
国家网络安全
宣传周
China Cybersecurity Week
网络安全
守护你我
2021
金融网络安全宣传手册
中国人民银行
THE PEOPLE'S BANK OF CHINA

大政方针

网络安全相关战略法规

网络安全是国家安全的重要组成部分，也是“十四五”规划建设数字中国战略的基座。网络安全不仅关乎国家安全、社会安全、城市安全、基础设施安全，也和老百姓的生活密切相关。

“没有网络安全就没有国家安全”

2018年4月20日至21日，习近平总书记在全国网络安全和信息化工作会议上发表讲话。他强调：“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。”

“十四五”规划高度重视网络安全

2021年3月，《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》正式发布，其中“网络安全”一词在文中出现14次，成为国家、社会科技发展道路上的重要议题。

努力把我国建设成为网络强国

2014年2月27日，习近平总书记在中央网络安全和信息化领导小组第一次会议上提出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建设成为网络强国。”

《国家网络空间安全战略》

2016年12月27日，经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》。《战略》贯彻落实了习近平总书记网络强国战略思想，阐明了中国关于网络空间发展和安全的重大立场和主张，明确了国家网络空间安全工作的目标、原则和战略任务，切实维护国家在网络空间的主权、安全、发展利益，是指导国家网络安全工作的纲领性文件。

目　标　和平、安全、开放、合作、有序。

原　则　尊重维护网络空间主权；和平利用网络空间；依法治理网络空间；统筹网络安全与发展。

战略任务　坚定捍卫网络空间主权；坚决维护国家安全；保护关键信息基础设施；加强网络文化建设；打击网络恐怖和违法犯罪；完善网络治理体系；夯实网络安全基础；提升网络空间防护能力；强化网络空间国际合作。

国家网络安全工作“四个坚持”

坚持 网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。

坚持 网络安全教育、技术、产业融合发展，形成人才培养、技术创新、产业发展的良性生态。

坚持 促进发展和依法管理相统一，既大力培育人工智能、物联网、下一代通信网络等新技术新应用，又积极利用法律法规和标准规范引导新技术应用。

坚持 安全可控和开放创新并重，立足于开放环境维护网络安全，加强国际交流合作，提升广大人民群众在网络空间的获得感、幸福感、安全感。

《中华人民共和国网络安全法》

2016年11月7日，国家颁布《中华人民共和国网络安全法》，自2017年6月1日起施行。这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。

《网络安全法》六大要点

- 一是明确了网络空间主权的原则。
- 二是明确了网络产品和服务提供者的安全义务。
- 三是明确了网络运营者的安全义务。
- 四是进一步完善了个人信息保护规则。
- 五是建立了关键信息基础设施安全保护制度。
- 六是确立了关键信息基础设施重要数据跨境传输的规则。

《中华人民共和国数据安全法》

为规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，国家制定《中华人民共和国数据安全法》，并于2021年6月10日正式发布，自2021年9月1日起施行。

《数据安全法》三大特点

- 一是坚持安全与发展并重。设专章对支持促进数据安全与发展的措施作了规定，保护个人、组织与数据有关的权益。
- 二是加强具体制度与整体治理框架的衔接。从基础定义、数据安全管理、数据分类分级、重要数据出境等方面，进一步加强与《网络安全法》等法律的衔接。
- 三是回应社会关切。加大数据处理违法行为处罚力度，建设重要数据管理、行业自律管理、数据交易管理等制度，回应实践问题及社会关切。

《中华人民共和国个人信息保护法》

2021年8月20日，《中华人民共和国个人信息保护法》正式发布，将于2021年11月1日起施行。《个人信息保护法》在有关法律的基础上，进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。

