个人信息安全防护

四川省交通运输厅信息中心 印制

2022 年 9 月

前言

随着信息技术应用范围的不断扩大和深入，个人信息安全也面临更加严峻的形势，信用卡明明在自己手里，钱却被人取走;手机号码只告诉了认识的人，却总是接到各种骚扰电话;随意晒一晒照片，马上便有人猜出拍照地点；还有近几年频频成为新闻焦点的网络金融诈骗事件等;隐私泄露层出不穷，财产受损现象频繁发生，‘我的信息安全吗？’已成为每个人关注的问题。

本宣传册针对《个人信息保护法》、《关键信息基础设施安全保护条例》、《数据安全法》、2021等保测评新规等政策文件进行解读，结合《中华人民共和国网络安全法》，围绕个人生活中经常使用的智能工具，用浅显易懂的语言重点讲述了电脑、手机、QQ、微信、电子邮件等的安全使用和防护方法，期望让每一位读者都能轻松地获知个人信息安全防护的基本知识。

政策解读

《个人信息保护法》

《中华人民共和国个人信息保护法》（下称《个人信息保护法》）历经三次审议及两次公开征求意见后，2021年8月20日由第十三届全国人民代表大会常务委员会第三十次会议通过，于2021年11月1日起施行。《个人信息保护法》内容共八章，吸取了来自世界各国和各地区个人信息保护的先进经验，以《中华人民共和国宪法》为依据，结合我国国情，保护自然人、互联网企业、国家安全和公共利益，形成一套全新的保护法。同时《个人信息保护法》作为个人信息保护领域的基础性法律，其出台解决了个人信息层面法律法规散乱不成体系的问题，与《数据安全法》、《网络安全法》、《密码法》共同构建了我国的数据治理立法框架。《个人信息保护法》厘清了个人信息、敏感个人信息、个人信息处理者、自动化决策、去标识化、匿名化的基本概念，从适用范围、个人信息处理的基本原则、个人信息及敏感个人信息处理规则、个人信息跨境传输规则、个人信息保护领域各参与主体的职责与权力以及法律责任等方面对个人信息保护进行了全面规定，建立起个人信息保护领域的基本制度体系。《个人信息保护法》堪称中国首部个人信息保护单独立法，翻开了我国个人信息保

《关键信息基础设施安全保护条例》

2021年，国务院正式颁布《关键信息基础设施安全保护条例》，不仅提升了我国关键信息基础设施安全保护依据的效力层级，更对一系列重要制度、机制加以完善和固化，必将推动开启我国关键信息基础设施安全保护的新格局。

整体来看，《条例》内容集中体现了“两个统筹”的特点。一是注重立法内容的统筹。与此前的征求意见版本相比，《条例》大幅减少了有关授权立制（规定、标准）的内容，对相关保护工作要求尽可能在条文中明确、不再过多以开放的方式留待未来制度或标准解决，从而能够大大减少因立制周期长带来的效率延误。二是注重权责划分的统筹。《条例》立足关键信息基础设施保护工作不同主体的核心职能优势，进一步明确了各主体担负的权责、明确了各主体间的工作协同机制，这无疑有利于减少因工作边界不清等带来的效率延误，也可充分调动各方面在保护工作中的主体意识和主动性。关键信息基础设施安全是网络安全的重要一环，《条例》通过“两个统筹”举措的提升，为我国关键信息基础设施的网络安全保护工作奠定良好的效率基础。

从内容来看，关键信息基础设施的范围界定、管理体系、检查检测机制和责任机制是《条例》所要重点明确的加强关键信息基础设施安全保护的四个基本问题。关键信息基础设施的范围如何界定，是开展保护要明确的首要和基础性问题，也是《网络安全法》颁布实施以来各界最为关切的问题之一。

《条例》的颁布实施，无疑是我国关键信息基础设施安全保护工作的一个重要里程碑。而《条例》自身内容的完善也将是一个循序渐进的过程。例如，省级相关部门在具体实施工作中与行业保护工作部门如何衔接？关键信息基础设施的日常检测与其系统上线前测试如何衔接？监督检查和保护检查检测工作的频次、实施流程如何规范？.....这些问题，都既需要保护工作实践的验证推进，也需要相关制度规范的延续拓展。“雄关漫道真如铁，而今迈步从头越”。《条例》已经开启了我国关键信息基础设施安全保护工作的新阶段序章，如何开创和巩固关键信息基础设施安全保护工作的新格局，更呼唤主管部门、行业企业和社会各界的同心戮力。

