身边的洗钱案例分享——警惕“高科技”陷阱，勿做洗钱“工具人”

随着数字金融、人工智能和跨境支付的快速发展，洗钱犯罪手段也“全面升级”，呈现出智能化、隐蔽化、碎片化的特征。本文将通过2025年真实发生的典型案例，带你解开新型洗钱的“科技外衣”，提高警惕，避免成为犯罪分子的“工具人”。

【案例一】AI换脸+远程操作：老人银行卡成“洗钱通道”

地点：江苏省南京市
时间：2025年3月

70岁的王阿姨接到“孙子”的视频电话，画面中“孙子”哭诉被警方扣留，急需2万元保释金。由于是实时视频，且声音相貌完全一致，王阿姨信以为真，立即转账。事后发现，这是诈骗团伙利用“AI深度伪造技术（Deepfake）”模拟其孙子形象实施的“亲情诈骗”，而收到钱的账户，正是一个被收购的“沉睡银行卡”网络。

后续调查发现：该账户背后牵出一个跨省“卡农”团伙，他们专门收购老年人、务工人员闲置银行卡，用于接收诈骗资金并快速拆分转移，完成洗钱“第一跳”。

警示：不要轻信未经核实的亲友“紧急求助”视频通话；老年人账户更需要家人共同监管，避免不法分子利用。

【案例二】“跨境电商代运营”实为洗钱平台

地点：广东省深圳市
时间：2025年4月

某“跨境电商孵化公司”宣称可帮助个人开设海外店铺，无需经验，月入过万。参与者只需提供身份证注册店铺，公司将“代运营”并定期打款至其国内账户。短短三个月，全国超2000人加入。

然而，警方调查发现：这些“店铺”并无真实交易，所谓“海外订单”全是伪造数据，资金来源于境外赌博和诈骗平台。该公司利用虚假贸易背景，将赃款伪装成“跨境电商货款”回流境内，完成洗钱闭环。

该案涉案金额达27亿元，是2025年迄今破获的最大一起“伪跨境贸易洗钱案”。

警示：凡是“零投入、高回报”的代运营项目，无比核实资质；收到不明来源的“货款”，可能已涉嫌洗钱。

【案例三】利用“数字人民币钱包”进行多层流转

地点：浙江省杭州市
时间：2025 年 5 月

一名大学生小李在社交平台看到“数字人民币红包任务”：下载指定 APP，开通数币钱包，完成几笔小额转账即可获得返现。他照做后，账户频繁收到来自不同地区的资金，并自动转出多个陌生钱包。

不久，小李的银行账户被冻结，警方通知其涉嫌参与洗钱。原来该 APP 是犯罪团伙开发的“跑分工具”，利用数字人民币可控匿名、离线支付、多钱包绑定的特点，实现资金快速拆分、跨区域流转，逃避传统金融监管追踪。

目前，公安部已联合央行建立“数字人民币反洗钱监测模型”，加强对异常钱包行为的识别。

警示：数字人民币钱包≠私人钱包，任何异常交易都会被追踪；切勿随意授权第三方 APP 控制你的数字货币账户！

【案例四】直播打赏+虚拟礼物：“榜一大哥”竟是洗钱团伙

地点：四川省成都市
时间：2025 年 2 月

某直播平台多名“土豪主播”收入暴增，背后缺失洗钱黑产。调查发现，一个境外犯罪团伙通过非法集资获取资金，雇佣“水军团伙”使用大量实名认证的小额账户，在直播间集中打赏虚拟礼物。主播收到平台结算后提现，资金即“合法化”。

更隐蔽的是，部分打赏资金通过虚拟商品二次交易（如将礼物转卖给第三方平台）再次流转，形成多层清洗链条。

该案涉及主播 137 人，打赏金额超 8.6 亿元，目前平台已被责令整改，加强打赏资金来源审核。

警示：理性消费，警惕“非正常打赏行为”；平台有责任对大额打赏进行身份与资金溯源。

来源：大连农商银行