主办单位：中国人民银行

国家网络安全宣传周
China Cybersecurity Week

网络安全 一路随行

2018年金融网络安全宣传手册

CYBERSECURITY

中国人民银行
THE PEOPLE'S BANK OF CHINA

长江财富
CHANGJIANG WEALTH & ASSET MANAGEMENT

前　言

2018年4月20日至21日，全国网络安全和信息化工作会议在北京召开，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化委员会主任习近平出席会议并发表重要讲话。习近平总书记强调，没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任。要依法严厉打击网络黑客、电信网络诈骗、侵犯公民个人隐私等违法犯罪行为，切断网络犯罪利益链条，持续形成高压态势，维护人民群众合法权益。要深入开展网络安全知识技能宣传普及，提高广大人民群众网络安全意识和防护技能。

目 录

《网络安全法》解读

《中华人民共和国网络安全法》（以下简称《网络安全法》）是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

一、《网络安全法》的基本原则

（一）网络空间主权原则。网络空间主权是一个国家主权在网络空间中的自然延伸和表现。各国自主选择网络发展道路、网络管理模式、互联网公共政策和平等参与国际网络空间治理的权利应当得到尊重。

（二）网络安全与信息化发展并重原则。国家坚持网络安全与信息化并重，遵循积极利用、科学发展、依法管理、确保安全的方针；既要推进网络基础设施建设，鼓励网络技术创新和应用，又要建立健全网络安全保障体系，提高网络安全保护能力，做到“双轮驱动、两翼齐飞”。

（三）共同治理原则。网络空间安全保护需要政府、企业、社会组织、技术社群和公民等网络利益相关者的共同参与。

二、《网络安全法》提出制定网络安全战略，明确网络空间治理目标，提高了我国网络安全政策的透明度

《网络安全法》第四条明确提出了我国网络安全战略的主要内容，即：明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。第七条明确规定，我国致力于“推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。”

三、《网络安全法》进一步明确了政府各部门的职责权限，完善了网络安全监管体制

《网络安全法》将现行有效的网络安全监管体制法制化，明确了网信部门与其他相关网络监管部门的职责分工。第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作，国务院电信主管部门、公安部门和其他有关机关依法在各自职责范围内负责网络安全保护和监督管理工作。

四、《网络安全法》强化了网络运行安全，重点保护关键信息基础设施

《网络安全法》第三章用了近三分之一的篇幅规范网络运行安全，特别强调要保障关键信息基础设施的运行安全。关键信息基础设施是指那些一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的系统和设施。网络运行安全是网络安全的重心，关键信息基础设施安全则是重中之重，与国家安全和社会公共利益息息相关。为此，《网络安全法》强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据应当在境内存储等法律措施，确保关键信息基础设施的运行安全。

“集赞有奖”的真假识别

陈女士的朋友圈被一家影楼的“集赞”活动刷屏了，消息称，转发影楼活动到朋友圈，集50个赞就能免费拍全家福，并领取一台多功能料理机，于是，陈女士也加入了此活动。

集齐50个赞的陈女士前往影楼预约拍照，却被影楼工作人员告知须在一周后才能预约，并需交500元押金，押金将在拍照之后退还。陈女士质疑为什么要交押金，对方解释如果参与者光拍照不取片，会导致照片积压难以处理，只要领完照片便会马上退款，陈女士打消顾虑后便交了押金。

一周后，陈女士致电影楼，被告知预约名额已满，让她一周后再约。不久，陈女士听说该影楼已关门，立刻前往核实，发现早已人去楼空。

安全解读：

不法分子发布集赞活动是为了吸引潜在受骗人参加，一旦信以为真，不法分子即以“押金”“保证金”等形式实施诈骗。如果消费者贪图这些小便宜，往往就会一步步落入圈套。

防范方法：

1.提高自己的辨识能力，不轻易传播未经核实的信息；

2.对于需要支付“押金”“保证金”等活动，一定要慎重考虑是否参与；

3.若发现某活动存在诈骗嫌疑，应立即报警或向有关部门举报。

兼职陷阱的正确识别

小星工作之余一直想做兼职。一天在网上被一条每月收入过万元的兼职广告吸引。小星和对方取得联系后，对方表示小星只需按照要求完成网购交易，就会返还购物本金和等于本金金额10%的佣金。刚开始小星接的都是小单，很快就收回了本金和佣金。此后小星刷单金额越来越大，先后完成了多笔交易，可对方却再也没有返还本金或佣金，直至对方完全失联，小星才意识到上当受骗。

安全解读：

不法分子利用学生或其他人员想找份兼职的心理，通过手机、互联网等，发布虚假招聘广告，广告内一般留有不法分子的QQ号。当兼职者添加QQ好友后，不法分子就开始指导兼职者进行刷单操作。第一单往往金额较小，会及时返还本金和佣金。此后刷单任务逐渐增多且金额不断增大，不法分子就会以订单异常等理由，不再返还本金或佣金。

