热线:96060 E-mail:xdkb@kuaibao.net 现代快报
责编:臧晓松 美编:陈恩武 组版:丁亚平 2015.12.10 星期四

点“客服”短信链接 网银就被盗 原来是伪基站作祟:能冒充任何号码!

江苏警方:即使短信显示为银行、运营商、保险公司客服号码,也不能轻信

收到“银行客服”提示短信,点链接积分兑换礼品,你点了,对不起,网银被盗;收到“学校”短信,点链接看孩子在校成绩,你点了,对不起,网银被盗;收到“运营商”短信,点链接积分兑换话费,你点了,对不起,网银被盗……这样的诈骗短信已经让很多人中招。那么这些短信从哪儿来的?答案是:伪基站。即日起江苏警方联合相关部门,开展打击利用伪基站发送诈骗短信专项行动。江苏省公安厅刑侦专家提醒广大市民,收到陌生短信千万不要点击链接,以免上当受骗。通讯员 苏宫新 现代快报记者 陶维洲

行人背包里可能藏着伪基站

背包开洞是为了给里面的设备散热

来看看,伪基站就长这样

警方缴获的伪基站

下面就是伪基站发送的短信

一旦点开钓鱼网站链接,填写银行卡信息,你就将面临被盗刷

本版图片由警方提供

案例 1

收“银行客服”短信,三小伙银行卡齐被掏空

11月23日中午12点左右,南京市公安局秦淮分局夫子庙派出所接到三个小伙的报警,称他们遭遇网银被盗,银行卡内存款被掏空,损失近万元。三人是同一公寓的租客,彼此是室友。其中一名小伙告诉民警,当天中午,他们三人的手机均收到了来自同一家银行客服的短信。短信通知称,他们的网上银行即将过期,为不影响使用,请到网站升级。短信里面还“贴心”地附上了一个升级网银的网址。

三个小伙确实都有这家银行的网银,且平时习惯于网购,所以对网银升级一事特别关心。因为看到确实是银行客服号码发来的短信,而且三个人都收到了,所以他们觉得应该是银行统一通知,所以不疑有他,立即点击短信中的链接开始操作。进入“升级”网站后,三人按照要求填写了银行账户信息、取款密码、身份证号码、手机号和短信验证码,很快完成了“升级”。

本以为这样就大功告成,但很快三人相继接到银行客服短信,称他们银行卡内的存款均被转账。此时,三人才意识到上当受骗。

案例 2

行驶记录良好,保险公司送积分奖励?

12月8日,南京市民杨先生刚驾车来到新街口,手机上便收到了一条短信。杨先生一看,是自己所购车险的保险公司发来的短信,上面称因为杨先生上个月行驶记录良好,获得了5000分的安全驾驶奖励,请他登录“vip.4008000000.com”领取,截止日期为2015年12月17日。由于短信上明确地写出了杨先生的姓名、车牌号码,所以感觉可信度很高。

“现在保险公司的服务真贴心,文明开车还有奖励。”杨先生心里想着,就要去点链接领积分。这时他突然一个激灵,“保险公司又没有成天跟着我,怎么知道我的行驶记录良好?”想到此,杨先生决定先不点链接,打保险公司客服咨询一下。果然,保险公司根本没有这项活动。同时,保险公司客服人员提醒杨先生,近期他们已经接到好多客户咨询此事,公司判断应该是诈骗短信,请杨先生千万别点短信中的链接,以免给自己造成损失。

随后,杨先生将此事向南京玄武公安分局新街口派出所反映,得知不少来到新街口的驾车人都收到了此类短信。警方判断,应该是诈骗分子刻意发送此类诈骗短信,请杨先生切勿相信。

警方揭秘

诈骗短信来自伪基站,能冒充任何号码

“上述两个案例,其实背后都是伪基站作祟。”江苏省公安厅刑警总队刑侦专家介绍,伪基站是一种信号发射装置,一般由主机和笔记本电脑组成,其可以伪装成运营商的基站,冒用任意号码强行向一定范围内的手机用户发送诈骗、广告推销等短信息。

“一定区域内好多手机都收到同样的短信,那么基本可以判断是伪基站推送的。”专家介绍,由于伪基站体积比较小,嫌疑人往往用车辆装载伪基站,向周围手机发送诈骗短信、垃圾短信。而且,伪基站可以伪装成任何号码发送短信,以假乱真。所以,即便是看到以银行、运营商、保险公司等官方客服号显示的短信,同样不能轻信。

伪基站流动性强,能车载还能随身背

最近,网上流传一张照片,一个带有散热孔的背包。照片说明指出,这种包里装的就是伪基站,如果看到有人背着这样的包,就说明他在用伪基站发送诈骗短信。那么这种随身携带的伪基站真的存在吗?

“这确实是有的。”刑侦专家表示,外地警方已经破获相关案件,但这种随身背包携带的伪基站在江苏尚未发现。“伪基站的体积越做越小,以前最常见的是放在车辆内,而现在已经出现了放在电瓶车上的伪基站,以及随身携带的伪基站。”刑侦专家介绍,其实,通过一定的技术手段是可以定位伪基站位置的,但由于其大多是流动的,所以很难将其逮个正着。

还能劫持手机,让你和外界失去联系

刑侦专家介绍,一般来说,伪基站推送的诈骗短信往往含有虚假网站和木马链接。这些短信的由头往往是银行积分兑换、奖励领取、网银升级等等,其短信内嵌入的虚假网站会要求你填写银行卡信息,甚至验证码。

事实上,这些虚假网站的后台会将所有信息窃取,然后对你的网银进行盗取。而嵌入木马链接的诈骗短信则更可怕,一旦点击链接,手机内便会种下木马病毒。此类病毒不仅会扫描的你手机,获取其中的一切信息,包括网银用户名、登陆密码,还会窃取你的手机通讯录,并用你的手机号向这些号码发送新的诈骗短信、木马链接,扩大受害人的范围。

“伪基站还能劫持你的手机,让其不能正常工作。”刑侦专家介绍,通过这一功能,骗子能让你的手机停止工作,和外界失去联系,以便他们从事电话诈骗,以你被绑架为由诈骗你的家人等等。

怎么防范

不管收到什么短信,陌生链接千万不要点

伪基站如此可怕,该如何防范呢?对此,刑侦专家表示,针对伪基站的作案方式,广大市民要做到的第一要诀就是,不管收到什么短信,里面的陌生链接千万不要点。“不管是银行客服还是运营商客服发来的短信,千万不要贸然点击里面的链接,而是应该关闭短信,自己通过客服号码进行咨询,以确认短信的真实性。如果是诈骗短信,果断删除。”刑侦专家说。

即日起,江苏省公安厅、江苏省通信管理局、中国移动江苏分公司已联合部署开展打击利用伪基站发送诈骗短信专项行动,坚决遏制此类案件增多的势头。在此,警方提请广大市民,接到疑似伪基站发送的诈骗短信后,第一时间拨打110或10086举报,说清短信内容、短信主叫号码,接收短信时具体位置,公安机关将及时开展查处工作。