



你是“易受骗体质”吗？

在上海，电诈受害人平均年龄为37岁

■劳动报记者 包璐影

信息时代，人与人的交流更加便捷，但也滋生了层出不穷的电信诈骗招数。2024年，上海反诈中心平均每天能拦截超过7万个涉诈电话、超过60万条涉诈短信、2.3亿次涉诈网站点击跳转。

那你知道什么年龄段的人最容易被骗吗？很多人或许会毫不犹豫地回答：老年人！殊不知，在上海地区，当下电信网络诈骗受害人群平均年龄居然只有37岁。

37岁最容易 被电信网络诈骗

截至2024年底，根据上海警方最新调查分析研究得出的结果显示，上海电信网络诈骗受害人平均年龄为37岁。

究其背后原因不难发现，三四十岁年龄段的人群通常具有较高的经济活动参与度，同时，却可能因为工作繁忙而对诈骗信息识别不足，或因为过度自信而忽视了对诈骗行为的防范。

不久前有这么一桩案例：一位37岁的上海女教师突然要取700万元现金给骗子，面对民警的不断劝阻，她振振有词，甚至还出言“怼”：我就喜欢把钱扔水里，我喜欢看那个溅起来的水花。最终，民警只能对账户进行保护性止付，这才挽回了当事人700多万元的损失。

其实，诈骗对象不分年龄，攻击的只是心理弱点。作为一位普通人，总是有弱点和盲点的，因此，面对狡猾的诈骗者，哪个年龄段都有可能成为受害者。所以，在骗术不断升级的情况下，不仅要通过持续不断的教育和宣传来增强大家的警惕意识，还有必要强化技术手段的应用，对诈骗行为进行监测和预警。

你是“易受骗体质”吗？ 这份模型图请收好

俗话说，知己知彼，方能百战不殆。记者从上海反诈中心了解到，专家通过大数据分析梳理出一份易受骗模型图，市民可对症下药，增加自己面对诈骗的“免疫力”。

其一，情绪强烈者易受骗。

一般而言，五花八门的诈骗手段大致分为两类。一类是“威逼”，比如冒充公检法工作人员，编造一些莫须有的罪状吓唬受骗者，令其恐惧不已。另一类则是“利诱”，诈骗者将天上掉人民币的美妙图景描述得天花乱坠，让潜在受

者欣喜若狂。其实，强烈的兴奋或恐惧都会让人过度关注引发这类情绪的信息，忽视其他重要线索，更易中招。

其二，动机迫切者易受骗。

天下熙熙皆为利来，天下攘攘皆为利往。“利诱”这种诈骗手段恰恰利用了人渴求利益这种动机。在迫切渴求金钱的人眼中，骗子开出的条件很诱人，他们因而会高估自己成功获得钱的概率。而“杀猪盘”等交友类骗局利用了人对亲密关系的渴求。如同久旱逢甘霖，越渴望与人建立情感依赖，人们越容易被骗子无微不至的关心打动。

其三，爱冒险者易受骗。

面对风险时，有“小心驶得万年船”；有人则冒险，认为“舍不得孩子套不到狼”。其实，骗子的伪装并非无懈可击。例如，电话中骗子操着极不标准的普通话。然而，面对这些信息，爱冒险之人往往不够警觉，出于赌徒心态放手一搏。

其四，过度自信者易受骗。

“我是大学生，怎么可能会被骗？”“我这把岁数了，吃过的盐比你吃过的米都多，骗子那点小伎俩还能蒙到我……”过度自信的人觉得被骗的都是笨人，而实际上，觉得自己不会被骗的人在遭遇

诈骗时更容易放松警惕。即使他人发现其受骗迹象，好心劝说，他们也会觉得自己面上无光，继续执迷不悟。

其五，盲目从众者易受骗。

“别人可以，我也可以。”“这么多人都做了，肯定没问题。”其实，很多骗术都利用人们这种随大流、盲目跟风的从众心理。例如，受骗者最初加入所谓的刷单兼职群时，可能还持观望态度，但看到群友不断晒着自己刷单赚钱的证据时，惯于从众者便会放下戒备。殊不知，群内100人，除了受骗者外的99人全是骗子雇来。

