

警惕“机票退改签”诈骗 护好财产安心出行

本版策划：省公安厅宣传处、刑侦总队

编者按

“双节”将至,出行增多,需高度警惕“机票退改签”类电信网络诈骗案件,此类骗局正严重威胁旅客的财产安全。诈骗分子往往通过非法渠道获取旅客航班信息,冒充航空公司、票务平台或机场客服,以“航班延误”“机械故障”“票务出错”等理由,诱导旅客办理所谓“退改签补偿”,进而骗取手续费、保证金或诱导进行屏幕共享,点击虚假链接,致使群众蒙受财产损失。

本期选取近期高发典型案例进行深度剖析,揭示其“精准切入、制造焦虑、步步诱导”的诈骗逻辑。郑重提醒广大旅客:凡收到航班变动短信或电话,务必通过航空公司官方客服、购票平台等正规渠道核实,切勿轻信陌生号码。凡是要求私下转账、提供银行卡密码或验证码的,均为诈骗!请提高警惕,护好个人财产,安心出行。

理赔变贷款!男子被诱导网贷,5.7万元遭盗刷

案情回顾

4月29日,威海市公安局环翠分局接到市民张某宁报警称,其因相信诈骗分子“机票退费”谎言,被骗走5.7万余元。当日,张某宁接到陌生来电,对方自称机场工作人员,告知他购买的机票需要改签,需要听从工作人员的指令操作。因为距离此次航班起飞时间较短,张某宁未能及时辨别此消息真实性,即听从诈骗分子的指令进行操作。

张某宁按照诈骗分子的要求下载了“信安云办公”App,并在诈骗分子的指引下打开手机摄像头,使用一台手机拍摄另一台手机的形式进行直播操作。诈骗分子要求张某宁在各大网贷平台进行贷款,张某宁未能及时判断此要求的合理性,通过“抖音放心借”“京东白条”“省呗”进行贷款,共计8万余元。随后诈骗分子要求张某宁在“美团”“爱奇艺”等非常见借贷平台继续贷款时,张某宁察觉到异常,要求对方出具工作证件,但对方未能提供,张某宁随即结束视

频会议。张某宁本以为将贷款还上即可,但是其已然忘记其手机页面已经全部通过直播的方式展现在诈骗分子眼前。诈骗分子获取到张某宁的验证码、支付密码等关键信息,并通过“无卡取现”“POS机消费”方式将张某宁银行卡内的贷款和个人存款转走,共计损失5.7万余元。

警方支招

针对此类诈骗案件,威海警方发出紧急提醒:

一是接到自称某某工作人员的陌生来电,切记通过官方途径核实身份后再进行操作。不随意加入陌生社交群,不点击不明来源的网址链接,切勿下载陌生App,此类平台多为诈骗分子搭建的虚假平台。二是遇事保持冷静,分析行为合理性,对于诈骗分子提出明显不符合合理的要求要及时拒绝。三是保护好个人隐私,不泄露验证码、银行卡号、支付密码等敏感信息,遇到诈骗分子要求提供个人隐私信息时,应当立即停止操作。

案情回顾

近日,正准备出行的临沂市民麻先生接到一个自称是某航空公司“客服”的来电,对方准确报出了他的姓名、身份证号、航班号等信息,并告知因飞机故障原定的航班已取消,现可为他办理改签,并可申请一笔300元的航班延误理赔。由于信息准确,且正值出行前的紧张时刻,麻先生并未过多怀疑。他按照来电“客服”指引,点击了对方发来的一个“官方理赔链接”,然而,页面却显示“理赔失败,暂未开通企业收款”,这时,“客服”解释称,这是因为麻先生的银行卡未开通相关权限,需要通过“远程协助”方式,指导他在手机银行上进行操作认证。

急于拿到理赔款的麻先生在“客服”的引导下,从对方提供的链接下载了一款陌生的远程会议软件,“客服”要求他打开“屏幕共享”功能,麻先生手机上的所有操作,都实时暴露给了网络另一端的骗子。随后,“客服”以“验证账户”“刷流水解冻”等名义,指引麻先生进行了一系列操作。在此期间,骗子通过后台秘密完成了转账。直至收到银行发来的扣款短信,麻先生才惊觉自己账户内的2.4万元已被全部转走,此时“客服”早已失联。

警方支招

守住钱袋,牢记“三不”: 1.不轻信主动赔付。航空公司或旅行平台不会主动致电乘客要求退改签、理赔等涉及资金的操作。所有声称需“屏幕共享”“远程协助”办理业务的,都是诈骗。 2.不点击陌生链接。切勿点击对方发来的任何链接或扫描二维码,更不要通过陌生链接下载不明App。应通过官方应用商店下载正版购票、航旅软件。 3.不泄露验证码。银行账户密码、短信验证码是资金安全的最后防线,绝不向任何人透露。请务必牢记,真正的客服人员绝不会索要这些信息。

