

这个“李鬼”很危险 小心高仿手机APP

为方便打理财务,济南市民韩先生下载了一款名为“××银行信用卡”的APP,不久后却发现银行卡被盗刷、莫名被贷款等情况。到银行营业网点核实,被告知所安装的客户端是高仿的。

网上转账缴费、处理罚单、买火车票……随着移动互联网的发展,越来越多的人习惯用手机APP处理各种事务。记者调查发现,在手机应用市场中,一些通过相近名称、类似图标制作的高仿APP令人难辨真假,给不少用户造成财产损失。

高仿APP“鬼”影重重设陷阱

济南市民成栋前不久为网上处理汽车交通罚单,试图在手机应用商店下载公安部推出的“交管12123”APP。搜索结果第一位的为一款名为“12123”的软件,且APP图标为一个“违”字。下载使用后发现,这款APP功能和页面都极其简陋,是一款高仿APP,不仅无法处理违章,还含有大量广告。

记者在多个应用商店检索发现,此类APP“李鬼”并不少见。例如,北京公交集团推出的“北京公交”APP,可用来刷码乘公交。但在安智网、酷安网等应用市场中检索“北京公交”,排名前几位的应用多为“北京实时公交”“北京公交在线”等APP,下载量最

高的达30.8万次。打开上述APP后,界面非常简单,也不具备刷码乘车功能,且都包含不少广告。在这些APP的用户评论区,许多使用者留言“根本用不了”“软件是骗人的”等。

值得警惕的是,一些高仿APP还通过伪装成官方软件窃取用户个人信息。济南市民罗腾告诉记者,他此前为在济南一家医院挂号,在应用市场中下载了这家医院的APP,并填写了电子病历,其中包含家庭住址、联系方式、职业等个人信息。但之后发现,所下载的并不是官方APP。“这款APP的下载量近10万,窃取了大量个人信息,侵犯个人隐私。”罗腾说。

记者发现,高仿APP除了集中在垂直的生活服务类软件,同时在电商平台的应用中也较为普遍。烟台市民马翹楚告诉记者,她曾在某应用市场搜索“淘宝”时,下载了一款名为“淘宝特卖”的APP,进入后发现,平台内不少商家销售价格低廉的山寨货品,并且购物的“三包”“退换货”等条款都不齐全。

记者联系了北京公交部门、山东交警部门以及淘宝服务热线,分别核实高仿APP“12123”“北京公交在线”“淘宝特卖”等是否与官方推出的应用有关联。相关工作人员均告诉记者,这些APP与官方应用无任何关系;类似的高仿APP很多,的确在一定程度上干扰了使用者,不少用户无法第一时间下载到官方应用。

5万元即可开发一个高仿APP

记者调查发现,不少高仿APP开发者为第三方公司。以“北京实时公交”为例,开发者为江苏一家商贸有限公司,在国家企业信用信息公示系统中,该公司经营范围为“化妆品、服装、日用百货销售”。此外记者还发现,应用市场中的一些高仿应用,开发者甚至为个人,网络上无法查询更多开发者信息。

业内人士告诉记者,高仿APP盈利主要靠应用内的大量广告赚取广告费,这类APP开发难度并不高。记者联系了一个APP开发团队,并向对方提出想开发图标和名字都模仿一款学习类应用的高仿APP。对方表示,只要不是要求“一模一样”,都可以实现。费用在5万元左右,开发周期大约一个月。

业内人士表示,开发一款高仿APP,花费数万元可以长期赚取广告收益。应用市场在对上架的APP进行审核时,机器审核只进行病毒和兼容性测试,人工审核一般只审核名称、内容是否存在违规,对APP名称、图标、宣传语等内容是否存在模仿,多数应用市场都疏于甄别。

