公民
防范电信网络诈骗手册

本书编写组 编

中国人民公安大学出版社
CPPSUP

公民防范电信网络诈骗手册

本书编写组 编

中国人民公安大学出版社
· 北京 ·

图书在版编目（CIP）数据

公民防范电信网络诈骗手册 / 《公民防范电信网络诈骗手册》编写组编. -- 北京 : 中国人民公安大学出版社, 2018.1

ISBN 978-7-5653-3047-6

Ⅰ. ①公… Ⅱ. ①公… Ⅲ. ①电信－诈骗－预防－中国－手册②互联网络－诈骗－预防－中国－手册 Ⅳ. ① D924.33-62

中国版本图书馆 CIP 数据核字（2017）第 221471 号

公民防范电信网络诈骗手册

本书编写组 编

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里甲1号
邮政编码：100038
经　　销：新华书店
印　　刷：天津嘉恒印务有限公司

版　　次：2018年1月第1版
印　　次：2018年1月第1次
印　　张：1.25
开　　本：889毫米×1194毫米　1/32
字　　数：27千字

书　　号：ISBN 978-7-5653-3047-6
定　　价：15.00元

网　　址：www.cppsup.com.cn　　www.porclub.com.cn
电子邮箱：zbs@cppsup.com　zbs@cppsu.edu.cn

营销中心电话：（010）83903254
读者俱乐部电话（门市）：（010）83903257
警官读者俱乐部电话（网购、邮购）：（010）83903253
公安图书分社电话：（010）83905672

前言

近年来，电信网络诈骗犯罪甚为猖獗，犯罪手段科技含量高，犯罪形式变化多样，给公民的财产安全带来了极大的风险。面对形形色色的电信网络诈骗形式，我们如何保护自己的财产不受损失？

《公民防范电信网络诈骗手册》从电信网络诈骗的基本套路出发，立足于揭露电信网络诈骗的种种手段，将31种电信网络诈骗预警信号公之于众，提醒公民当见到或感觉到“信号”出现时便要格外警惕，避免上当受骗、遭受财产损失。

希望通过本手册能够帮助您增强安全防范意识，掌握一定的财产安全防范知识和保护技能，当遇到电信网络诈骗时，能将个人财产损失降到最低。

本书编写组

二〇一八年一月

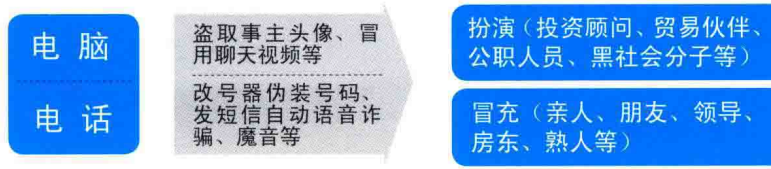
目　录

一、电信网络诈骗的套路

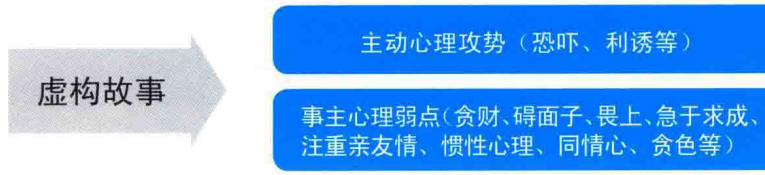
大数据时代的犯罪更加精准，但是手法万变不离其宗，识别“宗”，才能以不变应万变，避免上当受骗。

在骗子得手前，从任一环节将骗术识别出来都是成功的。

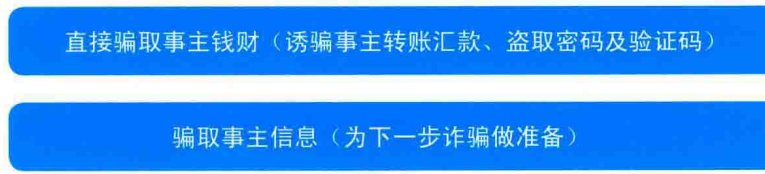
■ 骗子粉墨登场



■ 骗子行骗



■ 骗钱得手（或放长线钓大鱼）



二、电信网络诈骗的预警信号

下面罗列了31种电信网络诈骗的预警信号。

在使用通信、网络平台时，一旦出现这些预警信号，就要特别警觉，万分小心。

■ 骗子粉墨登场的预警信号

骗子利用电脑、电话等大众通信载体，通过采取某种技术手段盗取事主头像、视频、账号，或更改伪装电话号码等，扮演社会角色或冒充事主的关系人，来骗取事主的信任。

当出现下文中1～6类型的信号时，表明骗子粉墨登场了。

公职人员来电话，谨慎识别莫害怕
索要钱财的亲友，核实身份最关键
服务号码来电显，辨别真假是首位
语音电话接听后，内容不明果断挂
陌生图片和链接，病毒木马藏里面
“好心人”帮好心事，警惕设套把财骗

1. 政府公职人员

骗子冒充公安、法院、检察院、税务、海关、教育部门、社保局等公职人员打来电话，向事主告知一些事项，有时态度还很强硬。此时不要马上相信对方的说辞。应当：

（1）不妨先挂断电话，亲自去这些部门现场询问。

（2）通过正规渠道（114 查号台、政府官方网站）获取这些部门的电话，一定要亲自拨打过去询问。要知道，政府机关的电话不会从一个普通电话被人工转接，遇到这种情况时，要意识到这是个骗局。

