

卡在身上,钱却没了。通讯(网络)诈骗犯罪正在“升级换代”,利用伪基站进行犯罪以及骗取验证码成为最新趋势

一条“短信”背后的黑色利益链



本报记者 王晓峰
通讯员 林炳潮 徐露

卡在自己身上,密码也只有自己知道,却发现卡里的钱凭空消失了。这样的事,在通信发达的网络时代,从“天方夜谭”变成了活生生的事实。

近年来,通讯(网络)诈骗犯罪成为社会一大毒瘤,其诈骗手法更新之快、花样之多令人瞠目结舌。从传统的话术诈骗,发展到如今的技术+话术,通讯(网络)诈骗犯罪呈现出两大新趋势——利用伪基站和骗取验证码。

如何有效遏制这类犯罪,这是目前全国都在探索的难题。而在宁波市,经过各方努力,已初步编织出一张具有宁波特色的防御网。但不得不说的是,被动防御总会挨打,如今亟须各部门协力,一起来斩断这条“短信”背后的黑色利益链。

“积分兑换”的背后:伪基站犯罪

手机积分可兑换话费,这样的事不少人遇到过,可换成银行积分兑换现金大礼包这样的“福利”呢?从去年上半年开始,这样的骗局在镇海最先出现,随后在宁波市蔓延趋势,其背后就是伪基站在“作怪”。日前,镇海警方连续破获两起利用伪基站诈骗的案件,共抓获犯罪嫌疑人3名。

前不久,镇海警方连续接到市民举报,称近期“积分兑换”诈骗短信突然又多了起来,并不断有人上当受骗。王女士就是其中的一名受害者,她收到了这样的短信,一看是“银行官方号码”发来的,抱着试一试的心态点击进去。

“我先是点了短信里的一个网址链接,然后跟着操作提示输入了银行卡号、密码、手机号码等相关信息。”王女士说,在收到验证码并提交后,她立马就收到了银行卡余额变动的提醒短信,自己卡里2000多元钱被悉数转走了。

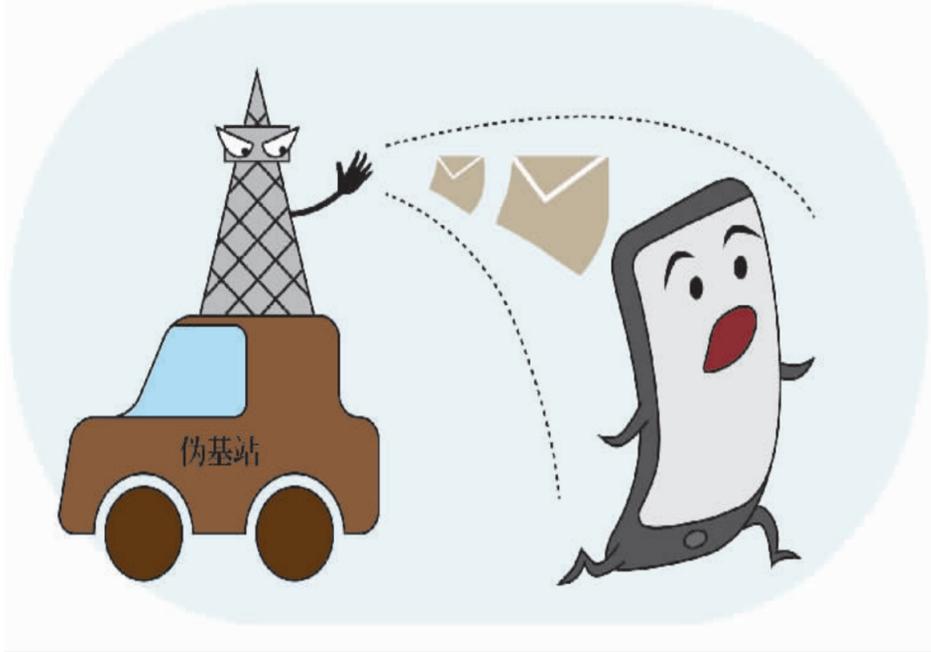
案件发生后,警方立即抽调精干警力展开侦破工作。“这是一起典型的伪基站诈骗案件,去年3月份我们这边就曾被破获过。”镇海公安刑侦大队队长董建说,接下去几天,他们不断接到有群众被骗的报案,由此判断犯罪团伙很可能还在镇海作案。之后,在多种协同配合下,警方发现居然有两个犯罪团伙活跃在此地。经过不断追踪和走访,办案民警最终锁定了伪基站的位置。

3月17日上午,专案组在余姚成功将犯罪嫌疑人朱某抓获。仅隔一天,专案组一行又在北仑某路口边的一辆白色轿车内,将正在作案的福建籍犯罪嫌疑人郑某和王某抓获,并在车内当场搜出“伪基站”短信发送设备、笔记本电脑等作案工具。

经审讯,3名犯罪嫌疑人供述称,他们从非法途径获得“伪基站”设备,随后将设备装载在车内,通过驾车流窜作案的方式,至外来人口较为密集的区域,发送诈



“伪基站”短信发送设备,体积与无线路由器差不多大,很难被发现。(王晓峰 摄)



