教职工政治学习参考资料

（2022 年第 4 期）

苏州大学党委宣传部编

2022 年 4 月 26 日

教职工政治学习参考资料

（2022 年第 4 期）

苏州大学党委宣传部编　　2022 年 4 月 26 日

● 学习内容

主题一：网络安全专题学习

主题二：《苏州大学立德树人之本科生成长陪伴计划指导方案》专题学习

● 参考资料

《个人信息保护法》解读

苏州大学

前言

随着信息化与经济社会持续深度融合，网络已成为生产生活的新空间、经济发展的新引擎、交流合作的新纽带。截至2021年8月，我国互联网用户已超过10亿，互联网网站超过400万个、应用程序数量超过300万个，个人信息的收集、使用更为广泛 。在信息化时代，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一。

党中央高度重视网络空间法治建设，对个人信息保护立法工作作出部署。习近平总书记多次强调，要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，对加强个人信息保护工作提出明确要求。2021年8月20日，《中华人民共和国个人信息保护法》正式颁布，于2021年11月1日正式施行。

苏州大学

案例1-APP收集个人信息

黄女士是个文学爱好者，工作之余，她最喜欢通过读书来放松身心。随着互联网技术的发展，手机APP电子阅读越来越普遍，除购买纸质书外，黄女士也开始使用一款名为阅读APP的软件，通过手机随时随地进行阅读。这样的阅读方式让黄女士觉得既方便又省心，但是有一天，黄女士使用阅读APP时发现，在其不知情的情况下，该软件自动关注手机联系人，默认开放读书记录，自己什么时候读了什么书，不仅是自己的联系人，该APP的任何用户都可以任意查看。黄女士感到非常生气，认为该阅读APP侵害了自己的个人信息权益及隐私权。

案例2-违规公布个人信息

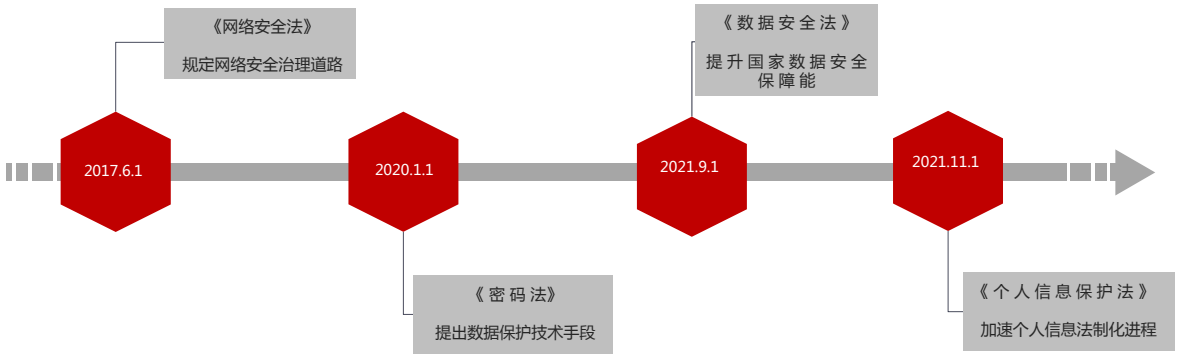
2020年7月，“A市B区物流园一冷冻仓库部分厄瓜多尔进口冻南美白虾外包装新冠病毒核酸呈阳性” 的新闻报道一出，相关部门迅速组织涉事产品及购买人员进行核酸检测。就在这时，某营销策划公司将一份名为《A市已购进口白虾顾客名单》的文章发布在其管理的公众号上，供网友下载。该名单包括A市各区县一万多名购买进口白虾人员的姓名、家庭住址、身份证号码、手机号码等详细个人信息。6月时，小李曾购买该白虾，因此名单上也有他的名字，还有他的家庭住址、手机号码等个人信息。这份名单在社区业主群中流传开后，很多业主对此表示担忧，质疑小李是否感染了新冠病毒，一些情绪激动的业主甚至要求物业封锁小李的住所。除此之外，小李还接到了不少骚扰电话，其和家人的工作生活都受到了极大的影响。

案例3-大数据杀熟

胡女士一直都通过某旅游app预定机票、酒店，因此她是该APP享受8.5折优惠价的钻石贵宾客户。2020年7月，胡女士像往常一样，通过该APP订购了某酒店的一间豪华湖景大床房，支付价款3000元。然而，行程结束退房离开酒店时，胡女士偶然发现，酒店的实际挂牌价仅为1400元。胡女士不仅没有享受到钻石贵宾客户应当享受的优惠，反而多支付了一倍的房价。胡女士与APP客服人员沟通，对方以其系平台方，并非涉案订单的合同相对方等为由，仅退还了部分差价。

苏州大学

个人信息保护领域里程碑



苏州大学

《个人信息保护法》总览

进程

《个人信息保护法》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，共八章74条，2021年11月1日正式实施。

目的

为了保护个人信息权益，规定个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

范围

1、以向境内自然人提供产品或者服务为目的，适用本法。
2、分析、评估境内自然人的行为，适用本法。
3、法律、行政法规规定的其他情形。

法律意义上的个人信息

第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

个人信息的处理

第六条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。

收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

个人信息的处理

第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

国家建立健全个人信息保护制度

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

公共场所收集个人信息处置

第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

敏感个人信息

第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

未成年人个人信息处理

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

境内个人信息处理

第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

个人信息防范

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

信息泄露处置

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：
（一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；
（二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；
（三）个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

个人信息权益被侵犯处置

第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责：
（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；
（二）接受、处理与个人信息保护有关的投诉、举报；
（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；
（四）调查、处理违法个人信息处理活动；
（五）法律、行政法规规定的其他职责。

案例1-APP收集个人信息

黄女士是个文学爱好者，工作之余，她最喜欢通过读书来放松身心。随着互联网技术的发展，手机APP电子阅读越来越普遍，除购买纸质书外，黄女士也开始使用一款名为阅读APP的软件，通过手机随时随地进行阅读。这样的阅读方式让黄女士觉得既方便又省心，但是有一天，黄女士使用阅读APP时发现，在其不知情的情况下，该软件自动关注手机联系人，默认开放读书记录，自己什么时候读了什么书，不仅是自己的联系人，该APP的任何用户都可以任意查看。黄女士感到非常生气，认为该阅读APP侵害了自己的个人信息权益及隐私权，欲将该APP的运营公司诉至法院，要求其立即停止侵权行为，删除相应信息并赔礼道歉。

法律解析：
互联网的应用尤其是特色化服务离不开用户的个人信息，包括定位信息、偏好信息等。但是《个人信息保护法》第五条规定“处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。”第四十四条规定：“个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理;法律、行政法规另有规定的除外。”可见，个人在个人信息处理活动中享有知情权和决定权，有权了解个人信息处理者收集使用了自己的哪些个人信息，并对是否授权作出自主判断和决定。互联网企业在使用用户信息的时候必须符合合法性、正当性和必要性的原则，同时也要征求用户的同意，如果互联网企业在开发新功能的过程中忽视了对用户个人信息权益的保护，一味过度地收集用户个人信息，未经用户允许就将其个人信息公开，乃至为了商业利益滥用用户个人信息，那么互联网领域将成为损害公民个人信息安全的重灾区。阅读APP强制黄女士授权其收集黄女士手机联系人信息，为其自动添加关注手机联系人，并且默认向未关注用户公开其读书信息的行为，严重侵犯了黄女士的个人信息权益。互联网企业应当遵循合法、正当必要和诚信原则，重视对用户个人信息的保护，对相关功能进行迭代优化，更加尊重用户的选择权，并对相关社交功能进行强提示，在满足用户知情权和决定权的基础上再做下一步的技术创新。

案例2-违规公布个人信息

2020年7月，“A市B区物流园一冷冻仓库部分厄瓜多尔进口冻南美白虾外包装新冠病毒核酸呈阳性”的新闻报道一出，相关部门迅速组织涉事产品及购买人员进行核酸检测。就在这时，某营销策划公司将一份名为《A市已购进口白虾顾客名单》的文章发布在其管理的公众号上，供网友下载。该名单包括A市各区县一万多名购买进口白虾人员的姓名、家庭住址、身份证号码、手机号码等详细个人信息。6月时，小李曾购买该白虾，因此名单上也有他的名字，还有他的家庭住址、手机号码等个人信息。这份名单在社区业主群中流传开后，很多业主对此表示担忧，质疑小李是否感染了新冠病毒，一些情绪激动的业主甚至要求物业封锁小李的住所。除此之外，小李还接到了不少骚扰电话，其和家人的工作生活都受到了极大的影响。

