

年底骗子冲业绩 四大骗局别中计 “年终防骗指南”请收好

年终岁尾,骗子也冲起了业绩,各种“符合时令”的骗局轮番上阵。如何才能守护好自己的钱包?请收好这份“年终防骗指南”,认清近期高发的四大诈骗套路,牢记防骗要领。

骗局1

机票退改签诈骗 帮退款是假 盗刷卡是真

“您好陈小姐,我是××航空的客服,您购买的北京飞往珠海的××航班因故取消,航空公司现在可以为您办理退款。”近日,陈女士收到了一通0085开头的陌生电话,因为对方报出了自己的姓名和准确的航班信息,她并没有引起警觉。

按照对方在电话里的指示,陈女士登录一个网址下载了一款App,并打开了App的视频会议功能。此时陈女士发现,自己的手机黑屏了一下,随后就不受控制了。但“客服”称这是正常的,工作人员正在后台帮助退款。

经过一番云里雾里的操作,“客服”表示,最后一步需要陈女士在手机银行App上验证“收款信息”。按照指示,陈女士按了好几次指纹,又填了手机银行的密码,之后还收到了系统发来的验证码。正当陈女士不明就里之时,自己的手机收到了一个10500元的转账信息,只不过这并不是收到了机票的退款,而是自己账户里的钱被骗子转走了。

■案例分析

“快到年底了,有出行计划的市民已经提前购票了,这时就有可能遇到这

种机票退改签诈骗。”北京市公安局朝阳分局民警王佳介绍,骗子会通过一些方式窃取到市民的身份信息和购票信息,随后假冒航空公司的客服,以各种理由假称航班取消或飞机无法起飞,诱导市民进行后续的退改签手续。“有些电话是在飞机起飞前一两天打来的,如果市民急于出行,骗子也会给出改签的选项,最终的目的就是引导市民进行下一步的操作。”

之后,骗子就会引导市民下载涉诈App。这类App都会有屏幕共享或远程控制功能,骗子可以实时监控事主的手机屏幕,或直接操纵事主的手机。“有了这种功能,事主输入的银行卡号、支付密码,接收到的手机验证码等信息,都会被骗子看到。在拿到这些信息的第一时间,骗子就会把事主的卡内余额转走了。”

■如何防范

- 1.收到机票退改签电话,要拨打公司官方客服电话核实。
- 2.收到机票退改签短信,不要点击链接。
- 3.不要下载任何来路不明的App。

骗局2

申领补贴诈骗 潜入工作群 发布假链接

近日,王女士在家中办公时留意到,一位同事在工作群里发来了“补贴申领通知”。点击之后则是一份声明,需要用户自行扫码申领。

因为页面上有人力资源和社会保障部的背景图,看起来还挺正规,王女士便扫了码,填写了身份信息。从办理进度来看,她刚刚通过的是“实名认证”环节,之后还有银行提交、信息审核、密码核实、短信验证等步骤。

“经查询本次实名信息符合补贴申请,预计本次可申请补贴金额:2375元”。以为多了一笔收入的王女士,按照系统提示,填写了个人银行卡号、支付密码等信息,而到了最后一步短信验证,她收到了一个验证码,并填写到了网站当中。可之后,她非但没有收到这2375元的补贴,自己的银行卡反倒多了好几笔扣款,总计金额8000多元。这时她查看自己的工作群才发现,有别的同事也已中招,而发来链接的人,根本就不是同事,而是骗子假冒的。

■案例分析

“骗子之所以能混入公司的工作群,靠的是在员工的电脑中植入病毒。”王佳介绍,从警方接案的情况来看,骗子会利用邮件等方式,诱骗员工点击病毒链接。而一种名为“银狐”的木马病毒就会悄然植入到电脑之中,这种病毒具有远程控制功能,会窃取公司内通信软件的信息和权限,骗子就能混入到公司的工作群当中了。

之后,骗子会伪造自己的身份,采用相同的头像和相似的群内昵称,在工作群内发送“申领补贴”的钓鱼链接。

■如何防范

- 1.不要点击陌生邮件,可能含有木马。
- 2.工作群内的信息,一定要核实发送人身份。
- 3.面对索取身份信息、银行卡支付信息的网站,要倍加警惕。

骗局3

积分清零诈骗 以为捡便宜 结果还搭钱

“清空通知:您号码×××手机累计366700积分明日失效,可兑金额:3667元,拒收请回复R……”手机收到这样一条短信,李女士下意识地以为,是电信运营商发来的积分清零通知。

