

一个月26人被骗85.1万元

全是电信诈骗,其中,一女子上月27日被骗了28万元

□记者 王震 报道
□通讯员 曲新峰

本报5月2日讯 近期,电信诈骗案件在威海高发,仅环翠区一个月就有26名市民上当,共被骗85.1万元。其中一女市民于4月27日被骗走28万元。警方发现其中规律:受害重点人群是老年人、家

庭主妇、打工者。
4月27日,市民赵女士接到了“厦门市公安局缉毒科”的电话,称其身份信息泄露,被贩毒团伙用以犯罪,将面临判刑。电话中,“民警”称要查看赵女士的银行账户,查验“资产来源”。赵女士吓得只会惶恐了,丝毫没有防备,按照那位“民警”指示,到银行自动取款机上进

行操作,结果,卡内28万元被全部转走。

4月4日,一市民进入网上搜索出的“工商银行官方网站”,结果被这个钓鱼网站骗走3.6万元。民警介绍,很多市民有通过网络搜索一些机构官方网站的习惯,这给了不法分子可趁之机,他们将钓鱼网站的界面设置得与正规网站相似,

网址也仅差一两个字母,很多市民因此上当。

随着湖南卫视《我是歌手》节目迅速走红,“中奖”类诈骗也“借”上了这一幌子,通过短信、电子邮件式发送“中奖”信息,诱骗市民上当。

4月10日、16日,两名市民分别被“我是歌手”骗走44300元、

4400元。而《我是歌手》官方网站早晨在今年2月就声明自己从未开展过任何场外观众抽奖活动。

另外几起电信诈骗案的具体事由还包括,冒充采购人员订货、诱骗经营者付款给“生产厂家”,发布虚假招商信息骗取受害人付加盟费,汽车退税,更多的是QQ“好友借钱”。

电信诈骗 就是不法分子利用手机短信、电话、信件、互联网等通讯工具,假冒国家机关、公司、医院、朋友等名义,编造谎言骗取受害人钱财的一种诈骗活动。
电信诈骗手段花样繁多,且不断翻新,令人防不胜防,但目的只有一个——把您的钱骗到他的账户里。
电信诈骗猖獗,本报特联合公安环翠分局汇集了电信诈骗的典型手法,总结出其特征与规律,希望有益于市民。

电话

- 1、退税。冒充国家税务机关工作人员谎称要退购车购置税或房产税,诱骗您到自动取款机上按其指令操作,操作程序实际为转账程序。
- 2、家人遭遇意外。事先电话骚扰身在外地的家人,待其不耐烦而关机后,打通您的电话,假冒医院领导、警察、老师、朋友的名义,谎称在外地的家人出车祸、患疾病,让您汇医疗费。
- 3、猜猜我是谁,听不出我是谁?电话中让您猜对方是谁,随即假冒多年不见的好友,谎称在您所在地的附近遇到嫖娼被罚、交通事故、生病住院等“急事”,借钱救急。
- 4、电话欠费和消费透支。冒充通讯公司或银行工作人员,告诉您话费欠费或信用卡异地消费,将电话转接“公安机关”,假民警称您的身份信息泄露并被用以重大犯罪,要求您把所有钱转入对方指定的账户。
- 5、领取法院传票、刑警办案、藏毒品的邮件等。冒充法院、公安局、邮局等单位工作人员,告诉您的身份信息泄露并被用以重大犯罪,要求您把所有钱转入对方指定的账户。
- 6、订货。骗子打电话来订一批货,并指定“生产厂家”,让您觉得这笔生意短期暴利,促使您把货款付给“生产厂家”。

短信



- 1、贷款或卖车。告知您可无抵押贷款、低息贷款、有低价走私车等,需事先付“手续费”及“风险抵押金”等。
- 2、中奖。冒充大型公司工作人员或者公证处工作人员,告诉您中大奖,领奖前需交“所得税”、“公证费”、“手续费”等。
- 3、认爹妈。冒充您的子女,谎称在外出事急需用钱。
- 4、收房租。短信内容为:“我是房东,把钱打到我老婆的卡上……”。
- 5、违章记录。短信内容为:“您有一次交通违法记录,请联系交警,电话为……”,继而诱骗您汇款。
- 6、信用卡升级。冒充银行,以信用卡升级为由,让您登录钓鱼网站,自动转走卡内余款。
- 7、招工。招牌男女公关,继而以收取报名费、面试费、服装费、保证金等名义,诱使您汇款。
- 8、消灾。冒充杀手或打手,称被人雇用要伤害您,威胁您汇款买平安。
- 9、激怒。陌生号码发来大段恶毒的话语,当您被激怒回电时,其实拨打的是吸金电话,话费很快就被扣光。
- 10、点歌。“您的好友某某为您点了一首歌曲,如收听请拨打……”,您若拨打,话费便被大量扣除。

