国家网络安全宣传周
China Cybersecurity Week

中共上海市委网络安全和信息化
委员会办公室

国家网络安全宣传周
China Cybersecurity Week

2024 CHINA CYBERSECURITY WEEK

网络安全为人民
网络安全靠人民

国家网络安全宣传周上海地区活动

宣传手册

○ 1.坚持党管互联网

报刊、通讯社、电台、电视台、新闻网站的所有工作都必须体现党的意志、反映党的主张，必须维护党中央权威、维护党的团结，做到爱党、护党、为党。

——2016年2月19日，习近平在党的新闻舆论工作座谈会上的讲话

要加强党中央对网信工作的集中统一领导，确保网信事业始终沿着正确方向前进。

——2018年4月20日至21日，习近平在全国网络安全和信息化工作会议上的讲话

○ 2.坚持网信为民

网信事业要发展，必须贯彻以人民为中心的发展思想。要适应人民期待和需求，加快信息化服务普及，降低应用成本，为老百姓提供用得上、用得起、用得好的信息服务，让亿万人民在共享互联网发展成果上有更多获得感。

——2016年4月19日，习近平在网络安全和信息化工作座谈会上的讲话

网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点，让人民群众在信息化发展中有更多获得感、幸福感、安全感。

——2018年4月20日至21日，习近平在全国网络安全和信息化工作会议上的讲话

○ 3.坚持走中国特色治网之道

我们要本着对社会负责、对人民负责的态度，依法加强网络空间治理，加强网络内容建设，做强网上正面宣传，培育积极健康、向上向善的网络文化，用社会主义核心价值观和人类优秀文明成果滋养人心、滋养社会，做到正能量充沛、主旋律高昂，为广大网民特别是青少年营造一个风清气正的网络空间。

——2016年4月19日，习近平在网络安全和信息化工作座谈会上的讲话

要提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。

——2018年4月20日至21日，习近平在全国网络安全和信息化工作会议上的讲话

○ 4.坚持统筹发展和安全

网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。我们一定要认识到，古往今来，很多技术都是“双刃剑”，一方面可以造福社会、造福人民，另一方面也可以被一些人用来损害社会公共利益和民众利益。

——2016年4月19日，习近平在网络安全和信息化工作座谈会上的讲话

要正确处理安全和发展、开放和自主、管理和服务的关系，不断提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力，把网络强国建设不断推向前进。

——2016年10月9日，习近平在十八届中央政治局第三十六次集体学习时的讲话

○ 5.坚持正能量是总要求、管得住是硬道理、用得好是真本事

现在，各级领导干部特别是高级干部，如果不懂互联网、不善于运用互联网，就无法有效开展工作。各级领导干部要学网、懂网、用网，积极谋划、推动、引导互联网发展。

——2016年10月9日，习近平在十八届中央政治局第三十六次集体学习时的讲话

我多次说过，正能量是总要求，管得住是硬道理，现在还要加一条，用得好是真本事。

——2019年1月25日，习近平在十九届中央政治局第十二次集体学习时的讲话

○ 6.坚持筑牢国家网络安全屏障

增强网络安全防御能力和威慑能力。网络安全的本质在对抗，对抗的本质在攻防两端能力较量。要落实网络安全责任制，制定网络安全标准，明确保护对象、保护层级、保护措施。哪些方面要重兵把守、严防死守，哪些方面由地方政府保障、适度防范，哪些方面由市场力量防护，都要有本清清楚楚的账。人家用的是飞机大炮，我们这里还用大刀长矛，那是不行的，攻防力量要对等。要以技术对技术，以技术管技术，做到魔高一尺、道高一丈。

——2016年4月19日，习近平在网络安全和信息化工作座谈会上的讲话

国家网络安全工作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。

——2019年9月，习近平对国家网络安全宣传周作出重要指示

○ 7.坚持发挥信息化驱动引领作用

没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济；要有高素质的网络安全和信息化人才队伍；要积极开展双边、多边的互联网国际交流合作。

——2014年2月27日，习近平在中央网络安全和信息化领导小组第一次会议上的讲话

当今世界，信息化发展很快，不进则退，慢进亦退。我们要加强信息基础设施建设，强化信息资源深度整合，打通经济社会发展的信息“大动脉”。

——2016年4月19日，习近平在网络安全和信息化工作座谈会上的讲话

○ 8.坚持依法管网、依法办网、依法上网

网络空间不是“法外之地”。网络空间是虚拟的，但运用网络空间的主体是现实的，大家都应该遵守法律，明确各方权利义务。要坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。

