

谨防网络「暗雷」新型诈骗

网上支付时输入1元，结果竟被扣费1000元……碰到这样的情况，极有可能是遭遇了网络“暗雷”新型诈骗。针对近期破获的多起利用“暗雷”手段实施诈骗的案件，警方提醒公众注意防范。

所谓“暗雷”，是网络黑产技术不断变种升级的又一衍生物。不法分子通过制作色情App、色情视频、虚假购物、网络交友等信息作为诱饵，诱导受害人下载含有木马病毒的App。当受害人下载该App，开通会员支付时，支付页面通常显示只需要1元钱开通，但当确认支付后，“1元就秒变800元或1000元”，此类制作虚假支付页面的障眼法在业内称为“暗雷”。这类App表面上与一般App无异，但受害人在下载安装该App后，往往会掉入不法分子事先设置的“超限采集”“虚假链接”等陷阱，且不法分子在后台操作时，无论是盗取红包、修改金额等，手机界面上都不会出现页面跳转等反应，毫无痕迹，极具迷惑性。

结合已发案件，警方归纳出3种高发网络“暗雷”诈骗手法：一是“虚假链接雷”。

以色情视频、网络刷单等为诱饵，诱导受害人下载暗藏虚假支付链接的不法App，当受害人点击链接进行支付时，实际进入的是虚假支付界面，表面上支付金额为个位数，但不法分子可在后台随意修改金额，造成受害人财产损失。二是“口令红包雷”。以网络色情、游戏低价充值等为诱饵，诱导受害人下载不法App，获取受害人手机的相册权限，引诱受害人生成支付口令，同时窃取口令截图并输入口令取走红包，造成受害人财产损失。三是“购物平台雷”。通过搭建仿真知名购物网站，诱导受害人下载后误以为在使用真实网站，在购物付款过程中，钱款支付进入不法分子搭建的支付通道中，造成受害人财产损失。

警方提示：“暗雷”引爆的前提是手机中必须安装不法分子提供的软件，其寻找“猎物”的渠道多以社交软件为主。因此，一定要从正规的手机应用商店中下载安装所需软件，切勿通过来路不明的短信链接、二维码等进行安装。上网时要保护好个人信息，不轻易泄露银行卡号、密码、动态密码等支付信息。一旦遭受诈骗，要及时留存相关电子证据并报警，依法维护自身合法权益。

躬 罔

摘编自《安徽日报》



魏宇/绘