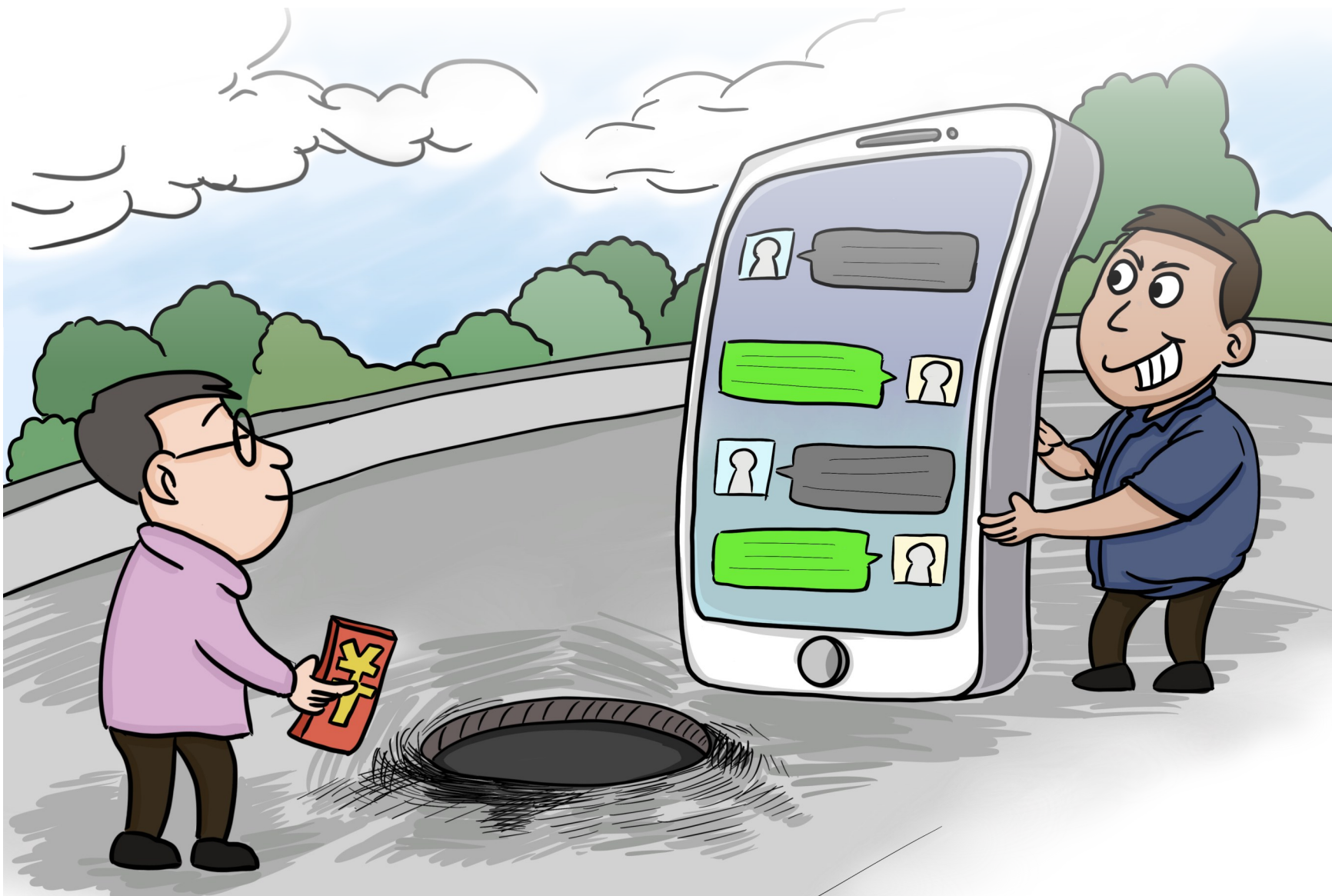


高举“法律之剑” 打造“技术之盾” 筑牢“反诈之墙”



■记者 王基诺 通讯员 董超君

今年12月1日,《中华人民共和国反电信网络诈骗法》将正式施行。电信诈骗犯罪这一发案率最高的突出犯罪,将迎来专门法律治理时代,接受“法律之剑”的制裁。

反诈不仅需要法律层面的顶层建构,更需要建立群防群治的全社会综合机制。近期,区公安分局依托“技术之盾”,通过反诈预警,加强受骗资金紧急拦截工作,筑牢全民反诈的“防护墙”。

帮你“日进斗金”? “炒股大师”设下暴富陷阱

11月15日晚8时许,区公安分局闻潮派出所接到反诈预警,辖区群众张先生正在被骗。反诈劝阻工作人员叶晨曦立即联系张先生,在电话接通后,马上表明身份,要求张先生停止转账操作,等待民警上门核校。