——2015年12月16日，习近平在第二届世界互联网大会开幕式上的讲话

要推动依法管网、依法办网、依法上网，确保互联网在法治轨道上健康运行。

——2018年4月20日至21日，习近平在全国网络安全和信息化工作会议上的讲话

○ 9.坚持推动构建网络空间命运共同体

网络空间是人类共同的活动空间，网络空间前途命运应由世界各国共同掌握。各国应该加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体。

——2015年12月16日，习近平在第二届世界互联网大会开幕式上的讲话

中国愿同世界各国一道，把握信息革命历史机遇，培育创新发展新动能，开创数字合作新局面，打造网络安全新格局，构建网络空间命运共同体，携手创造人类更加美好的未来。

——2020年11月23日，习近平向世界互联网大会·互联网发展论坛致贺信

○ 10.坚持建设忠诚干净担当的网信工作队伍

“得人者兴，失人者崩。”网络空间的竞争，归根结底是人才竞争。建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的。

——2016年4月19日，习近平在网络安全和信息化工作座谈会上的讲话

要不断增强“四个意识”，坚持把党的政治建设摆在首位，加大力度建好队伍、全面从严管好队伍，选好配好各级网信领导干部，为网信事业发展提供坚强的组织和队伍保障。

——2018年4月20日至21日，习近平在全国网络安全和信息化工作会议上的讲话

《网络安全法》

第八条 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照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

问：《网络安全法》中对于网络安全监管体制是如何规定的？

答：《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8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。这种“1+X”的监管体制，符合当前互联网与现实社会全面融合的特点和我国监管需要。

《数据安全法》

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

问：如何开展数据分类分级工作？

答：国家标准GB/T43697-2024《数据安全技术 数据分类分级规则》，给出了数据分类分级的通用规则。该标准明确了数据分类与分级的基本原则，包括业务相关性、数据敏感性、风险可控性等。具体而言，数据分类应根据业务特点和数据属性进行划分，如个人信息、商业秘密、国家秘密等；数据分级则应根据数据的敏感性、重要性和潜在风险进行划分，如一般数据、重要数据、核心数据等。

《个人信息保护法》

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。

问：敏感个人信息处理有什么特殊要求吗？

答：要求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。知情同意原则是个人信息保护领域公认的首要原则，既适用于敏感个人信息，也适用于非敏感个人信息。针对敏感个人信息的处理，应当取得个人的单独同意。在处理敏感个人信息时，概括同意或推定同意的授权模式为法律所禁止。法律、行政法规规定处理敏感个人信息应当取得书面同意的，还应取得书面同意。

《密码法》

第二十六条 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的机构检测认证合格后，方可销售或者提供。商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定，避免重复检测认证。

问：为什么密码法要对特定商用密码产品、服务实行强制性检测认证制度？

答：密码法设立该制度，是维护国家安全和社会公共利益的需要。商用密码产品、服务是专业技术性很强的特殊产品和服务，广泛应用于国民经济和社会发展各领域，应用于关键信息基础设施，其质量与安全性直接关系国家安全和社会公共利益，需要通过检测认证的方式对其质量与安全性进行技术把关。强制性检测认证制度仅适用于涉及国家安全、国计民生、社会公共利益的商用密码产品和使用网络关键设备和网络安全专用产品的商用密码服务，并通过制定产品、服务目录明确界定管理范围，不会对市场和产业构成不必要的限制。

《关键信息基础设施保护条例》

第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

问：对实施危害关键信息基础设施安全活动的个人和组织，或未经授权或批准，对关键信息基础设施实施漏洞探测、渗透性测试等活动的个人和组织，条例有哪些规定？

答：条例明确，任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。

《促进和规范数据跨境流动规定》

第二条 数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

问：如何理解数据出境活动所称的重要数据？

答：重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

《互联网政务应用安全管理规定》

第七条 机构编制管理部门为机关事业单位制发专属电子证书或纸质证书。机关事业单位通过应用程序分发平台分发移动应用程序，应当向平台运营者提供电子证书或纸质证书用于身份核验；开办微博、公众号、视频号、直播号等公众账号，应当向平台运营者提供电子证书或纸质证书用于身份核验。

