开学季 这些诈骗套路需警惕

眼下正值开学季,学生们即将开始新学期的忙碌,殊不知诈骗分子也蠢蠢欲动,针对不同年龄段的人群“因人施骗”,令人防不胜防。家长、学生以及老师一定要注意防范,防止上当受骗。

班级群收费骗局

骗子潜入家长微信群或QQ群,冒充班主任实施诈骗的事件层出不穷。这些骗子或以预收学费的名义,或称学校开设补习班,要求收取补习费用……由于其头像和昵称设置得与老师的相同,发布的内容和平时教育行政部门下发通知高度相似,部分家长信以为真,导致被骗。此类骗局有这4个套路:

套路一:广撒网、搜索QQ群

诈骗分子会在QQ内搜索班级群关键字,搜索到群后再冒充老师、家长等申请加入,如果没有设置相应的验证机制或者班主任验证不严格,骗子就容易趁虚而入。

套路二:套近乎、获取进群二维码

有不法分子在校园门口逗留,与其他家长闲聊、套近乎,向家长索要班级群的二维码。由于很多群并未开启“群主确认”功能,不法分子可直接扫码进群。

套路三:换头像、伺机行动

骗子进群后,伪装成学生家长添加班主任QQ/微信,通常会备注为“xxx学生父亲/母亲”,“潜水”观察班主任的活动规律,找机会将自己的头像换成班主任头像,并将自己的备注名改为和班主任一模一样,然后在群里发送相关通知,要求缴纳学费、培训费等各项费用。

套路四:利用时间差,实施诈骗

由于职业的特殊性,很多老师都开了消息免打扰功能,或者在上课期间关闭手机,不法分子利用时间差借机下手,让真老师不能及时发现,进而实施诈骗。

学费住宿费诈骗

骗子冒充学校职能部门工作人员,向学生发布链接或二维码等缴纳学费、住宿费的通知。

奖学金诈骗

骗子冒充高校老师或资助机构人员,以电话、短信或邮件等方式告知学生发放奖学金、助学贷款资金。要求学生提供银行卡号、密码等信息,从而转走账户余额,或指令学生在ATM自助取款机上进入英文界面操作,进而转走卡内钱款。

“伪装推销”诈骗

伪装学长或学姐推销是新生经常遇到的骗局,如:推销电话卡(没有售后保证,骗取身份证等重要信息用于电信诈骗);推销生活用品,如被褥等(可能是假冒伪劣产品);忽悠新生买“打折”辅导资料、健身卡等。骗子所推销的物品多与新生的学习、生活息息相关,新生辨别是非的能力尚浅,不好意思拒绝从而上当受骗。

注销“校园贷”诈骗

骗子冒充网贷、互联网金融平台工作人员,称学生之前开通过校园贷、助学贷等,再以不符合当前政策,需要清除校园贷记录或者校园贷账号异常需要注销,如不注销会影响个人征信等为由,骗取学生的信任。然后诱骗学生贷款,并转至其提供的账户上,从而骗取钱财。

提醒

- 班主任应及时对本班的群成员身份进行核查,对身份存疑的账号要尽快清除出群。启动入群验证功能,避免陌生人随意加入班级QQ群、微信群,验证时要对相关信息再次核实。
- 家长不要随意向他人透露微信群、QQ群的群名称和二维码等信息,保存好班主任老师的电话,了解学校的收费政策和流程,切勿轻信群成员要求转账收费的信息。
- 如果遇到自称老师的人员要求转账或是索要银行账号、密码等情况,家长应及时与老师和学校核实,不可盲目转账汇款或是透露个人重要信息。
- 要妥善处理填写有个人信息的单据票证,身份证复印件表明用途,在网络社交过程中不透露个人信息。
- 奖助学金发放等官方行为都有官方通知渠道与规定程序,不会通过电话、短信、微信等方式联系个人要求提供信息,更不需要缴纳手续费、保证金等任何费用。相关部门不存在所谓安全账户,更不会引导转账。
- 面对陌生人的热心要时刻保持警惕,手机、钱包、银行卡、证件、录取通知书等重要物品一定要随身保管携带。