法律解析：
为实现新冠肺炎疫情期间利用大数据实施联防联控和保护公民个人信息安全之间的平衡，中央网络安全和信息化委员会办公室专门发布了《关于做好个人信息保护利用大数据支撑联防联控工作的通知》。该通知指出，为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。若个别媒体和个人打着“为了社会公众利益、为了国家和公民人身安全着想”的旗号擅自将通过非法途径获得的为疫情防控、疾病防治需要收集的个人信息公之于众，严重侵犯公民的个人信息合法权益，甚至引发社会恐慌，扰乱社会秩序，干扰国家统一防疫调控工作，那么必将面临法律的制裁。大家在看到涉及公民个人信息的名单时，也不应进行转发、传播，而应及时提醒亲戚朋友删除，避免二次传播给他人造成更大的伤害。

案例3-大数据杀熟

胡女士一直都通过某旅游app预定机票、酒店，因此她是该APP享受8.5折优惠价的钻石贵宾客户。2020年7月，胡女士像往常一样，通过该APP订购了某酒店的一间豪华湖景大床房，支付价款3000元。然而，行程结束退房离开酒店时，胡女士偶然发现，酒店的实际挂牌价仅为1400 元。胡女士不仅没有享受到钻石贵宾客户应当享受的优惠，反而多支付了一倍的房价。胡女士与APP客服人员沟通，对方以其系平台方，并非涉案订单的合同相对方等为由，仅退还了部分差价。

法律解析：
APP“大数据杀熟”等问题是当今社会值得关心、关注的问题。商家利用收集到的客户个人信息，通过计算机技术进行自动化决策，对客户进行 “大数据杀熟”的行为，有违诚信原则，严重损害消费者合法权益。对此，《个人信息保护法》第二十四条第一款规定“个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇”，明确禁止商家“大数据杀熟”。

个人信息安全的意义

从《网络安全法》的施行，到《民法典》的编纂出台，再到《数据安全法》的出台，在数字经济发展和法治建设进程中，我国个人信息保护法律制度逐步建立并不断发展完善。制定个人信息保护法，是进一步加强个人信息保护法制保障的容观要求，是维护网络空间良好生态的现实需要，是促进数字经济健康发展的重要举措。

《个人信息保护法》是及时回应广大人民群众的呼声和期待，落实党中央部署要求而制定的个人信息保护方面的专门法律，其制定和实施，对于织密个人信息保护的法治之网，将人民群众个人信息权益实现好、维护好、发展好，具有重要意义。

苏州大学网络安全培训——挖矿

数据资源与信息化建设管理处

目录

01

比特币

什么是比特币；比特币的优势；
比特币的产生；比特币的价值

比特币——什么是比特币&比特币的优势

什么是比特币

- 比特币是一种基于区块链技术的数字货币。
- 是世界上第一个去中心化的数字货币。
- 比特币网络中的每一笔交易都会被记录在公开的账本中。
- 每个人都可以持有账本，所以每个人都是比特币银行的一部分。

比特币的优势

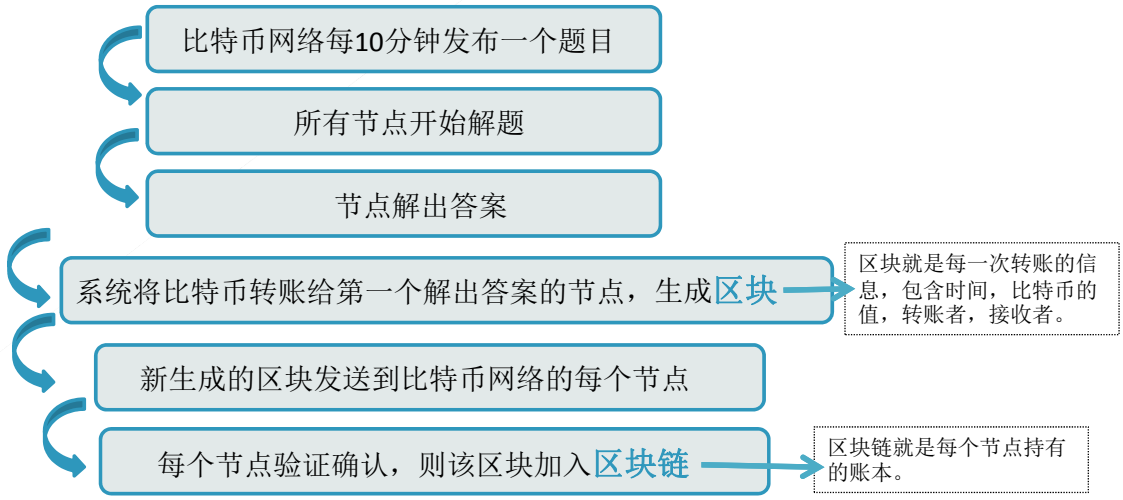
- 比特币通过互联网点对点交易，不通过银行或任何中介。这意味着拥有者可以省下非常多的手续费。
- 使用比特币时没有任何的条件或是限制。拥有者可以在任何国家使用。拥有者的账户也无法被冻结

比特币——比特币的产生

概述

比特币在2008年被发布的时候，创始人中本聪就设定了比特币的总量是2100万个，矿工们通过解决数学难题来获取比特币。系统每10分钟出一个题，因此比特币产出速度是固定的。接入网络的节点增加，算力增加，相应的挖矿难度也会增加，这样就可以维持比特币的产出速度。解决难题获取的奖励也是先定好的，最初是每个难题50个比特币，大约每四年减半，现在每解决一个难题有6.25个比特币。这种机制提供了一种发行货币的创新方式，之后也激发了人们参与挖矿的动机。比特币网络由矿工来保证安全。比特币交易需要矿工们验证，因此参与的矿工越多，网络越安全。

比特币——比特币的产生



比特币——比特币的产生

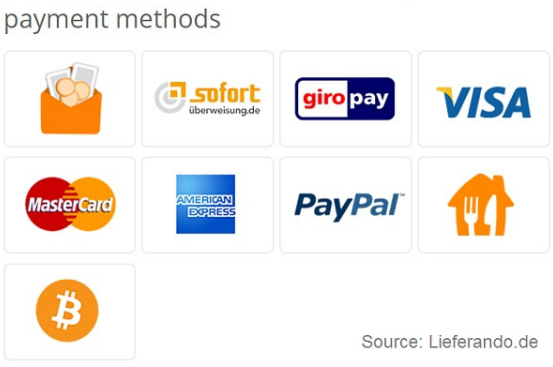
比特币网络难题

f（x）=y，f（x）是一个非常难的函数。
已知x，求y，非常简单。让计算机去运算可能只需要几毫秒。
但已知y，求x，则很难，计算机要一次一次试x的值。函数越复杂，尝试的次数就越多。
获得比特币的过程就是一个已知y，要去找x的过程。
比特币网络用的是SHA256函数，是一个哈希函数，无论输入值是什么，输出都是一个64位的哈希值。

如何获取比特币

假如系统给出哈希值：
A7FCFC6B5269BDCCE571798D618EA219A68B96CB87A0E21080C2E758D23E4CE9
要想获得比特币，我们就需要去试x，一次次执行SHA256（x）函数，匹配结果是否与这个哈希值一致。这就要求设备具有很强的算力。

比特币——比特币的价值



图：德国最大食品供应网站Lieferando.de接受比特币支付

- **比特币数量固定。**这可以避免类似各国货币的增发的情况，从而杜绝了通货膨胀。
- **比特币被认可。**比特币之所以会有价值，就是因为人们承认它有价值。更多的人认可、使用、流通使得比特币拥有更高的价值。戴尔、PAYPAL、微软、STEAM等相继支持比特币支付。日本、德国等国家的政府承认比特币作为合法支付手段。

02

挖矿和挖矿木马

什么是挖矿；挖矿设备；矿池；挖矿的危害；
什么是挖矿木马；为什么会中挖矿木马

挖矿和挖矿木马——什么是挖矿

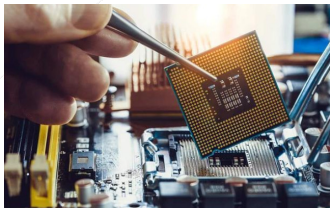
什么是挖矿

矿工们通过解决难题获取比特币的过程就称之为挖矿。挖矿是比特币系统中一个重要的组成部分，它确保系统的公平性，同时也保证比特币系统的稳定、安全、可靠。

挖矿和挖矿木马——挖矿设备

用什么挖矿

早期阶段，矿工们用**电脑处理器**去解决数学难题。不久之后，矿工们发现用**显卡**更适合用于挖矿工作。显卡速度快，但会耗费更多电力，温度也会过高。后来有人研发出了专门用于挖矿的矿机，矿机使用特定的芯片和程序，使得耗电相对减少和挖矿速度增加。



处理器

显卡

矿机

挖矿和挖矿木马——矿池

矿池

随着比特币的流行，越来越多的矿工加入这个行列，挖矿难度不断提升。为了克服这个问题，矿工们开发出了矿池，矿池能够比个人挖矿更快找到难题的解决方案。每个矿工依据他们的工作量按比例分配矿池的收获。