（3）不要被对方“强硬”的态度、“坚定”的语气所震慑，不要害怕，不要嫌麻烦，不要碍于面子，多一些耐心去核实。

2. 索要钱财的“亲人”“朋友”“同事”“熟人”“房东”“孩子的老师”等

骗子会利用时间差、视觉差、盗取账号等手段制造假象，冒充“亲人”“朋友”“同事”“熟人”“房东”“孩子的老师”等向事主索要钱财。

（1）时间差，利用亲友手机关机、银行休息等特殊的时间点，让你无法核实。

（2）视觉差，模仿亲朋好友的微信、QQ头像，甚至从其他平台盗取亲友视频等，让你信以为真。

（3）盗取亲友社交平台账号，直接骗取钱财。

切记，只要遇到有人在QQ、视频聊天、微信、短信中索要钱财，不论对方是你的什么人，一定要亲自拨打对方电话或当面询问，以核实真伪。

3. 服务电话

骗子会利用软件、设备等对电话号码进行伪装，让呈现在你眼前的这串数字变成他想要的任意号码。当来电是“110”“12345”“10086”“10010”“10000”等，或银行客服电话、“400”开头的企业客服电话时，不要一上来就轻易相信对方，特别是在对方让你告知或输入验证码、密码等情况下应格外警惕，这个电话很有可能是伪装过的诈骗电话。还有的骗子冒充银行工作人员，声称国家出台新政策，要求你进行实名补录，此时建议挂断电话后去银行柜台确认。

4. 语音电话

（1）接到自动播放的语音电话，直接挂断即可，不要收听其中的内容，更不能按照其中的提示去操作、拨号等。

（2）接电话后对方用你听不懂的方言不停地说话，或者出现歇斯底里的呵斥声，果断挂断电话，并且不要回拨。

5. 陌生链接、图片，以及需要下载、激活的软件

（1）当你不熟悉电信运营商、银行等机构的准确网址时，不能随意点开手机短信、APP 应用、网页中的疑似电信运营商、银行等的链接，因为有些是安装有木马和病毒的假地址。比如，一些骗子谎称银行系统升级要求你点击假链接进行升级。

（2）不要轻易点击那些自动弹出的需要激活或下载才能使用的软件。

（3）在微信、QQ、微博等互动平台不要随意点击陌生链接，不要为陌生消息点赞、投票等，一些平台装有木马、病毒，一旦点击，手机上的金融支付信息将会被盗取，造成无法挽回的损失。

（4）意外收到的短信链接，一定要先亲自核实内容的真伪，不要随意点击。

6.“好心人”

当你接到电话，遇到以下“好心人”主动帮助你时，要开始警觉了，他们都是骗子：

（1）帮助你解决涉案纠纷的“警察”；

（2）回购你藏品的老板；

（3）帮助你摆平法院官司的热心人；

（4）花钱帮你铲事儿的“黑社会”分子；

（5）告诉你彩票、股票赚钱方法的推销人员；

（6）告诉你投资挣钱方法的投资顾问；

（7）声称能够帮你通过考试的人；

（8）帮助你升级银行系统的工作人员；

（9）要跟你做一笔现成买卖的生意伙伴；

（10）要给你奖品的活动承办方；

（11）帮助你减免学费的“老师”；

（12）为你提供免抵押、低利息助学贷款的放贷人。

骗子首先让你看到获利或解决眼前棘手问题的希望，并且为你提供了一个看似很可靠的解决方案，以此吸引你，实际上那是他们精心设计的圈套。

■ 骗子行骗的预警信号

骗子通过虚构故事，然后利用主动的心理攻势（恐吓、利诱等）及事主的心理弱点（贪财、碍面子、畏上、畏权、急于求成、注重亲友情、同情心、贪色等），充分博得事主信任，进而骗取钱财。

大部分骗子都是急于求成的，他们希望在最短的时间内高效完成诈骗，有时他们会根据事先非法获取的事主信息，如性别、年龄、工作性质等，编造能够触动事主的故事，实施较为“精准”的诈骗。这就是大数据时代的犯罪。

当出现下文中 7 ～ 21 类型的信号时，表明骗子已经开始行骗了。

急需之时来人帮，不要轻信三思行
意外之财从天降，相信反倒入陷阱
飞来横祸不要慌，冷静处理方可度
个人信息遭暴露，千万小心多注意
线上爱情虚缥缈，当心线下索钞票
一丝一毫疑窦生，相信直觉不被骗

7. 从天而降的“帮助”

当你短时间内有紧急需求或想要完成一件事情时，如准备乘飞机、找工作、租房、领取助学金、参加考试、银行转账、交房租、购物退款等，突然接到与此事有关的电话、短信，一定要格外警惕，不能着急，此刻正是骗子利用你的最好时机。

即便对方准确地报出了你的名字及各种信息，也不要相信他，因为你的信息是他从非法渠道获取的。要亲自核实情况，给相关事主本人打电话，或通过 114 查号台等正规渠道查询相关机构的电话，亲自拨打进行核实。

8. 高额回报

打着高额回报的幌子吸引你的，一定是骗子。下面就是骗子利用高额回报诈骗的惯用手法：

（1）互联网金融理财，以保本收益、短期分红利诱，骗取理财本金；

（2）高时薪招兼职打字员、网络水军，骗取押金、诚意金后消失；

（3）淘宝代刷信誉，借用钓鱼网站盗取你的银行账号和密码；

（4）高回报项目投资，要求分期加投资金，一段时间后便消失；

（5）爱心基金会的行动，骗取会员费，并发展更多会员骗取钱财；

（6）低价销售回迁房、经济适用房等，骗取预付款或房款。

不要理睬包含上述信息的短信，不要点击链接，更不要回电话。