

公安部刑侦局详解:你是如何被诈骗团伙盯上的?

央视网消息:据公安部刑侦局公众号消息,电信网络诈骗大致可分为三个环节:引流环节、诈骗环节、洗钱环节。

首先开始的“引流环节”,通俗的讲,就是诈骗团伙在海选目标,可能我们只是接到一个电话、收到一个快递、点开一条短信,还没有来得及反应发生了什么,就已经掉入了骗子精心设计的陷阱。

这并不是危言耸听,引流的手段千变万化,比如:利用境外电话或者伪装电话假冒身份,发送虚假短信诱导点击不明链接,在街头街头扫码送奖品、通过物流寄送陌生快递诱导你扫描不明二维码,直播间内诱导你私信联系还有发送病毒木马邮件等等。

引流手段的迷惑性很强,是大家接触到电信网络诈骗的第一关,但它并不是无法破解的,如果我们在遇到高风险行为时提高警惕,就能避免掉入圈套,在源头上大大降低我们被骗的几率。

总结起来,常见的引流手段为三类:一是电话、短信引流;二是线上网络渠道引流;三是线下实体渠道引流,为你详细拆解常见的引流手段。

01 电话、短信引流

1、电话、短信中遇到这五类号码一定要谨慎,否则您的财产安全很有可能亮红灯!

95 开头的号码,一般为金融、航空、通信等企业的客服电话,如果接到95 开头并且超过8 位数的电话,可能为境外改号的诈骗电话。

00 或者+号开头的都是境外电话,如果您没有与境外电话联络的需求,并且接到了此类电话,大概率为诈骗电话,请直接挂断。

400 开头的电话号码为企业客服电话,此类号码一般不能外拨,如接到400 开头电话,不是诈骗就是推销。

106 开头的短信端口类号码,这类号码通常会给不同用户批量发送短信,短信中可能会包含一个链接,一旦点击就可能会让你的手机被病毒入侵,个人信息和财产都有可能被不法分子盗取。

显示未知的电话号码,身份和所在地都不显示,遇到这类电话直接挂断。

除了这五类电话、短信外,平时我们接到普通号码的陌生来电也不能掉以轻心。因为,随着我们打击的不断深入,骗子也在更新引流手段。他们利用GOIP 和 VOIP 设备远程控制电话卡

拨打电话、收发信息,将境外电话号码转换成境内的号码。一般人看到是境内电话就降低了戒备心,很容易上当受骗。

2、警惕“高仿”短信中的钓鱼链接 诈骗分子会根据官方短信提醒、广告信息的话术形式,制作仿冒短信,常见的有的 ETC 已停用,今日内点击XXX 链接认证;您的积分需要马上兑换否则清零;医保卡异常锁定,48 小时未处理将作废;航班取消!立即联系400-XXX 改签理赔等等。

这些短信的目的就是诱导大家点击短信中的链接,这个链接本身可能就是木马病毒,或者是诱导你下载诈骗APP,也有可能让你进入一个仿冒官方的网页,甚至远程操控你的手机,最终目的是通过各种方式获取你的通讯录,诱导你填写银行账户、密码、身份证号等个人信息,进而实施诈骗。

防范这一类引流短信,就要牢记一句话“未知链接不点击”。

02

线上网络渠道引流

诈骗分子会在社交平台以及网络直播间中,发布投资理财课程、无门槛兼职、高薪赴境外工作等内容的视频。在获得受害人关注后,诈骗分子会在评论区或者直播弹幕中发布“想了解更多,私信联系客服”等评论,引诱受害人越过官方平台加入所谓的“投资指导群”“配音群”“兼职群”“课程群”,进而实施诈骗。这种引流手段更具有迷惑性,有些甚至会铺垫几个月的时间,当你放松警惕之后才实施诈骗。不要轻信社交平台中短视频发布的内容。

03

警惕这五类号码!