全国“两会”和《纲要》

数字经济作为引领未来的新经济形态已成为我国高质量发展的新引擎，习近平总书记更是指出“数字经济是全球未来的发展方向”。加快数字化发展，是2021年政府工作报告中“十四五”时期的主要目标任务之一。《十四五规划和2035远景目标纲要》第5篇重点阐述了“加快数字化发展，建设数字中国”，第15-18章四个章节的内容，分别从数字经济、数字社会、数字政府到数字生态给出了介绍，充分说明和肯定了数字化对于经济、社会、政府和生态在升级和转型过程中的基础性和决定性作用。当然，在考虑数字化助力发展的巨大作用的同时，也不能忽略不同步构筑安全防护能力的巨大风险。数字化是助推数字经济大发展的“动力系统”，网络安全相当于“制动系统”，二者需要相互配合，协调均衡发展，动力系统越是强劲，制动系统越需要保持高效能。全国“两会”有近10份提案涉及到网络安全，《纲要》中“网络安全”一词更是出现了14次之多，这些都充分说明了网络安全是国家、社会发展面临的重要议题。数字经济时代，网络安全作为产业数字化的安全基石和基座，成为数字中国在各种风吹雨打中保持足够稳定的压舱石，同时，自身也成为关键业务，基于业务场景化的网络安全能力成为基本供给。

数据安全法

《数据安全法》

2021年6月10日，第十三届全国人民代表大会常务委员会第二十九次会议通过《数据安全法》三审稿，该法于2021年9月1日起正式施行。《数据安全法》全文共七章五十五条，分别从数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放的角度对数据安全保护的义务和相应法律责任进行规定。作为数据安全领域的基础性法律和国家安全法律制度体系的重要组成，《数据安全法》的出台有着深刻的时代背景和现实意义，是对当前数据安全内外部形势的回应，是护航数字经济发展的重要举措，开创新时代中国数据安全治理新局面。《数据安全法》全面贯彻落实总体国家安全观，确立国家数据安全工作体制机制，构建数据安全协同治理体系，明确预防、控制和消除数据安全风险的一系列制度、措施，提升国家整体数据安全保障能力。

《数据安全法》的颁布实施，应主动应对挑战，依法履行职责，服务发展大局，夯实社会数字化转型升级这一重大变革时代的工作内容。

首先，完善数据合规标尺。公安机关应充分落实《数据安全法》、《网络安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规要求，整合数据安全制度体系，包括不限于制定数据安全行政执法裁量基准，细化网络安全等级保护数据安全要求，强化关键信息基础设施及其承载的重要数据和个人信息的安全保护，形成从一般数据到重要数据、静态数据到动态数据、个人信息数据到非个人信息数据、结构化到非结构化数据、数据资产到数据资源的自洽体系，为开展数据处理活动的组织、个人提供规

其次，凝聚数据监管合力。公安机关应切实履行监督管理职责，依法定期组织重点行业、领域主管监管部门开展专项监督检查，推动重点单位、各类组织落实在数据采集、存储、传输、处理、使用、加工、交换、提供、共享、跨境、公开等环节的安全保护措施，提升相关单位和行业的个人信息和数据安全保护能力，促进数据安全有序流动。

最后，加大执法打击力度。公安机关应做好行刑衔接，针对侵害公民个人信息与数据安全各类违法犯罪，加强线索分析，追查数据源头，打掉危害数据安全的黑色产业链条，坚决维护国家安全、公共利益和公民、组织合法权益

2021等保测评新规

2021等保测评新规

2021年6月17日，GA部信息安全等级保护评估中心针对等保测评报告模板（2021版）主要修订的内容组织等保测评机构开展线上培训，要求等保测评机构自6月18日起针对建设过程中的测评项目执行新的标准。

在等保测评报告模板（2021版）中主要进行了三类修订：技术类（重大修订）、格式类（较大修订）和说明类（一般修订）。其中格式类修订主要是进一步规范了报告内容，例如提供表格编写示例等；说明类修订则是细化了报告相关内容的编写要求；而技术类修订属于重大修订，对其中大量内容进行了调整，与发布版相比差异较大。

在GA部此次举办的培训中列举了17个测评场景以及9个实例，相对于2019版公式，根据2021版公式所计算出的综合得分全部有不同程度的降低。甚至存在通过2019版公式计算得分在80分以上的，根据新版公式却无法通过等保测评的情况！自2019年12月1日等保2.0系列标准正式实施以来，新建网络和信息系统需要按照等保2.0系列标准要求开展建设工作，原有网络和信息系统运营者则重点关注等保1.0和2.0之间的区别开展整改工作。由于此次等保测评报告模板的修订，自6月18日之后国内所有测评机构都将按照新标准开展测评工作，这将直接影响到所有新建网络和信息系统的运营者如何开展等保建设工作。此外，在《网络安全等级保护条例》（征求意见稿）中明确指出“第三级以上网络的运营者应当每年开展一次网络安全等级测评”，面临网络和信息系统复测的运营者也需要考虑如果通过按照新版公式进行计算的测评。

