

# 10大新型网络陷阱,小心别掉“坑”!

“微信抢红包”、“您的订单遭遇卡单,请点击此链接处理”……近年来,随着一些新型的网络交易支付平台的广泛应用,网络诈骗等犯罪花样百出。岁末年初,案件高发,警方近日发布10种新型网络侵财案件类型,提醒广大市民在网络生活中加强防范意识,避免落入陷阱。

## 1 “超级网银”遇欺诈24秒转走10万元

“超级网银”通过建立统一的操作界面,让用户可以在短时间内实现多账户的查询和转账,所关联银行卡的持有者也可以是多人,家人、朋友之间都能通过便捷的签约成为互联账户。将另一张卡中的钱转入自己的卡中,整个过程甚至不需要另一位持卡人参与,用时不超过5分钟。

受害人陈女士在网上购买一条裙

子。按照店主要求,用“代付”方式进行支付后查询不到交易记录,陈女士赶紧追问店家,店家让其与异常订单处理中心QQ号联系。该QQ号客服表示,要解冻订单需要她进行“签约授权”的操作,并与银行联系。

按照客服要求逐步操作,陈女士发现一名陌生人在24秒内分两次将其账户内的10万元转出。

### ●警方揭秘

原来,黑客利用“超级网银”跨行账户管理功能,诱骗银行用户进行“授权支付”操作。

一旦受害人完成授权操作,其银行账户将会瞬间被洗劫一空。目前,“超级网银”安全漏洞已经被国家漏洞库收录,已有多家银行关闭了“超级网银”的非同名账户之间的授权功能端口。

## 2 扫二维码中木马5000元不翼而飞

邹先生是一名电商卖家,专门经营门窗制作和安装。不久前,一位陌生买家主动与邹先生联系,却不提想买什么商品,而是在聊天消息里发来一个二维码,说“用手机扫一扫就可以看到想要的门窗详细资料”。

为了做成生意,邹先生立刻拿出手机扫描了二维码,却没看到什么门窗信息,于是发消息询问,对方则继续下套:

“你下载安装后直接点开就可以看到了。”让邹先生没想到的是,他点击安装,实际上是把一个名为“隐身大盗”的木马装进了手机。

在安装了二维码中的软件后,对方以“方便联系”为由索要了他的手机号码,然后借口去吃饭而离开。一个小时后,邹先生发现自己的网络支付账号被盗,账户余额及银行卡关联账户损失5000余元。

### ●警方揭秘

这种手机“隐身大盗”木马,会拦截手机收到的验证短信,并直接转发给不法分子,重点攻击对象是网店卖家。不法分子常以“购物清单”等名义发送已被植入“隐身大盗”的二维码,卖家扫描后会下载该木马,一旦安装会导致手机号、短信等信息泄露,甚至危及网银和支付账户资金。

## 3 陷虚假团购骗局订餐费被骗走

“50元可享原价318元的特色自助餐”,白领小秦看到这个信息就信以为真,于是为家人订了8份团购的自助餐,本想一家人吃得开开心心,不想该团购完全是个骗局,压根就没有这回事,

400元的订餐费就这样被骗子骗走了,小秦十分郁闷。

### ●警方揭秘

骗子最新的手法是在正规电商平台伺机发布虚假的折扣信息,通过超低

的价格诱骗网购者登录虚假的团购网站参团购买。

因超低价商品在正规网站上也很常见,故此类型网购钓鱼比一般的虚假团购网站更难识别。

## 4 假网购客服欺诈买酸梅汤被骗3万

陈女士网购一箱酸梅汤,完成交易后接到陌生电话。对方自称是支付宝客服,因系统升级,款项无法打到对方账户上,也无法退到支付宝系统中,需要陈女士提供身份证号码和银行卡号,并登录淘宝网对照“备忘”里的提示操作。陈女士登录账号后,发现已购酸梅汤备