挖矿和挖矿木马——挖矿的危害

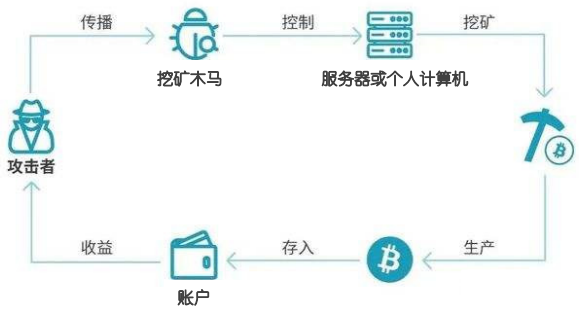
能源消耗

比特币的高耗电违背了中国的碳中和战略思想。
碳中和就是指全国生产生活在一定时间内产生的二氧化碳排放总量与通过植树造林等方式可以吸收的二氧化碳总量相当，实现零排放。
挖矿需要配置大量高性能的电脑主机，导致耗电量巨大。矿机运行产生的电费成了挖矿活动中最重要的成本。电力充足电费便宜的地区成为了矿场的聚集地，像火电丰富的新疆、内蒙古以及水电丰富的云南、四川、贵州等，仅新疆就占据全国比特币挖矿算力的35%，每年比特币耗电量高达1200亿度。中国目前是全球挖矿的主战场之一，耗电量占全球挖矿能耗总量的70%。显然，挖矿非常不利于实现我们的碳中和目标。

金融风险

比特币的总数有限，这就给投资者造成了奇货可居的错觉，但这也使得比特币的价格很容易被少数机构或个人影响和控制。不久前，以比特币为代表的虚拟货币的价格暴涨暴跌，炒作交易活动频繁，投资者购买比特币的交易风险非常大，合法权益和财产安全也受到了威胁。近年来，还有不法分子利用虚拟货币进行洗钱，将犯罪所得收益转换成境外的法定货币或财产。挖矿已经扰乱了正常的经济和金融秩序。

挖矿和挖矿木马——什么是挖矿木马



挖矿木马

由于比特币的成功，许多基于区块链技术的数字货币纷纷问世，如以太币、门罗币，达世币等。攻击者通过各种手段将挖矿程序植入受害者的计算机中，在受害者不知情的情况下利用其计算机的运算力进行挖矿获取数字货币，从而获取利益，这类非法植入用户计算机的挖矿程序就是挖矿木马。

挖矿和挖矿木马——为什么会中挖矿木马

垃圾邮件	软件捆绑	漏洞传播	网页挖矿	U盘感染
用户运行了钓鱼邮件中的附件，导致木马程序进入计算机。	用户下载并运行来历不明的破解软件，捆绑下载了木马程序。	用户没有及时修补漏洞，目前大部分挖矿木马都会通过漏洞传播。	用户访问了植入挖矿脚本的网页，浏览器会解析脚本进行挖矿。	用户在计算机上使用携带挖矿木马的U盘，导致挖矿木马进入计算机。

03

校内挖矿行为

现状；常见问题

校内挖矿行为——现状

现状

2021年至今，数据资源与信息化建设管理处发现校内挖矿活动事件共224起。经调查，无故意使用校内计算机以及校内网络进行挖矿活动人员，所有挖矿行为均由挖矿木马导致。

主要原因

- 在非官方网站下载软件，捆绑下载其他恶意程序。
- 未安装杀毒软件。

校内挖矿行为——常见问题

我的电脑不上外网，为什么会有挖矿木马？

计算机漏洞未及时修复，一些重要端口未关闭，使用携带挖矿木马的U盘等都可能导致挖矿木马进入计算机。

我的电脑配置很低/没有显卡，怎么可能会挖矿？

任何计算机都有一定的运算能力，CPU也可以用来挖矿，只是运算力比较低。挖矿木马进入计算机之后，计算机成为矿池成员，贡献运算力。

我自己下载并安装了网上的杀毒软件为什么还会有挖矿木马？

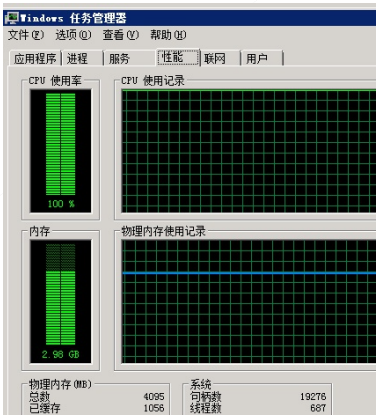
用户自行安装的免费杀毒软件病毒库更新不及时，不能像专业的杀毒软件一样第一时间获取最新病毒库，导致一些挖矿木马逃过杀毒软件查杀；用户下载杀毒软件后未定时对计算机进行查杀，导致一些挖矿木马未被检出。

04

挖矿木马预防

挖矿木马自查；预防措施；安全意识宣传

挖矿木马预防——挖矿木马自查



自查

通常对挖矿木马的感知，主要表现在主机的使用感上。如果中了挖矿木马，通常主机会突然变得卡顿，并且CPU的使用率高于正常使用时的数值或达到了100%。

判断挖矿进程的存在需要一定的经验，不一定占用CPU高、导致卡顿的进程都是挖矿进程，要注意区别是否为系统配置问题导致的卡顿。通常情况下，挖矿木马都会有系统驻留模块，会通过计划任务、服务等方式不断的拉起恶意进程，因此仅结束进程不一定能有效的清除，建议使用专业的安全软件进行处置。

挖矿木马预防——预防措施

杀毒软件

1.安装杀毒软件；
2.及时更新病毒库；
3.定时全盘查杀。

口令管理

1.主机和数据库都要避免使用弱口令；
2.避免多个设备使用相同口令。

漏洞管理

1.定期对系统进行漏洞扫描，及时修复漏洞，特别是挖矿木马常用的“永恒之蓝”漏洞；
2. Web服务器要及时更新组件，安装软件补丁；
3.对于数据库要及时更新数据库管理软件补丁。

挖矿木马预防——安全意识宣传

破解软件别滥用，邮件附件要当心。
定期杀毒别偷懒，电脑卡顿才麻烦。
简单密码一时爽，数据恢复哭断肠。
网络安全靠大家，保护信息你我他。

网络安全知识手册

苏州大学信息化建设与管理中心

前言

随着 5G 网络的全面覆盖，互联网科技飞速发展，智能手机和电脑成为人们传播信息、互相交流、学习知识、休闲娱乐的工具。然而，互联网为我们的生活、学习和工作带来便利的同时也带来了风险和危害。在互联网世界里，每个人都是“半透明”的状态，时刻都可能遭遇计算机中毒、文档意外丢失、黑客异常攻击、网络行骗诈骗、个人信息泄露等威胁。

本手册针对常见的网络安全问题，提供了一些简便实用的措施和方法，帮助大家提升网络安全防范意识、提高网络安全防护技能、遵守国家网络安全法律和法规，共同维护、营造和谐的网络环境。

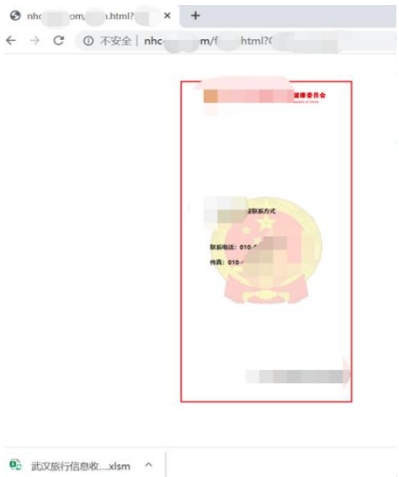
目录

一、案例

1. 疫情期间，境外多个国家和地区对中国发动网络攻击

从 2020 年 1 月下旬开始，有一个黑客团伙用防疫和中医药相关的文件作诱饵，通过他们伪造的 QQ 邮箱界面盗取用户邮箱账号和密码。文件中没有夹带木马病毒，杀毒软件也不会发现。一旦点击，用户账户信息就会完全暴露在黑客面前。黑客们攻击的目标都是政府部门职员，安全风险大大增加。

2020 年 2 月，印度 APT 组织“白象”（Patchwork、摩诃草）使用了一个伪装成我国卫生主管部门的域名，并借助新型肺炎为话题，伪造疫情相关文件，对我国医疗工作领域发动 APT 攻击。该组织于 2020 年 1 月注册仿冒域名“nhc****.com”，访问部分链接会直接下载名为“武汉旅行信息收集申请表.xlsm”、“卫生部指令.docx”的恶意文档，打开后将下载具备信息窃取、远程控制功能的木马后门。



2020 年 5 月，有国外机构披露，疑似与越南有联系的黑客组织 APT32（海莲花 OceanLotus）在过去的数月中，持续对我国重要卫生医疗机构发起网络攻击，以获取和新型冠状病毒相关的重要信息情报。该黑客组织用名为“冠状病毒实时更新：中国正在追踪来自湖北的旅行者.docx”、“湖南省家禽　H5N1 亚型高致病性禽流感疫情情况.docx”样本信息文件作诱饵，使用户执行木马程序，最终达到控制系统、窃取情报的目的。本轮攻击还使用了白利用手法绕过了部分杀毒软件的查杀。

