网络淫秽、网络欺诈、非法网络寄递……在互联网带给百姓方便快捷生活的同时,网络犯罪也在侵蚀网络生态,使广大网民蒙受巨大的损失。网络诈骗具有传播范围广、速度快、成本低、收益高、隐藏快等特点,因此屡禁不止。

网络诈骗有哪些类型?日常生活中该如何防范?我们整理了身边发生的一些典型案例,希望能对读者起到帮助。

■记者 闵波 通讯员 毛群

借你一双慧眼 远离网络诈骗

网络诈骗典型案例

中奖骗局

2009年10月9日,阿亮(化名)上网玩游戏时,电脑上弹出一则中奖公告。阿亮按对方要求操作,通过某银行汇了手续费、保证金、邮寄费等5300元后,对方以交个人所得税和保险费为借口又要求他汇款10000元。此后阿亮等不来奖品,方知道受骗,但汇走的15300元现金已无法追回。

彩票预测骗局

2009年10月21日,阿青(化名)在家上网时,打开“中国福利彩票官方预测中心”网站,对方称能预测中国福利彩票中奖号码。阿青便与对方取得联系,对方以加入会员、交预测费及资料费为由,先后分3次骗其汇款8598元。

2009年9月14日,受害人胡某到市公安局网监支队报案称,一个名叫“北京福利彩票官方网”的网站声称能够预测彩票中奖号码,他信以为真,先后被该网站的工作人员以注册会员费、专家预测费、保证金等理由,骗取现金48102元。

股票内幕消息骗局

2009年10月13日,阿云(化名)上网浏览股市信息时,在某网站留下联系电话。后来,一名自称是“中金公司”业务员的男子打电话与他联系,以帮助炒股获取高额回报为由,骗取阿云汇款11000余元。

网络购物骗局

2009年9月23日,郧西电信公司职工韩某报案称:其在互联网上购买笔记本电脑时被他人诈骗4500元。10月27日,郧西县公安局经过缜密侦查,在海南省定安县将犯罪嫌疑人吴某抓获。后查明,当年2月,吴某伙同他人在淘宝网和拍拍网上注册网店,销售笔记本电脑等物,在网民进行转账交易时,采取链接假网站的方式转移资金进行诈骗,受害网民达数十人,涉案金额10余万元。

QQ移花接木骗局

潘某是城区某单位职工,2010年1月24日,他用QQ和单位领导“李某”聊天时,“李某”说急需要用钱,让潘某向指定的账户汇款1万元。聊天时,“李某”还主动跟潘某视频,潘某信以为真,按照要求汇了款。事后潘某才知道,和他用QQ聊天的不是李某,而是骗子,潘某所看到的视频也是剪辑过的。

篡改高校招录网骗局

2007年7月30日中午,武汉大学招办工作人员发现,考生谢某高考成绩仅有313分,竟然被武汉大学“录取”。工作人员进一步核对,证实谢某并未真正被录取,其名字是被人非法添加到录取学生查询数据库中。该校迅速关闭网站,并向警方报案。武汉市公安局半个月后抓获了作案嫌疑人,排查出为非法招生提供活动平台的个人网站《高校招生网》及其建站人钟某。警方查明,一伙招生中介人员为炫耀招生实力,对外谎称可弄到“内部指标”,通过黑客技术篡改招生网页骗取考生和家长信任,从而诈骗钱财。据查,其中一个考生就被骗走10余万元。

◆诈骗种类◆

网络购物诈骗

(1)多次汇款——骗子以未收到货款,或提出要汇款到一定数目方能将以前款项退还等各种理由,迫使事主多次汇款。

(2)假链接——骗子为事主提供虚假链接或网页,交易显示不成功,让事主多次往账户里汇钱。

(3)拒绝安全支付——骗子以种种理由拒绝使用网站的第三方安全支付工具,比如谎称“我的账户最近出现故障,不能用安全支付收款”或“第三方安全支付工具要收手续费,如果不使用可以再给你算便宜一些”等等。

(4)收取订金——骗子要求事主先付一定数额的订金或保证金,然后才发货,利用事主急于拿到货物的迫切心理,以种种看似合理的理由,诱使事主追加订金。

(5)约见汇款——网上购买二手车、火车票时,骗子一方面约见事主在某地见面验车或给票,要求事主的朋友一接到事主电话就马上汇款,然后利用“来电任意显软件”冒充事主给其朋友打电话让其汇款。

