Service Science and Management 服务科学和管理, 2014, 3, 59-65
Published Online August 2014 in Hans. http://www.hanspub.org/journal/ssem
http://dx.doi.org/10.12677/ssem.2014.34B009

Hans汉斯

A Study of Online Financial Fraud in China: Case Study and Analysis cross Sectors in Suzhou

Yan Sun, Chenyao Hong, Yiyu Wang, Fangzhou Wu, Xinyao Wang, Hechen Yan, Hong Kuang

International Business School, Xi'an Jiaotong-Liverpool University, Xi'an
Email: Yan.Sun@xjtlu.edu.cn

Received 30 April 2014

Abstract

This paper introduces the current situation of the financial fraud during recent years, focusing on the typical and new cases related with the internet financial fraud that occurred in Suzhou, Jiangsu Province. The paper has made deep researches of the factors of frauds which are typical and general. It proposes solutions in terms of the electronic trading system, the customer individual cognitive-behavioral, laws, regulations and the network platform security.

Keywords

Financial Fraud, Online Payment Security Risks, Network Security, Case Study, Suzhou, China

关于中国网络金融欺诈的研究：苏州地区案例调查与分析

孙　研，洪辰瑶，王亦宇，吴方舟，王心瑶，闫赫辰，匡　泓

中国西安交通利物浦大学国际商学院，西安
Email: Yan.Sun@xjtlu.edu.cn

收稿日期: 2014年4月30日

摘　要

本篇论文介绍了近年来网络金融欺诈频发的现状，着重选取江苏省范围内尤其是苏州市涉及网络金融诈欺的典型以及新兴犯罪案例为代表，深入剖析诈欺成因，由典型案例推广到普遍情况，从电子交易系

统，顾客个人认知行为，法律法规，网络平台安全等多方面提出解决方案。

关键词

金融诈欺，在线支付安全风险，网络平台安全，案例研究，苏州，中国

1. 引言

随着电子信息时代的到来，计算机功能不断的提升，传统金融商务市场已经发生了翻天覆地的变化；以电子货币、网络银行、电子商务为特征的新的金融营运体系已逐渐发展成熟，并深刻影响着人们生活的衣食住行。截至 2013 年上半年，全国电子商务交易额已达 4.35 万亿元，同比增长 24.3%[1]。而江苏省历来是我国发展最繁荣的地区之一，素有“鱼米之乡”之称，其工业产值连续多年位居中国第一。在政府的大力支持下，江苏省的电子商务也发展迅猛。近年来，江苏省在企业电子商务应用，电子商务网络安全，网络支付，以及物流配送等方面均取得长期有效进展。至 2013 年，江苏电子商务销售额已突破千亿。但是，电子商务无疑是一把双刃剑，互联网在带给人们方便、快捷服务的同时，其特有的虚拟性，流动性也被不法分子利用以从事金融经济犯罪活动。网络金融诈欺手段层出不穷，根据《当前利用计算机网络从事金融犯罪的现状及预防，打击对策》[2]，近年来互联网金融犯罪主要有以下几种类型：

1) 建立虚假金融机构网站，客户登录后盗取客户填写的个人账号，密码等银行资料信息。
2) 假冒网上购物商城诱使客户购买产品或盗取客户信息。
3) 利用木马等黑客程序盗取银行卡或个人信息。
4) 直接使黑客技术攻击互联网造成经济损失。
5) 犯罪分子利用金融单位内部管理漏洞侵占公，私客户资金。

利用互联网实施金融诈欺的本质是一种运用高新技术或专业知识所进行的智能犯罪，犯罪分子利用互联网技术漏洞，网民淡薄的自我防范意识，或者未完善的法律漏洞实施犯罪。如何有效识别和打击网络金融犯罪迫在眉睫。

