

号称“低息贷款” 仿冒金融平台

打击虚假网贷App多方综合治理是关键



资料图片

虚假网贷诈骗防不胜防

“我们已经为你准备了40万贷款的额度，请注意查收”“无抵押，低利率，快放……”瞄准一些人“用钱心切”的心理，不法分子在网络上大量发布“黑户可贷”“秒审核”等广告信息，吸引用户上钩。

记者随机进入一个名为“黑户贷”的网站，该网站声称，“1分钟提交、3分钟到账，不用房车作抵押贷款、从25岁到50岁适用。无视黑白，百分百放款”。在网站

记者调查发现，近年来，诈骗犯罪分子变换作案手法，网贷诈骗 App 打擦边迭代更新，欺骗性更强。

——假借知名企业名头行骗。

诈骗分子仿冒京东金融、马上金融、借条等平台，推出大量“李鬼”式，以相似标志和产品介绍以假乱真，以“返利”等诱导网民访问下载，进而实施诈骗。平安银行曾发布声明，不法分子利用假冒 App、网站进行贷款诈骗。

家住福建福州的林先生就曾在自称“宜富有限公司郑州分公司”开发的宜人财富pp上被骗4000元解冻金。当他向“宜富”投诉，该公司回应称，其官方工作不会以任何名义收取费用，林先生遭遇冒网贷App诈骗。

值得注意的是，目前，涉诈金融类 App

引导下，记者留下电话号码，随即该网站弹出一款贷款 App，无需经应用商店即可点击下载。

“这些号码均是诈骗电话，切记不要下载软件，不要相信任何先支付后打款的承诺。”在记者暗访涉网贷 App 的过程中，民警通过电话多次发出预警，提醒记者存在被骗风险。

据公安部统计, 2021 年以来, 60%以上

“李鬼”式App迭代更新快

改头换面频繁。同一团伙往往通过更换涉诈App名称、域名等方式快速更新换代，有的可能仅存活几天就关闭，过段时间换个名字卷土重来。

——通过网站封装躲避审核。

记者调查发现,不少受害者根据“指引”下载的涉诈金融类 App 都是由黑灰产技术人员按照诈骗分子要求封装的。所谓封装,是将网址、应用名、LOGO、启动图打包形成一个 App 应用包,使网站以 App 形式呈现。

业内人士介绍，涉诈贷款网站经过封装，摇身一变成为涉诈贷款 App，成本极低，令人防不胜防。此前，一款名为“众安”的虚假贷款类诈骗 App，就是由一个租用境外服务器的虚假贷款网站封装而来。

中国信通院安全研究所防范治理电信网

的诈骗都是通过虚假手机 App 实施。其中，虚假网络贷款 App 诈骗是主要类型之一。

中国人民公安大学治安学院副教授李小波介绍，虚假网贷诈骗中，犯罪嫌疑人一般通过网络、电话、短信等方式发布办理贷款的广告信息，在被害人下载安装网贷App后，冒充银行、贷款公司工作人员联系被害人，以收取手续费、缴纳年息、保证金、税款、代办费等为由，诱骗被害人转账汇款。

络诈骗中心副主任常雯说，通过 App 封装分发平台，开发者只需简单点击操作，即可实现 App 自动生成与快速分发。涉诈 App 不上架手机系统内的应用商城，由诈骗者向被害人发送安装包或者链接进行下载，躲避应用风险审核及开发者信息登记制度。

——多方引流大量分发。

虚假网贷 App 的引流方式，既有搭建虚假贷款网站等待被害人上钩，也有通过电话、短信、微信群、QQ 群等多种渠道进行推广；既有面对不特定群体进行广撒网的，也有通过黑灰产业链条非法购买需贷款人员信息精准诈骗的。

山东警方介绍，诈骗分子还通过冒充快递员推广、在“宝妈群”发兼职广告、贴吧发广告等方式引流，渠道更多、频率更高、活跃度更强。

加强对广告客户、流量购买者的金融资质审核，杜绝传播虚假信息。

国家网信办有关负责同志指出，诈骗分子假冒投资平台诱导欺诈网民，让网民遭受严重的财产损失，还可能带来个人信息泄露，应引起足够关注。广大群众需通过官方正规渠道下载 App；出现非官方客服联系的情况，要注意核查对方身份，切勿进行转账操作。App 商店等平台应加强对可供下载 App 的安全性审核，防止虚假 App 浑水摸鱼，坑害广大网民。

热门网贷平台 不容“李鬼”缠身

7月1日，国家网信办公布了一批“李鬼”式投资诈骗平台，不法分子通过仿冒APP进行诈骗活动。

在公布的名单中,排名前十位的被仿冒 APP 名称依次为京东金融、有钱花、拍拍贷、马上金融、360 借条、宜人贷借款、海尔消费金融、平安好贷、易开花、东方财富。其中,已发现打击仿冒京东商城 APP 达 5677 个,仿冒度小满旗下的信贷平台有钱花和已在纽交所上市的金融科技拍拍贷 APP 的数量均超 1000 个。

看看这份名单，几乎时下市场上热门网贷平台都有“李鬼”缠身，令人防不胜防。

骗术并不怎么高明，诈骗分子通过相似标志和产品介绍以假乱真，以“小额返利”等诱导网民进行访问下载，进而实施诈骗。手段也很老套，与传统电信诈骗思路一致，即向用户表明需要通过资金验证或缴纳保证金，以此来骗取钱财。

从表面上看，只要用户严格一点，认真一点，谨慎一点，不该点的链接别点，下载时求证一下，都能避免。虽说用户是第一责任人，自己要擦亮眼睛，提高个人警惕，这些都没错，可是除此之外更要问用户谁是帮凶，假冒 APP 是如何通过手机应用商店进入到用户的手机里的。

现在基本上每一个手机品牌都有自己的应用商店，这里面存在良莠之分，有些品牌的手机对上架 APP 审核非常严格，基本上不会碰到类似问题，而有些则相对随意了。

类似的乱象我们在医疗行业也可以看到，一搜索某某疑难杂症，正牌的知名医院看不到，各种大鬼小鬼接踵而至。

李鬼式投资诈骗平台也是一样的套路，给用户识别真假增加了难度。大家为什么从应用商店下载，一个重要原因是相信手机应用商店会把好第一道关。如果要防着假冒APP，还要防着应用商店也会出问题，那这样的生态环境实在太不好了。这跟我们网上购物翻看好评差评，查看商品销量，冲着好评和销量而去，结果发现数据也会造假；或者我们去品牌商店购买绿色农产品，结果发现正规商店也会售假是一样的。

打鬼不能光指望个人炼就火眼金睛，每个人也不可能成为行业专家。互联网是个整体，信任来自于每个环节坚守自己的责任，一个环节没做好，可能导致其后很多环节都出现问题。在这方面，手机厂商真应该跟做得比较好的品牌好好学一学，手机品牌的竞争比的不光是硬件，更是软件和服务，每起类似案件的发生，侵蚀的都是品牌的影响力。你觉得没关系，其实关系大了去了。

(来源：新华社、钱江晚报)



资料图片