问：什么是机关事业单位电子证书？

答：机关事业单位电子证书，是指机构编制管理部门为机关颁发的统一社会信用代码电子证书，以及为事业单位颁发的事业单位法人电子证书，作为其在网络空间的权威身份凭证。机关事业单位网络身份凭证与机关统一社会信用代码证书、事业单位法人证书并行使用，具有同等效力。

《网络安全审查办法》

第七条 掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

问：网络平台运营者赴国外上市申报网络安全审查，可能的结果有几类？

答：对外开放是我国的基本国策，我们始终支持境内企业依法依规合理利用境外资本市场融资发展。申报网络安全审查可能有以下三种情况：一是无需审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。

《生成式人工智能服务管理暂行办法》

第七条 生成式人工智能服务提供者（以下称提供者）应当依法开展预训练、优化训练等训练数据处理活动，遵守以下规定：

（一）使用具有合法来源的数据和基础模型；

（二）涉及知识产权的，不得侵害他人依法享有的知识产权；

（三）涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形；

（四）采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性；

（五）《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律、行政法规的其他有关规定和有关主管部门的相关监管要求。

问：《办法》主要明确了哪些生成式人工智能服务规范？

答：《办法》要求采取有效措施防范未成年人用户过度依赖或者沉迷生成式人工智能服务。规定提供者应当按照《互联网信息服务深度合成管理规定》对图片、视频等生成内容进行标识。规定提供者发现违法内容的，应当及时采取停止生成、停止传输、消除等处置措施并采取模型优化训练等措施进行整改。明确提供者发现使用者利用生成式人工智能服务从事违法活动的，应当依法依约采取有关处置措施，保存有关记录，并向有关主管部门报告。

《互联网信息服务算法推荐管理规定》

第二十二条 算法推荐服务提供者应当设置便捷有效的用户申诉和公众投诉、举报入口，明确处理流程和反馈时限，及时受理、处理并反馈处理结果。

问：针对群众普遍关心的用户权益保护问题，《规定》是如何规定的？

答：《规定》明确了对于算法推荐服务提供者的用户权益保护要求。一是算法知情权，要求告知用户其提供算法推荐服务的情况，并公示服务的基本原理、目的意图和主要运行机制等。二是算法选择权，要求向用户提供不针对其个人特征的选项，或者便捷的关闭算法推荐服务的选项。用户选择关闭算法推荐服务的，算法推荐服务提供者应当立即停止提供相关服务。算法推荐服务提供者应当向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能。三是针对向未成年人、老年人、劳动者、消费者等主体提供服务的算法推荐服务提供者作出具体规范。如不得利用算法推荐服务诱导未成年人沉迷网络，应当便利老年人安全使用算法推荐服务，应当建立完善平台订单分配、报酬构成及支付、工作时间、奖惩等相关算法，不得根据消费者的偏好、交易习惯等特征利用算法在交易价格等交易条件上实施不合理的差别待遇等。

《未成年人网络保护条例》

第三十二条 个人信息处理者应当严格遵守国家网信部门和有关部门关于网络产品和服务必要个人信息范围的规定，不得强制要求未成年人或者其监护人同意非必要的个人信息处理行为，不得因为未成年人或者其监护人不同意处理未成年人非必要个人信息或者撤回同意，拒绝未成年人使用其基本功能服务。

问：在未成年人个人信息网络保护方面，《条例》主要作了哪些制度规定？

答：一是网络直播服务提供者应当建立网络直播发布者真实身份信息动态核验机制。二是明确规定未成年人的监护人也可以请求行使查阅、复制、更正、补充、删除未成年人个人信息的权利，拒绝请求的应当书面告知申请人并说明理由。三是规定网络服务提供者发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，应当及时提示并采取必要保护措施。四是规定个人信息处理者的工作人员访问未成年人个人信息的，应当经过相关负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法处理未成年人个人信息。

网络安全漏洞风险
——“重应用，轻防护”不可取

（1）典型案例

某地某一民营卫生机构官网由于未采取相应的安全防护措施，使用不安全的jQuery版本导致容易出现跨站脚本攻击。该网站虽已停止运营许久，但攻击者利用这种漏洞，能够在用户浏览网页时，执行恶意脚本或代码，从而盗取用户信息、破坏用户与应用程序的交互或进行其他危害行为，相关数据（患者注册信息、个人信息等）有可能在公共互联网上被未授权访问。