2. 网络金融欺诈案例分析

2.1. 利用新兴网络交流工具如微信进行网络金融欺诈

案例 1

2013 年 8 月 4 日晚上 10 点左右，网店老板张先生接到阿里旺旺的一个购买家具的用户发来的信息，对方称需要用手机接收购买清单，并要求张先生加其为微信好友。张先生用手机扫描对方发送的二维码后接收到一个安装提示，他当时没有在意内容就点击了确认。最后发现他并未加到对方微信，并且无法联系那位用户。第二天，张先生发现支付宝账户(与手机绑定)内的 49812.01 元被人转走。警方通过调查发现，张先生安装程序启动了木马，该木马拦截短信，并转发至指定手机号码，嫌疑人据此修改支付宝账户密码并转走账户内资金。

案例 2

2013 年 4 月，常熟市服装城派出所就接到一起犯罪分子利用微信进行网络诈骗的案件。报案人王女士称，她在常熟陆家角新村网上做淘宝生意时，一位买家联系其要买东西，之后对方要求加王女士微信好友，于是王女士就主动加了对方。不料到了 4 月 18 日王女士突然发现，支付宝绑定的银行卡上少了 4981 元人民币。

案例 1~2 分析

微信是腾讯公司于 2011 年 1 月 21 日推出的一款通过网络快速发送语音短信、视频、图片和文字，支持多人群聊的手机聊天软件。由于平台开放多元，成为了卖家的推广平台，方便了购买用户。但是其安全性广受质疑，虚假购物链接诱骗消费者案例层出不穷。2013 年 11 月淘宝网宣布关闭微信通道以防止消费者上当受骗；但是买家与卖家互加好友依然提供了金融欺诈的平台。上述案例的诈骗方式均为卖家通过诱使买家扫描二维码，借此将木马程序植入买家手机，从而获取与买家手机绑定的支付宝信息。犯罪分子可以根据信息修改支付宝账户密码并转走账户内资金。关闭淘宝网微信渠道一定程度上避免了买家打开钓鱼链接，但是不能从根本上解决微信金融诈骗。另一方面，作为新兴网络聊天工具的代表，微信仅仅是众多犯罪分子采用的工具之一，网络产业的快速发展无疑为不法分子提供更为先进的犯罪手段。

主要解决方法

买卖双方在公共平台的安全没有得到良好保障的情况下应使用交易平台的聊天工具。与传统支付方式相比，第三方支付平台作为新型的支付方式促使了犯罪群体趋向年轻化，犯罪智能化[3]。因此，新型的买卖家交流方式成为犯罪团体的目标。因为建议用户避免使用未经第三方平台安全认可的电子商务交易流程。电子商务发展迅速，目前我国还没有完善的网络法律支持，支付宝本身安全不能得到良好的保证[4]。新兴微信平台更是缺少法律的保护，也没有相关的产品营销规范。法律的不完善使得社交网络与电子商务的衔接受到阻碍。法律的有效性实时性应得到提高。信息流、商流、资金流、物流是电子商务运作模型和业务流程的四个关键环节[5]加强信息流的安全可靠性是防止诈骗的途径。微信诈骗显示出诈骗者利用了信息流和资金流的衔接漏洞。由于这些新兴的社交网络作为良好的信息流通平台为买卖双方提供了便利，也有助于产品的营销推广；单方面关闭淘宝网的微信渠道在一定程度上阻碍了电子商务的发展，这不是长久且有效的避免金融诈骗的方式。在社交网络平台的开发过程中，开发商应加强信息的私密性；例如案例中帐号与手机号连接而导致的诈骗可以通过设置帐号保护避免。其他方式诸如设置密保问题，陌生人申请好友拦截等。

2.2. 应用购物网站如淘宝进行金融诈骗

案例 1

10 月 19 日，苏州警方接到报案，苏大学生小张在网购时，因忘记支付宝密码，便网络搜索到一个淘宝客服电话，小张按其要求将自己的身份证号、银行卡号、手机号以及支付宝验证码等提供给对方，结果发现银行账户被转账 5000 元。警方分析，犯罪嫌疑人冒充淘宝网站客服，接收到受害人个人信息后，通过网上申请快捷支付从而将帐号内资金转走。

