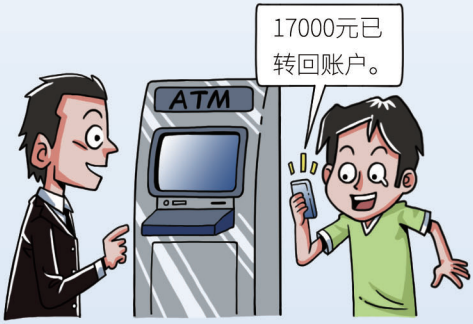
典型案例分析

案例1 网络诈骗被银行及时制止

张某不慎泄露了个人信息，不法分子利用其信息在网上购买基金，使张某收到其银行卡里17000余元被转走的短信，接着打电话自称能帮张某追回被转款项，试图通过取消基金认购操作制造将“被转款项”追回的假象，并诱骗张某将银行卡里的余额转至所谓“安全账户”（不法分子持有）。张某在操作时，A银行工作人员见其神色慌张便询问缘由，确认这是一起诈骗案件。A银行迅速启动应急预案，并协助张某到ATM操作，让对方听到ATM提示音获取信任，成功套取对方的银行卡号，并锁住该账户交易功能。随后，张某收到17000余元已回到账户的短信，被转的款项全部追回。



安全提示：

（1）不明扣款勿慌张，及时求助真银行。

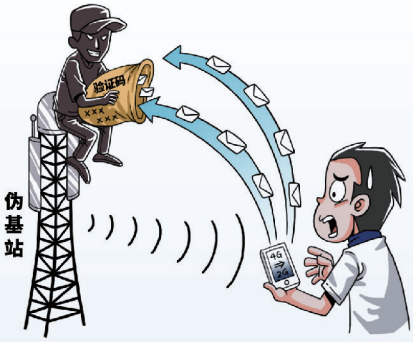
（2）诈骗套路千万项，安全意识要加强。

案例2 “伪基站”诈骗

小丁在睡梦中被持续的手机震动声吵醒，他起床发现手机连续收到了数十条短信验证码和消费通知，并且移动网络从4G下降到了2G。验证码的平台包括途牛网、瓜子二手车、支付宝、京东等。他通过短信消费通知发现，其绑定在APP上的银行卡正在被消费。

不法分子利用手机2G网络（GSM）不加密传输的漏洞，通过伪基站、短信嗅探器，在一定距离内，盗取受害者手机号、短信验证码，之后，再利用各大银行、网站、移动支付APP存在的漏洞和缺陷，窃取信息，修改支付密码，实现资金盗刷。

不法分子还会利用“伪基站”伪装成银行或通信运营商发送诈骗短信或二维码，引诱手机用户点击链接，填写个人身份证、银行卡等信息，从而获取用户的重要隐私和财产信息实施诈骗。



安全提示：

(1) 当发现手机网络突然变化，如“停止服务”、“4G变为2G网络”等情况，应尽量避免使用手机进行转账交易等操作。

(2) 手机应安装安全防护软件，并启用伪基站防护、垃圾短信拦截等功能。

(3) 睡觉时尽量关机或采用飞行模式，尽量关闭免密支付功能。

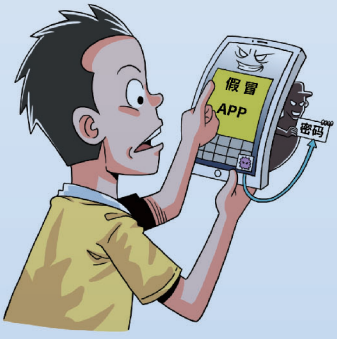
(4) 如果收到银行等金融机构发来的验证码，但不是本人操作，除了关闭手机，还要尽快冻结银行卡，减少损失。

案例3 假冒手机银行APP诈骗

王某收到一则短信，以10开头，内容为**银行网银升级，提醒用户升级手机银行APP，并提供下载链接http://******。王某没有丝毫怀疑，点击短信中的链接下载安装。安装到手机上后，该APP操作界面和之前使用的手机银行一模一样，王某按提示登录账户，填写手机号、银行卡、身份证号等信息，没有放在心上。不久之后，王某在银行网点查询卡内余额发现已被洗劫一空，才意识到自己中招了。