防范方法：

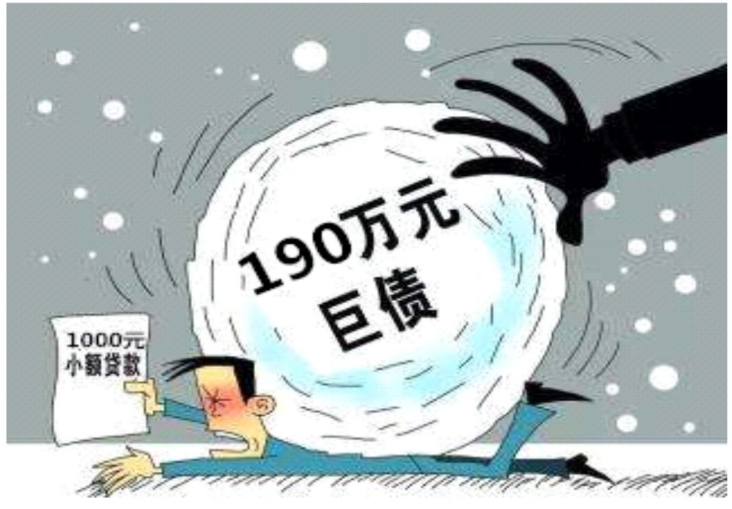
1.找兼职一定要选择有信誉且专业的兼职网站，并对兼职信息加以甄别；

2.万不可被“日结工资”或“高佣金”之类有噱头的广告词蒙骗，切记不要贪图小利，以免损失钱财；

3.不管是找工作还是找兼职，都要提高安全意识，避免上当受骗。

网贷陷阱的正确识别

赵某在某QQ群看到一则无抵押贷款广告，遂在网上向放贷人申请贷款1000元。放贷人让赵某打了1200元的欠条，扣除利息200元后，在网上付给他1000元。由于各种原因赵某无法按期还款，原放贷人便向赵某推荐了一名新的放贷人，而第二个放贷人也需要扣掉相应利息。就这样，赵某陷入了和之前一模一样的借贷套路。等到他还不起时，第三个、第四个和第五个放贷人会陆续登场。而此时，利滚利、本金滚本金，再加上违约金、滞纳金等等，赵某需要偿还的贷款越滚越多，已经累计到100多万元。此时，放贷人威胁赵某还钱，并恐吓他已到法院起诉，将要拍卖他的房屋和车辆。



安全解读：

不法分子从一开始就以非法占有借款人的财产、房产为目的，利用借款人社会经验不足的弱点，处心积虑地通过“双倍借条”或“平账”等手段，将原来的小额借款，变成难以偿还的债务，进而逼迫当事人抵押房产、签订长期租房合同，或者勾结黑中介直接“网签”卖房，一环套一环骗取受害人的房产。

防范方法：

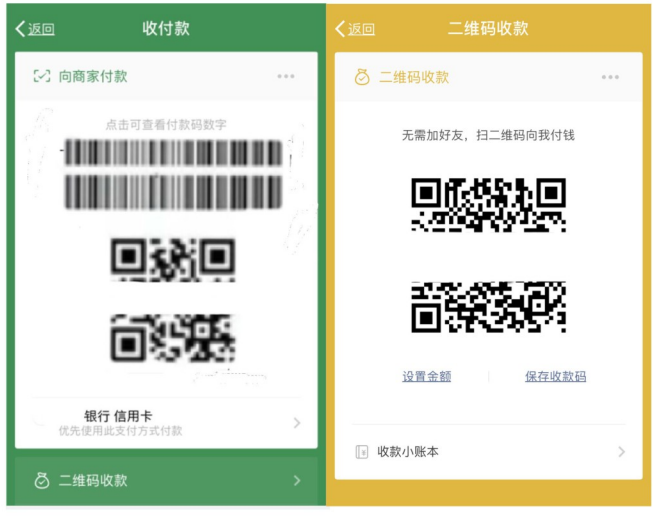
1.到正规的金融机构或平台贷款；

2.不要被“无需抵押，快速放贷”等广告诱惑，应详细了解后再做决定；

3.如不幸受骗，应第一时间向公安机关报案，同时保留好相关的借款合同，微信、短信的转账及聊天记录等证据，并及时提交公安机关。

二维码的正确使用

经营快餐生意的覃先生接到一个订餐电话，电话里有人要订35份快餐，总共消费499元，并希望通过微信付款，覃先生没有多想，在对方的指导下把自己微信二维码上的数字报给了对方。不久，覃先生收到一条转账499元的短信提示，才意识到自己上当受骗了，原因是错把付款码当作收款码来使用。