本报综合

收到自己的“不雅照”?截图保存 马上报警

试想一下,假如你突然收到一条陌生短信,里面竟有自己的“不雅照”,是否会心头一惊?近期,深圳公安发布一起警情,不法分子利用PS合成不雅照进行敲诈。

日前,陈先生收到自称是“私家侦探”的来信,信里附带陈先生与一名女子所谓的不雅视频截图,对方要求陈先生在收件后速与其联系,否则将视频散播到互联网。其实,信里附带的不雅视频截图是PS合成的,而寄件人也并不是“私家侦探”。

警方介绍,不法分子通过不法渠道收集或购买公众人物的公民个人信息,然后使用电脑软件“移花接木”,合成部分公众人物的虚假“不雅视频”或“不雅照片”,精准发送给对应的受害人,从而实施诈骗。

这类诈骗有三个特点:一是侵害对象广泛。侵害对象主要是企业家、各行业管理者、公职人员等社会公众人物。二是模板统一。不法分子按照固定模板合成制作虚假“不雅视频”或“不雅照片”,通过手机短信、纸质信件或电子邮件等匿名方式点对点发送给选定的公众人物。三是诈骗话术如出一辙。不法分子以恶意骚扰、所谓举报、向身边人散播等手段威胁敲诈受害人,迫使受害人将钱转入指定的银行账户。

警方提示,收到类似诈骗信息,不要害怕,更不要有“破财消灾”的念头,一旦回复、回电或转钱,不法分子会不断骚扰。要对相关信息截图保存,准确记下不法分子的电话号码,及时向公安机关报案,或者前往国家反诈中心APP举报。

本报综合

移动支付暗藏风险 民警传授“安全宝典”

□潍坊日报社全媒体记者 王晓萌

随着移动支付方式的普及,带来方便的同时也暗含不少风险。日前,青州市公安局民警发布“手机安全支付宝典”。

近日,青州市公安局开发区派出所接到辖区群众报警,称其公司支付宝收款账户被盗刷转账。根据报案人的描述,民警初步判定嫌疑人熟悉公司内部运作,很有可能是熟人作案。

民警调查发现,该公司的支付宝账号每个月都会从同一家淘宝店铺购买东西,而公司的支付宝账户支付时间与被盗刷的时间基本吻合,于是判定这家淘宝店跟嫌疑人有重大关系。经查,这个淘宝店铺的实际拥有人为该公司的离职人员王某某,有重大作案嫌疑。王某某到案后,对其盗刷公司支付宝账户资金的行为供认不讳。

原来,嫌疑人王某某去年接触公司采购工作时发现公司运营、款项支付等有漏洞,于是注册了一个淘宝店铺,将公司支付宝账户里的资金盗刷到自己的淘宝店铺账户。由于每一次盗刷的金额比较少,开始并未引起公司注意,直到2023年7月底才被公司老板发现。截至报警时,该公司被盗刷金额累计20余万元。目前,嫌疑人王某某已被依法采取强制措施。

民警提醒,移动支付给人们带来前所未有的便捷,但是便利的背后也存在着很严重的隐患,一定要养成良好的手机使用习惯。

设置手机开机密码,但不用生日日期、手机号做密码。

不要在手机里存身份证、银行卡照片。不要频繁刷机、随意ROOT,最好通过官方应用商店下载安装软件。

使用支付工具时不用公共电脑或使用免费WIFI,公共环境下的计算机很容易被植入病毒,侵入个人账户,泄露个人信息。

警惕钓鱼网站和软件,不扫不明二维码,不点不明链接。上网过程中,不要下载不明文件,不要随意相信高利息、高返点之类的活动。

支付工具要实名认证,绑定身份证,防止丢失后被恶意找回密码。关闭支付工具的小额免密支付功能,设定消费限额。

妥善处理好旧手机,将旧手机恢复出厂设置或格式化,断开手机云存储功能,卖给相对正规的商家。

验证码是保护账户安全的最后一道关卡,绝对不能告诉别人。

安全大讲堂