从网络和信息系统运营者的角度来看此次等保测评模板的修订，主要的关注点在于关键测评指标、重要测评指标以及如何对数据资源进行测评。三级通用标准共有211个指标，其中关键指标137个，占比65%；重要指标71个，占比34%；一般指标3个，占比1%。整体上来看，如果超过三分之一的关键指标不符合，测评就可能得“0”分。从137个确定的关键指标结合客户开展等保建设工作中的实际情况，此次修订是突出强调在等保建设过程中加强以下方面：态势感知、高级威胁检测、数据库安全（数据库审计、数据库加密、数据库脱敏、数据库防火墙等）等。

家庭篇

- 路由器的正确使用
- 智能摄像头的安全使用

路由器的正确使用

移动互联网时代，路由器几乎成为家庭网络的标准配置。市民何先生从不“蹭网”，家里的上网密码也只有家人才知道。然而何先生家的网络突然无法使用，显示密码不正确。经调查，何先生家的路由器遭到不法分子的攻击，何先生的个人信息被盗取，路由器的登录密码也被修改。

安全解读

由于路由器的产品特性，用户往往会忽视对路由器使用安全的管理防范，比如设定简单的密码，长时间使用同一密码等。不法分子利用这些“漏洞”入侵家用网络，可实时掌握用户利用该网络进行的任意互联网操作，甚至入侵接入设备，提取设备中的敏感信息，修改路由器登陆密码等，给用户造成密码输入错误或者路由器坏的假象。

同时，由于家庭网络一直将房主的设备列为可信任设施，一旦侵入这个网络，就可以对智能门铃、智能摄像头等智能设备进行恶意攻击。

安全小贴士

- 一定要修改路由器管理初始账户，并增加密码强度；
- 限定路由器管理IP，开启相关登录限制措施，如路由器自带的“MAC过滤功能”；
- 随时关注并清理路由器上未知接入设备。
- 不要使用破解路由器密码的应用软件，防止在破解他人密码的同时，也泄露了自己的个人信息。

智能摄像头的安全使用

越来越多的市民为了“看家”方便，在家中装设智能摄像头，有的是看护年岁较大的父母，有的是看护年幼的孩子，有的是为了监测家里宠物的情况，还有的为了防盗。用户在获得方便的同时，隐私也可能在不知不觉中遭到泄露。

市民尹先生称，自己和妻子平时上班都比较忙，家里的老人年岁已高，为了方便照看，就在家中安装了智能摄像头，没曾想，自己和家人的隐私居然被曝光在某网站。

经调查，尹先生的生活录像被曝光的网站为不法网站，该网站可自由查看多家家庭实时摄像画面。

安全解读

通常情况下，通过手机远程查看到摄像头内容，必须通过注册，甚至要求“一对一”。但是，个别品牌的摄像头与手机进行连接时，并无身份验证机制，这是一个非常严重的漏洞。通过这个漏洞，只要下载一个播放器，就能“在线观看”他人隐私，导致本来属于隐私的摄像头画面变成“公开”模式，任何人都可以看到，从而给不法分子带来便利。

安全小贴士

- 通过正规途径购买监控设备；
- 修改摄像头的管理账号及密码；
- 及时关注摄像头软件的提醒，如果绑定的手机上发现了请求验证码的短信，就应该立刻修改密码；
- 关注所用品牌摄像头安全方面的消息，如果发现设备漏洞应停止使用，等待厂家更新，并保证所使用的摄像头软件是最新版本；
- 摄像头避免安装在卧室等隐私区域。

出行篇

- 伪基站的防范
- 钓鱼Wi-Fi的防范
- 二维码的正确扫描
- 定位功能的正确使用
- 移动支付的安全使用
- ETC的安全使用
- 共享充电站的正确使用

伪基站的防范

市民郑女士收到“10086”发来的一条短信，称郑女士有大量积分，可以兑换一笔金额不小的话费。郑女士随后点击了短信上的网址链接，进入了一个兑换话费的网页，并按提示输入了自己的支付宝账号密码和银行卡密码。郑女士等了几天，说好的话费却迟迟没有到账，更蹊跷的是，她发现自己在支付宝上绑定的三张银行卡内资金莫名减少，共被转走2.7万元。