安全解读：

不法分子利用受害人无法有效区分“付款码”和“收款码”来骗取受害人的“付款码”信息，以达到骗取钱财的目的。另外，不法分子通过替换商户的收款码、共享单车二维码、罚单二维码等方式更改收款账户，或发布隐藏有木马病毒的二维码，一旦受害人扫码支付，便可轻松获取受害人的钱财。

防范方法：

1.注意辨别“付款码”和“收款码”，仔细观察二维码有无被替换；

2.扫描二维码后要求填写个人账户信息的，坚决拒绝；

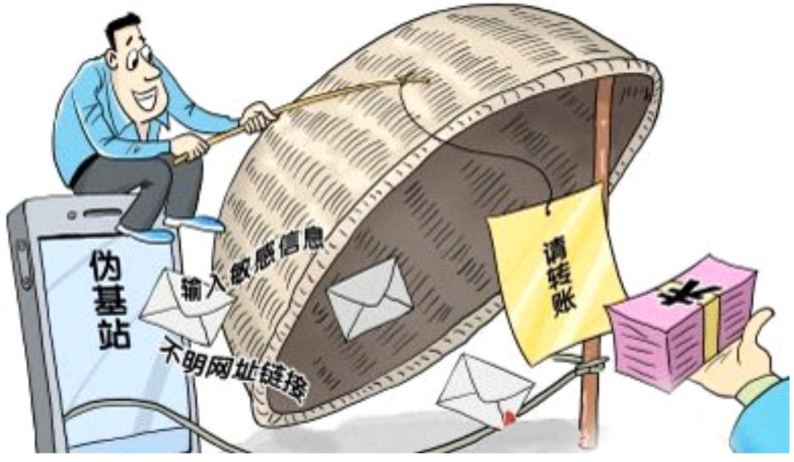
3.不要泄露支付软件上的条形码、二维码和数字编码；

4.不要在用于网上支付的银行卡中存储大额资金；

5.手机上应安装安全防护软件。

伪基站的安全防范

李女士正在玩手机，突然收到一条XX银行发来的银行卡消费积分兑换短信，没有多想就点开了链接，并按提示输入了自己的银行卡卡号和身份证号码，又输入了XX银行短信发来的验证码，没想到短短数十秒后，就收到多条共计转款99998元的短信，李女士这才意识到自己被骗了。



安全解读：

不法分子利用伪基站伪装成银行或运营商发送诈骗短信，引诱手机用户点击短信中的链接，从而将木马病毒植入用户手机，盗取用户账号、密码等敏感信息，实现骗取钱财的目的。

防范方法：

1.发现手机信号突然中断，应提高警惕，因为靠近伪基站时，手机一般会脱网，几秒后才恢复正常；

2.当收到“中奖”“转账”等短信时，一定要提高警惕，不要轻易点击短信中的链接，更不要转账汇款；

3.不要轻信各种积分兑换，正常的积分兑换应通过官方渠道；

4.手机要安装安全类软件，它们可以有效拦截垃圾短信。

网购退款的真假识别

陈女士在某网购平台上购买了一件价格几十元的物品，因对物品不满意申请退款。经沟通，网店同意退款并指导陈女士通过某支付平台办理退款手续，款项很快就退回至陈女士的银行卡，但金额却为1万元。网店的电话紧跟而至，声称由于误操作而错转成了1万元，要求陈女士把钱退回到指定的账户，否则就会报警。幸好陈女士警惕性较高，立即向公安机关报案，未造成资金损失。

经调查，在通过某支付平台办理退款时，陈女士实际上是点开了支付平台的贷款页面并操作成功，而不法分子却谎称是其退款操作错误，要求其退回，以此实施诈骗。

安全解读：

不法分子冒充网购平台客服，以“商品有质量问题”或“交易异常”等“退款”理由诱导买家开通支付平台的借贷项目，并以“错转”为借口要求受害人将钱款退回至指定账户。由于不法分子能准确说出订单详情，因此很容易获取买家的信任并实施诈骗。

防范方法：

1.任何时候都不点击陌生人发送的链接，不扫描陌生人发送的二维码；

2.网购退款时，要在电商平台的官方网站操作；

3.注意网址真伪，对需要登录的，谨防账号密码被盗；

4.网络购物要留个心眼，千万别贪小便宜上大当。

谨防“熟人”借钱的陷阱

庞某接到一个陌生电话，对方自称是其领导，要求庞某次日早上去其办公室一趟。第二日，庞某上班途中再次接到该领导电话，对方称其临时出差，马上登机，但家属有人突然住院急需用钱，叫其帮忙到银行汇款给亲属。随即庞某向对方提供的银行账户汇款2万元。经查，这是不法分子对不特定的人群拨打电话，以冒充领导、熟人的方式实施电信诈骗的犯罪行为。

