

【编者按】

在我们的刻板印象中,农村居民、青少年、老年人等群体是易受骗人群,而“脑子新”、警惕性强的年轻人相对不容易受骗。但一代人有一代人的“反诈盲区”,电信网络诈骗手法迭代翻新、隐蔽性更强,有些诈骗分子就是利用“灯下黑”谋取不法之财。面对诈骗别大意,我们一定要持续增强防骗、识骗、拒骗意识。

一代人有一代人的“反诈盲区”

一大学生好心帮填问卷却落入骗子圈套,网友:几乎没有大学生会怀疑调查问卷

近日,大学生小萧(化名)反映,在收到游戏中认识的网友发来的“调查问卷链接”后,自己好心帮其填写,结果手机相册和通讯录等个人隐私信息被盗,对方利用其手机相册里的自拍照合成不雅照片,进行敲诈勒索。

填调查问卷,手机被植入木马程序

据扬子晚报报道,小萧回忆,与常见的扫码填写不同,该问卷以网页链接形式发送,且进入页面需要输入对方提供的专属邀请码。出于对“朋友”的信任,小萧按照提示进行了操作。

在点击链接后,小萧手机相册、通讯录等个人隐私数据遭到窃取。对方获取信息后,利用小萧相册中的正常自拍照,通过图像处理技术伪造了多张裸照及床照,并以此作为筹码,威胁小萧转账,声称如果不配合操作,他会将这些伪造的“照片”发送给其通讯录中的所有联系人。

意识到遭遇敲诈勒索后,小萧第一时间删除了恶意链接,清理手机后台程序,并向警方报案。在警方的建议下,小萧向亲友发送了消息,提醒他们注意防范诈骗。“整个过程惊心动魄,大家一定要引以为戒!”

该事件在网络上引发热议,有网友评论:“天哪,几乎没有大学生会怀疑调查问卷。”还有网友说:“收到问卷后,大学生从头到尾检查了一遍——确认自己没有填错。”

一名曾处理过类似案件的民警介绍,应该是小萧点击链接和输入专属邀请码时,手机被植入了木马程序,然后对方通过屏幕共享的方式窃取了小萧手机里的通讯录和隐私照片。“嫌疑人对照片进行P图后,往往会通过彩信的方式发给当事人,索要钱财。”

公安部提醒大学生要注意这两类诈骗

此前,公安部曾发布针对学生群体的暑期防范电信网络诈骗安全提示。其中,针对大学生群体的,主要是刷单返利、虚假购物服务类诈骗。

刷单返利类诈骗主要针对大学生的兼职需求。诈骗分子先是发布兼职广告招募“点赞员”“推广员”等,或以免费技能培训为幌子将受害人拉入群聊。随后,诱导受害人完成刷单、关注公众号以及为短视频点赞、评论、刷粉丝等任务,通过发放小额佣金获取受害人信任。再以“充值越多,抢单越多,返利越多”为诱饵引导其下载诈骗App做“进阶任务”。最后,以“任务未完成”“卡单”“操作异常”“账户被冻结”等各种借口诱骗受害人不断投入钱款,进而实施诈骗。

虚假购物服务类诈骗主要针对大



诈骗,大学生

#大学生

事情经过如下:

今日晚上,我收到一位朋友的信息,想让我帮忙填写一份问卷调查,因为想着大学生互帮互助原则...就没多想。结果给我一个链接,然后还有访问邀请码,然后按照他发的邀请码进入,结果我的个人信息,包括手机相册,通讯录联系人等等被全部盗



小强 贵州 23小时前

天哪,几乎没有大学生会怀疑调查问卷



作者赞过

拾柒 北京 23小时前

关键是出了这种事以后让我们大学生怎么做调查问卷🙄

3条回复▼



视界A的平行... 河南 23小时前

真可恶,就这样利用别人的善良

近日,有大学生在网上发布自己被骗的经过。

组图/网络截图

“同学你好,请问你能点一下这个调查问卷吗?”

诈骗网站
学术调查问卷

等一下,不对劲!

……(难道暴露了)

这个问卷只能单选吗?



图/AI生成

深夜手机自己“动”了,银行卡莫名被扣几万元

警惕这些新型小众骗局

据媒体报道,7月21日,湖北省公安厅公布一批新型小众骗局典型案例,涵盖静默盗刷、文旅退税、征信诈骗等剧本,迷惑性极强。

装个App,熟睡时被盗刷近6万元

黄先生遇到的是目前十分冷门却极度危险的骗局。前段时间,黄先生因旧手机卡顿,在浏览器广告里下载了一款未上架应用商店的清理类App。“安装时我习惯性一路点‘允许’,软件也确实完成了垃圾清理,我就没放在心上。”

然而,令黄先生没想到的是,随手授权的无障碍权限,竟给骗子开了“后门”。深夜熟睡时,诈骗分子通过植入的木马远程操控手机,无需密码和验证码,在后台完成了多笔转账,全程没有任何弹窗提醒。

万幸的是,他的妻子半夜发现手机无故亮屏,核查后发现近6万元被盗。二人在被盗刷1小时内火速报警,警方紧急止付,最终全额追回损失。民警告诉他,再晚1小时,钱就很难追回了。

骗子报出消费记录,假装“退税”

另一位吴先生的经历,则戳中了很多出游人群的信息盲区。他接到一通自称是“文旅总局回访专线”的电话,对方准确报出了他一年前在景区买进口伴手礼的消费记录,时间、门店、金额、实名信息全部吻合,这瞬间打消了他大半的防备。

对方称吴先生所购物品符合跨境商品退税政策,除全额返款外还能领到3200元补贴,因是景区专项补贴,只能加私人微信走内部通道。

后续对方还发来带公章的文件、仿

冒官网链接,并要求吴先生填写完整银行卡信息,开启屏幕共享“核验余额”。

就在授权前一秒,他想起了社区民警的宣讲内容,立刻停手,挂断电话,先后登录文旅局官网,拨打12366税务热线和110反诈专线,三方均证实无此政策。此时微信那头还在施压——“限时2小时,逾期取消终身资格”,甚至发来伪造的失信告知书,吴先生果断拉黑,保住了卡里的8万元。

慎开“屏幕共享”等高危权限

以下三人遇到的骗局也极具迷惑性。

李先生接到冒充征信中心的电话,对方用“账户冻结、影响征信”制造恐慌,诱导他加QQ、开屏幕共享核验身份。他想到“官方不会私下办案”,立刻核实,成功识破骗局。

王先生接到境外售后电话,对方能报出完整订单信息,以“商品超标双倍赔付”为由,诱导他下载陌生软件打开投屏。他迅速联系官方客服核实,保住了卡里的12万元积蓄。

袁先生在二手平台卖手机,收到“客服”消息称订单冻结需缴保证金。他留了个心眼上网查证,发现是典型骗局,联系真客服举报后,未受损失。

公安机关提醒:请务必通过手机自带的应用市场下载软件,切勿点击浏览器弹窗广告或陌生链接下载安装包;对于“无障碍服务”“屏幕共享”“辅助功能”等高危权限要高度警惕,非必要不授权。一旦发现不明软件索要此类权限,立即拒绝并卸载;定期检查手机已安装的应用列表,发现陌生、可疑软件立即删除。

(新华社)