记者查询了多个应用市场的相关条款,只有“华为应用商店”等极个别应用市场在相关条款中要求,上架应用不得与其他开发者应用具有相同或相似的外观、名称、主题等。

专家建议严肃查处高仿APP

360发布的《2018年双十一购物安全生态报告》显示,一个月时间内虚假仿冒主流购物APP的数量接近4000个,覆盖设备超过30万个,高仿APP已形成危害用户网络安全产业链。

记者调查发现,近期福建、河北等地网信部门关停下架的应用中不乏高仿类APP。福建泉州网信办今年8月下架的43款违规APP中,就有模仿“天天快报”等APP的应用。

北京师范大学法学院副教授吴沈括说,高仿APP对于正版应用的模仿,已经涉嫌侵权,同时对用户产生了实质性危害。但是,目前在打击高仿APP的过程中,存在多方协调难、举报下架过程漫长、相关法律政策不完善等因素,给一些不法企业从事违规行为提供了空间。

多位专家建议,公安、市

场监管、网信等部门应进行联合执法,严肃查处高仿APP给使用者造成经济损失、个人信息泄露等情况。北京京师律师事务所律师张新年说,相关部门应通过案例发布、防范建议等形式提高用户保护个人信息和预防网络诈骗的能力。

吴沈括说,各大应用市场作为平台方,应进一步完善自身内部审核机制,对入驻应用软件提交的信息尽到法定和约定的审查、登记、检查监控义务,从源头治理高仿APP问题。

多位专家提醒,用户在使用APP过程中,尤其遇到要求转账汇款等情况时,应仔细分辨应用真伪,不轻易接受对方指令。此外,APP中要求点击的不明链接,用户也要谨慎甄别,尽量不在不明链接里输入个人信息,以免信息遭泄露。

据新华社



最高人民法院近日发布的《司法大数据专题报告:网络犯罪特点和趋势》(以下简称《报告》)显示,2016年至2018年网络犯罪案件已结4.8万余件。近两成的网络诈骗案件是在获取公民个人信息后进行的。

最高法信息中心副主任孙福辉介绍,网络犯罪案件量及在全部刑事案件总量中的占比均呈逐年上升趋势,以互联网为工具实施诈骗的情况在东南沿海地区最为严重,福建、浙江、山西等10地利用网络手段实施犯罪的案件占比超过全国平均水平。

平均每件网络犯罪案件涉及2.73名被告人;四分之三的网络犯罪案件被告人年龄在20周岁至40周岁之间,年龄为28周岁的被告人最多;未满18周岁的被告人占比逐年降低。网络犯罪案件中,从事信息传输、计算机服务和软件业的被告人最多,占比达37.21%。

网络诈骗案件中,近三分之一的案件属于网络诈骗案件。近年来,网络诈骗案件占全部诈骗案件的比例上升趋势明显,2017年为7.67%,2018年猛增至17.61%。

2018年,微信超过QQ成为网络诈骗犯罪中使用最为频繁的犯罪工具,超半数网络诈骗案件中有涉及应用微信实施诈骗的犯罪情节。

被告人在实施网络诈骗案件时,冒充他人身份实施诈骗的案件占比达31.52%,以招聘为诱饵实施诈骗的案件占比在2018年大幅上升。在冒充类型的网络诈骗案件中,被告人多冒充女性或熟人;近20%的网络诈骗案件具有精准诈骗特征。

最高法刑三庭副庭长罗国良介绍,近年来诈骗手法不断翻新,层出不穷,比如“杀猪盘”诈骗就是婚恋交友型诈骗和网络赌博型诈骗的结合。诈骗分子往往是在各大婚恋交友网站或社交平台寻找目标,以婚恋交友为幌子把这些人诱骗到早已设计好的境外博彩网站进行赌博,或在境外的网络平台进行投资,声称可以利用网络漏洞赚钱,诱骗受害人投入大量资金。犯罪分子把被骗的一方叫做“猪仔”,把建立恋爱关系的过程叫做“养猪”,把实施诈骗叫做“杀猪”。