(洪茜茜 绘)

骗短信,诱骗他人点击。

目前,这3人已被采取强制措施。警方共收缴伪基站设备两套,破获镇海区内通讯(网络)诈骗案件6起,串并宁波市范围内案件20余起,涉案金额10万余元,追回赃款2万余元。

“我们之所以要特意提及这起案件,是因为这背后有着通讯(网络)诈骗犯罪的最新“秘密”。老百姓知道了,就能减少被骗概率。”民警说,如今通讯(网络)诈骗犯罪正在“升级换代”,利用伪基站进行犯罪以及骗取验证码成为最新趋势。

机关用尽,只为获取隐秘信息

“伪基站”和“骗验证码”两者之间存在着千丝万缕的关系。前几年,我市的伪基站犯罪刚出现时,是以发送垃圾短信,做小广告为主。2014年,余姚、慈溪、镇海、宁海等地警方都曾破获过这类案件,不法分子最后也被一一判刑。

但从2015年开始,伪基站犯罪就转向诈骗领域了。最典型的就是去年3月底发生在镇海的“银行积分兑换”骗局,仅仅4天时间,不法分子就狂发30万条诈骗短信。并且,因为这种骗局是新出现的,受害人众多,仅镇海一地就有十多人。

今年以来,这类犯罪更加猖獗,仅记者本人上周就收到了十多条此类诈骗短信,名目众多;有银行积分兑换的、有孩子在校情况的、有同学聚会照片,甚至还有用桃色新闻吸引眼球的。尽管内容千变万化,但始终不变的是,短信结尾都会带有一个网址链接,引诱当事人点击。

“现在伪基站犯罪在全国各地不断发生,并且技术手段越来越高超,已经从单纯的让受害人填写信息并忽悠,发展成通过木马程序直接窃取。”民警说,随着智能手机的普及,手机绑定网银并消费已基本

成为标配,但群众的手机防病毒意识没有跟上时代。不法分子正是看到了这一点,想方设法对目标手机植入木马程序,随后窃取各类信息。

这并非危言耸听,央视前不久就做过一个“银行卡盗刷黑色产业链”的相关调查。有一位姓吴的先生突然收到一条陌生号码发来的短信,短信上写着他自己的名字,吴先生以为是某个没存号码的朋友发来的,就点击了短信中的图片。由于手机并未出现什么异常,吴先生便没太在意。可一个星期之后,银行突然发来一条消费短信,原本存有5万多元钱的一张银行卡,余额竟然只剩下300多元了。最终证实,吴先生的手机中了木马病毒,让其在一个月内丧失了接收短信的功能,取款验证码及提醒短信都被半路拦截了。

央视记者在深入调查时,有人向其爆料,在网络空间存在着一个规模庞大的窃取银行卡的黑色产业链,“神通广大”者5分钟就能搞到1000多条个人信息。随后爆料人果真给调查记者发了一份长达33页的名单文件,每条信息都有卡主的姓名、银行卡号、身份证号、银行预留手机号码以及银行密码。记者在文件中随机选取了70条来自不同省份的信息进行验证,恐怖的是,身份信息和电话号码全部正确,除了5个银行卡密码错误,其余65个银行卡密码也全都正确。

那么,如此庞大并且准确的个人信息,不法分子是怎么拿到的呢?根据目前破获的案件来看,除了市民自己不慎泄露外,主要途径有“伪基站发送的木马短信”“免费WiFi窃取个人信息”“手机应用软件窃密”以及“改装POS机提取银行卡信息”这几类。以伪基站为例,不法分子发送诈骗短信,受害人点击后,要么转到“钓鱼”网站,要么直接植入木马程序。就这样,受害人的各种隐秘信息在不知不觉中被盗走了。

福建就曾发生过一起“有趣的”案件:一名不法分子伪装成“快递小哥”上门,送上包裹后正要转身离开,受害人突然接到一电话,自称是快递公司的,送错了件,但打不通“快递小哥”的电话,请受害人将手机给予对方。“快递小哥”拿到受害人手机的那一刻,记下了刚发来的手机验证码并通知后方操作人员,瞬间将受害人银行卡里的钱转走了。显然,不法分子提前就获得了受害人的各项信息,但苦于没有动态的手机验证码,所以才上演了这样一出戏。

“现在的通讯(网络)诈骗犯罪,已转变为骗取受害人的验证码。因为其他信息对于他们来说都是单项透明的,唯有手机验证码是动态、难以掌握的。”民警说,技术高超的作案人,一般是先植入一套木马程序,秘密地控制受害人手机的各项功能,尤其是短信功能。之后短信全部被木马程序拦截并且对不法分子单向开放,验证码自然

就到了。更为恐怖的是,有些高级木马程序还有复制、传染功能,会按照受害人通讯录中的名单,一个个发送木马短信过去。

让手机中病毒是最为常见的拦截验证码方式,却不是唯一的方式。另外一种就是对手机信号进行干扰。当然,这种手法要提前知道对方所处的位置,毕竟干扰器作用范围有限。方法同样简单,冒充“快递小哥”,称受害人有一份快递,但地址不清晰,请再报一遍。