航班「故障」可理赔? 屏幕共享后2.4万元不翼而飞

收款码“不支持企业收款”?骗子借退改签名义,骗走2万余元

案情回顾

近年来,不少旅客会选择乘坐飞机出行,并提前购买机票,犯罪分子也打着“退改签”旗号进行电信网络诈骗活动,广大乘客务必提高警惕。今年3月,泰安市民张先生预定了从济南遥墙机场飞往深圳的机票。出发前一天,他接到“航班因

故延误需要改签”的电话。交流过程中,对方自称是航空公司工作人员,将对航班延误的乘客理赔300元。张先生查询了航班情况,发现确实延误,信以为真,就按照对方的提示进行操作。为了得到赔偿金,张先生先根据对方的要求下载了“办事通”App,开启了“语音会议”功能,然后登录了一个“航空公司”网站,并向网站上的“航空公司客服”进行交流。在

对方发送支付宝收款码后,客服声称张先生的收款码不支持企业收款,导致退款失败,只能通过其他渠道领取理赔。后诱导张先生打开各个手机银行,并下载各类网贷软件。完成相关操作后,客服又以进行账户认证为名要求张先生进行扫码支付,张先生共计被骗2万余元。

警方支招

购买或退改签机票时,要通过正规渠道办理,切勿轻信任何非官方平台的低价票或退改签等信息;在收到航班取消、延误、退改签等通知时,切勿直接点击链接或拨打通知中预留的电话,要第一时间向所乘航空公司官方渠道核实;任何退票、退款业务,均无需先向对方汇款,切勿向陌生人提供或在非官方网站输入银行卡账号及密码。

对方发送支付宝收款码后,客服声称张先生的收款码不支持企业收款,导致退款失败,只能通过其他渠道领取理赔。后诱导张先生打开各个手机银行,并下载各类网贷软件。完成相关操作后,客服又以进行账户认证为名要求张先生进行扫码支付,张先生共计被骗2万余元。

警方支招

购买或退改签机票时,要通过正规渠道办理,切勿轻信任何非官方平台的低价票或退改签等信息;在收到航班取消、延误、退改签等通知时,切勿直接点击链接或拨打通知中预留的电话,要第一时间向所乘航空公司官方渠道核实;任何退票、退款业务,均无需先向对方汇款,切勿向陌生人提供或在非官方网站输入银行卡账号及密码。

机票退改签要人脸识别?这样操作2.5万元瞬间被骗

案情回顾

近日,家住无棣县的王女士要出省旅游,但这天在家中突然接到来电显示是一串“00”开头的电话,电话那头精准地说出了王女士的名字,并自称是航空公司的工作人员,说王女士的航班飞机出现故障,可以给予王女士300元补偿款。因为王

女士的机票是朋友购买的,王女士并没有和朋友核实相关信息,就轻信了对方,于是按照对方短信提供的网址登录了所谓“中国民用航空局”的网站。王女士在登录网站后,对方要求王女士点击网页下方的理赔窗口申请理赔金,点击后需要王女士填写微信账号和手机号,并让王女士下载了一款“智会通”软件进行下一步操作,王女士也是第一次坐

飞机,并不清楚机票退改签流程,就按照对方的指示打开了屏幕共享,查看王女士银行卡号,接收验证码,要求王女士配合进行人脸识别,这时王女士察觉不对劲,便询问对方为什么要使用自己的银行卡,对方以王女士银行卡被锁定为由,又让王女士进行人脸识别操作,王女士看到自己银行卡内没有钱后发现自己被骗,连忙前往派出所报警,这时王女士银行卡内的2.5

万元已经被全部转走。

警方支招

诈骗分子在非法获取受害人航班信息后,冒充航空公司客服,谎称航班取消或者延误,承诺赔偿,诱导受害人登录诈骗网站或下载虚假软件实施诈骗。市民朋友们在接到机票退改签通知后,请直接联系航空公司官方客服核实,切勿相信陌生来电。

案情回顾

11月1日,招远市的孙先生接到一个号码归属地为香港的来电,电话那头告诉他,原计划于11月2日的航班因故不能起飞,需要改签,而且会给他补偿。过了一会,又有一个归属地为香港的号码跟他联系,对方在电话里要求其下载一个名为“Zoom Workplace”的App。孙先生下载安装后,对方给了他一个房间号,让他在这个软件里加入会议。对方在会议室里通过语音指导他提供银行卡号,让他先转账过去,然后对方会连同赔偿一起再给他转回来。

因为孙先生银行卡之前绑定的手机号码不用了,他就按照对方要求找到了朋友李先生,借用了他的一张银行卡。孙先生把他微信里的5万元钱转给朋友,朋友通过微信提现到这张卡里,孙先生又把这张卡的密码告诉了对方。到了下午,孙先生朋友的这张银行卡被扣走了5万元。对方又要求孙先生继续转1万元钱,孙先生称没钱了,对方又问他微信零钱余额,这时候孙先生才发现不对劲,感觉自己被骗,立即拨打110报警。