2. 多地高校数万学生隐私遭泄漏

2020 年 4 月，河南财经政法大学、西北工业大学明德学院、重庆大学城市科技学院等高校的数千名学生发现，自己的个人所得税 App 上有陌生公司的就职记录。税务人员称，很可能是学生信息被企业冒用，以达到偷税的目的。郑州西亚斯学院多名学生反映，学校近两万学生个人信息被泄露，以表格的形式在微信、QQ 等社交平台上流传。对此，该校官方微博在回应学生时称，已向公安机关报备，正在调查之中。5 月 31 日，有人在班级微信群中发来两份“返校学生名单”，该名单涉及近两万名学生，信息具体到名字、身份证号、年龄、专业及宿舍门牌号，等等。事件发生后，多名学生反映收到骚扰电话。

3. 微博 5.38 亿账号信息在暗网出售

2020 年 3 月，5.38 亿条微博用户信息在暗网出售，其中 1.72 亿条有账户基本信息，包括：用户名、关注数、地理位置、最后一次微博发布时间等微博公开信息，售价 1388 美元。有新京报记者在 Telegram 上向灰产人士购买了价值约 12 元人民币的积分，获得了 201 条微博用户信息，其中不少信息包括用户身份证号、手机号、密码、生日等私密信息。对于灰产人士提供的微博定向查询手机号服务，记者测试查询了 3 个已绑定手机的微博账号，结果有 2 个微博账号被查询到了正确的关联手机号码，其中 1 个还给出了微博绑定的 QQ 等更详细的信息。

4. 网络交友+投资=诈骗！

近期，社交软件流行网络，不少市民纷纷下载使用，但是不法分子也盯上了此类软件，通过搭建虚假投资平台，在交友骗取信任后以“稳赚不赔”“操作简单”等为卖点博人眼球，诱导群众充值投资，实施网络诈骗。

1 月 12 日，连云港市民李先生报警称，其通过某社交软件收到好友申请，后对方以投资理财向由向其发送二维码并让其扫码下载“兴业证券”APP 进行投资，被骗 13 万余元。

2 月 11 日，苏州市民张先生报警称，其在某软件上认识对方，对方在聊天中发送网址链接并让其下载“香港交易所”的 APP，张某按照对方指示进行投资，被骗 53 万余元。

2 月 12 日，　淮安市民贾女士报警称，其在“SOUL”APP 上，好友以追求其为由让其下载“恒泰财经”APP 进行投资理财，被骗 21 万余元。

5. 扫描二维码要小心

一天，小陈在网上冲浪时看到一个“扫码免费送 XX 视频会员”的广告，当他用 QQ 扫描二维码后，跳转到一个提示“您的身份已过期，请重新登录并领取”的页面，小陈没多想就输入自己的 QQ 账号密码并登录。

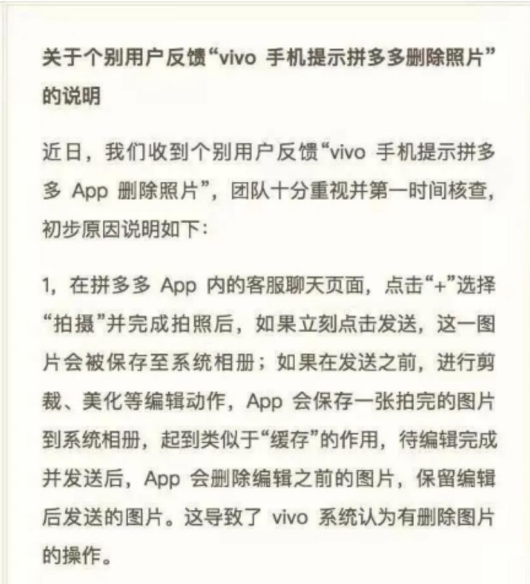
不久后，他发现自己的 QQ 显示在他人手机上登录，而 QQ 余额里的 2 万多钱也没了。原来，小陈扫码进入的是一个植入木马程序的假登录页面，不法分子在获取小陈输入的账号密码后，可随意登录甚至修改密码，还有可能将假海报自动群发给好友，导致更多好友遭遇。

6. 手机数据被远程删除

1 月 12 日，某网友在网上发布信息爆料，在与客服沟通领取“拼多多”红包后发现，其使用的 vivo 手机操作系统提示，“检测到‘拼多多’已删除照片或视频”，该网友表示，随后发现自己提供给客服的截图证据被删除，仅在已删除图片中可找到。

该名网友再次与拼多多客服沟通，质疑其侵害用户隐私。但拼多多客服不认为 App 有此行为，而是用户自己“误操作”或者“清除缓存”导致。该名网友遂又与 vivo 客服沟通，vivo 客服声称手机操作系统不会对图片和视频进行操作，如用户授予了 App 存储权限，则 App 是可以利用此权限执行相应操作的。

此事被曝光后，立即受到网民和媒体强烈关注，迅速登上了微博热搜榜。1 月 12 日晚上 19 点拼多多发布了《关于个别用户反馈“vivo 手机提示拼多多删除照片”的说明》，声明会删除客服聊天页面拍摄且编辑的照片原图。这则说明也表明了，App 在获取“存储”权限后，确实具备读增删改图片等的能力。



关于个别用户反馈“vivo 手机提示拼多多删除照片”的说明

近日，我们收到个别用户反馈“vivo 手机提示拼多多 App 删除照片”，团队十分重视并第一时间核查，初步原因说明如下：

1，在拼多多 App 内的客服聊天页面，点击“+”选择“拍摄”并完成拍照后，如果立刻点击发送，这一图片会被保存至系统相册；如果在发送之前，进行剪裁、美化等编辑动作，App 会保存一张拍完的图片到系统相册，起到类似于“缓存”的作用，待编辑完成并发送后，App 会删除编辑之前的图片，保留编辑后发送的图片。这导致了 vivo 系统认为有删除图片的操作。

7. 警惕手机病毒

2020 年 5 月以来，朝阳警方陆续接到受害用户报案称，自己的手机上不止一个 APP 账号被盗。朝阳警方迅速展开侦查，通过对受害用户的询问及相关案情的梳理、分析，民警锁定了一个可疑的抽奖链接。

被盗号用户均反映，他们在某知名网络交友 APP 上，曾点开过网友发来的“某交友软件 5 周年抽奖”的链接。随后几天他们发现，手机上多款 APP 的密码被人篡改，原密码无法登陆。

经民警核实，该款网络交友 APP 的运营商称，从未举办过 5 周年抽奖活动。民警进一步调查发现，“5 周年抽奖”链接实为不法人员设计的虚假网站链接，暗含木马病毒。网友点开该链接会导致手机中毒，不法分子即可盗取中毒手机上各类 APP 的账号信息等，并通过拦截手机短信、获取短信验证码进行密码修改，后通过出售账号、密码牟利。

二、上网安全

1. 如何防范病毒或木马的攻击

什么是木马？什么是病毒？

“木马”这个名字来源于古希腊传说特洛伊木马。在古希腊传说中，希腊联军围困特洛伊久攻不下，于是把一批勇士埋伏在一匹巨大的木马腹内，放在城外后，佯作退兵。特洛伊人以为敌兵已退，就把木马作为战利品搬入城中。到了夜间，埋伏在木马中的勇士跳出来，打开了城门，希腊将士一拥而入攻下了城池。

和故事中的“木马”一样，计算机病毒中的“木马”也是通过伪装成正常的程序吸引用户下载、执行，随后进入到电脑中的，通过特定的程序（木马程序）来控制另一台计算机。通常它有两个可执行程序：一个是控制端，另一个是被控制端。木马攻击者通过客户端与受害者的计算机服务建立远程连接，控制受害者计算机，盗取信息。

与木马程序不同，病毒具有传播性，以感染为目的，破坏计算机系统，占用硬盘空间，内存等物理设备导致计算机瘫痪。但现今单纯的病毒木马蠕虫等都很少了，绝大部分恶意软件都是混合型的。

安全建议：

1. 为电脑安装杀毒软件，定期扫描系统、查杀病毒；及时更新病毒库、更新系统补丁；

2. 下载软件时尽量到官方网站或大型软件下载网站，在安装或打开来历不明的软件或文件前先杀毒；

3. 警惕收到的陌生图片、文件和链接，不要轻易打开在 QQ、微信、短信、邮件中的链接；

4. 使用网络通信工具时不随意接收陌生人的文件，若接收可取消“隐藏已 知文件类型扩展名”功能来查看文件类型；

5. 对公共磁盘空间加强权限管理，定期查杀病毒；

6. 打开移动存储器前先用杀毒软件进行检查，可在移动存储器中建立名为 autorun. inf 的文件夹（可防 U 盘病毒启动）；

7. 需要从互联网等公共网络上下载资料转入内网计算机时，用刻录光盘的方式实现转存；

8. 对计算机系统的各个账号要设置口令，及时删除或禁用过期账号；

9. 定期备份，当遭到病毒严重破坏后能迅速修复。

2. 如何防范账号和密码安全

在信息化时代，各类交流平台以及各种工具平台都是通过账号密码进行验证和登录。账户安全的重要性不言而喻，它的范围之广，关系到每一个人，包括个人手机 APP 账户、电脑网站账户、银行卡账户密码等各类账号信息。如果这些信息被泄露或者是被不法分子利用，将会造成不可挽回的损失。