忘栏内写有“订单差异,需要填写退回款的卡号、有效期、三位尾数及手机验证码”等信息。陈女士按照提示操作后,信用卡很快被转走9999元,连续三次损失金额共计近3万元。

### ●警方揭秘

“备忘”欺诈是个人账户信息泄露后

最易遇到的高危风险。骗子假冒淘宝客服致电受害人,谎称某项交易异常,要求受害人查看淘宝交易记录的“备忘”信息,并诱骗客户输入银行卡密码、验证码等敏感信息,盗取钱财。实际上,交易记录中“备忘”内容只有买家自己才能填写,不熟悉此项功能的用户极易上当受骗。

## 5 虚构保障金骗局专骗淘宝卖家

网店卖家袁小姐反映,一位买家声称不能付款,没多久就有“客服”联系她,要她开通缴纳“消费者保障金”,并发来缴费链接。

结果等袁小姐缴费1000元后,交

易记录竟然显示在某游戏平台购买了游戏点卡。

### ●警方揭秘

虚假消费者保障金骗局,是骗子专门针对淘宝卖家“研发”的招数。

网络骗子先以消费者的名义,谎称淘宝商家的商品无法购买,再冒充淘宝网客服人员,以解除交易隐患或解决交易异常问题为由,向店主索要一笔“消费者保障金”并占为己有。

## 6 “好声音”中大奖领奖要先交钱

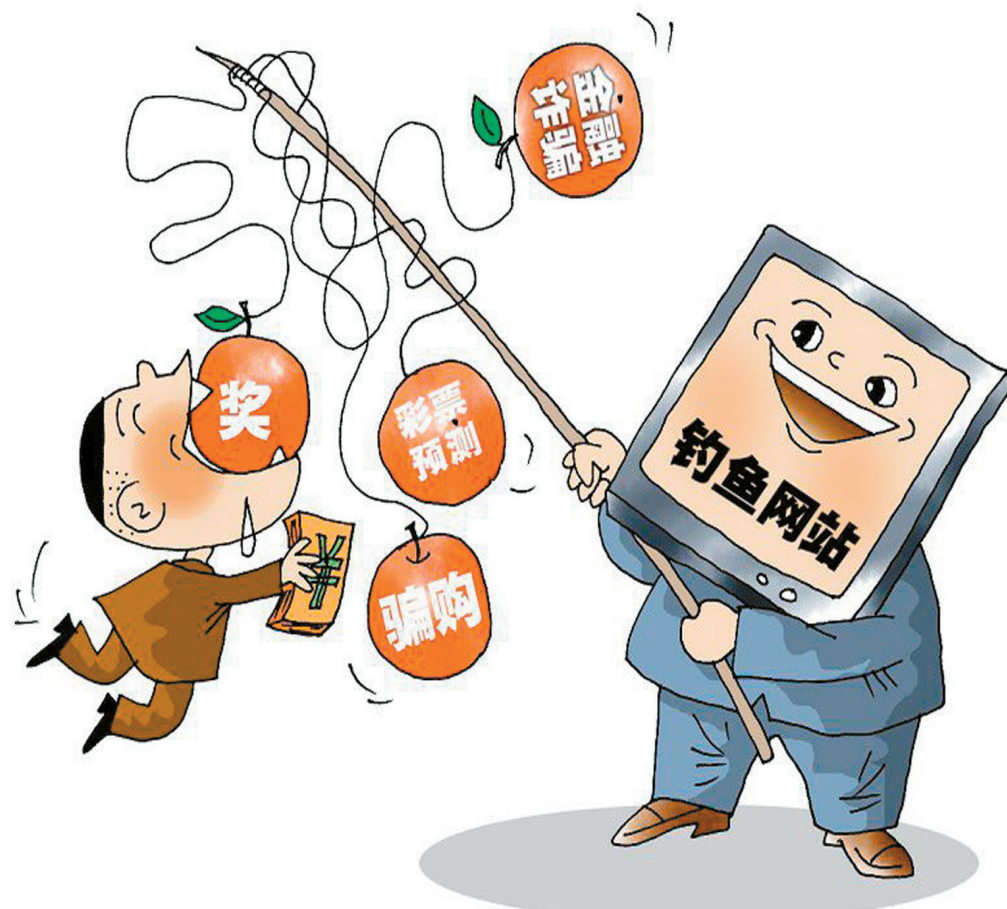
外省曾破获一宗以“中国好声音”中奖名义诈骗他人钱财的案件,抓获8名嫌疑人。经审查,该涉案团伙成员有4名,利用“中国好声音”虚假中奖信息诈