《个人信息保护法》十大亮点

- 一是确立个人信息保护原则，强调处理个人信息应当遵循合法、正当、必要、诚信、目的限制、最小必要等原则。
- 二是规范处理活动、保障权益，构建了以“告知-同意”为核心的个人信息处理规则。
- 三是禁止“大数据杀熟”，要求个人信息处理者保证自动化决策的透明度和结果公平、公正。
- 四是将生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等列为敏感个人信息，并给予严格保护。
- 五是规范国家机关处理活动，强调国家机关处理个人信息应当依照法律、行政法规规定的权限和程序进行。
- 六是明确公民对其个人信息的处理享有知情权与决定权、查阅复制权、可携带权、更正补充权、删除权、解释说明权等，有权限制或者拒绝他人对其个人信息进行处理。
- 七是强化个人信息处理者义务，明确个人信息处理者应当采取必要措施保障所处理的个人信息的安全。
- 八是特别规定了提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的义务。
- 九是设专章规定个人信息跨境提供的规则，规范个人信息跨境流动。
- 十是健全个人信息保护工作机制，明确履行个人信息保护的职责部门及监管职责。

《个人信息保护法》切实将广大人民群众网络空间合法权益维护好、保障好、发展好，使广大人民群众在数字经济发展中享受更多的获得感、幸福感、安全感。

《关键信息基础设施安全保护条例》

关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重。2017年8月17日，国务院公布《关键信息基础设施安全保护条例》，自2021年9月1日起正式施行。作为《网络安全法》的重要配套法规，《条例》的公布实施为建立健全关键信息基础设施安全保护体系，提升网络安全防护能力，提供了更具有操作性的法律依据，切实将网络安全法所规定的关键信息基础设施保护制度落到实处。

险象环生

网络安全风险就在身边

假冒WiFi热点

无线接入点 (Access Point, AP) 俗称热点，是无线网和有线网之间信号传输的桥梁，一些商业机构往往通过使用多个AP来扩大无线覆盖范围，提供方便用户“蹭网”的WiFi。攻击者通过架设名字相近甚至相同的虚假AP，引诱用户连接其提供的假冒WiFi热点。一旦连接假冒WiFi热点，攻击者就可以通过虚假AP对用户终端进行配置篡改、信息数据窃取、广告及恶意软件植入、产生流量费用等破坏。

如何防范假冒WiFi热点：

公共场所下避免连接免费的、无密码的WiFi热点，如需连接WiFi，应向公共场所的WiFi热点提供方确认热点名称和密码，看清WiFi热点名称，连接后使用安全软件对热点进行安全扫描。

使用公共场所WiFi热点时，不要进行网上购物、网银转账等操作，尽量避免登录手机银行等APP的个人账户，不要进行输入密码、填写身份证号等涉及个人敏感信息的操作，以免造成信息泄露。进行以上操作尽量使用电信运营商的4G或5G网络。

关闭终端的“WiFi自动连接”功能，避免自动连接黑客建立的同名假冒WiFi。为家用WiFi路由器设置复杂密码并定期更换。

恶 意 软 件

恶意软件是指可以影响或中断用户互联网设备正常运行、造成数据泄露或侵害用户权益等危害的软件，介于病毒和正规软件之间。如果设备中有恶意软件，可能会出现以下几种情况：上网时会有窗口不断跳出，设备配置被莫名修改，设备经常卡顿或死机，数据有丢失，文件打不开，新增大量来历不明的文件，内存或硬盘空间突然不足，操作系统自动执行操作等。

如何防范恶意软件：

下载软件要通过官方正规渠道，不要下载或安装来历不明的未知软件，不轻信标注“免费版”“破解版”的软件。安装软件前用杀毒软件进行查杀，不随意执行未经杀毒扫描的安装程序。

定期备份设备内的系统数据和文件，留意设备异常现象和告警，及时排查修复。为设备系统设置复杂密码并定期修改。

个人信息泄露

个人信息是指以电子或者其他方式记录的，能够单独或者与其他信息结合，识别特定自然人身份或者反映特定自然人活动情况的各种信息。个人信息泄露将导致骚扰电话、垃圾短信不断，关乎人身和财产安全的个人敏感信息泄露，更容易招致非法网贷、电信诈骗、敲诈勒索、人口拐卖等犯罪行为的攻击。

如何保护个人信息：

不要在网上晒个人证件及银行卡、证件照、手机号、出行票据、支付凭单、消费记录、住址定位、车辆信息、家人信息等敏感信息。关闭软件中的“定位”“附近的人”“允许陌生人查看”等功能。