“3000多块钱?可不能浪费。”李女士点击了短信里的链接,手机跳转到了一个积分商城页面,里面的商品琳琅满目,有手机、平板、电视等,每一样都“价值不菲”。

但李女士发现,虽然号称自己有3000多元的额度,但每一样商品,并非直接用积分就能全额兑换,而是只能用积分抵扣一部分,剩下的差价还要花钱来补。看看去,她最终选择了一个价值几百元的智能手表,积分抵扣之后,自己又花了129元。

在这之后,李女士等了一个多星期,依然没有收到这块手表。等她再次点进短信里的链接才发现,明明应该过期的积分还在,也依然能够换购商品。订单里,手表已经发货,但没有任何的物流信息。想问客服到底是怎么回事,才发现客服根本就是摆设,根本无人回复。种种迹

象让李女士意识到,自己是被骗了。

■案例分析

“这种骗局,骗子会以各种理由,营造出一种积分马上清零的假象。加上时间临近年底,市民就会信以为真。”王佳表示,伴随着这些积分清零短信发来的,都是骗子自建的虚假兑换网址。其中,有的网站会假称要赠送礼品,诱骗市民填写姓名、电话、住址等信息。这类骗局并非直接骗取受害者的钱财,而是在精准收集市民的信息,为下一次的精准诈骗做准备。

还有些骗局,则会像李女士遇到的一样,设计一个积分兑换商城,诱骗市民参与积分换购,但最终平台并不会真的发货,或是发来的都是山寨产品和残次品。还有的网站则完全是钓鱼网站,诱骗受害者填写银行卡、信用卡等支付信息,进行盗刷。

■如何防范

- 1.不要点击短信内的积分兑换链接。
- 2.去官方平台核实活动信息。
- 3.需要额外花钱换购的积分商城大概率是骗局。

骗局4

虚假投资诈骗 看似有收益 全都取不出

“您好,我们是××公司的客服,公司现在正在开展年终优惠活动,可以提供股票投资的免费指导,请问您有需求吗?”55岁的贾先生,近日收到了一通电话,抱着免费试试也无妨的心态,他添加了客服的微信,随后又被拉入了一个投资群当中。群内,有一个名叫“指挥长”的人,会定期发送股票信息。对股票一窍不通的贾先生,只能看到“指挥长”在一遍遍地炫耀,今天的收益是200%,明天的收益是300%。越发心动的贾先生,下载了“指挥长”购买股票的同款App。根据提示,向客服专员转账了5万元,随后也跟着“指挥长”一起“买进”“卖出”,账户里的钱还真的越变越多了。

到了11月初,客服在群内发布通知,称投资App需要升级,暂时无法使用。可等了好几天,App都没能升级完成。此时贾先生再咨询客服,对方已然不再回复,连微信群都被解散了,贾先生这才意识到自己受了骗。

■案例分析

“这种虚假投资骗局,根据我们的接案情况,在年底这段时间数

量是比较突出的。”王佳介绍,除了有直接拨打电话“拉客”的骗子,还有骗子会在社交平台上物色目标,通过谈恋爱的手段接近受害人,也就是俗称的“杀猪盘”。

无论是以什么理由,最终骗子都会以投资为名,吸引受害者下载虚假的投资App,其中所有的数据都是骗子在后台操控的,想让用户“赚”多少都可以。

“这类App,往往都不能直接转入资金。骗子会告诉事主,可以通过转账给某某人的方式代为充值。”在某些骗局案例中,骗子甚至会让事主购买黄金,邮寄到某某地址,或者让事主准备好现金,有专人上门领取。在这之后,事主的投资App上确实会显示金额到账,但这些数据也都是骗子操控的。

■如何防范

- 1.不要相信任何来源不明的投资广告。
- 2.不要下载应用商店里搜索不到的投资App。
- 3.要有基本的投资概念,不要相信过高的投资回报。

据 北京晚报