不法分子将手机木马伪装成常见银行的手机客户端，放在不安全的软件市场、论坛，引诱用户下载；或是通过伪基站发短信，引诱用户点击短信中的链接，下载安装。

该木马和正版手机银行客户端完全一样，诱导用户填写个人信息，并以短信形式发送到指定的手机号。不法分子获取信息后，此木马将隐藏图标，在后台偷偷拦截并转发短信验证码，这样不法分子就可利用“找回密码”修改中招手机用户银行交易密码，将用户银行卡内的钱财洗劫一空。



安全提示：

(1)在银行网点或正规渠道下载手机银行客户端。

(2)切勿轻信未经认证的软件市场，或是论坛、短信里的下载链接，不要随意点击。

(3)不要将有大额现金的银行卡绑定手机银行，设置银行卡转账限额。

案例4 二维码支付被盗刷

2019年4月21日至5月4日期间，四名消费者手持微信二维码在超市等待付款，在排队的几分钟里，被人从背后通过手机扫码，盗刷500元到900元不等的资金，扣款方都是名为“一站式24小时便利店”的账户，根本不是超市收款。

安全提示：

(1)关闭免密支付，或调低免密支付的额度。

(2)不要在排队购物时打开付款码，等到自己要进行支付交易时再打开支付用的二维码。

(3)仔细辨别付款码和收款码，对外收款时别使用付款码。

(4)尽量少让别人扫自己的付款码。

(5)对于网上支付账户，调低支付金额上限，或只存少部分钱。

案例5 网贷连环诈骗

刚毕业的福州网友小兰遭遇电信骗局，短短两天被骗走28万元。

小兰先接到自称“福州通信局”的电话，通知其手机号因群发赌博信息被举报，一号骗子利用威吓成功迷惑住小兰，二号骗子通过伪造公安官方电话的来电显示骗取信任，加了受害者QQ进一步制造行骗语境和场景，小兰完全陷入骗子杜撰的剧情，配合其调查一起涉嫌200多万的洗钱案件，将全部存款转到了所谓“安全账户”。为扩大诈骗“战果”，骗子继续诱导小兰从10家网贷平台借款并要求缴纳9万保证金，当小兰发现已无力缴纳保证金时，才发现自己受骗了。

安全提示：

(1) 但凡收到客服、有关部门或公检法的电话，切勿轻信。

(2) 切勿轻信以任何名义要求转账、借款、缴纳保证金，以免背上负债，造成损失。

(3) 如发现转账账户为个人账户，一定是骗子。

案例6 征信诈骗

山东的小张忽然收到一条短信，手机自动识别是“**银行”发来的，短信号码也是106开头（已认证号段），告知他的信用卡因严重逾期已临时冻结，逾期行为也被录入征信系统。小张准备买房，对自己的信用很是爱惜，他赶紧打短信中的电话询问情况，对方告诉他因为还款逾期要交2万元方可解冻，并告诉他只需关注一个“**银行自助服务中心”的公众号，即可迅速办理，否则影响以后的车贷、房贷。小张担心受影响，就在对方的提示下，在公众号转了2万元。后来小张觉得不对劲，拨打银行电话核实，得知其实根本没有逾期。

安全提示：

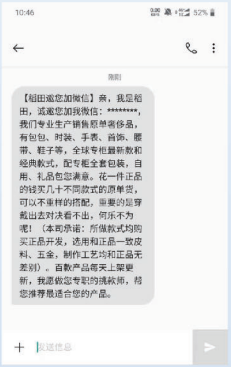
(1) 看到的信息不一定是真的(包括银行发来的短信以及所谓的认证公众号)。

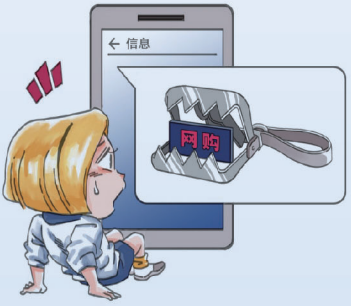
(2) 在接到类似逾期信息后，要及时通过官方客服或者到银行营业网点确认。

(3) 如有征信问题，可到人民银行或指定银行的征信柜台查询、打印。

案例7 网购A货遭骗

刚毕业的银小姐收入一般，但非常喜欢网购，看到同事、同学使用奢侈品，很羡慕。正好收到微商朋友的短信，可以低价购买原单奢侈品。按自己的需求，向对方支付了货款。开始对方还提供“快递”信息，并以海关检查为由，发送链接给银小姐，要求填写个人身份信息和个人账户信息，并录制了银小姐手持身份证的视频。7天后银小姐再次查询发货情况时发现对方已将其拉黑，同时有网贷公司联系银小姐询问还贷情况。