事后追查，郑女士是中了“伪基站”的诈骗。

安全解读

"伪基站"即假基站，不法份子利用现代计算机与通讯技术伪装成运营商的基站，向“伪基站”周边一定范围内的手机发送信息。伪装的号码多为银行、运营商、党政部门的官方号码。伪基站设备运行时，用户手机信号被强制连接到该设备上，导致手机无法正常使用运营商提供的服务，手机用户一般会暂时脱网8～12 秒后恢复正常，部分手机则必须重启才能重新入网。

在排除周边信号不好或者存在信号死角之外，当通话中信号突然中断时，很可能是被伪基站强制“吸”走，信号被“切断”。

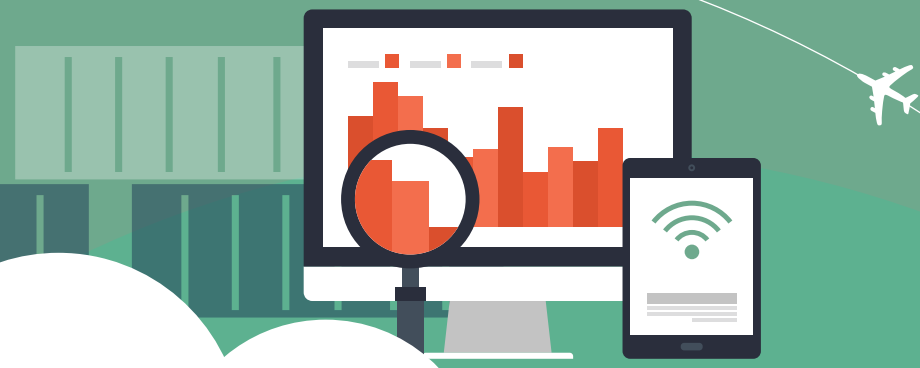
安全小贴士

- 不打开不明短信链接；
- 发现手机信号突然中断的时候，提高警惕；
- 遇到中奖、抽奖等字样时格外警惕；
- 在手机上被要求输入银行、支付宝等账号及密码时要格外小心，尽量不要在非官方APP或网页上进行操作。

钓鱼Wi-Fi的防范

公共场所免费Wi-Fi越来越多，人们进入酒店、餐馆、商场等公共场所后习惯先打开Wi-Fi功能，看一下是否有免费的Wi-Fi信号，甚至在家也有“蹭网”的习惯。

南京市民张先生使用公共场所的Wi-Fi后，电脑被黑客入侵，在U盾、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，与此同时他的手机也被黑客做了手脚，接收消费提醒短信的功能被屏蔽，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。



安全解读

钓鱼Wi-Fi的成本很低，黑客一般只需几百元便可以设置一个钓鱼Wi-Fi，并在公共场合部署，而且在名称上与免费Wi-Fi相似。例如：咖啡厅的正规Wi-Fi信号叫coffee-free，钓鱼Wi-Fi信号有可能取名叫coffee-free2等等。

受害者访问钓鱼Wi-Fi时，他的所有数据信息都可能会被钓鱼Wi-Fi记录下来，从而盗取QQ账号、微信账号、游戏密码等个人隐私信息，甚至导致严重的财产损失。

安全小贴士

- 关闭手机自动连接Wi-Fi的功能；
- 在公共场所，不要连接未知的Wi-Fi；
- 不要将自己家的Wi-Fi密码共享，定期修改密码；
- 在未知的Wi-Fi信号下不要输入QQ、微信、游戏、银行、支付宝等密码。

二维码的正确扫描

二维码已经在我们的生活中扮演着相当重要的角色，只要掏出手机扫一下别人，或者被别人扫一下，我们就可以做到吃饭不带钱，认识好友不带名片，偶尔还可以领取不要钱的小礼品。

天津市民王女士在某饭店就餐后，收到一张关于团购食品的宣传单，当即拿出手机，对宣传单的右下角的“二维码”进行了扫描。但此后王女士并没有收到任何关于团购信息的通知，话费却被吸走了119元。

安全解读

不法分子通常将一些带有木马病毒的网站制作二维码，对外宣称为优惠券、软件等，诱导用户进行扫描。受害人扫描二维码后，不法分子通过云端软件获取受害人的身份证号、银行账号、手机号码等重要信息，甚至可拦截短信验证码等关键信息，轻松转走受害人卡里的钱。