不在来路不明的网站、APP、软件、小程序内输入个人信息。使用各类软件或APP时，注意阅读运营商对通讯录、相册、定位等隐私数据进行访问或采集的请求，去掉不必要的勾选，发现违规采集行为，可依据《网络安全法》向网信、电信或公安部门举报。

钓 鱼 邮 件

钓鱼邮件是指在邮件内部嵌有钓鱼链接或恶意程序的邮件，一般由黑客伪装成同事、亲友等用户信任的人或医疗、教育、公检法等机构公职人员发送钓鱼邮件，诱使用户回复邮件、点击嵌入邮件正文的恶意链接或打开邮件附件以植入病毒，进而窃取用户敏感数据、远程控制设备或实施进一步的网络攻击活动。

如何辨识钓鱼邮件：

看发件人地址 通常会利用不易发现的拼写错误来仿冒邮箱地址，或用私人邮箱发送号称官方的邮件。

看邮件主题 一般涉及“订单发票”“通知”“会议”等看似内容很重要的关键词，“新冠”“防疫”等重大疾病灾害或社会热点事件关键词也会被用来借机传播。

看正文措辞 对使用“亲爱的用户”“各位同事”等泛化问候的邮件直接忽略。警惕指名道姓的邮件，可能存在个人信息泄露的情况。

看正文目的 对于邮件内索要身份证号、银行账户或任何密码等个人信息的，要提高警惕，不要乱填、乱回复。

看正文内容 不要好奇乱点邮件中的链接地址或“退订”等任何诱导点击的按钮，很可能是钓鱼链接或被植入恶意代码。警惕任何制造紧急氛围的邮件，如“请务必今日下班前完成”等，这是让人忙中犯错的手段。

看附件文件 文件名带有迷惑性的附件可能是病毒，轻易不要下载。如已下载，打开前先用杀毒软件扫描。

网络电信诈骗

网络电信诈骗通常指通过网络、电话、短信等途径，利用虚构事实或者隐瞒真相等手法，骗取他人财物的诈骗手段。

识别常见网络电信诈骗：

仿冒身份类诈骗

利用微信、QQ等聊天软件，通过盗号、模仿账号昵称及头像、伪造各类公文图片等方式，伪装冒充亲友或银行、公检法、医保社保、运营商等单位进行诈骗。

虚构险情类诈骗

通过捏造亲友车祸绑架、征信拉黑、涉嫌犯罪等各种意外、令人恐慌的消息，诱导用户在慌乱下盲目听从诈骗者引导，进行网络汇款、非法网贷申请、虚假机构APP注册等操作，达到诈骗目的。

钓鱼类诈骗

通过短信或邮件链接、二维码扫描、微信推送、免费WiFi热点广告推送等途径，引诱用户访问其仿冒的银行、电信运营商、电子商务等类型的网站或APP，诱骗“上钩”用户在其中填写个人敏感信息，从而“钓取”用户账号密码等隐私。

购物消费类诈骗

以线上客服、代购、快递员、电信运营商、物业楼宇管家等身份的口吻，向用户发送虚假销售或优惠信息、客服退款、车次航班取消退款、快递丢失赔偿、物业费及生活费用缴纳等虚假消息实施诈骗。

利诱类诈骗

以各种诱惑性的中奖信息、奖励、高额薪资、高收益投资理财产品、网上贷款等吸引用户输入个人信息或转账，从而进行诈骗，一般还会附带“转发即赠送”等条件诱惑用户通过网络传播扩散虚假信息，扩大诈骗范围。

木马病毒类诈骗

通过钓鱼邮件或短信、黄色广告弹窗、色情网站、游戏安装包、免费破解版软件安装包等方式，诱骗用户下载恶意软件或点击恶意链接，在用户设备中植入木马病毒，从而达到窃取用户密码等敏感信息的诈骗目的。

漏洞攻击

漏洞是指信息系统软件、硬件或通信协议中存在的设计、实现或配置缺陷，可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。当发现安全漏洞后，产品供应商一般会提供对应的修复程序，即补丁。但补丁发布后，往往不被用户及时安装，反而被更多黑客用来推断漏洞所在，仍会造成大量漏洞攻击。

