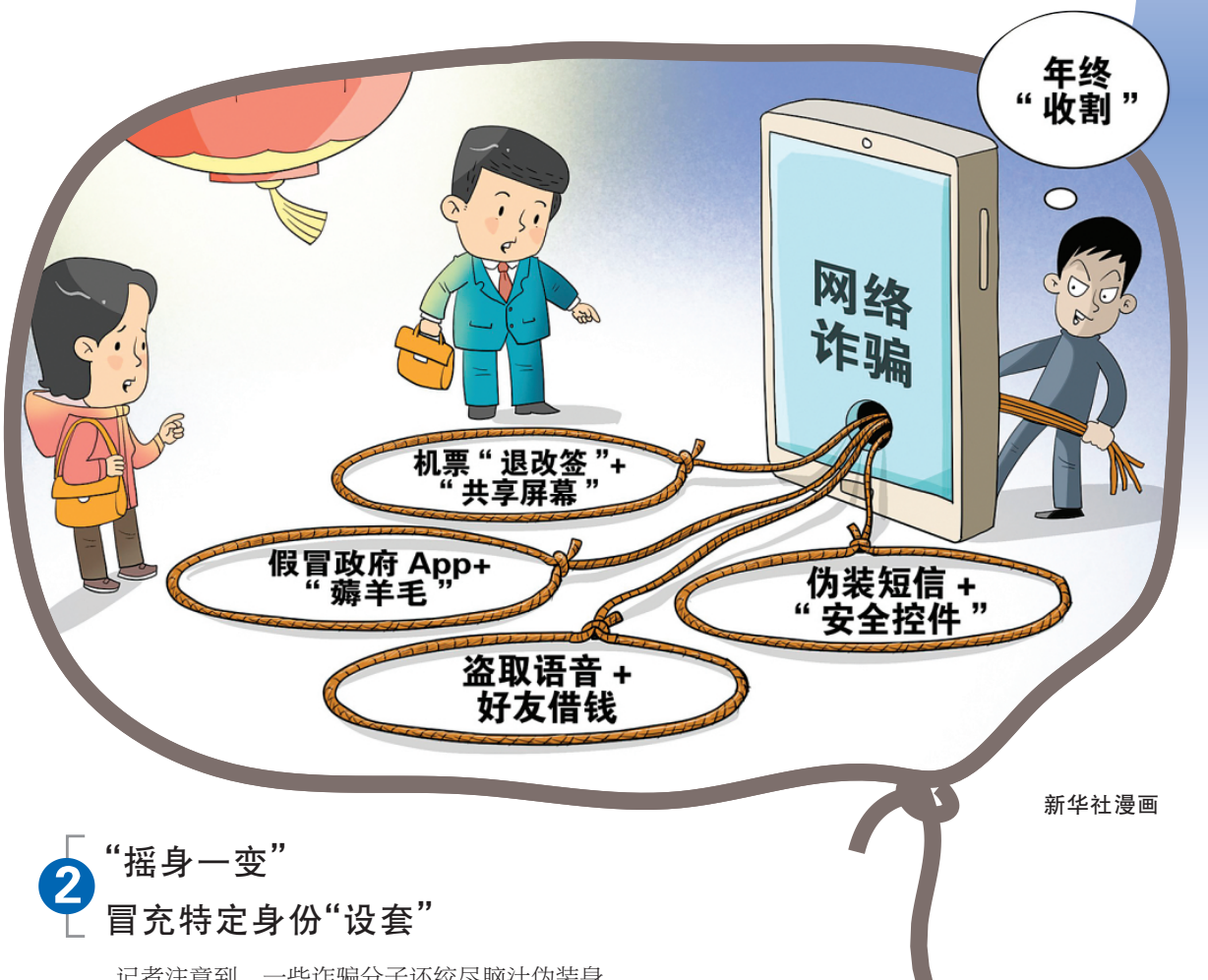
利用群众出行、购物、交友等各类机会精心设计骗局

年关将至 警惕这些新骗术

近日，一演员被拐骗事件引发关注，敲响反诈警钟。记者日前采访发现，随着年关将近，诈骗分子也企图开展年终“收割”，利用群众出行、购物、交友等各类机会精心设计骗局，值得警惕。



新华社漫画

1 “旧瓶装新酒” 网络诈骗套路频出

临近春节，诈骗犯罪易发多发。记者梳理发现，一些网络骗术通过“旧瓶装新酒”不断升级。

——机票“退改签”+“共享屏幕”。

近期，罗先生接到电话称他预订的航班取消了；对方表示，可帮助办理改签并支付航班延误赔偿金，但需要他下载相关软件，按提示操作。这一新型“退改签”骗局中，骗子诱导当事人下载“云服务App”会议软件，实现屏幕共享，期间打开银行App、付款码。一番操作下来，罗先生银行卡内的3万多元余额被转走。

记者了解到，“共享屏幕”已成为诈骗分子新手段，一旦开启此功能，屏幕上显示的银行卡号、密码，以及短信验证码等内容都会同步让对方看到。

——假冒政府App+“薅羊毛”。

不久前，北京市民徐先生通过朋友发来的二维码下载了一款“卫健委”App，里面还提供政府工作人员的微信。徐先生添加所谓“卫健委领导”微信后，进入“补贴群”，群里发布“血糖仪补贴”等项目，每天可领取几元钱的补贴，一个月群内会员就达到了400人。