安全小贴士

- 不要贪图便宜随便扫描未知二维码；
- 扫描后若要求填写个人账户信息，应当坚决拒绝，不要犹豫；
- 手机安装正规防病毒软件，定期扫描手机安全性。

定位功能的正确使用

智能手机定位功能可以记录用户所处位置、时间段、活动轨迹等信息。

近年来，利用手机定位功能实施犯罪的案件时有发生。武汉一起绑架案中，沈某通过手机定位功能掌握了受害人孙某的日常生活规律，在孙某每天晚上锻炼的途中实施了绑架。

安全解读

手机一旦开启GPS定位功能，在使用者不做任何其它设置情况下，会自动记录用户地理位置信息。不法分子通过攻击软件后台数据库，在手机植入跟踪软件，通过社交软件发布信息等方式收集定位信息。

安全小贴士

- 关闭手机定位系统功能，必要时开启；
- 在社交软件设置中增加好友验证功能，关闭“附近的人”和“所在位置”等功能；
- 手机安装正规防病毒软件，定期扫描手机安全性。

移动支付的安全使用

随着移动支付的盛行，为广大群众带来众多便利与快捷的同时，隐患也随之潜伏，随时随地可导致个人信息及财产受到威胁。其中，手机短信验证替代银行密码，在方便市民操作的同时，也留下了安全隐患。

市民李女士在跟朋友聚会的过程中，不幸挎包被盗，手机、身份证、银行卡都在包里。还没等她挂失，就发现银行卡被人通过支付宝盗刷了3700元。

李女士很纳闷，在没有密码的情况下，钱是怎么被划走的？

安全解读

微信支付、支付宝支付、Apple Pay等移动支付以绑定银行卡的快捷支付为基础，用户购买商品时，不需开通网银，只需提供银行卡卡号、户名、手机号码等信息，银行验证手机号码正确性后，第三方支付发送手机动态口令到用户手机号上，用户输入正确的手机动态口令，完成支付。不法分子从拿到受害人的手机和钱包，到绑定成功再到转账完毕，整个过程只需耗时3分钟。

安全小贴士

- 手机、身份证和银行卡，尽量不要放在一起，避免同时丢失造成损失；
- 第三方平台的支付密码与银行卡的支付密码不要相同；
- 第一时间到公安机关和银行办理挂失，及时关闭无线支付业务；
- 手机和第三方支付平台设置不同的解锁密码，手机内不要存储身份证及银行卡信息；若丢失，及时补办手机号。

ETC的安全使用

当今社会，几乎所有的商家都把“如何更加便捷的使用我们的产品”当作基本目标，因此便捷的出行、便捷的联系、便捷的支付等成为使用的热点。其中，便捷支付更是渗透到生活中各个角落。

日前，一段便携式POS机盗刷ETC的视频引发网友热议，不少网友开始担心ETC的安全性。视频显示，有人手持一台便携式POS机在一辆装有ETC的车前挡风玻璃处一碰，显示付款100元成功。随后，签购单显示，“交易金额未超300元，免密免签”。

安全解读

专家进行了专门的测试，结果显示，如果车上插的是ETC专用卡，不用担心被POS机盗刷，因为只有高速公路的收费站才能扣款。该手段是不法分子利用了银联卡小额免密的功能，在特定场景下实施的不法行为。

其中，在使用小额免密免签服务时，持卡人只需要把具有“闪付”功能的金融IC卡，靠近POS机等受理终端的“闪付”感应区“挥卡”，就可以完成支付；另外，所有商户POS机的申领和小额免密免签业务开通都需要满足一系列条件，且双免交易一般要求机器和IC卡距离在3到4厘米以内才行，超过这个距离无法进行交易。

安全小贴士

- 尽量使用ETC专用卡；
- 对于只有ETC用的卡片，关闭除ETC以外的其他功能；
- 可关闭所使用储蓄卡/信用卡等IC芯片卡的“小额免密支付”功能；
- 建议车里的ETC银行联名卡，在停车后最好拔下来；
- 若已有异常的免签免密交易发生，持卡人可以第一时间联系发卡银行申请补偿。

共享充电站的正确使用

共享充电站的出现，为广大群众带来手机随时有电的便利，但隐患也随之而来。

广州市民陈女士在使用共享充电宝半小时后，就接到电话。电话的一方清楚地知道陈女士还有多少贷款未还，并称如果陈女士不及时还款，将会影响明年的信用额度。见对方如此清楚自己的信息，陈女士便按要求转账了五千元，随即就被对方拉黑。

安全解读

市面上部分共享充电宝，除存在安全隐患外，甚至还可能被不法分子偷偷植入木马。一旦用户使用了被植入木马的共享充电宝，不法分子就能获取用户手机中的照片、视频、通讯录、短信等隐私内容。

