您上当了没有?

通讯网络诈骗手段

日常生活消费类欺诈

针对日常生活各种缴费、消费实施欺诈骗局

32. 冒充房东短信诈骗：犯罪分子冒充房东群发短信，称房东银行卡已换，要求将租金打入其他指定账户内，部分租客信以为真，将租金转出方知受骗。

33. 电话欠费诈骗：犯罪分子冒充通信运营企业工作人员，向事主拨打电话或直接播放电脑语音，以其电话欠费为由，要求将欠费资金转到指定账户。

34. 电视欠费诈骗：犯罪分子冒充广电工作人员群拨电话，称以受害人名义在外地开办的有线电视欠费，让受害人向指定账户补齐欠费，部分群众信以为真，转款后发现被骗。

35. 购物退税诈骗：犯罪分子事先获取到事主购买房产、汽车等信息后，以税收政策调整可办理退税为由，诱骗事主到ATM机上实施转账操作，将卡内存款转入骗子指定账户。

36. 机票改签诈骗：犯罪分子冒充航空公司客服，以“航班取消、提供退票、改签服务”为由，诱骗购票人员多次进行汇款操作，实施连环诈骗。

37. 订票诈骗：犯罪分子制作虚假的网上订票公司网页，发布虚假信息，以较低票价引诱受害人上当。随后，以“订票不成功”等理由要求事主再次汇款，实施诈骗。

38. ATM机告示诈骗：犯罪分子预先堵塞ATM机出卡口，并粘贴虚假服务热线，诱使用户在卡“被吞”后与其联系，套取密码，待用户离开后到ATM机取出银行卡，盗取用户卡内现金。

39. 刷卡消费诈骗：犯罪分子以银行卡消费可能泄露个人信息为由，冒充银联中心或公安民警设套，套取银行账号、密码实施犯罪。

40. 引诱汇款诈骗：犯罪分子以群发短信的方式直接要求对方向某个银行账户汇入存款，由于事主正准备汇款，因此收到此类汇款诈骗信息后，往往未经核实，即把钱款打入骗子账户。

钓鱼、木马病毒类欺诈

通过伪装成银行、电子商务等网站窃取用户帐号密码等隐私的骗局

41. 伪基站诈骗：犯罪分子利用伪基站向广大群众发送网银升级、10086移动商城兑换现金的虚假链接，一旦受害人点击后便在其手机内植入获取银行账号、密码和手机号的木马，从而进一步实施犯罪。

42. 钓鱼网站诈骗：犯罪分子以银行网银升级为由，要求事主登录假冒银行的钓鱼网站，进而获取事主银行账户、网银密码及手机交易码等信息实施诈骗。

其他新型违法类欺诈

43. 校讯通短信链接诈骗：犯罪分子以“校讯通”的名义，发送带有链接的诈骗短信，一旦点击链接进入后，手机即被植入木马程序，存在银行卡被盗刷的风险。

44. 交通处理违章短信诈骗：犯罪分子利用伪基站等作案工具发送假冒违章提醒短信，此类短信包含木马链接，受害者点击之后轻则群发短信造成话费损失，重则窃取手机里的银行卡、支付宝等账户信息，随后盗刷银行卡，造成严重经济损失。

45. 结婚电子请柬诈骗：犯罪分子通过电子请帖的方式诱导用户点击下载后，就能窃取手机里的银行账号、密码、通信录等信息，进而盗刷用户的银行卡，或者给用户通讯录中的朋友群发借款诈骗短信。

46. 相册木马诈骗：犯罪分子冒充“小三”身份激怒受害人点击“相册”链接，种植木马病毒获取用户网银信息等。

47. 金融交易诈骗：犯罪分子以证券公司名义，通过互联网、电话、短信等方式散布虚假个股内幕信息及走势，获取事主信任后，又引导其在自身搭建的虚假交易平台上购买期货、现货，从而骗取事主资金。