如何防范漏洞攻击：

安装杀毒软件、安全防护软件，定期对设备进行体检，及时排查漏洞隐患。关注各类软硬件产品安全提示和补丁修复提示，及时安装补丁。不用的服务、软件要关停或卸载，开启防火墙。

有备无患

树立防范意识从我做起

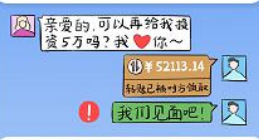
反诈骗灵魂八问

刷单前问问自己：

动动手指头就能赚钱的好事为啥能轮到你？

网恋前问问自己：

人靓声甜的小姐姐，温柔帅气又多金的小哥哥，为啥还需要网恋？



收到逮捕令时问问自己：

抓人还需要提前通知？警察是不是觉得自己太闲，怕坏人跑路跑得不够快？

裸聊前问问自己：

自己的身材值不值得美女与你“坦诚相见”？

网贷前问问自己：

无抵押还免息，对方为啥不直接送钱给你？

点陌生链接前问问自己：

查信息就查信息，为啥还要下载一堆东西？

理财前问问自己：

战无不胜的投资大师，为啥要苦口婆心地帮助非亲非故的你？

给领导转账前问问自己：

用自己的微信公然收受巨额资金，领导是不是嫌自己官干久了？

当遇到以上情况时，保持头脑冷静，心存防范，牢记“不决断晚交钱，睡一觉过一天，再找亲人谈一谈”的口诀，多留点时间给自己思考并核实相关情况，避免被诈骗分子套路。

互联网办公数据安全防护五大措施

工作账户必须设置强密码

如果工作账户密码设置过于简单，可能被黑客通过暴力破解轻易获取，从而直接“访问”工作单位及相关企业数据。建议在设置工作账户密码时，采用包含数字、大写字母、小写字母以及特殊字符组成的“强密码”。同时，工作单位如能在默认情况下对所有登录行为执行密钥验证，则可在更大程度上确保数据的安全性。

注重各终端设备的安全性

由于互联网在数据传输方面的方便快捷，办公过程中，常常有通过手机、平板电脑等个人终端设备与办公设备互联互通的情况。个人终端不同于办公终端，没有专人统一维护，更容易遭受黑客攻击或电脑病毒感染，从而在使用过程中对数据安全造成意想不到的安全威胁。因此，对办公终端需要采取以下安全措施：终端设备的软硬件及时更新并安装补丁，确保由厂商提供的数据安全防护功能不会过期或失效；在终端设备运用具备防病毒、防火墙、Web过滤、加密等功能的专业安全防护软件保障数据安全。

建立信息共享与保存准则

企业或单位如果对于数据的传输、存储和共享行为“放任自由”、未建立健全相关安全管理机制，比如通过电子邮件直接收发重要文件等，会造成重要、敏感办公数据泄露、丢失、篡改等安全风险。有意识地建立并严格落实对办公数据的共享与保存机制，对信息化办公中数据传输、存储和共享行为加以约束，养成安全的网络办公习惯，对办公数据安全意义重大。

规避潜在的网络安全威胁

办公终端暴露在互联网环境下，同样会面临钓鱼邮件或网站、假冒WiFi热点、恶意软件及链接、病毒攻击等网络安全风险。互联网办公期间，保持对公共场所WiFi、陌生蓝牙和共用USB设备等的安全防范意识，切勿轻率打开或点击、下载可疑电子邮件内的链接和附件，避免感染各类电脑病毒或被诱导至钓鱼网站，造成数据泄露及一系列后续安全隐患。

对重要数据及时做好备份

对重要办公数据时刻做好备份工作，是避免造成无法挽回的后果的最有效方法。可选择专业、可靠的云平台存储数据，不要将所有文件资料等信息保留在个人电脑等私人终端硬件上。同时请注意，除非已经过加密，否则切勿使用可能存在安全隐患的外部存储设备。

固若金汤

守护金融网络安全防线

手机银行安全使用Tips

谨慎开通勿出错

开通手机银行时，安装使用银行官方渠道发布的客户端，并确认签约绑定的是本人使用的手机号，同时根据平时转账金额设立合适的额度，如果只是小额支付，可以把转账额度设定小一些。

