【关注】中国支付清算协会春节反诈温馨提示：欺诈典型案例及风险防范

中国支付清算协会 2022-01-22 11:05

为深入学习贯彻习近平总书记关于打击治理电信网络诈骗犯罪的重要指示精神，落实党中央、国务院重大决策部署及人民银行有关工作要求，切实提高人民群众防范电信网络诈骗意识，助力建设更高水平的平安中国，中国支付清算协会坚持“为人民群众办实事”的宗旨，汇总国家反诈中心、会员单位、互联网络等发布的相关反欺诈案例素材，编写春节反诈温馨提示，引导普通老百姓正确认知和防范欺诈风险，牢牢守护人民群众的钱袋子安全。

案例一：充值折扣诈骗

李先生收到陌生人的好友申请，对方自称是李先生的一位朋友介绍的，李先生虽心存疑虑，但还是通过了对方的好友申请。之后，对方自称可以提供加油卡充值服务，春节期间实付91元即可获得价值100元的加油卡。

为了保险起见，李先生联系自己的朋友询问是否认识此人，朋友说好像有点印象，李先生便放松了警惕。随后，对方将他拉入了一个“充值折扣群”，群成员经常交流充值、折扣等内容。李先生先试着充值了少量金额，第二天充值金额就到账了。

一见如此，李先生便完全放下心来。之后，他想赚笔大的，便一次性转账5万元，可是第二天他在群里问充值情况时，却发现群内只剩下自己。李先生查询加油卡余额发现并没有金额到账，这才意识到自己被骗了。

防范提醒

陌生人添加微信，一定要确认好对方的真实身份。当对方谈到钱财时，要提高防范意识，莫贪小便宜。

案例二：针对财务人员诈骗

某公司会计小张接到一个自称是某银行工作人员的电话，称因银行需对其公司账户进行年检，需要公司提供一些资料，要求加小张QQ。

小张加了该工作人员的QQ后看到其昵称为“某银行X支行小黄”。随后，小张被拉入一个名为“XXXX有限公司”的QQ群。群里除了银行工作人员外，还有公司的两位老板“王总”和“李总”，两位老板的头像和名字都与现实中的老板相同。

小张进群后，“王总”要求其配合银行做好年检工作。之后，“李总”又在群里发消息，说有个项目已经备好案了，要求小张马上将30万元的项目款转到指定账户。小张头脑一蒙，就按“李总”指令操作了转账。

没过多久，小张忽然想到两位老板从来没有通过QQ下达过工作指示，于是赶忙向其本人核实，才发现被骗了。

防范提醒

年关将至，诈骗分子有可能在“年检”“年审”等事件上做文章。若接到涉及银行账户年检等问题的QQ讯息、电话或短信，不要轻信，应及时与开户银行官方客服电话核实确认。企业应严格执行相关财务管理制度要求，对QQ（群）、微信（群）等要求的转账汇款，必须经过企业老板当面或电话核实确认。

案例三：家长QQ群诈骗

寒假期间，部分欺诈分子潜入家长QQ群，冒充老师收取各种费用，典型作案手法如下：

欺诈分子A、B、C通过QQ搜索关键词“班级群”，申请并加入群聊，由于家长学生众多，老师可能不会一一核实，使得欺诈分子成功潜入家长群。

在获取班主任的头像、昵称、群备注等信息后，A趁其上课无法查看手机等时段，伪装成“班主任”，而B和C则将头像和昵称替换为群内的两位家长。

随后，A发起“寒假补课费”的群收款，B和C立刻予以回应。有了前面“家长”缴费的示范，家长们卸下防备，纷纷进行转账缴费，直到真正的班主任发觉时，骗局才会被拆穿。

防范提醒

此类骗局针对学生寒假补课、购买学习资料等场景，加上不法分子之间的“团伙互动”，提高了迷惑程度。家长在班级群里收到“交费转账”等通知时，牢记先与老师本人、学校核实，不要急于转账汇款！