账号密码安全风险主要有以下几方面：

1. 账号密码强度弱，被暴力破解；
2. 账号密码存储不当泄露；
3. 多个系统使用相同的账号密码，其中某个系统被拖库；
4. 在来历不明的网站，或者公共场所登录了账号密码，被恶意程序窃取。

安全建议：

1. 不要使用与隐私相关的信息作为密码，如姓名拼音、出生日期和手机号；避免使用有规律的字母或数字组合；根据账号的重要性，设置不同的密码，切忌“一套密码走天下”；
2. 对于极其重要的账户，可以通过动态密码、指纹验证、短信验证等相结合的多因子验证来提升账户的安全性；
3. 对于重要系统，要定期更换密码；
4. 账号密码在未经加密的情况下不要存储在互联网上或以纸质形式记录，这些存储方式同样容易导致密码泄露；
5. 不在公共场合随意输入自己的账号密码。

3. 如何安全使用电子邮件

电子邮件常见几种攻击形式有窃听攻击、钓鱼邮件、附件病毒。

窃听攻击

窃听攻击是指黑客在局域网里通过抓包的方式，窃取邮件的信息。比如当你在外通过被黑客破解了的无线路由器连接网络，如果黑客在无线路由器上安装了间谍软件，或者嗅探工具，去对无线网络里面的数据进行抓包，而此时通过该网络发的邮件没有加密，那么你的邮件就很可能被黑客在局域网里面通过抓包的方式，窃取了这封邮件的信息。

安全建议：

为了防止针对邮件的窃听攻击，我们不要通过不可控的网络传输敏感的邮件；收发邮件的时候，要确保传输通道是加密的，对附件实施加密，通过微信、短信或者打电话等其他的不同的传输渠道告知密码，确保传输信息的安全。

钓鱼邮件

钓鱼邮件指利用伪装的电邮，欺骗收件人将账号、口令等信息回复给指定的接收者；或引导收件人连接到特制的网页，这些网页通常会伪装成和真实网站一样，如银行或理财的网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等而被盗取。

安全建议：

遇到这种索要敏感信息的邮件，要保持警惕、保持冷静，提高警惕。如果不确认的话，第一时间主动联系发件人，确认他有没有发过这封邮件，提高个人的安全意识。尽量避免直接点击邮件中的网络链接。

链接、附件病毒

很多人看到邮件中有附件时，会习惯性的点开查看。但是电子邮件链接、附件中可能隐藏着大量的病毒、木马。一旦打开，这些病毒木马会自动进入电脑并隐藏在电脑中，造成文件丢失损坏甚至系统瘫痪。

安全建议：

确保自己的邮件客户端禁止访问可执行的文件；加强个人安全意识，遇到可疑的链接、附件不要轻易点开。

4. 如何防范钓鱼网站以及假冒网站

网页仿冒是通过构造与某一目标网站高度相似的页面诱骗用户的攻击方式。钓鱼网站是网页仿冒的一种常见形式，常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式传播，用户访问钓鱼网站后可能泄露账号、密码等个人隐私。

安全建议：

1. 留意网站配色、内容、链接等细微之处；
2. 注意提示，已被举报加入黑名单的网站，安全浏览器会提示“危险网站”；
3. 支付相关的网站一般网址以 https 开头，在网络地址栏会有彩色图标或锁头，可点击查看网站被权威机构认证的信息；
4. 不盲目相信搜索引擎的推荐，不乱点击邮件、微信、微博、短信中的网址，尤其是短网站；
5. 仔细辨别网址，比如工商银行网址 icbc.com.cn 被混淆为 Icbc.com.cn；
   www.microsoft.com 被混淆为 ww-w.rncrosoft.com；
6. 从 http://开始向右遇到第一个斜线，从该斜线向左至第二个“.”之间的网址是网站的真正域名。例如：http://www.sina.com.cn.sinainfo.cc/log-in/sina.com/index.html 的域名是 sinainfo.cc，而不是新浪。

5. 如何防范网络传销和诈骗

网络诈骗类型有如下四种：一是利用 QQ 盗号和网络游戏交易进行诈骗，冒充好友借钱；二是网络购物诈骗，收取订金骗钱；三是网上中奖诈骗，指犯罪分子利用传播软件随意向互联网 QQ 用户、MSN 用户、邮箱用户、网络游 戏用户、淘宝用户等发布中奖提示信息；四是“网络钓鱼”诈骗，利用欺骗性的电子邮件和伪造的互联网站进行诈骗活动，获得受骗者财务信息进而窃取资金。

安全建议：

1. 不贪便宜；
2. 使用比较安全的支付工具；
3. 仔细甄别，严加防范；
4. 不在网上购买非正当产品，如手机监听器、毕业证书、考题答案等；
5. 不要轻信以各种名义要求你先付款的信息，不要轻易把自己的银行卡借给他人；
6. 提高自我保护意识，注意妥善保管自己的私人信息，不向他人透露本人证件号码、账号、密码等，尽量避免在网吧等公共场所使用网上电子商务服务。

6. 如何安全使用网上银行

网上支付的安全威胁主要表现在以下三个方面：一是密码被破解，很多用户或企业使用的密码都是弱密码，且在所有网站上使用相同密码或者有限的几个密码，易遭受攻击者暴力破解；二是病毒、木马攻击，木马会监视浏览器正在访问的网页，获取用户账户、密码信息或者弹出伪造的登录对话框，诱骗用户输入相关密码，然后将窃取的信息发送出去；三是钓鱼平台，攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行诈骗，如将自己伪装成知名银行或信用卡公司等可信的品牌，获取用户的银行卡号、口令等信息。

安全建议：

1. 尽量不要在多人共用的计算机（如网吧等）上进行银行业务，发现账号有异常情况，应及时修改交易密码并向银行求助；
2. 核实银行的正确网址，安全登录网上银行，不要随意点击未经核实的陌生链接；
3. 在登录时不选择“记住密码”选项，登录交易系统时尽量使用软键盘输入交易账号及密码，并使用该银行提供的数字证书增强安全性，核对交易信息；
4. 交易完成后要完整保存交易记录；
5. 网上银行交易完成后，应点击“退出”按钮，使用 U 盾购物时，交易完成后要立即拔下 U 盾；
6. 对网络单笔消费和网上转账进行金额限制，并为网银开通短信提醒功能，在发生交易异常时及时联系相关客服；

7. 通过正规渠道申请办理银行卡及信用卡；

8. 不要使用存储额较大的储蓄卡或信用额度较大的信用卡开通网上银行；

9. 支付密码最好不要使用姓名、生日、电话号码，也不要使用 12345 等默认密码或与用户名相同的密码；

10. 应注意保护自己的银行卡信息资料，不要把相关资料随便留给不熟悉的公司或个人。

7. 如何安全网站炒股、购买基金

网上炒股面临的安全风险主要体现在以下几个方面：一是网络钓鱼，不法分子制作仿冒证券公司网站，诱导人们登录后窃取用户账号和密码； 二是盗买盗卖，攻击者利用电脑“木马病毒”窃取他人的证券交易账号和密码后，低价抛售他人股票，自己低价买入后再高价卖出，赚取差价。

安全建议：

1. 保护交易密码和通讯密码；

2. 尽量不要在多人共用的计算机（如网吧等）上进行股票交易，并注意在离开电脑时锁屏；

3. 注意核实证券公司的网站地址，下载官方提供的证券交易软件，不轻信小广告；

4. 及时修改个人账户的初始密码，设置安全密码，发现交易有异常情况时，要及时修改密码，并通过截图、拍照等保留证据，第一时间向专业机构或证券公司求助。

8. 如何安全网上购物

网上购物面临的安全风险主要有如下方面：一是通过网络进行诈骗，部分商家恶意在网络上销售自己没有的商品，因为绝大多数网络销售是先付款后发货，等收到款项后便销声匿迹；二是钓鱼欺诈网站，以不良网址导航网站、不良下载网站、钓鱼欺诈网站为代表的“流氓网站”群体正在形成一个庞大的灰色利益链，使消费者面临网购风险；三是支付风险，一些诈骗网站盗取消费者的银行账号、密码、口令卡等，同时，消费者购买前的支付程序繁琐以及退货流程复杂、时间长，货款只退到网站账号不退到银行账号等，也使网购出现安全风险。

