

学生暑期玩手机易被电信诈骗“围剿”

如何预防？且听大家怎么说

本报记者 岳端 实习生 曾继涛

暑假,由于学生能长时间“触网”,而且判断能力弱,电信诈骗分子将目光瞄向这一群体,诈骗手法经过精心包装不断翻新,让家长、学生防不胜防。电信网络诈骗都有哪些形式?家长和学生们又该如何预防?记者对此进行了采访。

网络诈骗进入“暑期档” 购买游戏装备要当心

最近,贵阳市的一名家长邱晓斌(化名)有些心烦——10岁的儿子正在放暑假,每天都要用他的手机刷一会短视频,结果被一条免费赠送“蛋仔派对”游戏币的视频吸引,在添加陌生人为微信好友后,被诈骗了1万余元。日前,邱晓斌已经报了警。

另一名来自贵阳的家长张媛(化名)的孩子也因使用家长手机玩“吃鸡”游戏时,结识了一名自称能低价出售皮肤的陌生网友,在购买皮肤的过程中被盗刷了5000多元。

近日,贵阳市公安局观山湖分局涉网违法犯罪侦防中心介绍,暑期以来,公安机关监测到的游戏产品交易类诈骗增多,像邱晓斌、张媛这样有类似遭遇的家长不少,目前已经监测到多起与“蛋仔派对”等游戏有关的电信诈骗案件,一个街道甚至在同一时期内发生了好几起。

“诈骗分子利用现在青少年中时兴的游戏IP为诱饵,通过在短视频平台投放免费赠送或购买皮肤、账号等内容的视频,引诱孩子上网,一旦诱导孩子添加好友,就是骗局的开始。”观山湖分局涉网违法犯罪侦防中心民警蒋玉婕告诉记者,每年暑假,他们都会遇到比平时更多类似的案子,并且绝大部分都始于刷短视频。

“小屏时代,短视频成为孩子们获取信息的主要渠道之一,诈骗分子也盯上这一趋势,在潜在受害人集中的短视频平台‘广撒网’。”蒋玉婕说。

“两卡”不出借 大学生暑期“触网”也需谨慎

除了中小学生学习游戏装备受骗外,大学生也会因为找工作等需求误入诈骗陷阱。暑期以来,大学生找工作、找兼职、安排娱乐活动需求旺盛,也让诈骗分子钻了空子。

相比中小学生学习,大学生更易遭受的网络诈骗类型主要集中在刷单诈骗、虚拟购物、高考招生诈骗等,其中虚拟购物诈骗可能使用的“诱饵”包括买游戏皮肤、漫画门票、演唱会门票等。

在大家防范网络诈骗意识普遍更高的情况下,骗子们也会想方设法对骗局进行包装,出其不意地抛出诱饵。

今年7月,在贵阳读书的毕业生小赵(化名)通过正规网站发布的招聘信息找到一份工作,公司证照齐全,各种手续完善,并承诺交纳五险一金,乍一看是份完美的工作。但小赵入职后,公司便开始以各种理由要求她刷单,刚开始是几十块,后来是几百块、几千块,让小赵渐渐起了疑心并报警。后经警方调查,这正是一种经过精心包装的刷单诈骗。

“一方面大学生找工作的需求比较迫切,另一方面他们会觉得自己已经长大具备判断能力,因而对反诈宣传比较抵触,导致大学生受骗的案件较多。”民警表示,作案手法不断翻新层出不穷,无论处于什么年龄阶段,都应该多学习反诈知识,在心里建起一道“心防”。

在一些案例中,诈骗分子在添加好友后会引导孩子下载共享屏幕APP,要求其打开共享屏幕功能并进行转账操作,通过共享可以马上看到孩子收到的验证码,还没等孩子反应过来就把卡里的钱转走了。

而在话术上,也有相似之处,“利诱+威逼”是最常见的套路。蒋玉婕介绍,首先是通过“免费”、“赠送”等字眼引诱孩子上当,再利用孩子年幼、心理不成熟、判断能力差的弱点恐吓他们,例如,在孩子领取礼物后,诈骗分子会谎称公司资金被冻结,让其配合操作,不然就抓捕其父母等。

在民警接处的案件中,还有诈骗分子冒充公检法人员称“如果不配合,就将其送上法院”,出于害怕,孩子被迫进行付款、转账等操作。这类网络诈骗呈现出针对性强、伪装性强、隐蔽性强等特点,在完成诈骗后还以哄骗、恐吓等方式要求孩子删除联系方式,使家长短时间内难以察觉,造成难以挽回的经济损失。

在观山湖分局涉网违法犯罪侦防中心监测到的案例中,近两个月来中小学生学习因类似手法受骗的金额最高达到2万余元,转账次数最多的达到57笔。

对此,警方提示,购买游戏装备一定要通过正规平台,切勿听信“免费、低价”等谎言,不轻信陌生人及网络游戏中的中奖信息或赠送信息,不私下添加对方的微信等社交账号,不随意点击陌生链接,不扫来历不明的二维码。