95开头的号码
00或+号开头的境外电话
400开头的企业客服号码
106开头的短信端口类号码
显示未知的电话号码

提高警惕,谨防诈骗

提防“数据刺客”窃密:送货上门、刷脸支付均要警惕

央视网消息:据国家安全教育部微信公众号消息,当前,数字化浪潮席卷全球,电子零售新业态蓬勃发展,只需使用手机线上选物下单,通过人脸识别完成支付验证,就能获得商品送货上门、即买即用等服务,使日常生活更加高效便捷。消费者在享受便利的同时,也应提高安全防范意识,提防“数据刺客”暗中窃密的多重手段。

安全隐患需留心

——寄送定位关联点位画像。通过APP、小程序等渠道,由手机下单将物品配送到指定位置的服务正逐渐流行。然而,部分线上商超在提供配送服务时,为获取买家的精确配送位置,可能会在配送地图上自动标注出一些敏感区域和点位,并根据消费频次、商品偏好、社交图谱等信息进行关联分析,形成该地区或点位的用户画像。这些看似普通、用于正常经营的信息数据,一旦被窃取,可能成为境外间谍情报机关或个别别有用心之人进行窃密渗透、技术攻击等不法行为的突破口。——刷脸支付窃取生物信息。随

处可见的自动贩卖机,可通过扫码、“刷脸”等方式购买商品,即买即取、操作简便。然而,此类设备通常搭载录音录像、生物识别模块,并配置有动态人脸识别、红外成像等技术,能够采集周边往来人员面部特征和使用者的虹膜纹路等生物识别信息。个别设备开启刷脸功能获取人脸数据后,还会进一步要求用户提供手机号、性别、出生年月等个人信息隐私信息,若其后台连接的信息系统存在安全漏洞,可能被攻击者入侵,进而引发数据泄露风险。

筑牢数据安全防线

电子零售行业的快速发展让便利生活触手可及,但面对其中潜在的风险隐患,我们应当提高警惕,自觉筑牢安全防线,对埋伏其中的“数据刺客”“见招拆招”,悉心守护数据隐私和国家安全。

——对合法经营划底线。电子零售行业从业者要时刻以规章制度为底线,明确数据采集的合法边界,杜绝以用户授权、促销需要为名过度收集地理位置、生物特征等敏感信息,严禁将

用户数据信息用于非必要场景。同时,要提升技术防护能力,定期开展数据安全审查,防止数据被截取或植入后门程序。

——对可疑要求说拒绝。消费者在租赁、购买电子零售产品时,要增强隐私保护意识,对于产品供应方提出的不合理要求,如过度采集生物特征信息等,以及含有“信任此设备”“开启USB 调试”等内容的可能授权提示时,应当谨慎操作。

——对敏感数据多留心。要强化对数据安全的敏感性,面对日常生活中一些看似寻常的数据信息,如分布于重要点位周边的坐标指向、人员分布、面部信息等,都应引起高度重视,从源头消除危害数据安全的风险隐患。

广大人民群众在进行电子零售商品的租赁购买时,如遇到可能危害国家安全的情况,可通过12339 国家安全机关举报电话、网络举报平台(www.12339.gov.cn)、国家安全教育部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。(来源:央视网)

车辆停放路边被撞 为何要承担次要责任?

近日,南京江宁区大队执勤二中队接到一起12345 工单。市民张某反映自己的车停着没动被撞了,还被交警认定承担次要责任,自己十分不解,要求判定对方全责。

执勤二中队交警调查后得知,当时张某驾车前往通淮街买早餐。因路边停车位已满,张某便将车临时停在了马路上。不料,后方的王某驾车从张某的车左侧经过,一时大意,未控制好距离,两车发生碰撞事故。经交警现

场勘察,王某在未保证安全情况下通行,需要承担责任。

不过,张某的车停放在马路上,占据了大半幅路面,影响车辆正常通行。因此,张某的车辆未按规定停放也是导致事故发生的原因之一,所以需承担次要责任。交警告知,该起事故责任判定没有问题。后经解释沟通,最终张某对事故责任认定表示认可。