张先生表示可以自行来派出所。据张先生述说,自己是通过某软件平台刷到了所谓的“炒股大师”,“大师”讲述的炒股赚钱操作特别吸引人,并称可以帮忙“指点迷津”。

于是,张先生添加“炒股大师”为QQ好友,并被对方拉进了所谓的炒股培训班,下载了某炒股软件进行虚拟股票投资,一开始确实小赚了几笔,本来还打算继续投钱进去,就接到了派出所的电话。

见张先生还是半信半疑,工作人员只能让张先生试着将投进炒股软件的钱提现,看能不能取出来。经过一番操作,张先生发现钱已经无法取出,又联系了客服、培训班其他人 and 所谓的“炒股大师”,才发现自己已经被拉黑,这才恍然大悟。

在工作人员的帮助下,张先生卸载了所谓的炒股软件,并下载了“国家反诈中心”APP。此次劝阻,成功为张先生止损6000元。

警方提醒:

市民的手机号、微信号等个人信息,需经过实名认证后才能使用,是个人与外界交流沟通的重要工具;上述号码结合其他信息能够锁定特定自然人信息,记录个人通信信息、关联个人财产信息,与个人人身安全和财产安全直接相关。我们在日常生活中,要注重养成良好的个人信息保护意识、掌握基本的个人信息保护知识和防护技能。不要随意向他人透露身份证号、银行卡号、密码及其他个人隐私信息,如遭遇个人信息泄露,可向相关部门投诉或向公安机关报案。

“投资”
网站
裸聊
“贷款”



贷款先交款? 虚假贷款越贷越穷

10月12日11时许,刘先生接到了某“银行客服”的电话。刘先生正好有贷款需求,得知贷款“十分容易,迅速到账”后,在对方的引导下,添加了对方的微信,并通过对方提供的二维码扫描下载了某软件,录入了身份及银行账户信息,申请了2万元的贷款。

然而,当一切看似十分顺利时,对方

却突然以“信息填写错误,需要另行支付保证金”为由,要求刘先生转一笔保证金。12时许,公安劝阻员陈子涵发现此事,并马上电话联系刘先生开展电话劝阻,告知他停止一切操作。刘先生意识到自己被骗,立即停止了操作。

警方提醒:
借贷要通过银行等国家正规金融

融机构申请,不要轻信任何网友、网站、手机应用发布的贷款广告;不扫描、不点击任何来源不明的二维码和链接,避免让人趁“需”而入;银行和正规贷款公司都不会要求借款人预先支付手续费等各类费用,任何要求事先支付资金的都是骗子!切勿上当。

“要脸还是要钱”? 裸聊诈骗当心“桃花劫”

11月17日深夜两点,临江派出所接到群众报警称,其遭到他人恐吓。然而,当值班民警问及具体情况时,该男子却始终支支吾吾,不肯说出真相。

该男子的异常表现引起了民警的重视,辅警陈祥和徐溢涛很快找到了报案人廖先生。在详细查看了廖先生某社交软件聊天信息后,确认其遭遇了裸聊诈骗。

原来,前几天,廖先生通过某社交软件认识了一位“女朋友”,两人越

聊越投机。一天晚上,对方竟主动提出想和他“坦诚相见”。面对从天而降的艳遇,廖先生欣然答应,殊不知这是犯罪分子为他精心编织的“桃色陷阱”。

裸聊后不久,“女朋友”突然发来两人的视频聊天截图,一改先前的甜言蜜语,态度强硬地要求廖先生转账,否则就把视频发送给廖先生的家人和同事。一番思想斗争后,廖先生鼓足勇气给临江派出所打来了报警电话。

警方提醒:

在裸聊诈骗中,诈骗分子通常不会一上来就狮子大开口,一般会要求你转一笔承受范围内的资金,并许诺转账后删除视频,但之后又会想尽各种办法要求转账。市民遇到此类情况,别犹豫,马上报警。

同时,市民要文明上网,洁身自好,不要向陌生人泄露身份和家庭等信息,不点击陌生链接,如遇电信网络诈骗,应保持冷静,立即向警方求助,切勿盲目转账。

在派出所他急忙写下13个字 这场“无声劝阻”更有声

近日,我区一位聋哑小伙遭遇电信网络诈骗,时间紧迫,焦急之际,辅警胡嘉靖灵机一动,拿出纸笔,上演了一场无声劝阻……

10月31日,区公安分局金沙湖派出所接待了一名求助男子,该男子神情慌张,不断地将自己的手机递给胡嘉靖看,但始终不说话。通过手机翻译器,男子告知胡嘉靖自己是聋哑人,由于不会在手机上进行转账操作,故而来派出所求助,希望有人可以帮助他完成转账。

经了解,男子姓李,在无意间加入一QQ群,看到了群内有人发布“清退投资金额,返还本金利息”的活动。恰好小李有投资失败的经历,且当时的投资款项一直没有拿回,便了解了群内的信息。