安全提示：

(1) 不占小便宜，通过官方渠道购买商品。

(2) 不随便点击他人发来的链接。

(3) 不要随意提供个人身份信息和个人账户信息。

(4) 不参与刷单、刷信用。

案例8 联手黑客网络敲诈

2019年6月21日，武汉市公安局江汉分局破获一起网络敲诈案。广东一对夫妻在深圳注册两家公司，并联合黑客攻击了国内多家公司的电脑，以解密为由索利，先后获利700余万元。

安全提示：

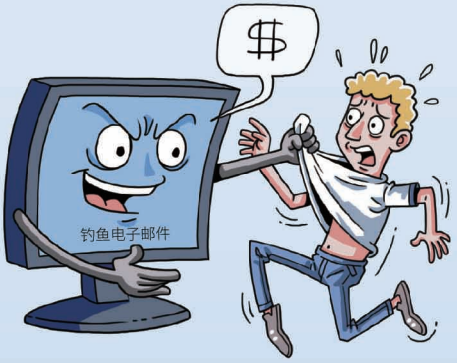
(1) 电脑连接互联网时一定要做好安全防护措施。

(2) 电脑应安装专业防病毒软件。

(3) 对于个人信息和重要数据，可采取加密等方法保存并做好备份。

案例9 大型企业遭攻击勒索

2019年3月2日，俄罗斯企业遭受大规模网络攻击。攻击者使用物联网设备，伪装成欧尚、马格尼特、斯拉夫尼奥夫等知名公司，向公司内部网站发送钓鱼电子邮件，对公司人员进行勒索攻击。



安全提示：

(1) 企业使用的电脑，连接互联网时一定要做好安全防护措施。

(2) 能够发送电子邮件的设备，如调制解调器、路由器、网络存储、智能家居生态系统和其他小工具，都是入侵者可用于网络钓鱼攻击的途径，对于这些设备的安全隐患要高度防范。

金融安全攻略

7个妙招防范网络金融风险

一 陌生短信不要回，不明链接不要点

大家都接到过陌生号码发来的中奖、兑换、配资等内容的短信，其中绝大多数是假消息。即使是标注为银行官方号码发来的也不要轻信、不要回复，犯罪分子很容易更改短信显示号码。短信中的链接就更不要点击，千万不要按其要求输入个人信息，否则您的信息很有可能会泄露。

二 金融支付要注意，多留心眼防盗刷

使用银行卡、移动支付等进行金融支付时一定要注意，千万不要让银行卡、手机离开自己的视线，移动支付时不要提前打开付款码，不法分子在手机上安装收款软件以后也能扫码收款，盗走您的资金。打开二维码后注意用手遮挡，也可在APP中设置支付时需要密码、指纹等再次确认的方式。

三 手机里千万别存身份证照片

身份证对于我们来说非常重要，在开立证券账户或办理其它网上业务时需要提供身份证照片，一定要记住身份证照片用完之后立即删除。如果您的手机不慎丢失并且存有身份证照片，那风险就大了，通过身份证照片及手机短信验证码，可以将您的各类账户密码重置，然后盗走账户中的资金。

四 有人跟您借钱一定要电话核实

如果有朋友通过微信或QQ跟您借钱，不要直接就把钱打过去，因为朋友的账号有可能被盗。这时候一定要拨打朋友的电话确认，如果朋友说不方便接听，那十有八九就是诈骗了，要及时通知朋友账号被盗，避免让其他人上当受骗。

五 短信验证码不要对任何人透露

千万不要忽视了短信验证码的重要性，实际上它比支付密码更重要。现在犯罪分子手段都很高超，可以用各种方法获取银行卡或网络支付密码，而短信验证码没法直接获取，有验证码就能在网上执行转账、消费等操作。所以，短信验证码不要透露给任何人，即使是您的亲友也要小心。

六 不要所有的账户都用一个密码

我们使用的密码越来越多，除了银行卡、信用卡密码外，还包括电商平台的密码、第三方支付密码等，很多人为了省事都用一个密码，这种做法存在极大的风险。一旦其中一个平台遭受攻击泄露了用户信息，所有账户都将处于危险之中。

七 高收益金融软件不要信，投资选正规途径

投资者在网上时常会看到一些声称包赚不赔的炒股或炒黄金软件，通过所谓的“专业”及虚假夸大宣传来引起投资者注意，并且承诺高额投资收益，还虚构一些“成功案例”现身说法。股票、基金、黄金投资市场都会有风险，不可能包赚不赔。投资者一定要通过正规途径投资。