密码复杂不外泄

为手机银行账户设置单独的、高安全级别的登录密码，尽量在8位以上、包含数字、大小写字母及特殊符号，务必保证与邮箱等其他账号密码有所区别。手机内不要存储密码，以防外泄。

登录退出多留意

尽量不在公共场所WiFi环境下登录或使用手机银行。每次登录要仔细核对欢迎信息、上次登录时间是否正确，发现异常情况立即退出。每次使用完手机银行后，一定要安全退出，避免手机银行在后台运行期间被攻击。

使用期间莫分心

不要在登录使用手机银行期间，随意查看来历不明的短信或邮件、点击不明链接、下载不明文件、扫描不明二维码，谨防木马、钓鱼邮件攻击。安装杀毒软件，定期查杀病毒并升级手机银行客户端。

交易信息要掌握

开通短信通知业务或银行微信服务号通知功能，即时掌握账户资金变动。如有手机银行被盗用的情况，能够第一时间发现异常支付信息，并联系银行客服查询或向公安部门报警。

手机遗失速冻结

一旦发生手机或SIM卡遗失的情况，尽快向提供服务的电信运营商办理挂失或申请停止服务，同时第一时间通过银行网点柜台或致电银行客服热线暂停手机银行服务、冻结网银功能，避免因手机中的账号或密码被盗而造成更大损失。

根据中国人民银行发布的《移动终端支付可信环境技术规范》(JR/T 0156—2017)，现在，不少手机银行运用了“手机盾”技术，基于手机芯片的TEE(可信执行环境) 和SE(安全元件)，实现硬件级的安全性，方便大众在手机上实现安全的大额转账、身份认证等功能。手机盾功能可咨询各大银行客服或前往柜台进行开通。

警惕网上购物陷阱

- 核实网站资质及联系方式的真伪，要到知名、权威的网上商城购物，不要轻信不知名网店的低价推销。
- 尽量通过网上第三方支付平台交易，并检查支付网站的真实性，切忌直接与卖家私下交易。
- 购物时要注意商家的信誉、评价和联系方式。
- 交易完成后，完整保存交易订单等信息。
- 直接使用银行账号、密码和证件号码等敏感信息时要慎重。

警惕网上贷款陷阱

- 警惕贷款前需要先行缴费的网贷机构，正规的贷款机构在放款之前是不会收取任何费用的。
- 银行对于无抵押贷款有严格要求，仅凭身份证是无法办理的，因此不要轻信“无抵押贷款”“低息”“免息”“当天放款”等广告标语，也不要相信仅凭身份证就可办理的贷款。
- 一旦发觉网贷机构可能是骗子，马上停止汇款操作并立即进行举报，可以拨打银行官网客服电话、当地派出所电话或110报警电话进行求证或举报。

虚拟货币与数字人民币

虚拟货币

虚拟货币是指基于区块链等技术，通过复杂数学算法产生的加密数字货币，如比特币、以太币等。虚拟货币不由中国人民银行发行，不具有法偿性和强制性等货币属性，并不是真正意义上的货币，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用。从我国现有司法实践看，虚拟货币交易合同不受法律保护，投资交易造成的后果和引发的损失由相关方自行承担。广大消费者要增强风险意识，树立正确的投资理念，不参与虚拟货币交易炒作活动，谨防个人财产及权益受损。

VS

数字人民币

数字人民币由中国人民银行发行，是有国家信用背书、有法偿能力的法定货币。与比特币等虚拟货币相比，数字人民币是法币，与法定货币等值，相当于“电子版人民币现金”，其效力和安全性是最高的。而虚拟货币是一种虚拟资产，没有任何价值基础，也不享受任何主权信用担保，无法保证价值稳定。这是数字人民币与比特币等虚拟货币最根本的区别。