安全小贴士

- 不要随意领取和购买来历不明的移动电源，如有需要，请选择正规产品；
- 对于共享充电站的权限请求，一律拒绝；
- 使用共享充电站时，将设备关机；
- 如有提供插座，用随身携带的设备进行充电。

社交篇

- 电信诈骗的正确防范
- 社交网络的正确使用
- 谣言的正确识别

电信诈骗的正确防范

电信诈骗近年来发展快速，涉及面广，后果严重。市民马女士在某视频平台认识名叫“大卫”的男性网友，该网友自称是美国大兵，其丰富的经历和幽默的谈吐吸引了马女士。一年多以来，“大卫”对马女士嘘寒问暖、赠送礼物，非常关心。在赢取了马女士的情感信任后提出了要前往中国定居为由，骗取马女士资金190万元。清华大学一名教师被“冒充公检法”的人员要求其将钱打入“安全账号”，结果被诈骗卷走1760万元。

安全解读

电信诈骗是近年来比较普遍的一种新型网络犯罪行为。不法分子通常使用任意显号软件、网络电话等技术，利用电话、短信、QQ、微信、微博公众号等社交工具，冒充公检法机关，医保、社保等政府部门和运营商、房东、客服等，以牵涉司法事宜、网购退款、恋爱交友等进行诱拐或恐吓威胁，骗取受害人汇转资金。

安全小贴士

- 凡是谈到银行账户信息、“安全账户”、“涉案”、“中奖”等，一律挂掉；
- 凡是谈到“电话转接公检法”，一律挂掉；
- 凡是短信、微信让点击莫名链接，一律不点；
- 凡是称领导、同事、家属出事要求汇款的，务必先核实身份；
- 如不幸受骗：

  ①保存好汇款或转账时的凭证并立即拨打110报警，或到当地公安刑警队、派出所报案；

  ②向警方说清被骗经过，准确提供受害人姓名、受害人转出现金的账户及开户行信息；

  ③向警方准确提供骗子的账号、账号用户名及账户开户行（银行柜台及银行客户均可以帮助查询）；

  ④向警方提供汇款凭证或电子凭证截图。

社交网络的正确使用

社交网络工具的广泛使用，使人们个人情感、生活和学识得到了更加充分的展示。然而，这些社交网络也潜伏着隐形的安全隐患。

杭州市民尤女士晚饭后带着6岁的外孙女茵茵到附近的广场跳舞，茵茵在广场上独自玩耍。一名约40岁的陌生女子问她是不是叫茵茵，随后还说出了许多与茵茵匹配的信息，并诱骗其一起去找妈妈。正在小姑娘犹豫的时候，尤女士的舞伴发现了端倪上前问询，陌生女子快速离开。

经查证，陌生女子是通过尤女士女儿的社交网络了解到茵茵的长相、名字、日常活动场所等信息，于是发生了广场诱拐茵茵的一幕。

安全解读

许多家长在社交网络“晒幸福”不经意间泄露了孩子的学校、相貌、家人等信息，这些都容易被不法分子利用，通过绑架、恐吓等方式向家长索要钱财，危害孩子的生命安全。信息发布时如果还带有炫富色彩，那就更可能被不怀好意的人“盯上”。

安全小贴士

- 不要暴露平常外出的日程、行踪，不要晒贵重物品等；
- 不要随意发布火车票、飞机票、护照、车牌、孩子照片及姓名等信息；
- 在手机中关闭位置设置功能；
- 在社交软件设置中增加好友验证功能，关闭“附近的人”和“所在位置”等功能。

谣言的正确识别

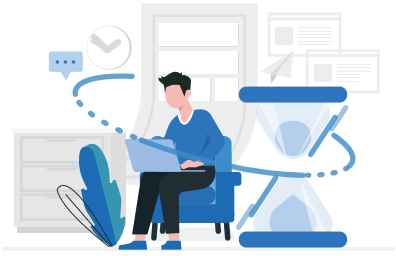
移动互联网时代，传播媒介的触手可及让信息发布的成本越来越低，谣言的数量也随之增加。新冠疫情期间，不少封校、封城的谣言四起，造成社会恐慌，物资抢购，严重影响人们的正常生活。还有部分谣言称用56°C的热水洗澡、多喝60°C的热水可以预防新冠病毒，这些错误行为都可能对人体造成伤害。

