@青少年，暑期请警惕这些电诈陷阱

正值暑期，一些不法分子盯上社会经验不足、警惕性不强的学生群体，以兼职刷单返利、网络游戏产品虚假交易等为代表的电诈类案件多发。还有一些不法分子以“轻松赚钱”为诱饵，诱骗青少年参与涉诈违法犯罪活动。记者梳理了多起公安机关新近查处的典型案例，带你提升反诈意识。

图为重庆警方开展反诈宣传活动。（重庆市公安局供图）

暑期兼职有陷阱 学会甄别是关键

近期，想打暑期工的重庆大学生李某，在社交平台上看到一则招聘兼职的帖子。他留言咨询后，对方要求李某扫描二维码添加微信“客服”，之后，微信“客服”以需要安排专业老师指导为由，引导李某通过QQ添加刷单“老师”并加入相关QQ群。

令李某没想到的是，他正在掉入诈骗分子精心设计的陷阱：在刷单“老师”的语音指导下，李某通过转账购买其指定的商品，完成了刷单任务。随后，对方又以退还垫资为由，引导李某下载“teams”软件并开启屏幕共享，套取了李某相关密码。之后李某收到银行扣款通知，才知道被划走了2.5万元。

“这起针对学生群体的兼职诈骗案件手段极为典型。”重庆市公安局刑侦总队反诈支队办案民警介绍，暑期是学生兼职的高峰期，诈骗分子往往抓住学生兼职需求较高的心态，在社交平台广泛投放兼职广告，吸引受害人主动联系，此后又不断切换身份，增加迷惑性。

警方提醒，暑期找兼职务必通过正规渠道；要求先垫资做刷单任务的都是诈骗；最重要的是不要随意和陌生人开启屏幕共享，生活中请务必保护好个人信息，以防被诈骗分子利用。

“免费皮肤”套路深 虚假交易需警惕

“警察同志，我孙子玩个游戏，7000多块钱就没了！”近日，家住重庆市北碚区金华路的曹大爷心急如焚地来到北碚区公安分局北泉派出所报案。

原来，曹大爷10岁的孙子小曹在家用手机玩游戏时，一名陌生网友主动发来对战邀请。对方谎称是名游戏主播，精通各类游戏，还抛出极具诱惑力的诱饵：“只要按照我说的做，免费送你稀有游戏皮肤。”

爱玩游戏的小曹感觉天上掉下了馅饼。在对方步步诱导下，小曹层层掉入陷阱——他不仅登录了对方提供的账号、开启屏幕共享，还毫无防备地将手机验证码全盘托出，最终被骗走7000余元。

由于假期家长容易疏于监管，爱打游戏的部分青少年易被“免费领取游戏皮肤”“高价收购游戏账号”等话术吸引，进入虚假交易平台进行所谓“交易”，落入“网络游戏产品虚假交易”骗局。

北泉派出所民警徐文鹏介绍，诈骗分子通常以购买游戏账号为由，引导受害人私下联系，提供虚假交易凭证，联系假客服。接着，诈骗分子再以缴纳保证金、积分不足、信用额度不够等为由，引导受害人向指定账户转账，直至受害人被骗。

警方提醒，买卖游戏装备、皮肤、账号等，须通过官方平台交易；家长要保管好自己的手机和支付密码，引导孩子养成良好、正确的上网习惯。

“轻松赚钱”不可信 以身试法不可取

记者采访了解到，还有一些不法分子以假期“轻松赚钱”为诱饵，诱骗青少年买卖、租借电话卡及银行卡，或参与“跑分”洗钱、帮打诈骗电话、转发诈骗信息等违法犯罪行为。一些青少年由于没能抵制诱惑，最终受到法律惩处。

重庆公安机关破获的相关案件显示，有诈骗分子利用青少年境内手机或电话卡与受骗人通话或视频，或发送短信，以误开抖音会员或快递未取等理由，诱骗他人开启屏幕共享，套取个人信息，实施诈骗。

“经过研判，我们发现作案者多为15岁左右的青少年，且多为同学关系。”重庆市公安局刑侦总队反诈支队情报研判大队教导员杜泽松说，有的青少年实施组织、提供租借手机及手机卡业务，或者直接操作，充当境外诈骗分子与境内受害人通联的桥梁，以获取几十、上百元好处费。目前警方已抓获多名犯罪嫌疑人，其中既有组织者，又有参与者。

“侦察发现，打着‘招工’‘兼职’名义的广告通过网页和社交媒体大量传播，声称不需要任何技术和资金投入，只要提供手机和银行卡、电话卡就能轻松挣钱。个别青少年由于法律意识淡薄，沦为诈骗分子的帮凶，有的涉嫌犯罪。”杜泽松说。

警方提醒，当前电信网络诈骗犯罪整体形势依然严峻，诈骗技术和手法花样翻新，迷惑性极强。青少年要提高法律意识，特别是要抵制诱惑，切勿因蝇头小利误入歧途。

防诈不从诈，才能快乐过暑假。广大青少年要做到不当电诈“受害者”，更不沦为电诈“工具人”。家长们也要注意假期中对孩子网络行为的关注，共同了解学习反诈知识。一个安全而愉快的假期需要全社会参与和共建。

来源：新华社

AI语音变声让电话钓鱼诈骗升级

这些行业多发

“随着AI语音合成与变声技术的进步，网络犯罪分子利用这些工具实施更具欺骗性的电话钓鱼(Vishing)攻击已成为新趋势。”

记者从中国互联网络信息中心公共互联网反网络钓鱼工作组获悉，此类攻击通过AI变声模拟银行客服、公司高管甚至亲友的声音，极大提升了诈骗的成功率。

据介绍，受害者在接到此类电话时，往往难以分辨真假，极易泄露个人信息或企业机密。尤其是在金融、医疗和大型企业领域，Vishing攻击造成的损失逐年上升。

专家建议，企业应加强员工培训，提升对Vishing攻击的识别意识，并推行多因素身份验证和回拨核实机制。个人用户遇到涉及敏感操作的电话时，也应主动通过官方渠道核实身份，防止信息泄露和财产损失。

另外，AI变声技术的普及对传统身份验证手段提出更高要求，安全防护亟需升级。

与此同时，最新研究显示，人工智能已成为垃圾邮件和恶意攻击的主力技术。AI生成的垃圾邮件现已占全部垃圾邮件总量的50%，内容更加个性化、难以识别，极大提升了钓鱼攻击和诈骗的成功率。

“AI技术正被广泛用于自动化暴力破解、账户接管和信息窃取，攻击者通过机器学习不断优化攻击策略，绕过传统检测。AI还能模拟人类语言风格，生成高仿真钓鱼邮件和虚假客服对话，迷惑用户并窃取凭证。”公共互联网反网络钓鱼工作组表示。

专家建议，企业应采用AI驱动的安全检测系统，提升对新型AI攻击的识别能力。加强员工安全培训，提醒用户警惕可疑邮件和异常账户行为。个人用户应启用多因素认证，定期检查账户安全，防止因AI自动化攻击带来的信息损失和财产风险。**来源：中新网**