牢记这20个关键词 远离电信诈骗

为帮助广大群众提升识骗防骗能力，公安部刑侦局通过对近期侦破的电诈案件进行分析研判，系统总结提炼了20个防诈关键词，助您识别电诈套路。

关键词1 ▶ 屏幕共享

在电信网络诈骗案件中，诈骗分子会使用多种话术、套路诱导受害人下载、安装具有屏幕共享功能的应用程序，再利用屏幕共享功能获取受害人的账户信息、银行卡号、验证码等，从而骗取钱款。

警方提示：在未确认对方身份前，切勿随意点击对方发来的下载链接或开启屏幕共享功能，在涉及资金操作时需格外谨慎。

关键词2 ▶ 百万保障

诈骗分子冒充客服，以受害人误开启“百万保障”为由，诱导其进行退款操作，从而实施诈骗。

警方提示：“百万保障”服务是自动开通且完全免费的。如果对“百万保障”相关业务有疑问，可联系官方平台客服咨询。接到引导关闭“百万保障”功能的陌生来电，均是诈骗。

关键词3 ▶ 安全账户

诈骗分子冒充公检法等国家机关工作人员，以“账户被冻结”“资金有风险”等理由要求受害人将资金转入所谓的“安全账户”，并承诺资金核查完毕后进行返还，从而实施诈骗。

警方提示：公检法机关没有所谓的“安全账户”，凡是接到陌生电话，自称国家机关工作人员，要求把资金转到指定账户或提供银行账号、密码、验证码的，都是诈骗。

关键词4 ▶ 修复征信

征信记录是个人或企业在信用机构管理下的信用活动记录。如果征信出现问题将对工作、生活产生重要影响。诈骗分子常常以可以帮助“修复征信”为由，利用受害人急于清除不良记录的心理实施诈骗。

警方提示：个人征信由中国人民银行征信中心统一管理，任何公司和个人都无权删除和修改。

关键词5 ▶ 刷单做任务

在刷单诈骗中，诈骗分子通常以刷单做任务为由诱导受害人进行转账，前期给予小额返利，当受害人加大投入后，诈骗分子随即切断联系。

警方提示：网络刷单是违法行为，不要轻信网上“高佣金”“先垫付”等兼职刷单的信息，馅饼之下藏着的是陷阱。

关键词6 ▶ “色情小卡片”

“色情小卡片”是刷单诈骗的变种引流手段。诈骗分子以色情信息为诱饵，在一些公共场所散发附有二维码或联系电话的小卡片，吸引受害人扫码。受害人一旦“上钩”，就会被诱导进入“刷单返利”“同城约会”等群聊或虚假平台。

警方提示：传播色情信息及刷单均属于违法行为，切勿因猎奇或贪利陷入电诈分子的圈套。

关键词7 ▶ 未知链接、二维码

诈骗分子利用各类网络平台或聊天软件，向受害人发送虚拟链接或二维码，诱导受害人点击或扫描。当用户点击访问时，可能被引导至恶意网站，进而被不法分子获取个人信息；也可能被诱导下载病毒、木马程序或其他诈骗软件。

警方提示：不要随意点击未知链接或扫描二维码，以防财产损失。

关键词8 ▶ 境外来电

境外来电是电信网络诈骗常见的一种引流方式，来电号码通常以“+”或“00”开头，多为虚拟号码。

警方提示：如确无境外通联需要，建议联系运营商开通拦截境外来电服务，从源头上防范电信网络诈骗。

关键词9 ▶ 小众聊天软件

小众聊天软件系用户基数相对较小、知名度较低的聊天类应用，极易被电信网络诈骗分子用来隐匿犯罪行为、销毁犯罪证据，有的甚至专门用来实施电诈犯罪，社会危害性极大。

警方提示：切勿点击陌生链接下载陌生软件，如有下载软件需求请通过官方应用市场等正规渠道。

关键词10 ▶ 内幕消息

诈骗分子通过虚构或夸大“内部消息”“独家情报”等概念，诱导受害人进行所谓“稳赚不赔”的投资或交易，从而实施诈骗。

警方提示：凡是宣称“稳赚不赔”“高额回报”或有“内部消息”的投资理财都是诈骗。

关键词11 ▶ NFC盗刷

目前，NFC（近距离无线通讯）技术应用广泛，如移动支付、公共交通、门禁卡等。然而这项技术被一些不法分子盯上，他们要求受害人将手机与银行卡贴靠，通过NFC功能，将银行卡与手机上的虚拟App软件绑定，进而转移卡内资金。

