad，学费援助和课程注册邮件。Harrison 等人(2016)发现奖励钓鱼邮件和警告钓鱼邮件成功率没有显著差异，但是错误地认为退款是一个“赚钱机会”的被试网络钓鱼风险更高。

综上所述，情境因素是影响钓鱼邮件成功的重要因素，攻击者通过操纵邮件特征和内容为用户设置心理陷阱攻破人类防火墙，因此有必要结合人的特点以及邮件特征展开系统研究，以达到提高防范钓鱼能力的目的。

2.3. 系统因素

系统特征是影响人机协作的重要因素(Chancey, Bliss, Proaps, & Madhavan, 2015)，现有很多反钓鱼工具帮助降低网络钓鱼风险，但是有人发现这些工具是低效的(Alsharnouby, Alaca, & Chiasson, 2015)，并且用户会忽略警报继续浏览危险网页(Egelman, Cranor, & Hong, 2008)。因此研究者开始思考邮件系统特征对防范网络钓鱼的影响，反钓鱼工具的作用通常与用户对该系统对信任有关。虽然在网络钓鱼领域中系统可靠性相关研究较少，但人机交互相关的文献可作为重要的参考，常见的特征包括：可靠性(Chen, Mishler, Hu, Li, & Proctor, 2018)，反馈(Chen et al., 2018)，系统透明性(Ramesh, Selvakumar, & Venugopal, 2017)等。

2.3.1. 系统可靠性

可靠性是系统在一定时间区间内完成一定功能的能力(Barlow, 1984)，是系统信任形成的基础，可靠性越高用户对系统的信任水平越高(Chavaillaz, Wastell, & Sauer, 2016)。研究发现，当用户发现系统产生显而易见的错误时会降低信任水平(de Vries, Midden, & Bouwhuis, 2003)，这种质疑会影响任务表现(Chancey, Bliss, Yamani, & Handley, 2017)。Hillesheim 和 Rusnock (2016)等人发现可靠性水平越高被试绩效越好。在使用邮件系统时，邮件系统可靠性也会影响用户的回复行为，Chen 等人(2018)发现可靠性越高，被试对邮件系统越信任，感知到邮件系统越可靠，判断正确率也越高。

2.3.2. 系统反馈

用户对系统的信任受到反馈的影响，如反馈准确性和真实性(Sharples et al., 2007; Spain & Bliss, 2008)。在网络钓鱼研究中，在没有反馈时，被试对系统漏报有虚高的遵从率，但提供反馈后遵从率降低，说明反馈有可靠性矫正的作用(Chen et al., 2018)。提供系统反馈后被试会更加信任系统，更多听取系统建议，做出决定的时间更短。

2.3.3. 系统透明度

系统透明度也会影响网络钓鱼风险。研究表明提供系统解释信息可以提高用户对系统的理解程度和信任水平(Ramesh et al., 2017)。Ramesh 等人开发了反钓鱼工具，当用户点击邮件链接时，查找与链接最相似的官方链接，帮助对比确认邮件的准确性。研究结果发现提供邮件系统判断的标准和解释可以帮助

用户理解系统决策，提高对邮件系统的信任水平，减少进入钓鱼网页的概率。Chou 等(2004)开发的反钓鱼插件，在用户浏览钓鱼网站时会显示网站的危险程度和对网站 URL，图片域名等一系列检查结果，帮助用户判断。

综上，系统的可靠性、反馈方式和透明度会影响用户使用系统时的感受和情绪状态，并间接影响对系统决策遵从等行为进而影响对钓鱼邮件鉴别。目前这一领域的相关研究较少，结合个体差异和情境因素的研究将有助于开发反钓鱼辅助系统，改善人与系统协作程度，降低网络钓鱼风险，提高网络安全性。

2.4. 网络钓鱼的心理加工过程模型

除了单方面思考网络钓鱼影响因素之外，各因素之间联结的心理加工过程也是研究者关注的重点。网络钓鱼过程模型是分析用户处理钓鱼邮件动态过程建立的理论模型，其中较有影响力的模型为：Vishwanat 等人的整合信息加工模型(2011)和 Harrison 的个体加工过程模型(Harrison et al., 2016)。