安全建议：

1. 核实网站资质及网站联系方式的真伪，尽量到知名、权威的网上商城购物；
2. 尽量通过网上第三方支付平台交易，切忌直接与卖家私下交易；
3. 在购物时要注意商家的信誉、评价和联系方式；
4. 在交易完成后要完整保存交易订单等信息；
5. 在填写支付信息时，一定要检查支付网站的真实性；
6. 注意保护个人隐私，直接使用个人的银行账号、密码和证件号码等敏感信息时要慎重；
7. 不要轻信网上低价推销广告， 也不要随意点击未经核实的陌生链接；
8. 如果发现受骗，应及时联系银行报告欺诈交易，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告并配合调查举证。

9. 如何防范虚假信息传播

互联网时代下，网络已经成为人们获取信息、资讯的重要渠道。与传统媒体相比，网络媒体时效性更高、信息资源更丰富，使受众从中可以获取更多、更新、更全面的新闻信息。也正是因为网络媒体的这种优势，使得信息在网络中很容易被发布，更容易出现虚假信息。虚假信息一旦踏入互联网这一快速通道，不仅会造成网络自媒体公信力的下降，还会对虚假信息中当事人产生影响，甚至一部分用户也因此蒙受了一定的损失。

安全建议：

1. 选择正规的信息获取渠道；
2. 提升自身的信息辨别能力。一方面提升自身的知识面，与相关领域的专家进行交流，另一方面扩大信息获取渠道，进行相关信息的对比。
3. 不造谣、不信谣、不传谣，发现疑似谣言信息及时举报。

三、移动终端安全

1. 如何安全使用 wifi

（1）免费 Wi-Fi 或公共 Wi-Fi

在餐厅、商场、火车站、机场等公众场所，通常都部署了免费的 Wi-Fi 热点，然而，攻击者可能会创建一个有迷惑性的 Wi-Fi 热点，一旦连接到这些恶意热点，可能会导致信息泄露、流量劫持等风险。

免费 Wi-Fi 加密方式通常较弱，一旦被破解，会导致所有接入者有被攻击者攻击的风险。

一些广告公司会在公共场所部署“Wi-Fi 探针”，当用户手机开启 Wi-Fi 功能时，探针盒子可以自动识别到手机的 MAC 地址、RSSI 值等信息，从而掌握用户的行为轨迹。 如果将这些信息与大数据进行匹配，可能会关联到用户的设备 ID 和手机号码，再据此进行有针对性的营销推广。

安全建议

在公众场所链接 Wi-Fi 前，应留意周围的提示，接入官方提供的网络；在同一地区，警惕有相同或相似名字的 WiFi，很有可能有黑客搭建钓鱼 WiFi；在处理重要信息或进行移动支付时，不要使用公用网络，最好使用工具（比如：手机）自带的 4G/5G 网络。

在公共场所，尽量不要自行搭建个人热点，不要使用“Wi-Fi 分享器”等设备；如确有需要，在架设无线路由器前必须进行安全检查，Wi-Fi 应使用 WPA/WPA2 的加密方式、设置复杂密码、保证密码定期更改。

在不需要使用 Wi-Fi 和蓝牙时，将手机的 Wi-Fi、蓝牙功能关闭；使用手机安全软件，根据数据库中保存的记录，对潜在的推销电话进行拦截。

（2）家庭 Wi-Fi

一些 Wi-Fi 密码共享类 APP 会在安装后自动上传所有已经连接过的 Wi-Fi 密码，其中很可能包含一些家庭、工作单位的密码。一旦攻击者使用这类工具，可以轻而易举地连接到家庭或单位的办公网络。

安全建议

避免使用 Wi-Fi 密码共享类 APP；如果需要使用，建议首先关闭自动上传密码功能。

尽量区分自用 Wi-Fi 和客人 Wi-Fi，避免来客有意无意地获取隐私信息。

2. 如何安全使用智能手机

智能手机在使用时必然要联网，否则无法体现其“智能”之处。当其联网时，和所处的网络有很大关系，也和手机本身的设置有关系，更和使用的人有关系。

安全建议

1. 为手机设置访问密码是保护手机安全的第一道防线，以防智能手机丢失时，犯罪分子可能会获得通讯录、文件等重要信息并加以利用；
2. 不要轻易打开陌生人通过手机发送的链接和文件；
3. 为手机设置锁屏密码，并将手机随身携带；
4. 在 QQ、微信等应用程序中关闭地理定位功能；
5. 仅在需要时开启蓝牙；
6. 经常为手机数据做备份；安装安全防护软件，并经常对手机系统进行扫描；
7. 到权威网站或应用市场下载手机应用软件，并在安装时谨慎选择相关权限；
8. 不要试图破解自己的手机，以保证应用程序的安全性。

3. 如何防范伪基站

当用户发现手机无信号或信号极弱时仍然能收到推销、中奖、银行相关短信，则用户所在区域很可能被“伪基站”覆盖。

安全建议

1. 不要相信短信的任何内容，不要轻信收到的中奖、推销信息，不轻信意外之财；
2. 不要轻信任何号码发来的涉及银行转账及个人财产的短信，不向任何陌生账号转账；
3. 安装手机安全防护软件，以便对收到的垃圾短信进行精准拦截。

4. 如何防范骚扰电话、电话诈骗、垃圾短信

广告、骚扰电话和短信几乎每天都能见面，尤其当个人信息被泄露时，这类电话、短信会尤其的多，但并不是所有电话、短信都可以被忽略。

安全建议

1. 克服“贪利”思想，不要轻信，谨防上当；

2. 接到培训通知、以银行信用卡中心名义声称银行卡升级、招工、婚介类等信息时，要多做调查；

3. 不要轻易将自己或家人的身份、通讯信息等家庭、个人资料泄露给他人，对涉及亲人和朋友求助、借钱等内容的短信和电话，要仔细核对；

4. 不要轻信涉及加害、举报、反洗钱等内容的陌生短信或电话，既不要理睬，更不要为“消灾”将钱款汇入犯罪分子指定的账户；

5. 到银行自动取款机（ATM 机）存取遇到银行卡被堵、被吞等意外情况，应认真识别自动取款机“提示”的真伪，不要轻信，可拨打 95516 银联中心客服电话的人工服务台了解查问。

5. 如何防范智能手机信息泄露。

智能手机泄露个人信息的 4 种方式：

1、恶意软件：在手机中预设软件，或通过远程植入软件，实时窃取用户信息：在盗取用户手机后，人工安装窃听软件或病毒软件。

2、病毒和木马：通过广告，邮件，APP 应用软件或二维码等途径传播手机病毒和木马，暗中破坏或窃取手机用户信息。

3、截获设备：通过专门的设备截获手机的通话和收发信息的内容。

4、恶意 WiFi：通过未加密的恶意 WiFi 连接，以设伏方式获取用户手机中的信息。

安全建议

1、通过正规渠道购买手机，选择正规手机售后维修店去维修，避免不法分子趁机安装窃听软件。

2、为智能手机安装一些正规下载的专业防火墙和防病毒软件，定期查杀病毒并进行软件升级。

3、不要随意点击身份可疑的广告，短信，二维码，不要轻易下载和安装网上搜索到的来历不明的 app 应用软件。

4、不要轻易连接免费和不设密码的 WiFi，使用要看清 WiFi 热点名称。

5、关闭手机中一些可能泄露用户隐秘信息的服务，比如用户位置定位。

6、不要轻易将智能手机交给他人保管和使用，在手机失而复得或维修后应进行必要的专业检测。

7、长期不上网应关闭手机的无线连接功能及蓝牙，USB 接口等。

8、将私密数据加密保存，不轻易发送私密信息或以加密方式发送。

9、一旦发现手机流量异常或可疑应用上传隐私数据，应及时求助于正规售后服务商。

10、不把手机当密码记录本，不把身份证号，地址，银行卡号等敏感信息存在手机里，一旦手机丢失或中病毒，面临泄露风险。

6. 如何保护手机支付安全

手机支付和手机有关，也有二维码等媒介有关，所以当手机本身的设置以及手机本身所处的环境有问题时，会产生手机支付安全问题；当二维码有问题时，也能产生手机支付安全问题。

安全建议

1. 利用手机中的各种安全保护功能，为手机、SIM 卡设置密码并安装安全插件，减少手机中的本地分享，对程序执行权限加以限制；

2. 谨慎下载手机应用，尽量从正规网站下载手机应用程序和升级包，对手机中的 Web 站点提高警惕；

3. 登录手机支付应用、网上商城时，勿选择“记住密码”选项；

4. 禁用 Wi-Fi 自动连接到网络功能，尽量不使用公共 Wi-Fi 来进行手机支付；

5. 如有必要，降低“小额免密”的支付额度；

6. 勿见二维码就刷。

7. 如何正确扫描二维码

如今，在餐厅，地铁，商场，甚至街边小广告上，二维码已无处不在。可是，由扫二维码带来的风险也日益显现。由于很多人的支付宝账号就是手机号，恶意二维码的始作俑者通过其他辅助手段就能很容易划走顾客支付宝内的钱。