骗被害人童某华3.2万元。

### ●警方揭秘

热门电视节目一直是钓鱼网站模仿的对象,《中国好声音》、《我是歌手》、

《爸爸去哪儿》等热播节目曾被骗子作为钓鱼诱饵模仿。网民一旦误信“领奖”内容,骗子会以缴纳“保证金”、“手续费”等为由,借机诈骗“领奖人”的钱财。



## 7 微信抢红包遇陷阱几天输掉十几万

年轻的女老板小妍加入行业内一个微信群,没料到误入以抢红包形式进行赌博的群。

受群主唆使,小妍参与了“抢红包游戏”,几天时间就输掉十几万元。

### ●警方揭秘

微信发红包被一些人利用作为新的赌博工具,参赌的群友赢钱几率非常低,而群主和“代包手”则坐收渔利。

## 8 网上兼职淘宝刷单大学生被骗上千元

大学生李某在QQ群中看到一条招聘淘宝兼职的广告,称帮网络商家店铺“刷信誉”可以赚佣金,足不出户便能日赚百元。李某立即加了对方名为“淘宝代刷”的QQ,对方给李某提供了一个网址链接,李某点击链接登录后,网页上显示要求李某注册自己的个人信息,包括身份证号码、银行卡号等。注册完毕后购买该网站内的电信充值卡帮对方刷信誉。第一次购买时,对方如约将佣金支付给了李某,但之后李某再次帮对方刷信

时对方就再无音讯了。李某先后购买了10余次,受骗金额共计上千元。

### ●警方揭秘

骗子通常先在聊天群、论坛发布虚假招聘信息,诱骗求职者购买充值卡、游戏点卡等虚拟商品,谎称会返还本金和佣金,最后却以各种理由拒绝返还,并借机诱骗受害者购买商品或洗劫网银。此类骗局中,受“就业难”困扰的“90后”大学生是主要的受害群体。

## 9 伪基站发短信钓鱼盗刷账户资金

日前,王先生收到了一条10086发来的短信,说是可以积分换话费。“他让我输入身份证号码、姓名、银行卡号。”王先生说,输完之后,也没见到充上话费,他也没当回事。结果,当天下午2时左右银行客服给他打来电话,说是有一笔交易有点异常。王先生觉得很奇怪,自己并没有进

行任何交易,于是就报了警。

### ●警方揭秘

不法分子利用伪基站在人群密集区自动搜索附近手机卡信息,强行向用户发送垃圾广告或诈骗短信,冒充银行甚至110等号码,诱骗中招者访问虚假网银,盗刷受害人账户资金。

## 10 遭网购木马攻击瞬间被扣1万元

张先生购买商品时,总是付款失败,为了激活订单,轻信卖家并安装了对方发来的“订单解锁”文件,结果该文件竟被植入木马,当支付完1元的激活款时,自己银行卡却被扣款1万元。

### ●警方揭秘

受害者遇到的是网购木马攻击,电脑又没有

安装有效的安全软件保护。

木马运行后潜伏在系统后台,实时监视浏览器地址栏。

一旦受害者在购物网站为商品付款,木马就会篡改交易数据,将付款对象转换为不法分子的“洗钱账户”将钱转走。



# 有国才有家