Vishwanath 的整合信息模型如图 1 所示。他们认为邮件负荷、卷入程度、知识经验等个体差异形成处理邮件前的心理倾向，这个倾向会影响对邮件各元素的注意进而影响邮件的分析加工，最终形成回复行为。结果发现，整个模型可以预测 46%的回复行为，卷入程度和邮件负荷会影响对邮件元素的注意力分配，这种注意力分配偏差会影响后续分析加工最终影响网络钓鱼易感性。对紧急线索和标题的注意会增加回复行为，而对邮件来源和拼写语法的注意会减少回复行为，所以个体差异会影响对钓鱼邮件的注意加工进而影响网络钓鱼回复行为。

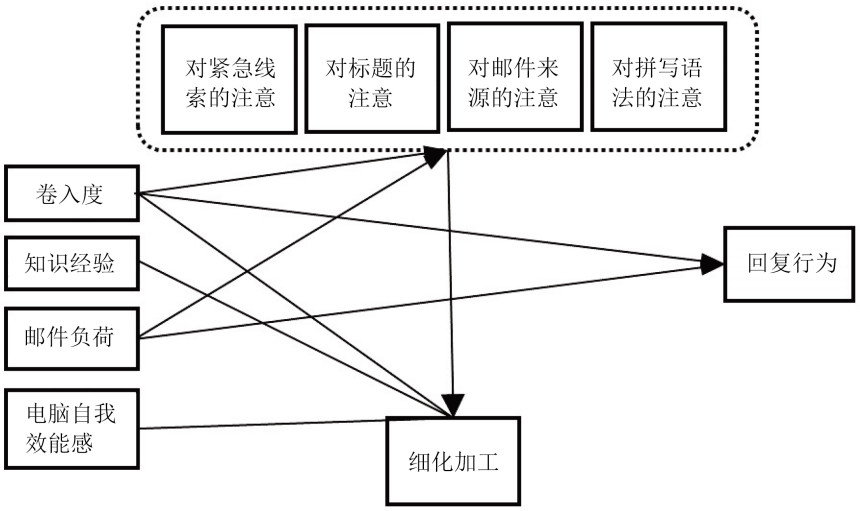

Figure 1. Vishwanath's (2011) integrated information processing model of phishing susceptibility
图 1. Vishwanath (2011)的钓鱼易感性整合信息加工模型

Harrison 等人(2016)认为邮件特征与个体差异会影响用户的认知加工过程进而影响网络钓鱼易感性。其钓鱼邮件个体加工模型如图 2 所示。作者认为邮件说服性信息和邮件拼写错误会影响被试对钓鱼邮件的加工处理，并且邮件知识经验和网络钓鱼知识会形成对邮件加工的图式影响对邮件的注意与评估，最终影响网络钓鱼易感性。研究结果证实了邮件经验和网络知识丰富的被试对邮件注意和加工水平更高，他们会对邮件进行深层次的加工进而降低回复可能；虽然不同说服性线索的邮件回复率没有差异，但是认为“退税是一个赚钱的机会”的被试更多的回复钓鱼邮件。由此可见，个人特质和邮件特征会共同影响网络钓鱼易感性。

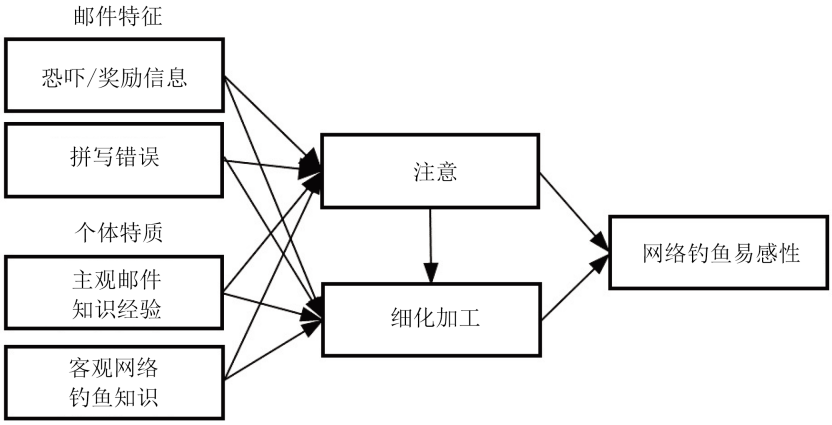

Figure 2. Harrison's (2016) individual processing model of phishing email
图 2. Harrison (2016)的钓鱼邮件个体加工过程模型

