警惕移动支付欺诈陷阱

移动支付在给网民带来便利的同时，也成了不法分子眼中的“吸金利器”，短信诈骗、篡改网页支付信息、发布病毒二维码等成为骗子最爱用的诈骗手段，涉案金额少则几百元，多则上百万元。

扫一张二维码 农村家庭损失29万元

近日，李同学收到了朋友发给他的一张图片，图片上面写着：“扫描二维码关注，可以免费领取50元手机话费。”他扫描二维码并关注了一个名为“聚XX”的微信，按要求给好友群发了图片并且截图发给“聚XX”微信，还提供了手机号码。

两天后的早晨，李同学刚开机就看到一百多个来自亲朋好友的未接电话。他回拨了妈妈的电话，妈妈听到儿子的声音，急忙问：“你没出事吧？昨天你们‘辅导员’打电话说你吸毒欠钱被人绑架了，要拿30万元才放你，不然早上就……”李妈妈已经讲不出话了。李妈妈对儿子说，家人听到消息后急得没有办法，不仅取出了银行里的13万元存款，还四处找亲戚朋友借了16万元，辅导员也帮着垫了1万元，就这样，29万元转给了骗子。

罪魁祸首就是前几天李同学群发的图片，骗子通过图片获取了李同学的手机号和好友关系链，通过网络透传技术，把电话号伪装成李同学的电话并给李妈妈发了短信，提供了所谓的“辅导员”的手机号。

移动支付诈骗方式花样翻新 6种手法要认清

为防止公众受到移动支付新型诈骗的侵害，福建省厦门市公安部门近日公布了6种利用木马病毒实施诈骗的新手法，提醒人们加强防范。

1.“二维码”暗藏木马 网购族得当心

扫扫二维码，优惠便利跟着来，但二维码有时也成为骗子们的“新花招”。

警方介绍，诈骗分子在网上下载一款“二维码生成器”，再将病毒程序的网址粘贴到二维码生成器上，就可以生成一个“有毒”的二维码。

利用这些二维码，诈骗分子会将手机木马病毒植入被害人的手机中，并自动提取相关信息，短短几秒钟，手机号、卡号、密码等私人信息就可能已经传到了他人手中。

2.“官方服务号码”发来短信 提醒安装APP换积分

犯罪分子通过群发信息设备假扮官服号码，群发诈骗短信，称可以兑换积分，其实短信中内置了一个钓鱼网址。

用户按照短信要求登录钓鱼网址，输入个人信息后，会被要求安装一个手机APP。这个APP里也带有木马病毒，用户手机内所有的短信，均会被拦截到诈骗分子设置的短信接收手机号码上。然后，诈骗分子通过电商和支付平台发起购物申请时，快捷支付向用户手机号发送的短信验证码会被手机木马病毒读取并发送，通过短信验证码，诈骗分子可完成银行卡盗刷，使用户的财产遭受损失。

3.QQ木马专盯财务人群 骗走149万元

诈骗人员通过QQ搜索财务人员群等，加入后向目标人发送木马链接，只要目标人点击打开，再次点击登录，嫌疑人从后台就可看到QQ账号和密码，从而窃取目标对象的QQ信息，然后冒充老板、朋友等对其同事、亲友等进行诈骗。

4.木马病毒植入淘宝支付链接

犯罪分子先冒充客户，将显示未支付成功的订单号（事先已制作好）发给淘宝商家，再冒充淘宝客服，以升级支付权限为由，将花钱买来的新型木马病毒发给淘宝商家安装。商家一旦安装，病毒就会植入支付链接页面，造成支付成功的假象，骗子继而蒙骗淘宝商家并套现。

5.投放抢红包软件 引诱用户下载

很多骗子会制作一些抢红包软件投放在网络上，引诱用户下载，或是通过二维码，将木马不知不觉中植入用户的手机中。这些木马软件通过盗取用户信息，截取用户短信，获取验证码等方式，悄悄转移用户财产。

警方表示，手机一般情况下是不会自动下载木马软件的，当抢红包时要求下载软件或是扫描二维码时，市民就要多留一个心眼，不要轻易上当。

6.发送含有木马病毒链接的短信

犯罪嫌疑人利用非法手段获取他人的手机号码，并发送含有木马病毒程序链接的欺骗短信，受害人点击后，手机就中了木马病毒。该新型木马病毒能拦截手机短信，并转发至另一个指定手机号码上。犯罪嫌疑人利用受害人的手机号码等信息非法获取其身份信息和银行卡信息，并通过被拦截的手机短信，利用网络支付漏洞，使用受害人的银行卡，通过网上支付为他人支付电费、充值游戏点卡等消费返现，非法获利。

（央新）

六招教你防范被骗

1.对不明的链接、网址、红包等不要点击，对可疑软件以及未经确认的链接不点击、不下载。

2.安装防病毒安全软件等防护程序，智能手机和网银用户要对手机定期杀毒。

3.各种银行、支付宝转账要通过官方网站下载的APP软件进行网银操作，不要轻易向他人泄露银行账号、密码、身份证号和交易验证码等相关信息。设立支付宝和网银的每日消费上限，不存过大数额的资金。

4.如果手机、QQ、微信等收到不明链接，应采取不予理睬的态度，不点击、不查看，避免“好奇心”被利用。

5.不要扫描来路不明的二维码，不要因贪图小利拨打短信中的陌生电话，以防受骗。

6.不要将资金转入陌生的账户。