数字人民币具有双层运营、支持银行账户松耦合、双离线支付、点对点交付、高可追溯性等特点。

警钟长鸣

金融网络安全典型案例

网贷陷阱

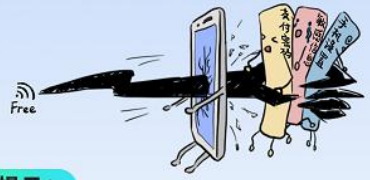
做小本生意的刘先生因为疫情损失订单、缺少流动资金，陷入困境。这时，他接到骗子的短信和电话，骗子冒充银行客服人员，表示可以为刘先生办理无息贷款，需要他缴纳十万元押金。刘先生先后两次打电话咨询银行正规客服，客服均回复没有这类贷款，提醒刘先生小心被骗。病急乱投医的刘先生在骗子的一再诱惑下，决定通过网银给骗子转账。刘先生来到银行网点，银行工作人员发现刘先生曾多次咨询客服，立即核实情况，与刘先生沟通，阻止了刘先生被骗，并为刘先生办理正规贷款，解决燃眉之急。

安全提示：

通过网络借贷平台贷款前需要通过官方渠道查验真伪，切勿相信非法网贷、校园贷等非正规渠道贷款，不要被“无抵押”“到款快”“无息”等广告诱惑。建议尽量通过银行等金融机构的正规渠道贷款。

免费WiFi陷阱

市民张先生使用公共场所的WiFi后，电脑被黑客入侵，在U盾、银行卡均未丢失的情况下，网银被他人在两天内盗刷69次，卡上的6万多元仅剩下500元。更可怕的是，他的手机也被黑客做了手脚，接收消费提醒短信的功能全部被屏蔽，所发生的69次交易他根本没收到任何短信提示，钱在不知不觉中被转走了。



安全提示：

关闭手机和计算机的自动连接WiFi的功能。在公共场所，不要连接未知的WiFi。不要将自己家的WiFi密码共享，定期修改密码。在未知的WiFi信号下不要输入QQ、微信、游戏、银行、支付宝等密码。

新冠疫苗骗局

罗先生收到一条“疾管中心”发来的手机短信，称“新冠疫苗接种预约已在我市开放，名额有限，截止于本周五前暂停报名”，并附带一个预约报名链接。随后，罗先生接到自称社区卫生服务中心打来的电话，声称要统计社区居民新冠疫苗接种情况，如果在月底前仍未接种将限制跨省出行，并督促罗先生尽快按照短信通知预约。罗先生赶紧访问短信链接，在未能识别其为钓鱼网站的情况下，按照提示依次输入了姓名、身份证号、银行卡号、密码等信息。十分钟后，罗先生收到了银行卡消费8000元的短信，才意识到被骗。

安全提示：

对于提及“新冠”“疫苗”等与当下重大疾病、灾害或热点相关的信息，要提高警惕。对可疑的电话或短信不要轻信，更不要直接与短信内给出的电话号码联系，有疑问应及时致电相关单位官方电话核实，银行账户、密码，特别是手机验证码不得外泄，做好个人金融信息保护。

弱密码泄露

某天，李小姐的银行卡发生“隔空被盗”的现象，卡好好地揣在兜里，却莫名收到了钱被跨国刷走的短信提示。经过警方与银行联合调查，发现是专业黑客从银行、商场等地窃取了李小姐的银行卡信息，转卖给国际盗刷组织。由于李小姐银行卡使用了生日这样的弱密码，被黑客轻易破解，盗刷金额上万元，损失惨重。

安全提示：

弱密码也称弱口令，指容易被他人猜测或被破解工具破解的密码。银行卡、手机银行、网银、第三方支付软件等的登录及支付密码应杜绝使用弱密码，密码应同时包含大写字母、小写字母、数字和特殊字符，不包含连续字符（如“123456”“qwertyui”）、重复字符组合（如“AAAAAA”“123123”）、特殊含义字符组合（如“5201314”）、完整英文单词（如“password”“iloveyou”）等，也不包含个人及父母、子女、配偶的姓名、生日、手机号等信息。不与其他社交账号、游戏账号共用相同密码，养成定期更换密码的习惯。