经过案件约谈和调查询问，企业已认识到在网络安全管理上存在的漏洞，采取了内部排查、员工教育、关闭网站等措施。属地网信办根据违法违规事实，依据相关法律法规，给予其行政警告的处罚。

（2）问题分析

一些单位存在“重应用、轻防护”的心态，对网络安全的重视不足，在网站平台建设和运营过程中未采取相应的安全防护措施，网站平台停止运营后未及时关停服务、删除数据等，留下了安全隐患。

（3）法律法规

《中华人民共和国网络安全法》第二十二条规定：网络产品、服务应当符合相关国家标准的强制性要求。发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

（4）防范指南

1.定期对平台系统存在的安全风险进行检测评估，及时发现并修复网络安全漏洞。

2.及时更新系统和软件到最新版本，打上安全补丁。

3.制定网络安全事件应急预案，定期开展应急演练，确保在出现网络安全事件时能够迅速有效地应对。

钓鱼邮件升级
——细心检查莫入圈套

（1）典型案例

在生成式AI兴起的潮流中，不法分子利用生成式AI技术制作高仿真度的钓鱼邮件，高度伪装成知名平台官方通知邮件，在邮件内容中制造紧迫感、鼓励诱使收件人点击恶意链接并输入账户信息。有不少亚马逊卖家称收到伪装成亚马逊官方的钓鱼邮件，该邮件的发件地址与亚马逊官方高度相似，内容仿制官方通知风格，要求更新紧急联系人信息。按照邮件指引操作后，卖家会被引导至一个仿造的亚马逊网站，要求输入邮箱、密码及二次验证码，最终导致账户被盗用，重要账户信息被提取，有卖家在短短一夜之间损失高达40万。

（2）问题分析

受害者往往因为对品牌的信任，对官方通知风格的邮件缺乏足够的警惕，容易在紧迫感的驱使下，忽略安全性、真实性检查。随着生成式AI技术的兴起，钓鱼邮件生成手段日益翻新，不法分子利用AI技术降低制作虚假邮件等信息的成本和提高其逼真度，增加了钓鱼获取账户信息的成功率。

（3）法律法规

《中华人民共和国网络安全法》第四十八条规定：任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

（4）防范指南

1.增强安全意识，对任何要求输入敏感信息的邮件保持警惕，不轻信看似官方的邮件通知。

2.对邮件的发件地址和邮件中的链接进行仔细检查，确认其是否指向真实的官方网站。

3.启用多因素认证增加账户安全性，即使不法分子获取了登录信息也难以直接访问账户。

供应链安全
——网络安全中的重要一环

（1）典型案例

7月19日，微软集成的第三方安全软件公司CrowdStrike安全产品，因升级更新出现错误，导致Windows电脑蓝屏死机情况。这一事件全球范围波及广泛，受影响的机器不仅自动蓝屏，还无法通过重启解决问题，多家知名机构和企业的因此业务中断。在航空业，美国达美航空、联合航空和美国航空等主要航空公司的所有航班受蓝屏事件影响，宣布当天上午停飞。金融市场，英国伦敦证券交易所宣布因蓝屏事件暂停交易，金融市场的稳定性受到威胁。公共交通领域，日本轨道交通公司因蓝屏事件无法查看列车实时运行情况，被迫取消多条线路，影响了无数通勤者的出行。

（2）问题分析

因供应链安全问题,导致应用系统源代码泄露、IT系统出现故障,造成重大不良影响。为了确保关键信息基础设施供应链安全， 关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的，应当进行网络安全审查。

（3）法律法规

《关键信息基础设施安全保护条例》第十九条规定：运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

（4）防范指南

1.强化供应链安全风险意识，对采购网络产品和服务提出具体要求。

2.在合同中明确双方的安全责任，要求合作第三方定期进行自评估，并及时反馈评估结果。

3.定期开展供应链安全风险评估，避免因产品或服务断供或出现安全问题导致业务持续性遭受负面影响。

数据泄露后“一删了之”
——对数据安全责任意识缺失企业“一案双罚”

（1）典型案例

L公司因数据库存在未授权访问漏洞，造成部分数据被境外IP窃取的事件。国家网信部门接通报后立即通知企业处置，并赶赴现场核查。涉事公司运维工程师费某出于销毁证据、逃避责任的考虑，在网信部门工作人员到达企业前，自行将涉事数据库删除。