安全建议

手机用户不要轻易扫描来源不明的二维码，如需扫描，可通过手机安全软件进行扫码，识别带毒二维码，保护移动支付宝及其他支付工具。

8. 如何防范虚假公众号

在互联网技术迅速发展给公众带来巨大便利的同时，也隐含着对公众不利的危险因素，公众普遍缺乏有效甄别网络平台上海量信息的能力，并且相应的行业规范和法律规范未能及时跟上技术的发展，这也给不法分子以可乘之机。

安全建议

1、对于网络用户而言，应当慎重加入公众号，尤其要警惕那些没有规范途径的或者自己非常陌生的公众号，提高对个人信息尤其是敏感信息的保护意识，防患于未然。

2、对于网络平台运营者而言，其是有效规避、防范真假公众号的核心，因此应当强化管理意识并提高管理水平，及时发现并封禁违法违规的公众号，及时通知并配合公安机关开展相应的调查和处理；对于因为网络平台运营者的过错而导致相应损害发生的，网络用户有权向其主张承担相应的民事法律责任。

3、对于监管机构而言，应尽快建立监测、研判、预警、处置和追踪的网络安全问题联合处置机制，为包括公众号运营在内的网络环境提供完善的监管机制。并依法及时对违反网络安全运营职责的平台予以处理，使其能够在规避防范问题公众号时真正发挥核心功能。

9. 手机遗失的风险

手机遗失，并不仅仅是丢失了一部手机。

智能手机中安装了各种应用，这些应用不仅涉及到个人隐私，更涉及到资金的安全。当手机没有设置开机口令或仅设置了弱口令时，则手机内容将被一览无遗。

安全建议

1.为手机设置开机密码；
2.安装手机安全软件；
3.备份联系人和短信；
4.取消单独绑定手机的账号和密码；
5.修改家人手机号的备注名称。

当确定手机确实是遗失了而无法找回时：

1.致电手机运营商挂失手机号码；
2.挂失银行卡；
3.手机绑定支付宝的，拨打 95188 挂失；
4.微信用户登录 http://110.qq.com/冻结微信账号；
5.修改各相关应用软件的登录密码；
6.向常住户口所在地派出所申报丢失补领身份证；
7.补办手机卡。

10. 处理旧手机时的注意事项

现在手机的更新非常频繁，有的人一年就更新手机，最多两三年也会更新手机。买了新手机的你当然非常高兴，但是，千万不要忘记要好好处理淘汰的旧手机。处理旧手机的关键是防止手机信息泄露。

旧手机信息是怎么泄露的？

1、普通删除或恢复出厂设置并不能抹去数据，系统在执行文件删除时，仅是被做了一个“删除”的标记，但储存的数据本身依然存在，只是处于一个可覆盖的状态，照片，短信，通讯录，视频等都可以恢复。

2、如未进行新的数据操作，最上层信息很容易被恢复。因为硬盘上的数据可反复被覆盖，数据恢复一般只能读取覆盖在最上层的信息。

安全建议

1、将手机恢复出厂设置或格式化，再存入一些无关紧要的内容，将手机的存储空间占满；

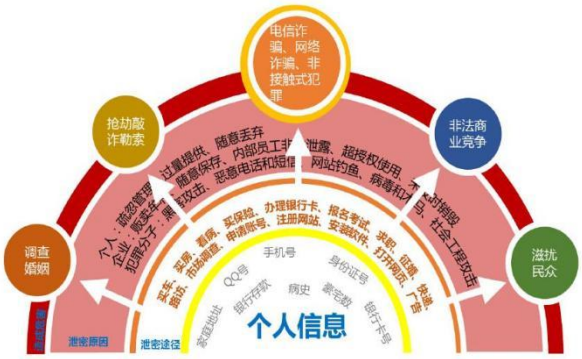
2、不要将手机作为一般的生活垃圾扔掉，可卖给相对正规的厂家。

四、个人信息安全

1. 什么是个人信息

以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息，不包括匿名化处理后的各种信息。个人信息可以分为个人一般信息和个人敏感信息。

个人一般信息是指正常公开的普通信息，例如姓名、性别、年龄、爱好等。个人敏感信息是指一旦遭泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。



2. 个人信息泄露的途径和后果

目前，个人信息的泄露主要有以下途径：

1. 利用互联网搜索引擎搜索个人信息，汇集成册，并按照一定的价格出售给需要购买的人；

2. 旅馆住宿、保险公司投保、租赁公司、银行办证、电信、移动、联通、房地产、邮政部门等需要身份证件实名登记的部门、场所，个别人员利用登记的便利条件，泄露客户个人信息；

3. 个别违规打字店、复印店利用复印、打字之便，将个人信息资料存档留底，装订成册，对外出售；

4. 借“问卷调查”之名，窃取群众个人信息。有人宣称只要在“调查问卷表”上填写信息，就能获得不等奖次的奖品，以此诱使群众填写个人信息；

5. 在抽奖券的正副页上填写姓名、家庭住址、联系方式等可能会导致个人信息泄露；

6. 在购买电子产品、车辆等物品时，在一些非正规的商家填写非正规的“售后服务单”，从而被人利用了个人信息；

7. 超市、商场通过向群众邮寄免费资料、申办会员卡时掌握到的群众信息，通过个别人向外泄露。

8. 手机的定位功能如果被不法分子利用，就会对手机持有者进行跟踪，并窃取有关个人的一些信息。

9. 用户分享网盘上的内容时不设置提取码或者密码，则里面的内容有可能会被网上的爬虫抓取到并索引，文件就会变成公开访问并可以被任何人下载。

10. 家用监控摄像头可能导致用户监控视频被泄露，甚至会出现智能摄像头被恶意控制的风险。

目前，针对个人信息的犯罪已经形成了一条灰色的产业链，在这个链条中，有专门从事个人信息收集的泄密源团体，他们之中包括一些有合法权限的内部用户主动通过 QQ、互联网、邮件、移动存储等各类渠道泄露信息。还包括一些黑客，通过攻击行为获得企业或个人的数据库信息；有专门向泄密源团体购买数据的个人信息中间商团体，他们根据各种非法需求向泄密源购买数据，作为中间商向有需求者推销数据，作为中间商买卖、共享和传播各种数据库；还有专门从中间商团体购买个人信息，并实施各种犯罪的使用人团体，他们是实际利用个人信息侵害个人利益的群体。

据不完全统计，这些人在获得个人信息后，会利用个人信息从事五类违法犯罪活动：

1. 电信诈骗、网络诈骗等新型、非接触式犯罪。

2. 直接实施抢劫、敲诈勒索等严重暴力犯罪活动。

3. 实施非法商业竞争。不法分子以信息咨询、商务咨询为掩护，利用非法获取的公民个人信息，收买客户、打压竞争对手。

4. 非法干扰民事诉讼。不法分子利用购买的公民个人信息，介入婚姻纠纷、财产继承、债务纠纷等民事诉讼，对群众正常生活造成极大困扰。

5. 滋扰民众。不法分子获得公民个人信息后，通过网络人肉搜索、信息曝光等行为滋扰民众生活。

3. 如何防范个人信息泄露

1. 在安全级别较高的物理或逻辑区域内处理个人敏感信息；
2. 敏感个人信息需加密保存；
3. 不使用 U 盘存储交互个人敏感信息；
4. 尽量不要在可访问互联网的设备上保存或处理个人敏感信息；
5. 只将个人信息转移给合法的接收者；
6. 个人敏感信息需带出公司时要防止被盗、丢失；
7. 电子邮件发送时要加密，并注意不要错发；
8. 邮包寄送时选择可信赖的邮寄公司，并要求回执；
9. 避免传真错误发送；
10. 纸质资料要用碎纸机销毁；
11. 废弃的光盘、U 盘、电脑等要消磁或彻底破坏。
12. 关闭不必要的软件定位功能，在社交平台发布信息时尽可能的避免发布位置信息；
13. 使用网盘分享文件时使用加密分享方式、并设定有效时间段，不要分享个人隐私信息，定期整理网盘内文件，尽可能避免将隐私信息存储在网盘上；
14. 使用家用监控时要选择正规产品，注册账户时使用高强度密码，避免摄像头正对隐私区域，不随意分享监控拍摄画面，不使用时应及时关闭电源。

4. 发现个人信息泄露时怎么办

公民发现泄露个人身份、侵犯个人隐私的网络信息，或者受到商业性电子信息侵扰，有权要求网络服务提供者删除有关信息或者采取其他必要措施予以制止，必要时可向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。

公民还可依据《侵权责任法》、《消费者权益保护法》以及《个人信息保护保护法》等，通过法律手段进一步维护自己的合法权益，如要求侵权人赔礼道歉、消除影响、回复名誉、赔偿损失等。