上述模型都对处理钓鱼邮件的认知过程提出了各自的假设并且可以部分解释网络钓鱼易感性，但是侧重点不同。其中 Vishwanath 的整合信息加工模型将邮件内容拆解为多个元素，侧重解释对邮件不同元素注意的重要性；而 Harrison 的个体加工过程模型还思考了邮件特征的影响，认为情境因素和个体先验因素会影响认知加工过程进而影响网络钓鱼易感性。但是上述模型没有量化各因素在共同作用中的作用比重，因此无法预测一个因素发生变化时最终网络钓鱼易感性会怎样变化，并无法了解如何调整各因素比重实现有效的干预，所以后续研究量化各因素的作用比重才能实现最终目标。

从网络钓鱼心理加工模型可以看出，个体特质和邮件特征不是单独作用于钓鱼邮件的加工过程，因素间的作用也会影响回复行为。用户的知识经验与卷入程度等心理倾向和邮件特征的外部刺激会共同作用于认知加工过程进而影响决策行为，所以后续干预手段不仅要注重单因素的影响作用，也要注意因素间联结的动态过程。

3. 评价与展望

3.1. 小结

综上所述，网络钓鱼作为一种网络欺诈手段，主要利用人的心理弱点进行诈骗。本文从个体，邮件和系统三个层面总结网络钓鱼影响因素，并探讨多方面因素联结的动态过程。个体差异不仅会直接影响甄别钓鱼邮件的能力，还会间接影响线上行为和行为习惯进而影响网络风险，所以为不同的人群定制网络安全使用建议会更好的帮助用户规避安全风险。攻击者操纵邮件特征激发用户强烈的情绪反应，加速决策过程，诱使用户点击邮件链接，所以帮助熟悉钓鱼邮件特征是提高甄别钓鱼邮件能力的有效方式。系统特征会影响用户对系统的理解程度和信任水平，从而影响用户与系统的协作和网络风险。所以邮件系统需要提高可靠性，提供系统决策解释信息和反馈帮助检测钓鱼邮件。除了单方面因素会影响网络钓鱼易感性，因素间的交互作用也会影响回复行为。个体差异和邮件特征会共同作用于认知加工过程，进而影响最后决策行为，所以后续干预手段不仅要注重单方面影响因素的作用，也要注意因素之间联结的动态过程。

3.2. 展望

关注网络钓鱼最新研究结果及方向，可以看出网络钓鱼具有广阔的研究前景，未来的研究可以从以下几个方面展开：

首先，探讨和细化个人特质对网络钓鱼风险的综合影响。以往研究证明了个人特质会影响网络钓鱼风险，但是研究较少考虑各因素的交互作用。所以后续研究可深入探讨各因素对网络钓鱼风险的具体影响，确定个人特质如何影响用户加工处理钓鱼信息，帮助识别网络钓鱼易感性高的用户进行针对性的培训干预。

其次，量化邮件特征在用户动态决策过程的作用。目前研究证明了邮件的物理属性会直接影响网络钓鱼风险，但是无法了解如何调整邮件特征来实现邮件过滤，所以后续研究可以量化邮件特征的作用比重并探讨邮件特征与个体特质的交互作用，帮助改善钓鱼邮件识别算法，提高钓鱼邮件识别率。

最后，揭示系统特征与个体特质，邮件特征的交互作用，建立三者结合的防御系统。现有研究证明系统特征会影响网络钓鱼风险，但是大多局限于系统层面，没有考虑用户的个体差异和情境因素，后续研究中可考虑三者的交互影响，建立网络钓鱼多维评价指标体系。在此基础上构建反钓鱼防御系统，将有助于帮助用户更有效地抵御钓鱼邮件的攻击。

基金项目

国家重点研发计划项目(2017YFB0802803)支持研究成果。

参考文献

顾威(2017). 防火防盗反钓鱼 2016 年全球网络钓鱼总汇概览. *计算机与网络, 43(Z1),* 78-84.