案例 2

苏州杨小姐被骗子诈骗对方谎称网上购物交易失败，随后发给杨小姐链接要求其再次开通另一家网上银行。杨小姐并没有起疑，先后按照对方要求的程序开通数次，第二天杨小姐发现自己的银行卡被骗子通过快捷支付的方式划走 10,000 余元。

案例 1~2 分析

所谓网络淘宝诈骗是指犯罪份子利用消费者对信息技术以及电子商务认识的不足和自我防范意识的薄弱，网络上存在安全制度的不足进行骗取钱财的行为。这种行为严重的阻碍了电子商务模式的发展.这类案发的主要原因还是受害者生活经验不够丰富并且自我防范意识不强。其次，网络购物平台自身没有对安全方面进行强有力的监察，案例二中犯罪分子与受害者相隔千里，却能得知他人客户的购买信息，因此购物网站是否利用客户个人信息来赚取私利引人深思。第三，支付宝作为重要的第三方平台发展仍

不成熟，用户无法获得全方位的服务，例如：即使找回密码，联系客服等。最后，在信息爆炸时代的大环境下，人们普遍缺乏对信息真伪的识别处理，缺少相应机构和法律对此提供帮助。

主要解决方案:

1) 用户的网络安全教育必不可少，用户在进行任何一次网上交易时尤其是在输入帐户名与密码的时候都要仔细深思，排查钓鱼网站的可能性。用户可以在线搜索买主的信息以核实买主的网络身份是否正确。由于很多敲诈团伙都重复使用相同的帐户号码，此举可以进一步降低接触犯罪分子的可能性。一般情况下，正规的网上交易买主不会提供链接让顾客填写一些涉及私人隐私的信息。如果遇到类似情况，买家应该留心。其次，用户可以通过下载相应的银行理财软件来及时了解自己银行卡的余额状态，交易时与卖家的给出的信息相比较以防止上当受骗；如果发现不正常的情况(例如理财软件显示的帐户余额与淘宝客户端显示的余额不同)用户应立即报警寻求帮助。

2) 提高个人隐私问题保密性，建设网络信息安全制度将成为新实际淘宝乃至电子商务技术关注的新焦点。法律应当适当给与帮助，严惩网络诈骗行为。例如提高电子商务市场准入准出原则(国家对电子商务的经营者有关信息建立数据库，在网站相关位置明示自己的相关生产批准标号并链接到数据库查询，从而买家可以明确卖家身份，减少欺诈)；建立电子商务交易平台与实际经营者的责任连带制度(交易平台总是以没有明确的法律规定条款来逃避责任，相关部门应对其用户进行严格考察，减少欺诈发生)；将电子商务增加到法律监管领域(同步进行技术的更新，国家的制度与政治管理)[6]。

2.3. 利用虚假网站包括钓鱼网站发布虚假信息进行诈骗

案例 1

市民余先生用支付宝拍下一卖家的充值卡商品之后用淘宝旺旺与卖家取得联系。对方并没有按照常规流程提供移动充值卡密码，而是要求他到一个网上交易平台支付 0.1 元提取一个订单号，余先生便打开其提供的网站，选择支付了 0.1 元。到了第二天，余先生查询自己的银行卡，发现里面突然少了 35,000 元人民币。

案例 2

许先生家住太仓璜泾，做生意的他因为资金紧张，就在网上发布了想借贷的信息。很快，他的需求引起了一家担保公司的注意，该公司表示愿意借贷给许先生，不过先要他支付 300 元材料费和 22,500 元的偿还保证金，急需用钱的许先生问朋友借钱打入对方账号。随后，对方数次要求许先生汇款，许先生产生怀疑并向警方报了警。今年 7 月 29 日，太仓警方在湖北省随州市曾都区，抓获涉嫌网络诈骗的犯罪嫌疑人李某、孙某、饶某等 6 人，当场缴获作案工具笔记本电脑一台、手机 25 部、身份证 13 张、银行卡 25 张，以及非法所得 57,600 元。经审查，犯罪嫌疑人交代了在互联网发布无抵押贷款信息，并以缴纳手续费、担保金为由，诈骗受害人许先生现金 22,800 元的犯罪事实。