五、计算机安全

1. 计算机中毒有哪些症状

1. 经常死机；
2. 文件打不开；
3. 经常报告内存不够；
4. 提示硬盘空间不够；
5. 出现大量来历不明的文件；
6. 数据丢失；
7. 系统运行速度变慢；
8. 操作系统自动执行操作。

2. 在使用电脑过程中应该采取哪些网络安全防范措施

1. 安装防火墙和防病毒软件，并经常升级，及时更新木马库，给操作系统和其他软件打补丁；
2. 对计算机系统的各个账号要设置口令，及时删除或禁用过期账号；
3. 不要打开来历不明的网站、邮件链接或附件，不要执行从网上下载后未经杀毒处理的软件，不要打开聊天软件上收到的不明文件。
4. 打开任何移动存储器前用杀毒软件进行检查；
5. 定期备份，以便在遭到病毒、木马或恶意软件等的破坏后能迅速修复。

3. 如何防范 U 盘、移动硬盘泄密

1. 及时查杀木马与病毒；
2. 从正规商家购买可移动存储介质；
3. U 盘、移动硬盘介入电脑前，先进行病毒扫描；
4. 定期备份并加密重要数据；
5. 不要将办公与个人的可移动存储介质混用。

4. 勒索软件的防范建议

1. 拒付赎金：支付赎金会助长攻击者的气焰，攻击者还会通过用户支付的赎金速度对用户财务、数据价值等情况进行分析，可能从此被盯上；

2. 防毒杀毒：尽量到官方网站下载软件，安装正规杀毒软件，运行下载软件之前先进行病毒扫描；

3. 及时更新：关注操作系统安全公告，及时安装安全补丁，尽早堵住漏洞；

4. 封堵端口：关闭无用的计算机服务/端口，开启 Windows 防火墙；

5. 做好备份：使用光盘/移动硬盘等介质，对文档、邮件、数据库、源代码、图片、压缩文件等各种类型的数据资产定期进行备份，并脱机保存。

六、相关法律法规

1、《中华人民共和国网络安全法》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

2、《国家网络空间安全战略》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

3、《中华人民共和国密码法》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2019-10/27/c_1573711980953641.htm

4、《中华人民共和国电子签名法》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2004-08/28/c_126468489.htm

5、《全国人民代表大会常务委员会关于加强网络信息保护的决定》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2012-12/29/c_133353262.htm

6、《全国人民代表大会常务委员会关于维护互联网安全的决定》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2000-12/29/c_133158942.htm

7、《互联网域名管理办法》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2017-09/28/c_1121737753.htm

8、《网络安全审查办法
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

9、《网络信息内容生态治理规定》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

10、《儿童个人信息网络保护规定》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2019-08/23/c_1124913903.htm

11、《互联网信息服务管理办法》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2000-09/30/c_126193701.htm

12、《公共互联网网络安全威胁监测与处置办法》
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2017-09/14/c_1121660498.htm

13、《个人信息和重要数据出境安全评估办法》（征求意见稿）
来源：中共中央网络安全与信息化委员会办公室
http://www.cac.gov.cn/2017-04/11/c_1120785691.htm

14、《中华人民共和国个人信息保护法》（草案）
来源：中国人大网
http://www.npc.gov.cn/flcaw/flca/ff80808175265dd401754405c03f154c/attachment.pdf

15、《数据安全管理办法》（征求意见稿）
来源：中华人民共和国司法部网站
http://www.chinalaw.gov.cn/government_public/content/2019-05/28/657_235862.html

苏州大学信息化建设与管理中心


天赐庄校区：东校区教育超市北
独墅湖校区：一期 304 号楼 5 楼
阳澄湖校区：行政楼 401


0512-65880000


its.suda.edu.cn

苏　州　大　学

苏大学〔2021〕29号

关于印发《苏州大学立德树人之本科生成长陪伴计划指导方案》的通知

各学院（部）、部门、直属单位：

《苏州大学立德树人之本科生成长陪伴计划指导方案》业经学校 2021 年第 8 次校长办公会议审议通过，现印发给你们，请遵照执行。

特此通知。

苏州大学

2021 年 7 月 9 日

苏州大学立德树人之
本科生成长陪伴计划指导方案

为深入贯彻习近平总书记关于教育的重要论述精神，全面落实立德树人根本任务，深化“三全育人”综合改革方案，进一步提升人才培养质量，现结合学校实际，制定苏州大学立德树人之本科生成长陪伴计划指导方案。

一、指导思想

以习近平新时代中国特色社会主义思想为指导，以立德树人为根本任务，坚守“为党育人、为国育才”初心，坚持以学生发展为中心，强化引领保障，培养德智体美劳全面发展的社会主义建设者和接班人。

二、总体思路

将立德树人融入思想道德教育、文化知识教育、社会实践教育各环节。围绕人才培养目标，顺应学生成长成才意愿，尊重学生个性化发展需求，以生涯规划指导为主线，以“导师+导生”制度为抓手，从思想引导、学业辅导、生活指导等方面陪伴学生成长，发挥需求满足、思想纠偏、目标引领、动力激发的作用，进一步实现“全员、全方位、全过程”育人。

三、基本原则

（一）坚持标准规划与个性设置相结合

根据学校指导方案要求，结合学院（部）办学特色和发展目

标，制定个性化的学生成长陪伴方案。

（二）坚持问题导向与精准帮扶相结合

在全面陪伴的基础上，坚持问题导向，聚焦重点环节和重点学生群体，实行分类指导，科学施策，提升成长陪伴，特别是服务引领的精准度。

（三）坚持教育管理与指导服务相结合

陪伴过程中形成全员参与、全方位引领、全过程陪伴的氛围，寓教育于指导，寓管理于服务。

四、实施内容与具体措施

本科生成长陪伴计划由校领导统筹协调，党委宣传部、人力资源处、党委教师工作部、财务处、教务部、学生工作部（处）、党委研究生工作部协同落实。

（一）陪伴模式

学院（部）根据实际情况，确立本学院（部）学生成长陪伴模式，如“一对一”（一个导师陪伴一名学生）、“一对多”（一个导师陪伴多名学生）或“导师+导生”团队陪伴模式。如选择“导师+导生”团队陪伴模式，则每支团队服务学生的总数不超过20人。

导师和导生的选聘采取个人申报和学院（部）选聘相结合的方式，导师由专业教师、辅导员、关工委成员等担任。导生由研究生、高年级本科生担任。

（二）陪伴内容

陪伴团队主要从思想、学业、生活等三个方面开展陪伴工作。思想引导以引领学生践行社会主义核心价值观为目标，面向学生开展思想政治教育和道德品质教育。学业辅导以生涯规划指导为主线，面向学生开展专业学习教导、科研方法指导、学科前沿引导和学术规范督导。生活指导以促进学生身心健康为目标，培养良好的学习生活习惯，提高身体心理素质，提升自我管理能力，为学生健康成长、顺利发展提供必要的、有针对性的社会支持。每支陪伴队伍每学期开展活动的总次数不少于 4 次。

（三）考核激励

学校建立校院两级考核机制，学院（部）每学年进行一次中期检查和一次年度考核。对于工作突出的单位和团队，学校进行优秀表彰，并将成长陪伴计划参与度纳入教师评奖评优、职称申报体系。

学校按本科生人数和相关标准在年度经费预算中安排学生活动经费，协助解决工作所需，保障团队活动顺利开展。导生津贴纳入本科生勤工助学和研究生“三助”体系。导师津贴由各学院（部）根据教师社会工作量的要求，统筹安排，学院（部）应努力创造条件，积极推进该项工作。

（四）平台搭建

将本科生成长陪伴预约功能纳入“云中苏大”，为学生配备导师提供更为便捷的途径，满足学生个性化发展需求。打造学生

需求数据采集与分析系统，随时记载学生线上、线下需求数据，定期进行分析，形成学生发展需求报告，为完善学院（部）人才培养方案、本科生成长陪伴计划提供数据支撑。

五、预期成效

（一）中期建设目标

本科生成长陪伴计划在未来一到三年内分三个阶段实现中期建设目标。

1、试点探索阶段。选取部分学院（部）开展试点工作，在试点学院（部）建立本科生成长陪伴机制。

2、全面推进阶段。在全校所有学院（部）按年级逐步推进本科生成长陪伴计划的实施，完成本科生成长陪伴机制的建立。

3、优化完善阶段。优化完善本科生成长陪伴机制，提高成长陪伴工作成效，提升人才培养水平与质量。

（二）长期建设目标

1、进一步增强协同育人合力，优化完善全员人才培养体系，实现从学生入学到毕业的全过程覆盖，从课堂内到课堂外的全方位覆盖，完成人才培养闭环。

2、形成学生全面发展与个性发展、全体发展与个体发展支持机制，全面提升学生获得感、幸福感。

抄送：各党委、党工委，校党委各部门，工会、团委。

苏州大学校长办公室　　2021年7月10日印发