吴少华, 胡勇(2014).社会工程在 APT 攻击中的应用与防御. *信息安全与通信保密, (10),* 93-95.

杨明, 杜彦辉, 刘晓娟(2012). 网络钓鱼邮件分析系统的设计与实现. *中国人民公安大学学报(自然科学版), 18(2),* 61-65.

Aaron, G. (2019). *Phishing Attack Trends Report-1Q 2019.* https://apwg.org/

Alseadoon, I., Othman, F. I., & Chan, T. Z. (2015). What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails? *Advanced Computer and Communication Engineering Technology, 315,* 949-962. https://doi.org/10.1007/978-3-319-07674-4_89

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why Phishing Still Works: User Strategies for Combating Phishing Attacks. I*nternational Journal of Human-Computer Studies, 82,* 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Barlow, R. E. (1984). Mathematical-Theory of Reliability—A Historical-Perspective. *IEEE Transactions on Reliability, 33,* 16-20. https://doi.org/10.1109/TR.1984.6448269

Bullee, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear Phishing in Organisations Explained. *Information & Computer Security, 25,* 593-613. https://doi.org/10.1108/ICS-03-2017-0009

Chancey, E. T., Bliss, J. P., Proaps, A. B., & Madhavan, P. (2015). The Role of Trust as a Mediator between System Characteristics and Response Behaviors. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 57,* 947-958. https://doi.org/10.1177/0018720815582261

Chancey, E. T., Bliss, J. P., Yamani, Y., & Handley, H. A. H. (2017).Trust and the Compliance-Reliance Paradigm: The Effects of Risk, Error Bias, and Reliability on Trust and Dependence. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 59,* 333-345. https://doi.org/10.1177/0018720816682648

Chavaillaz, A., Wastell, D., & Sauer, J. (2016). System Reliability, Performance and Trust in Adaptable Automation. *Applied Ergonomics, 52,* 333-342. https://doi.org/10.1016/j.apergo.2015.07.012

Chen, J., Mishler, S., Hu, B., Li, N., & Proctor, R. W. (2018). The Description-Experience Gap in the Effect of Warning Reliability on User Trust and Performance in a Phishing-Detection Context. *International Journal of Human-Computer Studies, 119,* 35-47. https://doi.org/10.1016/j.ijhcs.2018.05.010

Chou, N., Ledesma, R., Teraguchi, Y., & Mitchell, J. C. (2004). Client-Side Defense against Web-Based Identity Theft. *Proceedings of the Network and Distributed System Security Symposium (NDSS'04),* San Diego, 1-8.

Dambacher, M., Hübner, R. (2015). Time Pressure Affects the Efficiency of Perceptual Processing in Decisions under Conflict. *Psychological Research, 79,* 83-94. https://doi.org/10.1007/s00426-014-0542-z

de Vries, P., Midden, C., & Bouwhuis, D. (2003). The Effects of Errors on System Trust, Self-Confidence, and the Allocation of Control in Route Planning. *International Journal of Human-Computer Studies, 58,* 719-735. https://doi.org/10.1016/S1071-5819(03)00039-9

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral Response to Phishing Risk. *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit (eCrime'07)*, October 2007, 37-44. https://doi.org/10.1145/1299015.1299019

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. *Proceedings of the 26th Annual Chi Conference on Human Factors in Computing Systems*, April 2008, 1065-1074. https://doi.org/10.1145/1357054.1357219

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly, 27*, 51-90. https://doi.org/10.2307/30036519

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. *Journal of the Association for Information Systems, 18*, 22-44. https://doi.org/10.17705/1jais.00447

Griffin, R. J., Neuwirth, K., Giese, J., & Dunwoody, S. (2002). Linking the Heuristic-Systematic Model and Depth of Processing. *Communication Research, 29*, 705-732. https://doi.org/10.1177/009365002237833

Halevi, T., Lewis, J., & Memon, N. (2013). A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits. *Proceedings of the 22nd International Conference on World Wide Web (IW3C2)*, May 2013, 737-744. https://doi.org/10.1108/OIR-04-2015-0106