警方提示：切勿随意将手机与银行卡进行贴靠，谨慎使用手机NFC功能进行陌生支付操作。

关键词12 ▶ 积分清零

一些平台、网站的积分通常具有一定期限，如未及时使用将过期或被清零。诈骗分子通常以“积分清零”为由进行引流，诱导受害人点击木马链接，进而实施诈骗。

警方提示：遇到积分兑换或清零提醒，应通过官方渠道核实。勿轻信非官方渠道发布的积分清零通知，避免盲目操作落入诈骗陷阱。

关键词13 ▶ 快递引流

诈骗分子利用快递包裹作为媒介，通过在快递包裹里附加传单或小礼品吸引受害人注意，引导受害人扫码添加联系方式，再将其拉入诈骗群聊中，进而实施诈骗。

警方提示：不要随意扫描快件里的二维码，遇到邀请进群、转发可领礼品等情况，务必高度警惕。

关键词14 ▶ 虚拟货币

诈骗分子通常以“虚拟货币投资理财”为名搭建虚假平台诱导受害人进行投资，并以线上交易存在风险等理由，扮演“币商”指导受害人操作，从而骗取钱财。

警方提示：虚拟货币交易不受法律保护，所谓“兑换虚拟货币投资”均为诈骗。

关键词15 ▶ “电诈工具人”

在电信网络诈骗犯罪链条中，诈骗分子为完成违法犯罪行为，需要大肆收购、获取“两卡”和个人信息，发展跑分洗钱、推广引流等网络黑灰产，利用多种手段诱骗群众成为“电诈工具人”。

警方提示：订购现金花束、扫码送礼品、帮助取现等看似平常的事情很有可能“埋雷”，务必提高警惕。

关键词16 ▶ “帮信”行为

“帮信”行为是指帮助信息网络犯罪活动的行为，即明知他人利用信息网络实施犯罪，仍为其提供技术支持或帮助的行为。

警方提示：根据刑法规定，构成帮信罪、情节严重的可判处三年以下有期徒刑或拘役，并处或单处罚金。任何出租、出售“两卡”或参与引流、洗钱的行为均属违法犯罪，切勿贪小失大。

关键词17 ▶ “两卡”

“两卡”是手机卡和银行卡的统称。手机卡不仅包括日常使用的移动、电信、联通、广电等运营商的电话卡，还包括虚拟运营商的电话卡以及物联网卡。银行卡包括个人银行卡、对公账户、结算卡以及非银行支付机构账户，如微信、支付宝等第三方支付平台。

警方提示：买卖或租借“两卡”均涉嫌违法。切勿将自己的手机卡、银行卡以及微信、支付宝等第三方支付平台账户出租、出售给他人。

关键词18 ▶ 取现、买黄金

在电诈案件中，诈骗分子通常以各种理由诱导受害人进行线下取现、购买黄金或其他易变现物品等操作，再通过跑腿、网约车、快递等方式将现金或财物交付给指定人员，以逃避资金监管和侦查。

警方提示：凡是要求取出现金或者购买黄金，并通过货运、网约车、邮寄、跑腿等方式转交给陌生人的，都是诈骗洗钱手法。

关键词19 ▶ 购物卡

为逃避资金追查，诈骗分子通常要求受害人将资金转换为购物卡，从而进行套现洗钱。

警方提示：凡是要求大量购买购物卡并提供卡号和密码的，务必提高警惕。

关键词20 ▶ “刷流水”

“刷流水”是指通过制造虚假的资金流动记录，从而增加账户交易流水的行为，主要用于提升信用评级或满足贷款审批要求。诈骗分子通常以“刷流水”为由，诱导受害人向指定账户转账。

警方提示：“刷流水”是违法行为。如在办理相关服务时，遇到对方要求“刷流水”的，务必提高警惕，切勿向对方指定的账户转账。

据“公安部”微信公众号