(本版照片均为警方供图)

电诈手段不断升级 千万元养老钱差点“一键飞走”

当前，实施诈骗的引流方式从传统的电话、短信等向互联网平台，尤其是手机应用端发展蔓延的趋势明显。为此，记者梳理了近期升级后隐蔽性极强的典型电信网络诈骗案例。

■案例一

网上卖块“劳力士” 成了骗子“洗钱”的“帮凶”

不久前，杨先生在二手交易平台上寄售“劳力士”手表，开价271000元。当天一个买家声称有购买意向，但次日早上，对方忽然说自己因为工作抽不开身，委托了一个“鉴表师”朋友前往交易。提供给对方的银行账户里当场收到了269900元。对于那少掉100元，对方当时表示当作是优惠。杨先生本以为钱已落袋为安，可第二天，他所有的银行支付功能都被外省市的公安冻结了。因为当地有被害人因机票改签被诈骗，而转账给骗子的钱一部分进了杨先生的这张卡里。

原来，骗子拿到了杨先生的账户信息，就将杨先生的卡号作为涉诈的一级卡散布到整个团伙。目的就是为将诈骗得来的赃款通过交易换成实物手表，随后再将表卖出，如此便能成功洗白。

【警方提醒】：如果在二手交易平台上寄售奢侈品，在交易前，务必要让买家提供真实的身份信息，以及未来将要转账钱款的银行卡号，如此便可防范此类洗钱陷阱。

■案例二

直播会员服务到期了？ 点击链接后1400万元差点“飞走”

今年1月，朱阿姨收到一条短信，告知她的直播间会员即将到期，如果不取消，每个月需缴纳几百元会员费。此后，她手机被对方远程控制，卡里1400多万元理财被操作赎回，好在民警及时切断网络，挽回损失。

朱阿姨平时是该短视频平台的用户，当收到短信时，以为自己不小心点击了会员功能，于是按短信提示联系对方。所谓的客服要求朱阿姨加QQ好友，并向她发送了一条链接。这个链接点击进去之后就是骗子自己做的网页，界面和短视频平台的客服界面完全一样。对方将如何取消会员费的信息发送至聊天界面，并附上另一个链接地址，引导老年人点开。

这恰恰就是含有屏幕共享功能的某软件下载链接。诈骗分子会通过开启屏幕共享功能并操作银行账户，进而获取被害人的银行账号密码、验证码，转移卡内资金。

【警方提醒】：当听到陌生人要求“下载软件”或者听到“屏幕共享”时，很有可能遭遇电信网络诈骗。一旦意识到自己被骗，务必及时把手

机关机，然后立即报警。

■案例三

电话喊你买黄金，还要网约车送 这是“洗钱”升级新模式

去年底，闵行区一家金店来了一名年轻男子。在购买价值4.7万元的黄金首饰时，在付完钱后，男子一边打着电话，一边还要求店员提供快递盒。其实，男子的种种表现就是典型的“买黄金+网约车转移”洗钱模式。在登记了对方信息后，店员第一时间和警方取得了联系，民警立即拨通了男子戴先生的电话。

原来，为了赚取外快，戴先生在网上加入了一个刷单群。对方要求他去购买黄金。戴先生表示，自己按对方的要求将打包完成的黄金交给网约车司机，目的地是江苏省千灯镇的一个地点。最终，根据网约车公司提供的司机信息，民警展开联动。网约车司机李师傅及时配合，这才没让戴先生进一步掉入诈骗陷阱。

【警方提醒】：如今，“线上转账”升级为“线上诈骗+线下取现”，诱骗受害人通过网约车、快递、闪送等方式转运现金、黄金，进行“洗钱”。

■劳动报记者 包璐影