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual Processing of Phishing Emails: How Attention and Elaboration Protect against Phishing. *Online Information Review, 40*, 265-281. https://doi.org/10.1108/OIR-04-2015-0106

Hillesheim, A. J., & Rusnock, C. F. (2016). Predicting the Effects of Automation Reliability Rates on Human-Automation Team Performance. *Proceedings of the 2016 Winter Simulation Conference (WSC)*, Washington DC, 11-14 December 2016, 1802-1813. https://doi.org/10.1109/WSC.2016.7822227

Holm, H., Flores, W. R., Nohlberg, M., & Ekstedt, M. (2014). An Empirical Investigation of the Effect of Target-Related Information in Phishing Attacks. *Proceedings of IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*, Ulm, 1-2 September 2014, 357-363. https://doi.org/10.1109/EDOCW.2014.59

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications of the ACM, 50*, 94-100. https://doi.org/10.1145/1290958.1290968

Modic, D., & Lea, S. E. G. (2011). How Neurotic Are Scam Victims, Really? The Big Five and Internet Scams. *Proceedings of the 2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology*, 1-23. https://doi.org/10.2139/ssrn.2448130

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which Phish Get Caught? An Exploratory Study of Individuals' Susceptibility to Phishing. *European Journal of Information Systems, 26*, 564-584. https://doi.org/10.1057/s41303-017-0058-x

Nicholson, J., Coventry, L., & Briggs, P. (2017). Can We Fight Social Engineering Attacks by Social Means? Assessing Social Salience as a Means to Improve Phish Detection. *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS13)*, Santa Clara, 12-14 July 2017, 285-298.

Ramesh, G., Selvakumar, K., & Venugopal, A. (2017). Intelligent Explanation Generation System for Phishing Webpages by Employing an Inference System. *Behaviour& Information Technology, 36*, 1244-1260. https://doi.org/10.1080/0144929X.2017.1369569

Sharples, S., Stedmon, A., Cox, G. et al. (2007). Flightdeck and Air Traffic Control Collaboration Evaluation (FACE): Evaluating Aviation Communication in the Laboratory and Field. *Applied Ergonomics, 38*, 399-407. https://doi.org/10.1016/j.apergo.2007.01.012

Spain, R. D., & Bliss, J. P. (2008). The Effect of Sonification Display pulse Rate and Reliability on Operator Trust and Perceived Workload during a Simulated Patient Monitoring Task. *Ergonomics, 51*, 1320-1337. https://doi.org/10.1080/00140130802120234

Vishwanath, A. (2015). Examining the Distinct Antecedents of E-Mail Habits and Its Influence on the Outcomes of a Phishing Attack. *Journal of Computer-Mediated Communication, 20*, 570-584. https://doi.org/10.1111/jcc4.12126

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of Phishing Susceptibility. *Communication Research, 45*, 1146-1166. https://doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R. et al. (2011). Why Do People Get Phished? Testing Individual Differences in Phishing vulnerability within an Integrated, Information Processing Model. *Decision Support Systems, 51*, 576-586. https://doi.org/10.1016/j.dss.2011.03.002

Wang, J. G., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. *IEEE Transactions on Professional Communication, 55*, 345-362. https://doi.org/10.1109/TPC.2012.2208392

Weirich, D., & Sasse, M. A. (2001). Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World. *Proceedings of the 2001 Workshop on New Security Paradigms (NSPW'12)*, September 2001, 137-143.

https://doi.org/10.1145/508171.508195

Welk, A. K., Hong, K. W., Zielinska, O. A. et al. (2015). Will the Phisher-Men" Reel You In?: Assessing Individual Differences in a Phishing Detection Task. *International Journal of Cyber Behavior, Psychology and Learning, 5*, 1-17. https://doi.org/10.4018/IJCBPL.2015100101

Wright, R. T., Jensen, M. L., Thatcher, J. B. et al. (2014). Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information Systems Research, 25*, 385-400. https://doi.org/10.1287/isre.2014.0522

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where Did They Go Right? Understanding the Deception in Phishing Communications. *Group Decision and Negotiation, 19*, 391-416. https://doi.org/10.1007/s10726-009-9167-9