案例 1~2 分析：

案例一便是典型的钓鱼网站诈骗。此类攻击方式范围很广；攻击者建立假冒的银行，购物网站，炒股网站等寻常网站用以窃取用户信息。案例中的假冒网上交易平台诱骗用户输入银行卡号，密码等银行信息，最终使消费者造成严重的经济损失。通常攻击团体常常会伪造一个真实的网站，伪造网站与真实网站有着相似的域名，甚至是几乎一模一样的页面。图 1 是诈骗过许多消费者的假冒工商银行网站，图 2 是真正的工商银行网站。对比发现，钓鱼网站确实可以达到以假乱真的效果。

除了钓鱼网站，传统虚假网站也不能小觑。随着获取信息的渠道拓宽以及网络经验的增加，越来越多的人不会再轻易相信中奖信息。然而每年因虚假网站遭受经济损失的用户不在少数，尤其是涉及股票投资，基金理财等内容的网站，其承诺的低息贷款或高息收益常常诱使网民将大笔资金转入不法团伙的

Figure 1. Bogus ICBC website
图 1. 假冒工商银行网站

Figure 2. Official ICBC website
图 2. 官方工商银行网站

账号。

犯罪分子主要利用社会工程学，针对受害者好奇，贪婪的心理弱点而采取灵活缜密的欺骗等危害手段，比如以大型贷款公司，与多家银行有着良好的合作关系为由，骗取私营业主和个人的信任，通过开设虚假网站、手机短信、小卡片或在报纸上登载广告等途径发布“无抵押贷款”、“低息贷款”、“免息贷款”等贷款信息，猎取侵害对象。上述案例中，许先生因资金紧张而轻易相信了虚假信息。由此可见，消费者往往在情况紧急，急需用资的情况下相信可以给自己带来好处的信息而放松警惕性。除了此类受害者，一些缺乏网络经验，年纪较大的网民往往也是这类诈骗的主要侵害对象。

主要解决方案

随着钓鱼网站的迅速增长，电子商务在发展过程中不得不对其严加防范与监管。对于用户个人来说，应该保持高度警惕。同时，以下这些技术手段对用户进行网站的真伪鉴别也有很大的帮助。

1) 访问相关网站时用户应当详细检查域名信息。用户可通过搜索网站查询，细致对比域名信息以及网页内容信息。以上述真伪两张工商银行的截图为例，域名的长短差别可以被轻易发现。有时用户还必须细致校对 URL 内容。比如是否有字母，“.china”等细微差别。

2) 针对大型电子商务网站或网银站点，用户可以通过数字证书鉴别真伪。目前在大型电子商务网站或网银站点进行网络转账等访问时一般都使用 HTTP 协议。安装了数字证书 SSL 的网站，一般可通过“https”开头的网址进行访问，并在浏览器地址栏处显示小锁标志，此类显示意味着网站经过了 SSL 技术加密和严格的身份认证。最新的高端 SSL 证书产品是扩展验证(EV)SSL 证书。在 IE7.0、FireFox3.0、Opera 9.5 等新一代高安全浏览器下，使用扩展验证 VeriSign(EV)SSL 证书的网站的浏览器地址栏会自动呈现绿色，从而清晰地告诉用户正在访问的网站是经过严格认证的[7]。

3) 安装安全防护工具。用户可以选择安装具有钓鱼网址提醒功能的杀毒软件，以保护用户免受诈骗。如 360 网盾，能够及时提醒用户所访问的网站可能是钓鱼网站，及时避免损失。

4) 消费者要保持清头脑，不要轻易相信莫名的中奖信息或是低价甩卖，免息贷款等信息；不对他人透露个人信息，银行账号，存款信息等。对于缺乏上网经验的老人，更要对他们进行网络安全教育，防止他们轻信不法分子的勾当。其次，用户应该具备相应金融常识。比如贷款需要当面检验证件、办理手续，直接在不见面的情况下通过网络放贷是不被允许的。