安全解读

谣言的兴起一方面源于网民的无意传谣，另一方面源于有意者的故意造谣。造谣者通常出于报复、个人利益、吸引眼球等目的，故意制造谣言，扰乱社会治安，影响人们的正常生活。

安全小贴士

- 积极学习科学常识，面对谣言保持独立思考；
- 鉴别信息来源是否可靠，多方验证；
- 对于危言耸听、带有极强煽动性的标题、导语，保持警惕性。



工作篇

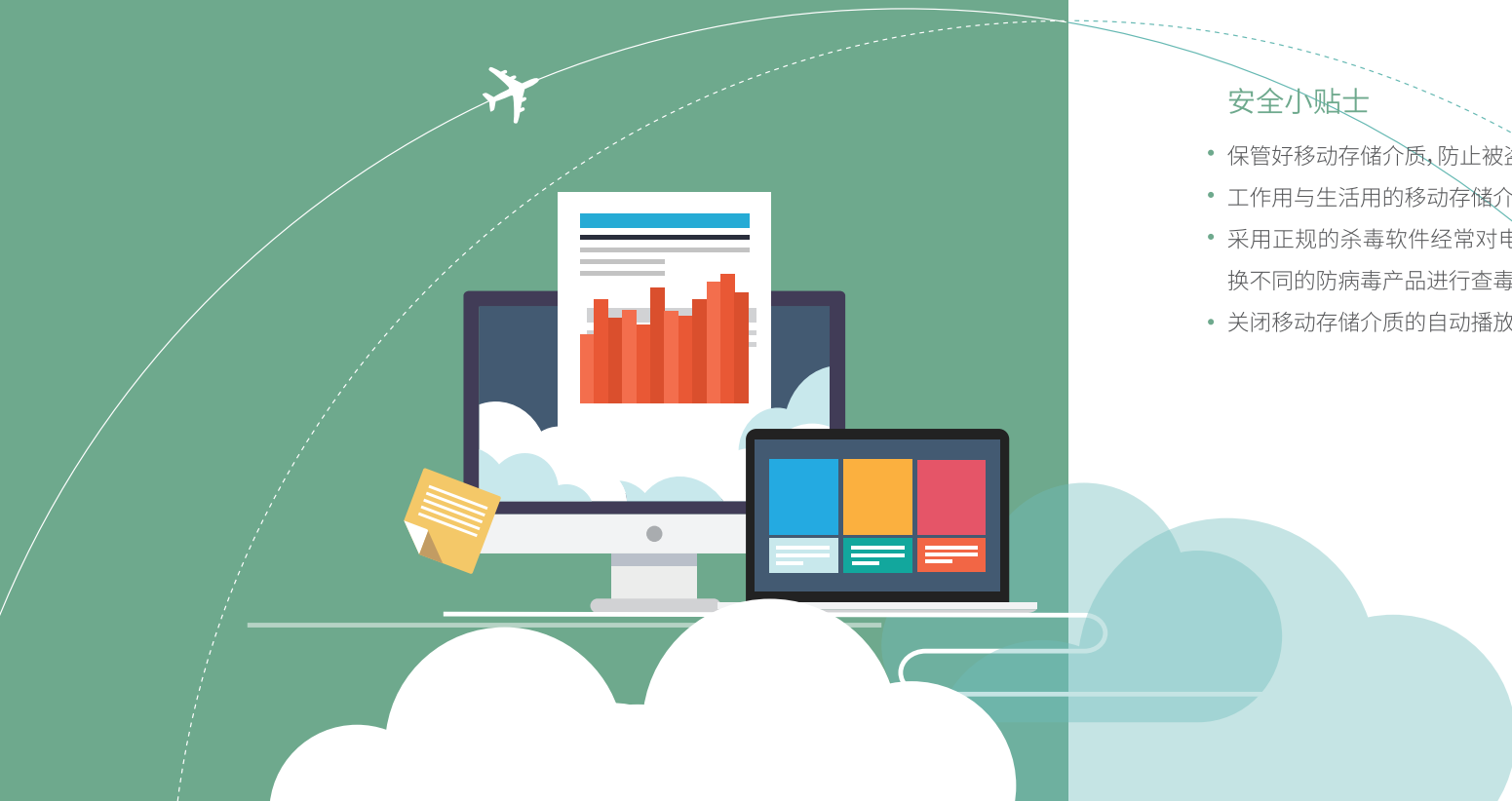
- 移动存储介质的正确使用
- 正确使用网盘
- 勒索病毒的正确防范
- 密码的正确使用