应对新骗术,“信息泄露”如何防

在“大数据”时代,“泄密”无时无刻不在进行。有调查显示,如今很多人还不知道智能设备正在“被动”地让自己的信息“裸奔”,只有44%的人知道这个隐患。

要防止“信息泄露”,需要多方同时行动。就个人而言,要养成良好的手机使用习惯:不要轻信陌生号码发来的短信,即使号码像是常见的服务号,或是好友号码发来的短信,也要对内容进行认真鉴别;不管收到什么短信,只要其中含有陌生链接,就不要轻易点击打开;手机也不要随便“刷机”,容易出现程序漏洞并被有心人掌控;不要随意拨打对方提供的所谓咨询电话,或者自己上网查百度,这样特别容易遭遇骗子,最佳方法是自己拨打114查询。

同时,个人要学会定期更换密码,并且设置密码时要有“技术含量”,千万别干“生日当密码”“所有账号同一个密码”这类傻事。此外,一旦发现自己被骗,除了第一时间报警外,也要学会自我止损。方法有两个——电话银行冻结和网上银行冻结,即针对诈骗账号乱输密码,多次输错后即可暂时冻结。

就执法部门而言,应该加强打击力度,尽可能遏制这类犯罪。据悉,目前宁波市也正在朝这方面努力,今年不仅成立了反欺诈中心,还召开了整治通讯(网络)新型犯罪的联席会议,30多家单位联动应对此类犯罪。截至目前,宁波市已初步建立“银行—基层派出所—110指挥中心—反欺诈中心”这样一张覆盖面较广、层次分明的防御安全网。年初以来,我市通讯(网络)诈骗案件环比下降三成多,效果较为明显。但不得不说的是,针对伪基站这类新型犯罪,相关职能部门也需要更新战术,积极探索更加高效的应对打击策略。

最后,政府部门应该行动起来,督促电信和金融行业落实实名制,把反通讯(网络)诈骗犯罪纳入智慧城市建设体系。今年全国两会期间,就有人大代表和政协委员提出了这方面的建议。他们呼吁,在严打个人信息泄露、交易的同时,银行、电信运营商还必须抓好实名制的落实,增加不法分子的犯罪难度和犯罪成本。

新闻背后的热词

通讯(网络)诈骗犯罪

通讯(网络)诈骗犯罪,指利用现代通信技术、网络技术、网银等手段进行的诈骗。犯罪分子借助手机、固定电话、短信群发器、计算机、网络服务器、银行卡、ATM机等工具,利用网银技术、变号技术、网络电话技术、伪基站技术、短信群发技术实施诈骗活动,具有涉及范围

广、高科技性、隐蔽性等特点。通讯(网络)诈骗犯罪是一大社会公害,它不仅大量侵害群众财产安全,而且对社会诚信造成危害,影响政府公信力和企业形象。由于通讯(网络)诈骗犯罪具有非接触式、跨区域甚至跨国作案等特点,此类犯罪活动打击成本高,是一个全国性难题。

相关链接

各地严防通讯(网络)诈骗

去年年初,海宁警方成立了“通讯(网络)诈骗案件云分析平台”。它可选择任一时间段,对该市发案形势、多发类型、资金流向进行全面监测和自主分析,一键生成研判报告。对两次以上临柜转账、3次以上ATM机转账的银行网点,一方面会通过短信和电话联系银行实时提醒,另一方面会指令治安、巡特警等部门开展重点防范和巡逻值守,对发案3起以上的社区,则会通过平台推送辖区派出所,开

展防控补强。去年12月,温州市反通讯(网络)诈骗中心成立,该市反通讯(网络)诈骗联席会议领导小组同时揭牌。中心接到通讯(网络)诈骗警情,第一时间对涉案银行账户进行查询,快速锁止,并利用自动回拨,对涉案通讯号码快速封堵。通讯运营商的工作人员则利用专业知识配合办案。中心还将自动收集诈骗电话,再通过运营商关停涉案通讯号码,有效打击诈骗犯罪。

国外如何遏制通讯(网络)诈骗

美国针对此类诈骗案件的主要控制手段是完善法律。除通过法律保护用户的信息外,还赋予了银行、运营商以主动封锁账户、拦截电话等权利。鉴于通讯(网络)诈骗犯罪的手段变化多端,美国对此类诈骗案的控制也逐步由通讯渠道转向银行渠道。美国法律规定:当事人转账后可以对自己的转账行为提出异议,

并有权要求立即冻结对方账户。为严控“汇款诈骗”发展,日本制定了银行、通信行业实名认证制以及严格的审查手段,确保银行及通信账户均可追查到人。设立实施“汇款诈骗救济法”,一旦发现账户异常,银行可直接冻结相关账户,并返还被诈骗金额。从2011年开始,日本部分银行在ATM机上安装了手机信号干扰器。

数说



制图:洪茜茜