3. 采访调查

针对网络金融诈欺，本文采取随机访问调查的形式收集数据，共有 60 人参与随机调查，其中年龄超过 25 的被采访者有 24 人，均已参加工作；其余 36 人年龄在 18~25 之间，均为在校大学生。此次调查询问了被采访者对网络金融诈欺现状的理解以及意见。36 位大学生中有两位曾遭遇淘宝卖家不守信用的事件，他们在成功发送网络购物订单后，买家迟迟不发货。由于自身的警惕意识，这两位被采访者在等待几日后便取消订单，避免了潜在的欺诈风险；另外有 10 位大学生曾经遭遇钓鱼网站，这些网站散布虚假用户中奖消息，有的借此骗取用户经济信息，有的以需要注册费等借口要求用户往指定账户转账。在已经工作的 24 位被采访者中，有 2 人表示自己接触网络经验不多，有 6 位曾经收到诈骗短信，4 人在上网过程中遇到钓鱼网站。值得庆幸的是，即使遭遇各种网络诈骗手段，所有被采访者均没有轻易上当受骗。在所有被采访者中，48 人认为避免网络金融诈骗的关键在于自身的安全意识和辨别能力；11 人认为国家采取网络严打手段是杜绝网络金融欺诈的最有效方法，1 人认为预防网络金融诈欺必须结合用户，公安，网络第三方等多方合作，建立完整的预防犯罪体系。

4. 结论

本文主要通过案例分析以及随机调查探索了网络金融诈骗发生的原因并提出实际可行的解决方法。

在互联网金融的主要经济活动中，数字化信息代表了各类货币资金，在无形的网络中流动。由于这种活动不受地域以及时间的限制，交易双方不需要进行面对面商谈便可达成一致协定，从而导致了网络金融诈欺危害的传播速度加快，影响范围扩大，国家对金融诈欺的监管难度也随之加大[8]。金融欺诈源于用户对于电子商务的流程和正规渠道不熟悉，电子商务平台本身不完善且未得到良好的监督，以及国内针对网络交易的配套措施如监管法规、消费者保障制度等还不完善。这些风险因素在不同的交易环节中会损失户利益并且阻碍电子商务的发展。

对于用户而言，建议使用网络平台认可的正规交易流程，加强安全意识和基本的网络知识，安装安全防护工具，对于未使用过的支付网站和支付方式不要轻易尝试。而网络社交、购物平台都应加强对于用户信息的保护，普及网络交易的安全知识，加强信息流和资金流的衔接。长远来看，虽然目前金融诈骗在中国网络交易中所占比例不显著，但随着电子商务的迅猛发展和普及，诈骗形式趋于多样化，潜在欺诈发生的风险也随之增加，相关法律法规亟需完善；其中，我国的网络信息安全法制建设需要逐渐提上日程，应汲取发达国家网络立法实例，解决立法建设技术障碍，及时更新法律建设，完善网络信息法制的反馈渠道[9]。只有多方合作，不仅仅强调单方建设改善，才能真正有效避免网络金融诈欺。

参考文献 (References)

[1] 中国电子商务研究中心 (2013) 中国电子商务市场数据监测报告.

[2] 戴辉 (2006) 当前利用计算机网络从事金融犯罪的现状及预防，打击对策. *中国人民公安大学学报*, **4**, 65-67.

[3] 龚培华, 陈海燕 (2010) 第三方支付平台中的犯罪问题与法律对策. *法治论丛*, **1**, 48-53.

[4] 董仁涛 (2006) 支付宝：从淘宝网看电子商务支付方式. *商场现代化*, **455**, 133-136.

[5] 董燕丰 (2007) 关于国内第三方网上支付平台之支付宝资金支付的研究. 北京邮电大学, 北京.

[6] 张樊 (2006) 电子商欺诈问题的法律应对办法.

[7] 贾春福 (2013) 全国计算机等级考试三级教程——信息安全技术. 高等教育出版, 北京, 203-204.

[8] 杨群华 (2013) 我国互联网金融的特殊风险及防范研究. *金融科技时代*, **7**, 100-103.

[9] 罗云 (2011) 网络信息安全的法律问题. 重庆大学法学院, 重庆.