此外,民警还提示,8月底将进入准备开学物品的集中网购时段,也是网络诈骗高发期。“比如‘扫码领奖’广告,当受害人扫码后,诈骗分子先会予以小利获取信任,再引诱受害人下载指定APP,以‘刷单返利’为由将其引入刷单骗局。”民警说,遇到这样的广告要留个心眼。

一些诈骗的发生是因为防范意识不强,而另一些诈骗的发生则是因为法律意识的淡薄。

“GOIP”和跑分是近年来出现的新颖诈骗手法。通过“GOIP”这种硬件设备,能将传统电话信号转化为网络信号,犯罪分子在境外通过国内的“GOIP”设备远程控制国内的电话卡实施诈骗,以逃避打击。跑分则是利用银行账户或第三方支付平台账户为他人代收收款,再转账到指定账户,从中赚取佣金的洗钱行为。

目前,这两种犯罪手法已有盯上学生的苗头。“通过‘高薪兼职’‘高价收购’等噱头哄骗青少年出租、出借银行卡、电话卡,很多学生并不了解,这种做法即使不直接参与,也已经属于犯罪。”

采访过程中,警方呼吁关注未成年入出借“两卡”现象,希望家长们在平常生活中能加强对孩子管理好“两卡”的教育。



打卡拍照反诈宣传发个圈扩大影响力。



民警进校园发放反诈宣传资料。



在贵州开放大学设立反诈宣传展台。



开展共建无诈校园活动。

众家长的反诈方法

电信诈骗诈骗无孔不入、防不胜防,在诈骗分子盯上未成年人的同时,暑期是否让孩子玩手机?如何控制用手机的时间?怎样降低被骗风险?家长们各抒己见——

单机游戏 限制玩

“信息爆炸的时代,孩子们接收到的信息是过去的几百倍、几千倍,网上的东西鱼龙混杂难以分辨,稍不注意就可能被不法分子钻了空子。”贵阳市民董女士有一个8岁的儿子,因为经常接触到类似的诈骗案例,董小姐的反诈意识特别强,“不会让他接触到手机,短视频更不准刷。”

但堵不如疏,为满足儿子玩游戏的愿望,董小姐还是会让孩子玩switch等功能单纯的游戏机,每天规定1小时的游戏时间。

眼皮底下 监控玩

也有一部分家长认为完全不给孩子玩手机是不可能的事。“毕竟孩子通过手机也能拓宽视野,了解一些大人无法解答的问题。”贵阳市民高小姐说,所以她每天会给孩子规定1小时使用手机的时间,但是在这段时间内,她会守在孩子的身边,时不时瞟一眼孩子在看什么内容,没有和陌生人聊天等。

北京芳草草地国际学校贵阳分校的一家家长称,暑期孩子在使用手机的过程中接到一名自称是保险公司的客服赠送保险,这个电话会一步步引导接听者关注微信公众号,输入账号等操作。“幸好我就在旁边,孩子立刻就把手手机给我了。”

设置拦截 警惕玩

除此之外,还有家长通过设置付款拦截、电话拦截、青少年模式等方式减少孩子使用手机消费、充值的情况。贵阳四十二中的一位家长表示,游戏在青少年当中越来越流行,因此周边的家长都普遍关注暑期游戏充值诈骗的行为,希望学校、社区能加强对青少年的宣传教育,游戏公司能设置充值金额限制,防止青少年上当受骗。

社会共同反诈

还有一名家长表达了对短视频平台的期望:“希望短视频平台能够收紧对内容的审核,尤其是小孩感兴趣的游戏、动漫等内容,更多地考虑到可能造成的社会后果。”

家长们也普遍表示,能够感受到学校、社区、警方都在努力营造一种反诈氛围,例如周边张贴的反诈宣传广告,要求下载国家反诈中心APP,接到警方打来的预警电话等。

游戏公司已有回应

事实上,针对孩子暑期上网安全问题,企业也作了相应举动。今年暑期,网易游戏发布“2024年暑期未成年人游戏限玩日历”,并同步启动“暑期未成年人保护专项行动”,联合第三方平台,严厉打击游戏黑产和游戏域外诈骗,保护未成年人的合法权益。今年以来网易游戏通过举报和申诉,已封禁近万个游戏域外涉诈直播间、短视频、QQ群。

支付宝也于几年前推出对风险交易进行15分钟拦截保护或提供24小时延时到账功能,用户一旦发现被诈骗,转账24小时内向警方报案后,可在支付宝申请撤回交易,尽量避免资金损失。

暑期接近尾声,但防范网络诈骗还需久久为功。民警提示,家长应及时下载国家反诈中心APP或各辖区推出的反诈预警系统,加强对孩子的反诈宣传教育,密切关注孩子的上网情况,不要将银行卡、支付宝等密码透露给孩子,或给孩子使用未绑定付款账户的手机,谨防上当受骗。一旦发现被骗,立即报警。