(6)以次充好——用假冒、劣质、低廉的山寨产品冒充名牌商品,事主收货后连呼上当。

网络钓鱼诈骗

(1)发送电子邮件,以虚假信息引诱用户中圈套。不法分子大量发送欺诈性电子邮件,邮件多以中奖、顾问、对账等内容引诱用户在邮件中填写银行账号和密码。

(2)不法分子设立假冒银行网站,当用户输入错误网址后,就会被引入这个假冒网站。此外,犯罪分子通过发送含木马病毒的邮件等方式,把病毒程序植入计算机内,一旦客户用中毒的计算机登录网上银行,其账号和密码就可能被不法分子所窃取。

利用QQ盗号和网络游戏交易进行诈骗

(1)冒充QQ好友借钱。骗子使用黑客程序破解用户密码,然后张冠李戴冒名顶替向事主的QQ好友借钱,或者通过盗取图像的方式用“视频”聊天博取信任。

(2)利用网络游戏装备及游戏币交易进行诈骗。常见的诈骗方式一是低价销售游戏装备,犯罪分子在骗取玩家信任后,让玩家通过线下银行汇款购买游戏装备;二是在游戏论坛上发表代练帖,待得到玩家的汇款及游戏账号后,代练一两天后连同账号一起侵吞;三是在交易账号时,提供比较详细的资料,待交易结束后,再盗取账号,造成玩家经济损失。

(3)交友诈骗。犯罪分子利用网站以交友的名义与事主初步建立感情,然后以缺钱等名义让事主汇款,最终失去联系。

面对以上形形色色的网络诈骗手段,应该如何有效地识别、应对和防范?别着急,警方给你支招:

1、使用QQ或其它及时通信工具聊天时,当有人要求汇钱,应通过电话核实,不要相信聊天信息或聊天视频。

2、一旦发觉对方可能是骗子,马上停止汇款,防止扩大损失。或者拨打官网客服电话或110报警电话向有关部门进行求证或举报。

3、网上购物时不要被某些价格低廉的商品所迷惑,要选择知名、信誉较好的网站进行交易。进行支付时,最好找支持中间支付平台的卖家,避免通过银行汇款。

◆警方支招◆

4、妥善保管自己的私人信息,如证件号码、银行账号、密码等,不向他人透露,并尽量避免在网吧等公共场所使用网上电子商务服务。

5、以短信或网上发布招工、代办贷款信息,并预收手续费,要谨慎,最好当面考察,确认无误后再交易。

6、不要相信网站系统消息弹出的“中奖信息”,更不要支付任何费用。

7、不要相信所谓的预测彩票中奖号码、合作炒股票等虚假网站,没有谁可以预测彩票中奖号码或保证某股票绝对上涨。

8、打电话告知当事人,其家属、朋友涉嫌违法或发生意外,需用大量现金,并提供汇款账户,一般不要相信。

9、安装正版杀毒软件,并及时升级,定时对电脑扫描杀毒。其它应采取的网络安全防范措施还包括:禁止浏览器运行JavaScript和ActiveX代码;不要上一些不太了解的网站;不要执行从网上下载后未经杀毒处理的软件。

网络诈骗让人防不胜防,需要从法律层面予以打击。在今年全国两会上,提请十一届全国人大四次会议审议的最高人民检察院工作报告中强调,要依法打击利用互联网传播淫秽信息等网络犯罪,净化网络环境。两会代表委员结合审议、讨论的“两高”报告,建议用三大手段遏制网络犯罪。

◆打击遏制◆

1、摧毁网络欺诈的“歪门”

除了以中奖、网购、网银、招聘、电邮等方式出现的网络诈骗案件外,虚假宣传、商业攻击等新型网络欺诈行为愈演愈烈。在今年全国两会上,全国人大代表、广东东莞电信公司副总经理邓海玲建议,按照“谁主管、谁负责,谁经营、谁负责,谁接入、谁负责”的原则,严厉打击网络欺诈,同时尽快推进网络信息安全立法。全国人大代表、律师陈舒提交的议案写道:“对网络欺诈行为应设立惩罚性赔偿,而不仅仅是实际损失赔偿,以真正遏制犯罪行为。”

2、封死非法网络寄递的“暗门”

最新修订的《邮政法》规定,邮政企业须依法执行邮件收寄验视制度。对交寄物品一律进行验视,否则不予收寄。“非法网络寄递,最终要落到快递和物流企业的头上,网络寄递市场安全形势严峻。”全国人大代表邓海玲说,一些快递企业收递员从不开包验视违禁物品,也不核对邮递人的有效证件,这为不法分子提供了可乘之机。

3、堵住网络诈骗的“命门”

今年3月,最高人民法院、最高人民检察院发布了《关于办理诈骗刑事案件具体应用法律若干问题的解释》。对电信诈骗数额难以查证,但发送诈骗信息5000条以上的,拨打诈骗电话500人次以上的,或者诈骗手段恶劣、危害严重的,即可以诈骗(未遂)罪追究刑事责任。《解释》于4月8日开始实施。