# 警惕！这些新型网络犯罪，每一个都在你身边

随着网络的广泛应用，传统犯罪加速向以互联网为媒介的非接触式犯罪转移，手段迭代更新，形式层出不穷，成为影响部队安全稳定的一颗“毒瘤”。本期，小编结合常见的新型网络犯罪案例，帮助大家共同了解犯罪手段，提升防范意识，掌握应对方法。

**“AI 换脸”，暗藏诈骗有风险**

一日，李某收到老同学“贾某”的视频通话，通话中画面卡顿，人脸细节模糊，十几秒后就以信号差为由挂断电话，转为文字聊天。“贾某”称工程急需用钱，但自己不方便出面，希望借李某账户做个周转，随后向李某索要了银行卡账号，表示已转账 40 万元并发来“转账截图”。基于信任，李某将钱款转入指定账号，正当想再次发起视频通话时，发现已被对方拉黑。意识到被骗的李某由于报警及时，最后成功“截获”被骗走的 40 万元。

【防范提示】虽然“AI 换脸”技术越来越逼真，但仍可以通过观察声音和图像是否同步、神情是否自然、画面有无停顿等方式发现破绽。如遇到熟人在网络上要求转账，要多重核验对方身份，一旦被骗要立即报告并报警处理。

**编造谣言，吸粉引流无下限**

前段时间，某博主发布关于在国外旅游时捡到国内小学生寒假作业的视频，并喊话当事人来拿作业。视频一经发布，迅速登上热搜。众多媒体竞相跟进炒作，被网友质疑后，博主又晒出与“当事人妈妈”的微信聊天记录截图。后经公安机关查证，“小学生丢作业”事件是网民徐某与同事薛某为吸粉引流，共同策划、编造的谎言闹剧。目前，徐某、薛某及所在公司已被依法行政处罚。

【防范提示】网络不是法外之地，无论动机如何，只要在网上编造传播虚假信息、造成不良影响，都会受到法律制裁。面对不明就里的网络热门事件，要理性看待，不能妄加评论、造谣传谣，避免成为谣言传播的“推手”。

**“话费慢充”，洗钱陷阱藏其中**

王某在网上看到代充话费的广告，售价远低于一般话费充值业务，便向对方支付560元，并在7天后到账700元话费。到账次日，王某的电话突然被停机，后被公安机关告知涉嫌犯罪需要配合调查。经查证，充入其手机的话费是犯罪分子以非法手段获得的赃款，下单的王某间接成了“洗钱”团伙的帮凶。

【防范提示】“话费慢充”实际是“洗钱”团伙使用赃款充值话费，从而实现赃款“洗白”的掩饰手段。贪图小利、乱“薅羊毛”极易掉入“洗钱陷阱”，要选择正规平台合法充值，不给犯罪分子可乘之机。

**网络“嗅探”，隔空盗刷难阻断**

深夜时分，刘某在睡梦中被手机提示音吵醒，发现收到数百条短信，其中包含多条银行卡转账的支付验证信息，银行卡里的1万元也不翼而飞了，刘某立即报了警。经公安机关查证，犯罪嫌疑人陈某使用“嗅探”设备，采集附近人员的手机号和短信验证码，进而实施银行卡盗刷、网络诈骗等犯罪活动。

【防范提示】“嗅探”设备实际是一种“伪基站”，通过“吸附”附近2G网络下的手机信号获取手机号码和短信。当手机突然变成2G网络，并频繁收到不明短信验证码时，很可能正在被“嗅探”设备攻击，应立即打开飞行模式或关机。同时，要设置支付多重验证，关闭免密支付功能，从源头上做好自我防护。

**帮“打电话”，充当工具涉电诈**

李某在浏览手机时看到一则广告，声称只需要2部手机、每天打几个电话就能拿到200元报酬。李某立马添加“客服”QQ，并按要求准备2部手机，其中一部和“客服”接通QQ电话，另一部拨打对方提供的号码，接通后将两部手机放在一起打开扬声器，由“客服”伪装成某APP客服与对方交流、实施诈骗。最终，李某因涉嫌帮信罪，被依法追究刑事责任并处罚金。

【防范提示】网络上“轻松赚大钱”的广告层出不穷，但天上掉下的往往不是“馅饼”而是陷阱。面对蝇头小利的诱惑，要擦亮双眼，切勿财迷心窍、以身试法，一个举动很可能就让你充当了不法分子实施犯罪的“工具人”。

**黑客技术，传播违法被惩处**

张某是一名黑客，因收入微薄便打起了传播黑客技术赚钱的主意。他创办会员制黑客技术交流网站，相关视频教程仅限会员用户下载使用，以此吸引大量用户注册充值，从中收取会员费 4 万余元。网站创办不久，张某便被网安部门侦控抓获。

【防范提示】利用黑客技术实施网络攻击、窃取信息数据是典型的违法犯罪行为，传播黑客技术同样触犯法律。战友们需要注意的是，每台电脑都有对应 IP 地址，任何黑客行为都会被追踪溯源，我们要远离黑客，严禁传播黑客技术，依规上网用网。

（来源：澎湃福建，转引自：复旦大学中国反洗钱研究中心，网址：http://www.ccamls.org/newsdetail.php?did=47045。时间：2024 年 6 月 3 日。访问时间：2024 年 6 月 7 日 16:55。）