警方支招

1.通过正规渠道购票:购买机票要通过航空公司官方渠道、正规在线票务服务平台,尽可能避免信息泄露。 2.核实信息真实性:收到航班取消、延误、退改签等通知时,切勿直接点击链接或拨打通知中预留的电话,应第一时间通过航空公司官方客服电话、官方网站或购票平台进行核实。 3.警惕陌生链接和App:不要随意点击短信或电话中提供的陌生链接,更不要下载来路不明的App,以防被诈骗分子套取个人信息。 4.拒绝先汇款要求:任何退票、退款业务办理,均无需先向对方汇款,切勿向陌生人提供或在非官方网站平台输入银行卡账号及密码。

“开通企业收款”是骗局!一连串操作后,8万余元再也追不回

案情回顾

近期,家住日照市东港区的何先生接到一通自称“航空公司人员”的电话,对方表示何先生从西安飞攀枝花的航班因机械故障取消,询问其需要退票还是改签。何先生没有多想,继续与“客服”交谈。

“客服”为何先生提供了几个不同时间点的改签选项,何先生挑选了一个时间合适的航班,表示同意改签。对方表示需要何先生领取航班补偿,一张机票补偿金是300元,共600元,并且只

有在补偿金领取后才能确认改签成功。急于出差的何先生没有多想,为了尽快确认航班改签,同意了领取所谓的补偿金。

“客服”紧接着表示需要通过支付宝里的企业收款功能领取,何先生表示他的支付宝内没有这项功能。对方称他们有“技术人员”,可以指导其开通这个功能。何先生同意后,“技术人员”就把语音通话打了过来,提供了一个网址,何先生打开网址输入手机号并收到了验证码,此时“技术人员”向何先生询问验证码,何先生便告诉了对方。紧接着,骗子又提供了另一个网址,点开

后跳转到了一个对话界面,在骗子的引导下,通过这个对话界面给“客服”发送信息开通企业收款功能。“客服”先让其申请临时乘机证明,又发过来一串账号和激活密码,又发过来两次订单链接申请开通服务但都开通失败,又让其更换银行账户重新申请……在这一连串眼花缭乱的指挥操作下,何先生已经彻底丧失了判断力,只是一味的按照引导进行操作。

最终,“客服”发送了一个二维码,何先生扫码后“技术人员”指挥其通过手机银行进行转账,还称所有的转账都是为了测试账户是否开通企业收款

功能。3张银行卡都是首先给对方的账户转几块钱,对方退回后又让其转8万元,这一转,就再也没有退回来。

警方支招

1.当接到航班取消需要退款或者改签的电话时,不要慌张,一定要通过官方电话或App进行核实。 2.不要随意点击陌生链接,不要随意下载陌生App。 3.不要随意提供或输入银行卡账号、密码、验证码等涉及财产安全的重要信息。

改签要开屏幕共享?男子照做后,1万余元被隔空转走

案情回顾

11月30日,德州天衢新区的王某接到一自称某航空公司工作人员的陌生来电,对方以其预订的航班延误,可以退票,且有延误补偿,诱导王某下载了一款聊天App并开启屏幕共享功能。随后,对方发来一个网站链接,王某点击进入人与“客服”办理理赔。王某按指示操作,在网站链接填写了退费收款的银行卡号、验证码,直至收到银行的扣款通知,才惊觉自己银行卡内1万余元存款被转走。

网络诈骗手段,警方拆解了诈骗话术与手段。

精准信息获取:诈骗分子通过非法渠道(如黑客攻击、信息买卖)获取乘客的航班信息,包括姓名、航班号、起飞时间、身份证号等,使受害者误以为对方是正规客服。

冒充客服联系:冒充航空公司客服或票务平台工作人员,通过电话、短信或社交媒体联系乘客,告知航班因机械故障、天气原因、航线调整等被取消或延误,需办理改签或退票手续。

制造紧迫感:以“仅剩少量改签名额”“需在短时间内完成操作”等理由,催促乘客尽快办理,利用乘客担心

耽误行程的心理,使其失去冷静判断能力。

诱导操作陷阱:发送虚假链接或要求下载手机共享屏幕软件,引导乘客进入钓鱼网站窃取银行卡号、密码、验证码等信息。以“验证账户”“开通理赔通道”“转账刷流水”等为由,要求乘客进行转账操作,或将资金转入指定账户。要求乘客开启屏幕共享功能,实时监控操作过程,直接获取银行卡信息及转账资金。

拖延与失联:若乘客发现异常或要求退款,诈骗分子会编造“系统故障”“资金审核”等理由拖延时间,待资金转移完毕后失联。

警方支招

购买或退改签机票时,要通过正规渠道办理,勿轻信任何非官方平台发布的退改签信息。在收到有关航班取消、延误、退改签等电话或短信时,切勿直接点击链接或下载App,要第一时间通过航空公司官方渠道核实。正规退改签不会主动来电要求操作转账交费,切勿向陌生人提供或在非官方网站平台输入银行卡账号或密码。如已遭遇机票“退改签”诈骗,要立即报警。

先转钱再返补偿? 男子轻信航班改签,0.7万元被骗走

不要下载来路不明的App,以防被诈骗分子套取个人信息。 4.拒绝先汇款要求:任何退票、退款业务办理,均无需先向对方汇款,切勿向陌生人提供或在非官方网站平台输入银行卡账号及密码。