当会员领取了几十元补贴后，群内又发布一个超长期特别国债项目，声称“最少可投资3000元，每日利息45元；最多可投资5万元，每日利息高达1550元”。北京通州警方调查发现，这款App后台地址在境外，是一款涉诈App，该案诈骗项目涉案金额约50万元。

——盗取语音+好友借钱。

近年来，群众对微信好友“借钱”越来越谨慎，但骗子却设法盗取语音信息，增大骗局迷惑性。北京警方披露的一起案件中，孙女士沉迷某款手游，骗子以“帮你充值游戏点券”为名和她语音聊天，并诱使她提供微信账号、密码。

其间，骗子故意询问孙女士是否为该游戏昵称本人，轻松得到语音回复“是我是我”。随后，孙女士的微信好友便接连收到“孙女士”向他们借钱的消息，听到“是我是我”的语音回复后，4个好友相信并转账。

——伪装短信+“安全控件”。

年底，不少商家推出积分清零活动，骗子也瞅准“契机”。杨某收到“积分兑换空气炸锅”的提醒短信后，看到短信中的网址与真实网址相似，没多怀疑就用手机打开链接，进入“掌上营业厅”页面填写了姓名、身份证号、信用卡卡号、交易密码。

值得注意的是，骗子还会引导当事人进入“全国银联信用卡提额专用”页面，下载的所谓安全控件实际上是木马程序。杨某提交信息后没多久就发现，自己的信用卡被盗刷近8000元。

2 “摇身一变” 冒充特定身份“设套”

记者注意到，一些诈骗分子还绞尽脑汁伪装身份，达到精准施骗的目的。

——冒充租客“杀猪盘”。

近日，有骗子通过网络平台找到当事人史某，称要长期租一套用于出差住宿的房子。双方达成租赁合同，商定押金5500元，定金1000元，每月租金5500元。骗子自称是某科技公司程序员，和房东聊得甚是投机，还讨论金融投资等话题，说自己通过AI算法可以预判股市走向。

信以为真的史某主动在对方推荐的网站上申请账号，陆续投入60万元，直到发现平台无法登录才意识到被骗。

——以上门维修为由偷装VOIP设备。

有不法人员冒充联通、移动、歌华有线工作人员，上门以维修、网络提速等理由安装VOIP设备。北京市公安局一位反诈民警告诉记者，境外诈骗分子进行远程拨号，经过VOIP设备转换，被害人手机上的来电显示就是国内的固话号码，大大降低了被害人的防范心理。

在北京朝阳警方2024年破获的一起案件中，嫌疑人在网上应聘安装设备的工作后，“老板”与其联系后派发了假冒宽带公司客服的工牌，快递VOIP设备，并告知安装地点。一个月内，该人员共安装设备数十台，获利近万元。

——冒充快递员实施“刷单”诈骗。

随着公安机关打击力度不断加大，诈骗分子转移涉诈资金盯上了黄金、现金转移。近日，刘女士被假冒的“顺丰快递员”添加好友，并被拉入一个微信群，群内展示各类礼品图片，由刘女士自行挑选。在挑选的礼品送达后，对方便诱导其下载自制的刷单App。App中，客服发布包括为淘宝商家点赞、关注等在内的任务，并声称刘女士完成任务后可通过微信红包获得返利。

当刘女士申请提现时，对方以需要支付“救援金”为由，诱使刘女士通过网约车向指定位置运送88000元现金，所幸刘女士的行为及时被警方拦截。

3 增强警惕意识 防患于未然

据了解，2024年以来，北京市公安局刑侦总队紧盯高损电诈案件及新型诈骗手段，全年电诈破案、刑拘数同比分别上升26.9%、36.8%；将打击涉诈黑灰产业链作为主攻方向，创新建立多部门综合联动打击治理机制，成功打掉取现团伙80余个、抓获犯罪嫌疑人500余名，实现涉诈线下大额交易逐步清零，2024年全年累计返还被骗群众资金7.4亿余元。

多位反诈民警表示，反诈不是“遭遇战”，而是“持久战”；要增强警惕意识，提防各类新型诈骗手法。

首先，对于陌生好友申请、陌生短信链接要加强防范甄别，避免落入陷阱。例如，骗子仿冒运营商发来的短信中，利用群众对英文字母“l”和数字“1”的低辨识度，用“10086”冒充“10086”。

其次，注意保护个人隐私，不下载陌生App。多地消委会近日发出节前提醒，来路不明的应用程序可能包含恶意软件，一旦安装，可能会窃取银行卡密码、验证码等个人信息。消费者不要在未经核实的平台上填写姓名、身份证号、银行卡号、密码等，尤其是涉及金融相关信息，要格外谨慎。

最后，需要以有效方式强化防诈措施。受访者表示，可通过开启手机银行App的“夜间锁”、支付软件的“夜间保护”功能，减少银行卡盗刷风险。

据新华社