**通讯网络出现九大新骗局**

**警方教你防范“必杀技”**

近日，江苏警方启动“净网行动”，明确将九大骗局列为“围剿”重点，其中“发给你看看”的“相册诱惑”骗局是最新型的通讯网络诈骗手法。近日，江苏省公安厅刑侦局不仅详解了“相册诱惑”骗局的两种“吸金”方式，还发布了九大新骗局防范“必杀技”，提醒市民加强防范。

【骗局一】“相册诱惑”：短网址迷惑性更强

“同学聚会的照片整理好了，在这里下载……”“你老公跟人开房被拍了照片，想看点这里……”“五一节一起拍的照片弄好了，点击下载”……如果收到这样的短信，千万不要点击，因为这就是今年最新出现的通讯网络诈骗手法——“相册诱惑”，一旦点击短信中的链接，手机就会被植入木马，从而导致信息泄露。江苏省公安厅刑侦局相关负责人介绍，这一诈骗手法出现后，省内已经有不少人中招，但由于该手法的迷惑性、隐蔽性较强，究竟有多少人中招难以统计，“但数量应该相当可观。”

据介绍，之所以说“相册诱惑”骗局诱惑性、隐蔽性强，是因为在这一手段中，不法分子运用了最新的木马技术，而且还糅合了心理暗示等手法，让人防不胜防。“同学聚会的照片、老公开房的照片，这些都戳中了人们的好奇心，想看看的心理暗示强烈，很多人随手便点击了发来的链接。”民警说，而且在此类诈骗短信中，不法分子使用的都是当前最流行的短网址，比如“t.cn/RADJ4HC”，这类链接常见于银行客服的推送以及在微信微博中使用。“潜移默化中，很多人认为这样的链接是可信的。”民警说，事实上，这种链接和以前常见的长网址没有任何区别，同样可以加载木马病毒。同时，“相册诱惑”使用的木马病毒无痕无迹，一旦点击链接，无需你同意，便自动安装。而且安装后，在手机里根本找不到安装的位置，也无从卸载。“和电脑中毒一样，一旦手机中毒，你的手机也就成了不法分子的‘肉鸡’，对于手机中的信息，他们可以为所欲为。”

“吸金”两道：窃网银、骗亲友

今年5月11日，南通的宋先生收到朋友手机发来的短信，称“五一节一起拍的照片弄好了，在t.cn/RADJ4HC下载”。宋先生随即点击该链接，下载了一个名为相册的软件。随即，其手机通讯录内的联系人均接到了宋先生手机发来的短信，内容是：“我在开会，不方便电话，急需2500元汇至我朋友账号上，卡号为：6212XXXXXX，开卡人姓名：XXX”。

“通过点击链接让手机中毒，然后窃取手机上关联的网银信息，从而盗取机主银行卡上的钱款，这确实是‘相册诱惑’骗局的一大‘吸金’手段。”民警介绍，不过就像上述案例描绘的“相册诱惑”还有第二大“吸金术”，就是不仅骗机主本人，还要骗他的亲朋好友。由于手机通讯录中存储的都是关系比较亲近的人的联系方式，所以当他们收到类似求助短信时，往往不加核实便进行汇款。