案例四：新冠特效药诈骗

回家过年的刘先生接到一个陌生电话，对方自称是当地防控中心的工作人员，声称刘先生的健康码和检测报告上有异常，可能感染了新冠肺炎，不过还在潜伏期，情况不算太严重。对方接着说现在有一款特效药，5000元三个疗程，每天坚持服用就会恢复健康。

由于回家路上途经风险地区，刘先生非常害怕，立马向对方提供的账号转账，然而迟迟没有收到接受治疗的通知，这时刘先生才反应过来自己被骗了。

防范提醒

防疫工作人员不会直接推销产品、擅自收取费用，不要轻信陌生电话！

案例五：抢红包诈骗

春节前夕，微信朋友圈和群里再现一条诱人信息：“春运补贴领取通知，我已领到XX元...”点开这条微信链接后，是一个显示有“春运补贴领取通知”字样的红包页面，正中是一个大大的“抢”字。点击“抢”字后，进入显示抽中红包的页面，但还需要分享到微信群或者朋友圈才能领取。不过当用户按要求分享后，界面却提示“分享失败”，但这条信息实际上已经分享成功，你的个人信息可能也已经泄露。

防范提醒

对类似上述来源不明的中奖、拆抢红包等相关信息，只要记住“别点别转”这四个字，即可避免上当受骗。

案例六：积分兑换诈骗

秦先生收到一条积分兑换短信，内容如下：“尊敬的用户您好：您的话费积分3160即将过期，请手机登录XX网址激活领取现金礼包。”

见到短信是由自己手机号对应的运营商的号码发送的，且网址与真实网址近似，秦先生并没有过多怀疑，点击链接后进入一个标题为“掌上营业厅”的页面，要求填写姓名、身份证号、信用卡卡号、交易密码、预留手机和卡背后三位等信息。

秦先生按照要求填写了相关信息并提交后，又进入了一个标题为“信用卡提额专用”的页面，继续填写信息后被要求下载一个“安全控件”。秦先生提交信息并下载软件后，页面进入了一直等待的状态。不久后，秦先生收到多笔消费短信，提示自己的信用卡被累计消费了7000余元。

防范提醒

由于有伪基站技术的存在，即便是自己熟悉的客服号码发来的短信，也不能轻易相信。特别是当短信中有网址链接时，一定要谨慎打开。最好是向服务商的官方客服渠道核实之后再查看！

案例七：票务诈骗

春节前夕，张先生查遍各大订票网站均未订到心仪的机票，最后通过搜索引擎找到一个小网站，上面刚好出售一班时间比较合适的机票，且价格低廉，但库存紧张。

张先生觉得自己捡了大便宜，赶忙预订付款。但付款成功后，页面显示“出票失败”，并建议购买更高等级舱位。张先生见更高等级舱位售价仍低于市场价，便再次付款。但付款成功后依然显示“出票失败”。这时张先生察觉到不对，想要退款，却发现没有退款通道，这才意识到自己被骗。

防范提醒

请务必通过正规渠道购买车（机）票，不要轻易点击、扫描任何来历不明的网址链接、二维码，防止手机中毒，银行账户被盗！

案例八：冒充客服诈骗

过年期间，蒋女士接到一个陌生电话，对方自称是XX购物平台的售后服务人员，称蒋女士之前在平台上购买的商品没有达到国家检测标准，现将以商品的三倍价格退还金额到蒋女士账户。

由于春节前在网上置办了部分年货，蒋女士信以为真。在对方的诱导下，将自己的银行卡号、短信验证码等信息告知对方，直到蒋女士银行卡内的钱被转完后，蒋女士才意识到自己被骗，共计损失4万余元。

防范提醒

电商平台退款通常是原路返还购物者的银行账户或支付账户，无需购物者在其他软件中进行操作，更不会要求购物者通过扫码、点击链接、提供银行卡密码、短信验证码等方式进行退款！

· END ·