进行兼职型诈骗的犯罪分子通过网络平台发布网络兼职信息,利用“刷单返利”作为幌子,只要参与就要交一定的保证金。前期,犯罪分子会给一部分兑现返利,但到一定时候就会分配一个大资金任务,完成任务才能获得返利。受害人就不断地陷进去,最后血本无归。

此外,常见的还有“低息免押连环套”,诈骗分子往往抓住借款人急于用钱的心理,以低息免押等为噱头,但放款要先收各种手续费,本是一个小额贷款,最终却让受害人付出了高额的代价。

罗国良说,这些诈骗手段就是利用了两个字,“贪”和“急”。他提醒,有效防范电信网络诈骗,第一,要有强烈的个人隐私保护意识,个人信息不要存手机里,不要轻易向陌生人提供。第二,做到几个“不要”,不要向陌生账号汇款;不要连接陌生的WiFi;不要向他人透露短信验证码;不要轻信各种网络交友;不能有贪小便宜、想一夜暴富的想法。“天上掉馅饼,必定有陷阱”,遇到可疑情况要及时报警,配合公安机关及时破案。

(王亦君)

据《中国青年报》

超半数网络诈骗案件均有涉及应用微信实施诈骗犯罪情节

微信成网络诈骗使用最频繁的作案工具

还在朋友圈帮忙砍价? 这是新型骗局! 慎点

尽管“双11”的网购狂欢已经结束,但近期微信朋友圈内的各类“砍价”网购活动,呈现越来越活跃的势头。11月18日,太原市反诈骗中心发布警情提醒:市民对朋友圈发布的砍价赢大奖、砍价购物的营销,应保持高度警惕,切勿轻易填写个人信息,特别是敏感信息。对于要求转账汇款的,一定要核实清楚对方身份后再定夺。



不久前,北京市民郭先生在朋友圈看到一条帮忙“砍价”购物的链接,上面写着“找朋友帮忙砍价,最低0元就可以购买苹果×手机。”郭先生当即点了进去,帮朋友点上了“砍价”键,留下姓名和电话后,页面上显示“你已帮朋友砍了68元! 活动时间有限,只要填写信息参与活动,找朋友参与砍价就能零元购手机。”郭先生不假思索地将链接转发到了朋友圈,并给好友发信息要求帮忙“砍价”。正在忙活的时候,郭先生却收到了一条信息,上面显示他的银行卡被划走了600元。“密码不知道怎么被泄露了,余额一次性被转干净了。好在微信绑定的不是我存钱的卡,不然损失肯定更大。我怀疑是填写的个人信息泄露了。”

除了郭先生,太原市民李先生近日也因为“砍价”,遭遇了闹心事。“我朋友给我发了一个要求帮忙砍价链接,我没有多想就点了进去。”李先生称,根据“砍价”页面的要求,他在相关信息栏目内输入了自己的手机号码。

此后,页面也显示“你已帮朋友砍了××元”。可让李先生没想到的是,几个小时后,他的许多朋友都收到了留着李先生名字的诈骗短信。李先生怀疑,自己和朋友的个人信息,就是这次“砍价”活动泄露出去的。

太原反诈中心提示:微信“帮砍价”活动,起初只用于营销。后因成本低、操作简单,被不法分子盯上,用于收集个人信息和骗钱,演变成了一种新型骗局。受骗者会收到大量广告短信和诈骗短信。至于所砍价的“低价商品”,起初找朋友砍一次,都是砍掉几十上百元,而到了后面,一次只能砍掉几分钱,几乎是没法拿到的。而一些不法分子甚至将朋友圈的嵌入式广告,链接至钓鱼网站。广大市民需对类似的朋友圈发布的砍价赢大奖的营销保持警惕,切勿轻易填写个人信息,特别是敏感信息。一旦被骗,一定要保存好聊天记录、转账汇款凭证,并及时拨打110报警。

(辛戈)

据《山西晚报》