移动存储介质的正确使用

U盘、移动硬盘、内存卡等移动存储介质，在为我们工作带来便利的同时，也带来了不容忽视的信息安全隐患。

市民王先生，在家办公将相关工作资料拷贝到U盘中，带到公司继续工作。在U盘插入电脑一分钟后，电脑突然死机，再次开机后显示该电脑已中病毒。

事后调查发现，王先生的U盘在家使用时已被植入恶意病毒。



安全解读

借助U盘传播病毒早已成为病毒传播的主要方式。U盘病毒通常是利用Windows系统的自动播放功能进行传播，当用户打开U盘浏览内容的同时，病毒便会自动运行。

安全小贴士

- 保管好移动存储介质，防止被盗、丢失造成泄密；
- 工作用与生活用的移动存储介质区分，减少在多台电脑上的交叉使用；
- 采用正规的杀毒软件经常对电脑、移动存储介质进行病毒查杀；不定期更换不同的防病毒产品进行查毒；
- 关闭移动存储介质的自动播放功能，先查杀病毒再使用。

正确使用网盘

随着信息化的快速发展，云存储服务出现了，在线存储的容量更大功能更丰富更具吸引力。于是，网盘（云盘）成为办公、生活、娱乐的重要存储方式。网盘又称网络U盘、网络硬盘，可提供文件的存储、访问、备份、共享等文件管理功能。不管是在家中、单位或者其他任何地方，只要连接到因特网，就可以管理、编辑网盘里的文件。不需要随身携带，更不怕遗失。因此，使用人群也越来越广泛。

近日，某知名在线数据管理网站被发现其文件共享机制存在安全风险，导致许多企业的部分机密数据和文件可以被谷歌、必应等搜索引擎直接检索。

安全解读

专家测试后表示，许多网盘在进行数据上传和下载的过程中，客户端和服务器传输的数据是没有经过加密的明文，攻击者（黑客）可以直接截取数据包。同时，黑客还能够利用窃取到的用户历史访问数据，适当修改文件名和路径，对用户的所有数据进行读取和删除操作。给网盘使用者带来重大损失。

安全小贴士

- 尽量不要用网盘存储私密信息，以防止信息泄露；
- 网盘里的储存内容一定要在本地备份，避免被不法人士删除、修改；
- 使用网盘传输文件后，应做出删除之类的处理。

勒索病毒的正确防范

勒索病毒是近年来流行的一种新型电脑病毒，发展迅速，危害面广，一旦感染将加密电脑中绝大部分文件，并索要赎金。华东多地医院曾出现集中感染勒索病毒事件，一时间，医院电脑接连被感染，不少联网设备宕机，挂号、缴费、取号等常规业务均受到影响。某高校学生电脑在连接学校网络时，被通过校园网主机系统漏洞进入的勒索病毒感染。在支付近1万元赎金后，病毒团伙并没有提供任何解密方式。

安全解读

勒索病毒主要通过系统漏洞、邮件、程序木马、网页挂马等形式进行传播。不法分子通过发送恶意钓鱼邮件，或发布破解版程序，恐吓威胁或诱骗用户进行点击、安装，一旦点击，病毒程序就会自动运行，加密用户电脑文件。

安全小贴士

- 通过正规软件商店或网站下载应用程序；
- 谨慎点击来历不明邮件中的链接、附件；
- 使用可靠移动储存介质；
- 及时更新电脑补丁，打开电脑防火墙，安装防护软件；
- 定期备份计算机中的重要数据。

密码的正确使用

近年来，随着各类平台、APP的数量越来越多，为了方便记忆，人们总是习惯于设置相同又简单的账号密码。市民李女士在丢失信用卡后，接连收到短信提示，显示信用卡分别被刷走15000元和2000元。事后调查发现，李女士信用卡密码为6个“1”，属于典型的简易密码。于是在被人捡到信用卡后，轻易地猜中密码并盗刷。

安全解读

简易密码通常被认为是容易被他人猜测到或能够被破解工具破解的密码，具体表现为简单数字组合、顺序字符组合以及初始密码等。这些密码容易被不法分子所破解，导致个人信息泄露，甚至钱财损失。

除此之外，如果在多个网站使用同一个账号与密码，一旦某个网站遭到入侵导致账号和密码被泄露。不法分子将会利用已泄露的信息在其他网站上尝试登录，尤其是有价值的金融行业，给个人造成经济损失。

安全小贴士

- 在设置密码时最好使用字母（大小写）+数字+符号的组合形式，避免使用生日、姓名缩写等容易联想密码；
- 不同的账户设置不同的密码，定期修改密码；
- 使用公共电子设备登录账户时，不要点击保存密码选项；
- 设置账户时采用多方验证方式，如手机验证码、密保问题等。