安全解读：

不法分子通过非法手段获得受害人的姓名及电话号码，打通受害人电话后以“猜猜我是谁”，冒充领导、熟人等方式，谎称其遇到需给领导送礼、生病住院、交通事故赔钱等“急事”，以借钱救急为借口，骗取受害人将钱款打到指定的银行账户。

防范方法：

1.凡是自称领导、同事要求汇款的，一律不理；

2.凡是告知“家属”出事需要先汇款的，一律不管；

3.凡是涉及到银行账户信息的，一律挂掉；

4.注意保护个人信息，以防泄露；

5.如不幸受骗，应及时报警。

投资理财需谨慎

张小姐喜欢炒股。最近她所在的股票交流群里来了一位阿牛老师，时常推荐一些理财信息，张小姐加了他的QQ。阿牛老师推荐张小姐炒外汇，称他们现在有个外汇操盘团队，有庄家在操盘，盈利后五五分成，张小姐很心动。

在阿牛老师的指导下，张小姐注册使用了该平台，一开始只投入几百元，很快就赚钱了，而且第二天就能提现，于是她渐渐加大投入，短短几天赚了1万多元。这时，阿牛老师提出可以私下给张小姐带单，赚的钱不需要分成。看到炒外汇赚钱这么容易，张小姐便介绍了闺蜜向小姐加入，向小姐很快也赚了几千元。随后，闺蜜俩各自往账号里充了5万元准备做笔大单时，却发现该网站已关闭，阿牛老师联系不上，钱也取不出来。两人才发现被骗了，于是到公安局报案。

安全解读：

不法分子通过给受害人推荐“股票分析师”获得信任，一步步骗取受害人钱财。不法分子还会特意架设一个黑网站平台，操控客户的盈亏、提现等。他们一般会让客户先赚一点，然后再引诱客户投入更多的钱，等客户投入的资金达到一定金额后，不法分子便会拿钱跑路。

防范方法：

1.投资时，应选择正规的投资平台；

2.不要随意加入各类投资群，这类群里很可能除了你之外，其他所有人都是骗子；

3.不要有一夜暴富的幻想，号称高回报、高收益都是不法分子常用的伎俩。

网游交易要小心

胡某在游戏中看到一个叫“小呆”的玩家要低价出售游戏装备的消息，便立即加“小呆”为QQ好友。随后，“小呆”发送了金额为19.8元的收款二维码给胡某，让其支付购买游戏虚拟装备的货款。胡某支付成功后，“小呆”又发送了一份“装备须知”的文件和收款二维码给胡某，称只需支付0.05元，完成支付后，短信提示的付款金额竟为9998元！原来，该二维码实际收款金额为9998元，但被不法分子修改为0.05元。

安全解读：

不法分子通过低价出售各类游戏装备及游戏币，将有病毒的文件传给受害人，受害人中招后，其付款金额便可被不法分子任意修改。无论实际支付多少金额，支付页面上均显示0.05元。

防范方法：

1.购买网游装备等物品，必须通过正规网站，以免被骗；

2.不要随意下载QQ或微信等社交软件中不明用户发来的文件；

3.不要贪图网购中的小恩小惠，以免上当受骗；

4.电脑或移动终端安装安全软件，并定期进行安全扫描。

应对冒充公检法诈骗的正确方法

市民小林接到一通自称是“市XX区电信局”的电话，对方称小林在该市开户的电话欠费1000元。小林否认后，对方又称是其身份信息被冒用所致，应该立即报案，并帮其把电话转接到“市公安局XX分局”。一名自称是XX分局民警的男子接听电话，以小林涉嫌洗黑钱犯罪为由，诓骗他将名下存款转到指定账户以证清白。小林信以为真，遂将自己银行卡内的几十万元人民币分多次转账到不法分子提供的账户内。

安全解读：

不法分子冒充“公安局”“检察院”“法院”等单位“工作人员”，威胁受害人涉嫌洗钱、贩毒、拐卖儿童、买卖器官、经济犯罪等，利用受害人急于“摆脱干系、减少损失”的心理，诱使受害人将钱款转入不法分子提供的所谓安全账户，以达到诈骗的目的。

防范方法：

1.所谓“安全账户”“秘密账户”都是陷阱，切记不相信、不转账；

2.所谓提示登录指定网站、输入密码进行转账操作的都是陷阱，切记不相信、不转账；

3.所谓行政执法部门、人员以办案为名要求转账、汇款的都是陷阱，切记不相信、不转账；

4.所谓提示登录网站查看网上通缉令、协查通报的都是陷阱，切记不相信、不转账；

5.收到冒充公检法查案的电话或短信时，应及时与家人朋友商量，切不可盲目听从电话内陌生人的指挥。