网购退款诈骗

大学生王同学手机收到一条陌生号码发来的短信，称王同学网购的商品订单系统出错，要王同学联系订单中心办理退款。王同学按照短信上提供的号码拨打过去，对方能准确说出王同学的订单号，并声称该订单被冻结了，需要去附近银行解冻。当王同学质疑为何不能直接退回支付账户时，对方称，由于该订单在系统升级时出现了问题，无法通过原账户进行退款，并叮嘱王同学要尽快完成这笔退款，不然会更麻烦。当天下午5点，王同学在校园内的ATM机上按对方的指示操作，向对方账户汇了1888元的“订单解冻金”，直到收到银行卡被消费1888元的信息，王同学才反应过来被骗。

安全提示：

网上购物选择可信度高的电商网站，不要乱晒网购订单、购物凭证，不要随意丢弃含个人信息的快递单、快递盒。收到各类网购异常提示的短信或电话，先直接拨打购物网站的官方客服热线进行查询核实，对于要先汇钱或提供卡号密码等信息再退款的要求一概不予理会。

二维码陷阱

张女士发现自己路边停放的车上被贴了罚单，上面还印有快速缴费二维码，张女士随即扫描该二维码并缴纳罚款。事后，经朋友提醒，张女士打电话咨询交管部门，才发现自己扫描了假的二维码。

安全提示：

不法分子常通过伪造带有二维码的交通罚单、物业费缴纳单、学费单、党费单等，引诱大家扫码支付。一定要通过官方联系渠道与收款方确认二维码真伪，不要随便扫描未知二维码。扫描后若要求填写个人账户信息的，坚决拒绝。警惕商户或出租车费支付、共享单车或共享充电宝租借等张贴在公共区域的二维码，扫描前检查是否有被人替换、覆盖的痕迹，扫描后擦亮眼睛，看好商户信息或应用信息后再支付。使用付款二维码时，不要将付款码暴露给身边的陌生人，防止不法分子利用“小额免密”功能盗刷。

虚拟货币骗局

张先生用手机浏览网页时，无意中弹出的一个“XX云币”虚拟货币投资网站，详细介绍虚拟货币投资情况和收益报表，看到购买后每周都有收益，回报还不低，他就想试一下，随即添加该网站客服的微信号进行咨询。随后，张先生按照对方指引，用手机下载了该虚拟货币平台APP，并转账100元到该APP上提供的银行账户，租用了100元的矿机（用于赚取虚拟货币的计算机）。一个星期以后，他看到之前租用的100元矿机真的有收益进账，觉得可信，就继续租用了一种1000元的矿机试一下。大约一周后，张先生欣喜地发现自己在该网站平台APP的账户上又新增一笔数目可观的收益。这时，客服向他推送了“租用5000元矿机送200元话费”的“优惠活动”，尝到甜头的张先生决定放手一搏，租用了一批5000元的矿机，既能充话费，又能尽早赚够可以提现的收益。可张先生等了一整天，却始终不见赠送的话费到账，联系客服也迟迟没得到回复。张先生心生怀疑，再次用手机登录该网站平台APP，才发现APP已经无法登录，微信客服也已将他拉黑。意识到上当受骗的张先生，立即向公安机关报了案。

安全提示：

随着以比特币为代表的虚拟货币规模不断扩大，各种以“区块链”“虚拟货币”为噱头、打着“金融创新”技术旗号的骗局也层出不穷，如一些注册在境外的ICO项目、虚拟货币交易平台等，实际上只是“借新还旧”的庞氏骗局，其资金运转难以长期维系。对于此类非法集资诈骗，广大消费者要擦亮双眼，保持理性，强化风险防范意识，自觉抵制与代币发行及“虚拟货币”相关的非法金融活动，切勿盲目轻信天花乱坠的承诺，避免自身财产受到损失。

不幸被骗怎么办

- 及时致电发卡银行客服热线或直接前往银行网点向柜台报告欺诈交易，监控银行卡交易或冻结、止付银行卡账户。
- 对已发生损失或情况严重的，应及时向当地公安机关报案，配合公安机关或发卡银行做好调查取证工作。
- 仔细回想此次受骗过程中是否泄露了个人信息或密码、泄露了哪些信息，尽快阻断信息泄露渠道，并更换可能受到牵连的账户密码，避免损失扩大。

网络安全为人民　网络安全靠人民

守牢金融数据安全底线

促进金融数据综合应用

10月11日至15日下载云闪付APP
扫码参与金融网络安全有奖答题