不久,QQ群内有人主动联系小李,称可以退还小李5万余元投资款,但需要小李先缴纳20%的手续费。紧接着,对方向小李发送了一个软件下载链接,引导他下载了一个陌生软件,并按步骤在该软件中操作“转账”。

胡嘉靖了解相关情况后,随即判断小李疑似正在遭遇电信诈骗,由于沟通不易,胡嘉靖灵机一动,马上在手边的纸上写下“诈骗”“不要信”“群退掉”“千万别转账”等13个大字。通过书写文字的方式劝说小李停止一切操作,同时立即将相关情况汇报至值班民警周杰栋。

经周杰栋再次甄别,确定了小李正在遭遇电信诈骗,随即,再次通过书写等方式开展劝阻工作。起初,小李觉得“自

己不会被骗”,想要离开自行研究转账。见状,周杰栋立即拦住小李,逐步引导小李在群内发信息,表明自己已与派出所对接。

谁知,当小李在群内发送完消息后,便立马被踢出了群聊,小李这才确信自己刚刚遭遇了电信诈骗。至此,金沙湖派出所紧急止付资金11080元。

警方提醒:

除了投资诈骗,广大残障人士还要提高警惕,预防诈骗分子利用政府提供的惠残政策、专项调查、残疾人证办理等事由进行诈骗。做到不轻信陌生人电话,不轻易将个人信息、财产信息、身份证号、残疾人证号、银行账号等提供给陌生人。一旦接到诈骗信息,要及时报警。

钱塘说法

借助科技手段,骗子会假冒运营商、银行的官方平台,向市民发送“通知短信”,如果大家没有仔细辨认,就容易落入他们的圈套。在此我们整理了十条防诈骗秘籍,大家千万要记牢。

1. 有人要“验证码”,别给

验证码很常见,但它并不是简单的几个数字,代表的是身份的验证。来源不明、自己不知情的验证码千万不要提供给别人,尤其是不能发给陌生号码。一旦不法分子获取了验证码,后果将不堪设想。

2. 短信内带链接,别点

大家要记住:链接是个坑。虽然手机短信中也有银行等机构发来的安全链

接,但现在伪基站、改号软件一波刚死一波又起,诈骗分子总有各种办法伪装自己,很多人难以通过对方短信号码、短信内容、链接形式等辨别真伪。建议大家不要点击短信中自带的任何链接。

3. 手机不显号码,别接

目前,任何政府、企业、银行、运营商等机构均有官方电话,“无显示号码”基本上来源网络电话,要么是打广告的,要么就是诈骗,宗旨就是看到“无显示号码”来电,直接挂断就好。

4. 询问银行卡号,不说

无论电话、短信、QQ聊天,微信对话中都绝不提及银行卡号、密码、身份证号、医保卡号码等信息,以免被诈

骗分子利用。就算是和“熟人”聊天也要谨慎,可能存在朋友被盗号的情况。

5. 有些号码可以拨打验证真假

诈骗分子通过虚拟改号软件,模仿运营商、银行的官方客服拨打电话。最近就有不法分子利用改号平台冒充“中国移动国际漫游服务热线13800100186”,骗取用户信息。遇到这种情况,大家可以直接挂断,再主动拨打相关电话询问,注意不要直接回拨。

6. 钱财“只能进不能出”

任何要求打款、汇钱的行为都值得怀疑。孩子住院了,你被告了要交保证金之类的都别信。警方建议就算真的要汇款,最好选择去线下银行柜台办

理,把事情的头末向银行柜台工作人员描述一遍,咨询更多人的意见。

7. 叫出你名字的人不一定是熟人

诈骗分子能够通过非法的行为掌握到用户的一些个人信息,并以此作为证据骗取信任,此时切记不能相信陌生人,就算电话号码是朋友家人的,如非当面沟通也不要轻易相信。

8. 养成核实网址、网站域名的习惯

利用伪基站假冒10086不说,还模仿中国移动的官网做钓鱼网站。切不可轻易信任那些看上去与官方网站长得一模一样的钓鱼网站,不仅可能中病毒,还可能被骗走钱财。大家一定要养成

核实网站域名、网址的习惯。例如中国移动的官网是以10086.cn为后缀的。

9. 不信天上掉馅饼

诈骗分子常常利用最新的时事热点涉及骗局内容,并用中奖等信息诱惑用户,如疫苗补偿、孩子退学费、海淘退税、热播电视节目中奖等都常常被骗子利用。一定要警惕这种天上掉下来的馅饼,不要误信掉入陷阱。

10. 请下载“国家反诈中心”APP,并开启来电预警

牢记96110,如果遇到可疑情况,不确定是否为网络诈骗,就打电话进行咨询,预警人员会耐心地聆听、真诚地解答,随时为您提供帮助。