网络

- 1、植入木马。通过电子邮件、论坛发帖或QQ群,发送“快来看看聚会照片”、“大量美女图供你看”等链接网址,点击进入后电脑自动感染木马,个人账户及密码信息被不法分子自动获取。
- 2、假网站。不法分子设立网址和界面与正规网站极为相似的“钓鱼”网页,诱骗您登录,骗取您的个人账户及密码。
- 3、假号码。您图省事,直接在网上搜索一些网站删帖、订票退票、信用卡服务等客服电话,而大量客服电话是骗子故意公布在网上的,拨打后就会被逐步带入圈套。
- 4、虚假信息。通过邮件、QQ群、社区论坛等,发布大量的出售走私车、无息贷款、中奖、股市指导等信息,继而诱骗您汇款。
- 5、QQ好友借钱。不法分子已经盗用了您的好友QQ,并窃取了视频资料,当您和QQ好友视频聊天过程中,对方通过文字聊天借钱。
- 6、重复交易。您网购时,卖家称下订单时卡单,要求您重新支付或重新下订单。
- 7、换店购物。您网购时,卖家称缺货,发给您另一个网铺的网址让您去选购,该网址实际为钓鱼网站。

传真信件

- 1、培训。冒充消防、税务、工商、海关等国家机关,伪造国家机关公文,以传真形式向企业等单位发“培训通知”,要求其派员参加培训,并让把“培训费”打到其指定的银行卡帐户上。
- 2、售书。企业收到“消防”、“工商”、“税务”等部门邮寄来的书籍,或只接到电话,要求付书款。
- 3、中奖。接到某大型企业发来的刮奖单,中轿车、电脑等大奖,“公证处”工作人员电话中要求您缴纳“所得税”、“公证费”、“手续费”等。
- 4、异地违章。异地“交警部门”发来罚款单,您的身份信息无误,车却不是您的,需汇款交罚款。
- 5、最后通牒。银行发来“最后通牒”,您的身份信息无误,信用卡不是您办的,需偿还信用卡欠款。



常见伎俩

- 1、改号。不法分子使用“来电任意显”软件,让您的来电号码显示为公安局、法院、朋友的电话号码。
- 2、言语恐吓。电话中,不法分子往往以“重大犯罪”、“要判刑”等言语进行恐吓,让您六神无主,更方便对方顺利设套。
- 3、保密。不法分子一般要求受害人不要挂断电话,并以“卫星监控”、“泄露国家机密”等恐吓言语控制受害人,并教受害人以“帮子女买房买车”为由骗过银行柜台工作人员。

特点

针对性强、迷惑性大,犯罪成功率高。犯罪嫌疑人首先从各种途径获取受害人的基本信息,编造出各种诈骗的幌子,再利用一些科技手段对来电号码进行处理,配以心理战术迷惑受害人。
团伙作案、分工明确,组织化程度高。此类案件作案成员一般在3人以上,呈

公司化、集团化管理。手段先进、行为隐蔽,反侦查意识强。如使用任意显号软件、网络电话等科技产品,这些虚拟电话可同时捆绑、转接多部电话(包括座机、手机、小灵通等),可以由主叫方任意设置主叫号码而且具有异地转接功能。犯罪分子在设置虚拟电话转接时,可以在号码前加

上某地区的区号或其他号段,误导被害人认为是该地区的固定电话或服务电话。
异地操控、异地取款,破案难度大。犯罪分子通常具备一定的银行和电信业务知识,作案手段比较专业,实行异地操控,异地取款,加大了公安机关的破案难度及破案成本。

如何防范

“不相信,不回应,不泄露,不转账”。一般骗局,可通过回拨电话识破。如有疑问,及时向公安机关、亲友求助。