(来源:扬子晚报)

电动自行车私改强光灯害人害己

让“小改装”不再成为“大隐患”,治理还需多管齐下。要完善制度规范,强化源头监管,软性引导与基础设施保障也不可忽视

“电动车这灯比大车远光灯都亮,太晃眼了!”“电动车的灯有必要这么亮吗?眼睛缓了好久才恢复过来。”近日,不少人在社交平台吐槽,部分电动自行车私自改装、加装强光灯,刺眼到让人不得不躲避视线。看似不起眼的“小改装”,正成为影响交通安全的“大隐患”。

表面上,改装强光灯让骑车人“看得更远”,实际上却在增加风险。超强灯光容易让对向司机和行人产生短则几秒、长则数十秒的视觉空白,难以看清前方路况,无法对安全距离、方向速度等作出准确判断,极易导致事故发生。老年人或眼疾患者受强光刺激后恢复更慢,甚至可能造成眼部损伤。更值得警惕的是,这类强光灯本身也暗藏风险。公安部道路交通安全研究中心调查显示,市面上大量产品缺乏质量保证,“买来就装、装上就亮”,但电路设计、光束控制、防水防尘等均不过关,容易出现短路、自燃等情况,加之部分车主改装方式粗糙——有的用螺丝随便固定,甚至靠魔术贴粘贴,长期行驶中不利于车体安全,看似一时方便,实则害人害己。

为何私自改装强光灯现象屡禁不止?在不少车主的认知里,一些道路照明条件不足,夜间视野受限。原本在规定限速内,原厂车灯即可满足照明需求,但部分车主在道路上超速行驶,试图通过改装来增强照明,忽视了其中的风险。此外,电动自行车改装渠道多、价格低,车主很容易就能在销售店或维修店内完成改装。网络教程触手可及,也降低了亲自动手的门槛,不少车主自己就能完成简单的改装。这背后折射的,不仅是个别车主的侥幸心理,更是监管环节的漏洞。

事实上,《中华人民共和国道路交通安全法》明确规定,驾驶非机动车在道路上行驶应当遵守有关交通安全的规定。但现实中,电动自行车保有量大、分布广,执法力量有限;违法成本较低,难以形成威慑;相关法律法规较为模糊,电动自行车技术指标无强制性标准,依赖于各地出台的规范性文件……种种因素,让监管难以落细落实。近年来,针对电动自行车私自改装强光灯乱象,不少地方出台细则,比如《上海市非机动车安全管理条例》规定,禁止销售或驾驶拼装、加装、改装的非机动车;《南昌市电动自行车管理条例》也明确,不得实施在电动自行车上安装高分贝喇叭音响或者高强度照明灯等影响交通安全的行为。北京、上海等地交管部门开展夜查行动,重点排查电动自行车加装、改装灯光情况,强化查处力度,发现后责令现场拆除。

要让“小改装”不再成为“大隐患”,治理还需多管齐下。一方面,完善制度规范,在国家层面明确标准,细化电动自行车技术指标,各地根据实际情况制定规范性文件,约束改装行为,让交管部门执法有规可依;同时,强化源头监管,从销售商、维修门店、电商平台等入手,市场监管部门与交管部门协同,既查路面,也查渠道,对违规经营主体依法处罚,堵住私自改装流通渠道。另一方面,软性引导与基础设施保障也不可忽视,普及“强光不等于安全”的常识,让更多车主意识到私自改装车灯的危害;聚焦“照明盲区”,补齐道路照明短板,确保城乡道路夜间可视性。

电动自行车强光灯治理,关乎千家万户出行安全,交通安全不是比谁的灯更亮,而是靠交通参与者共同遵守规则,维护秩序。改装有禁区,执法有标准、观念有转变,才能让夜间道路明亮而不刺眼,给城市交通添一份安心。(来源:人民日报)