据了解，上述案例中宋先生的朋友收到求助短信后，有10人进行了汇款操作。而当警方追查到骗子提供的这一账号时，发现上面已经有45万元汇款。也就是说，至少有180人被骗。目前，江苏警方正对此案展开调查。
　　【防范“必杀技”】陌生链接不要点
　　面对“相册诱惑”骗局，该如何防范？江苏省公安厅刑侦专家给出了“必杀技”，不管谁发来的信息，包括短信、微信、邮件，看到陌生链接不要点击，就能避免手机中毒。同时，所有智能手机用户应该安装市场上主流的手机防护软件，在和手机病毒斗争的路上，他们是值得信赖的力量，不仅能主动拦截病毒，对于一些欺诈网站也会有相应的提醒。
　　另外，如果收到亲朋好友发来要求汇款的短信，如果对方自称不方便电话，那么可以回个短信进行询问，这样就能有效识破骗局。
　　如果已经点击了陌生链接，该如何自救？刑侦专家建议，立即将手机格式化，然后送到官方机构进行刷机，重装系统。同时，立即找一台安全的手机，将“中招”手机上关联的所有信息，诸如网银密码、QQ密码、微信密码等等，全部进行修改，以免不法分子盗取。另外，还应该和手机捆绑的银行账户客服联系，修改接收验证码的手机号，以免不法分子拦截验证码窃取银行卡资金。
　　【骗局二】“我是你领导”，骗你没商量
　　今年3月的一天下午6点左右，苏州市民蒋先生接到一陌生电话，对方在电话中问蒋先生是不是下班了，让他明天到其办公室去一趟。蒋先生听对方说话的口气像总公司的领导，当即满口答应。次日上午，蒋先生来到总公司楼下，拨通对方手机后，对方表示正在开会没法见面。之后又说过完年刚上班，要给领导红包，身上没现金，让蒋先生先帮忙垫付。之后，蒋先生通过手机银行向对方转账3笔，共计被骗12万元。
　　这一骗局已经流行一段时间，并有了升级版——“我是你老师”。
　　【防范“必杀技”】核实对方身份
　　刑侦专家表示，不管对方自称“我是你领导”还是“我是你老师”，只要通过自己的途径核实一下对方身份，就不会中招。“其实，在接电话过程中就可以询问‘是哪位领导’，如果对方不能直接、正面回答，那么可以判定就是骗子。”
　　【骗局三】“淘宝客服”来退款
　　今年5月，南京市民殷某在淘宝网购买一双鞋子，次日接到电话，对方自称淘宝客服，称殷某在网上买的鞋子操作流水出现问题，不能发货。对方要将购买鞋子的钱退还给殷某。之后，对方通过QQ发了一个退款网址链接过来，殷某点击进入网站后，按照网站提示输入自己的支付宝账号、密码、姓名、身份证号码、银行卡卡号、取款密码、网银登录密码、银行预留手机号，后发现其银行账户内5万余元被人取走。
　　目前，不法分子不仅冒充淘宝客服，还会冒充京东等其他大型购物网站客服实施诈骗。
　　【防范“必杀技”】打客服电话咨询
　　刑侦专家介绍，破除这类骗局，最有效的方法是直接拨打购物网站的官方客服咨询。当然，客服电话一定要从官方网站获取，通过搜索引擎搜到的很可能还是骗子电话。
　　【骗局四】网络兼职刷信誉
　　今年4月，无锡市民王某在58同城网查招聘信息，发现有人招聘兼职——帮网店刷信誉度，坐在家里就能赚钱。于是，他欣然应聘，按照对方操作提示购买2000元充值卡，对方返还15元。之后。嫌疑人不停地叫王某做任务，要任务全部做完后才有返还。王某在购买10余次充值卡汇出4万余元后，没有拿到任何返利，这才发现被骗。
　　【防范“必杀技”】自己先掏钱的兼职都是假的
　　刑侦专家表示，天上不会掉馅饼，网上兼职不能都说是假的，但如果要你先掏钱再赚钱，那么这种兼职肯定是假的。
　　【骗局五】网购低价二手货
　　今年4月，徐州市民邓某在58同城网上看到一条二手摩托车信息，随即和对方QQ联系。对方自称在广东汕头，可以通过物流将摩托车发过来，价格为6500元，这远远低于市场价。次日，卖家打电话给邓某，称摩托车由某物流公司发过来，已经在物流包装好，让其和物流公司联系。和物流公司联系后，对方以种种理由要求邓某汇款，导致邓某被骗一万多元。
　　【防范“必杀技”】网购就上正规购物平台
　　刑侦专家表示，私下交易风险无限，要网购还是得上淘宝、京东、苏宁易购等正规购物平台，资金有保障、维权也有门。
　　【骗局六】伪基站诈骗
　　今年5月，孔某在餐厅吃饭时，手机收到“10086”发来的一条短信，称其积分可兑换189.36元现金即日将过期，请立即登陆移动商城“10086uq.cn”，根据提示下载激活码领取。后孔用手机登陆对方提供的网址，按要求输入银行卡号及密码，并下载了所谓激活码，后手机收到多条银行卡消费记录，银行卡上少了3450元，孔发现被骗。事实上，所谓的“10086”短信，是不法分子通过伪基站发送，细心一些也会发现移动商城的网址多了点什么。
　　【防范“必杀技”】自己找官方网站登陆
　　刑侦专家表示，破解这一骗局最直接的办法就是不要点对方发来的链接，自己上移动公司官网查看。
　　【骗局七】“残联”给你发补贴
　　今年5月，残疾人李某接到自称江苏残联的电话，称李符合国家残疾人发放补贴政策要求，残联将给李打5000元，让李提供银行账户转账。李某即按对方要求让其妻子在ATM及操作，对方通过电话联系李妻子称转账失败，索要李的银行卡密码称为其银行卡直接转账操作，后银行卡内现金被转走。这一诈骗形式和早先的“生育补贴”“二孩补贴”“汽车退税”等等手法如出一辙。
　　【防范“必杀技”】补贴、退税不会在ATM机上领
　　刑侦专家表示，不管是退税还是补贴，如果对方提到去ATM机上操作，那么百分百是假的，应果断挂电话。
　　【骗局八】邮包藏毒电话诈骗
　　今年3月，常州市民张某手机接到一个座机号码的电话，电话自动播放语音：称其有包裹未领取，详情致电XXXX。张某拨打该电话后，对方称其邮包有违禁品，之后电话转给“陈警官”。“陈警官”称张某的银行账户信息外泄，被人冒用从事运毒犯罪，让张某升级银行卡并加密，骗其到ATM机操作，被骗1600元。
　　这一骗局是比较传统的电话诈骗手法，已经存在多年，但仍不时有人上当。和其同类的骗局还有以“电话欠费”“有线电视欠费”“法院传票”“公安通缉”等由头的诈骗手法。
　　【防范“必杀技”】公检法不会电话办案
　　刑侦专家介绍，公检法机关不会通过电话办案，一旦有所谓的“警官”“检察官”“法官”在电话里指示你做这做那，肯定是骗局。
　　【骗局九】老总QQ喊会计汇款
　　今年5月的一天，盐城某公司会计刘某接到公司财物总监庄总QQ信息，让她马上汇一笔钱到朋友账户上。刘某没有怀疑，当即汇款43000元。后电话联系庄总得知被骗。
　　【防范“必杀技”】汇款前先打电话核实
　　刑侦专家表示，作为虚拟通讯工具，QQ那头是谁无法知晓。遇到此类情况，只要在汇款前打电话核实，就能识破骗局。