48. 办理信用卡诈骗：在媒体刊登或通过QQ、微信等发布办理高额透支信用卡广告，事主与其联系后，以缴纳手续费、中介费等要求事主连续转款。

49. 贷款诈骗：犯罪分子通过群发信息，称其可为资金短缺者提供贷款，月息低，无需担保。一旦事主信以为真，对方即以预付利息、保证金等名义实施诈骗。

50. 复制手机卡诈骗：犯罪分子群发信息，称可复制手机卡，监听手机通话信息，不少群众因个人需求主动联系嫌疑人，继而被对方以购买复制卡、预付款等名义骗走钱财。

51. 虚构色情服务诈骗：犯罪分子在互联网上留下提供色情服务的电话，待受害人与之联系后，称需先付款才能上门提供服务，受害人将钱打到指定账户后发现被骗。

52. 提供考题诈骗：犯罪分子针对即将参加考试的考生拨打电话，称能提供考题或答案，不少考生急于求成，事先将好处费的首付款转入指定账户，后发现被骗。

53. 盗用账号、刷信誉诈骗：犯罪分子盗取商家社交平台账号后，发布“诚招网络兼职，帮助淘宝卖家刷信誉，可从中赚取佣金”的推送消息。受害人按照对方要求多次购物刷信誉，后发现上当受骗。

54. 冒充黑社会敲诈类诈骗：犯罪分子先获取事主身份、职业、手机号等资料，拨打电话自称黑社会人员，受人雇用要加以伤害，但事主可以破财消灾，然后提供账号要求受害人汇款。

55. 公共场所山寨WiFi诈骗：犯罪分子设置山寨信号，这类信号就是一些盗号者在公共场合放出的钓鱼免费WiFi，当连接上这些免费网络后，通过流量数据的传输，黑客就能轻松将手机里的照片、电话号码、各种密码盗取，对机主进行敲诈勒索。

56. 捡到附密码的银行卡：犯罪分子故意丢弃带密码的银行卡，并标明了“开户行的电话”，利用了人们占便宜的心理诱使捡到卡的人拨打电话“激活”这张卡，并存钱到骗子的账户上。

57. 账户有资金异常变动：犯罪分子首先窃取了受害者网银登陆账号和密码，通过购买贵金属、活期转定期等操作制造银行卡上有资金流出的假象。然后假冒客服打电话确认交易是否为本人操作，并同意给用户退款骗取用户信任，要求受害者提供自己手机收到的验证码，受害者一旦把短信验证码提供给了对方，对方就得手了。

58. 先转账、再取现、后撤销：犯罪分子利用银行转账新规中转账和到账时间的“时间差”来设置圈套。采取先转账、后给现金的诈骗套路，在骗取到受害人现金后，撤销转账。

59. 补换手机卡：犯罪分子先用几百条垃圾短信和骚扰电话轰炸手机，以掩盖由10086客服发送到手机号码上的补卡业务提醒短信；然后，拿着一张有受害者信息的临时身份证，去营业厅现场补办手机卡，使得机主本人的手机卡被动失效，从而接收短信验证码把绑定在手机APP上的银行卡的钱盗走。

60.“换号了请惠存”：这属于冒充熟人的电信诈骗的“升级”。犯罪分子通过非法渠道获得机主的通讯录资料后，假冒机主给手机里的联系人发短信，声称换了新号码，然后向其手机里的联系人进行诈骗。

警方提示

只要涉及钱财，不见面、不轻信、不给验证码！

据警方介绍，虽然骗术五花八门，其实归结起来就是利用了大家的五种心理：一是贪财、好占小便宜或者是赚钱心切；二是担心自身财产安全；三是担心人身安全或者个人隐私；四是网上购物、银行转账时的疏忽；五是对熟人求助、官方机构不设防。

如何防范通讯（网络）诈骗，最简单也最有效的方式是牢记三句话，即掌握应用“一分析，二咨询，三打110”的防范“三步法”——

1. 多分析。接到要求转账汇款的电话、短信、微信等，一定要先作仔细分析，辨明真伪，千万不要轻易汇款！要牢记天上不会掉馅饼，无抵押无担保的低息贷款、无缘无故的中奖等都是假的。当然，接到法院给你发传票、公安机关来电要你接受调查这类电话，也不要相信，不可抱着“花钱消灾”的心思转账汇款。

2. 多咨询。当我们一时分辨不清时，应立即向亲友咨询，中老年人更应向年轻人多咨询。只要多向身边的亲友询问，也很容易被识破！

3. 打110。假如我们通过分析、咨询，仍无法辨明真伪，可以直接拨打110电话，向公安机关进行咨询，他们会给予热心、明确的答复。假如已经被骗，要立即报警，争取挽回损失。

记者　张贻富　通讯员　王西泽