经调查，涉事公司未建立健全全流程数据安全管理制度，未采取相应的技术措施和其他必要措施保障数据安全，同时企业私自删除涉事数据库逃避责任、没有按照规定及时向网信部门报告，未有效履行数据安全保护义务。针对其违法情况，属地网信部门依据相关法律法规，对涉事公司作出责令改正、给予警告，并对涉事公司及直接责任人员处以罚款的行政处罚。

（2）问题分析

涉事公司的行为反映了一些企业在面对数据泄露时的恐慌和逃避心理，担心数据泄露事件会严重影响其声誉和经济利益，因此可能会选择掩盖事实而非积极应对。但这种数据泄露后“一删了之”的行为，不仅未能掩盖数据泄露的事实，反而会给企业带来更加严重的处罚后果。

（3）法律法规

《中华人民共和国数据安全法》第二十九条规定：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

（4）防范指南

1.企业应建立健全的网络安全和数据安全管理制度，定期进行安全审计和风险评估。

2.制定应急预案，在发生数据泄露事件时，立即采取补救措施，按照规定及时告知用户并向有关主管部门报告，不隐瞒、不销毁证据。

3.企业应充分认识到维护平台数据安全的法律责任，履行网络安全保护义务，在发生数据安全事件时，采取正确积极的应对方式。

售卖数据牟利
——违法侵害他人权益

（1）典型案例

媒体报道，一家名为“XX查”的平台正在大规模售卖企业家个人信息，号称覆盖数亿企业数据库，拥有亿条线索联系方式”。经与企业家本人或接近企业家的知情人士确认，核实到多位企业家手机号在该平台售卖，且均为其本人所有并正在使用。

（2）问题分析

随着数据价值不断提升，一些组织利用“大数据+超链分析”技术抓取、整合各平台信息，或向各大平台支付费用购买信息，违法收集售卖个人信息等数据牟取利益，侵害了个人权益和社会公共利益。

（3）法律法规

《中华人民共和国数据安全法》第三十二条规定，任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

（4）防范指南

1.不轻易在公开平台发布或在非正规活动平台填写真实个人信息。

2.网上涉及个人信息的内容，要及时退出、删除痕迹或销毁；对于长期不用的平台或网站，要及时取消授权、注销账号。

3.未经个人同意，个人信息处理者不可公开或向他人提供其所获取的个人信息。

个人信息“裸奔”
——个人信息保护措施须到位

（1）典型案例

很多企业在收集、存储、使用和传输个人信息的过程中，未能采取足够的安全措施，导致大量敏感个人信息处于未加密的“裸奔”状态，极易遭受非法访问和数据泄露。例如，某知名火锅餐饮连锁企业存储的手机号码、邮箱号码等1.5亿条会员个人信息以及包括身份证号码在内的18万条本公司员工个人信息；某知名房产中介收集的200万条用户数据中的20万条客户手机号码等个人信息；某知名培训机构存储的4万条学生姓名、监护人手机号码等个人信息，均未按规定采取加密、去标识化等安全保护措施。

网信部门根据前期检查、立案、约谈和调查询问的情况，对上述单位作出罚款的行政处罚。

（2）问题分析

属地网信部门通过现场检查发现，企业在个人信息保护方面仍存在“五类问题”：（1）在收集环节仍然存在强制要、过度取个人信息问题；（2）在存储环节大量个人信息未加密处于“裸奔”状态；（3）在使用传输环节企业随意授权放权管理不到位；（4）在管理制度上企业关于个人信息保护措施明显缺失；（5）在安全防护上网络信息系统存在安全漏洞等。

（3）法律法规

《中华人民共和国个人信息保护法》第五十一条规定，个人信息处理者应当采取措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失。

（4）防范指南

1.企业应制定和完善个人信息保护的内部管理制度和操作规程

2.采用加密技术对存储和传输的个人信息进行保护

3.严格按照法律法规的要求收集和使用个人信息，避免非法获取和滥用用户数据。

人脸识别滥用
——强制“刷脸”须整治

（1）典型案例

某地游泳馆在更衣柜安装人脸识别设备，遭到用户投诉。网信部门与市场监管部门开展现场督查，发现商家在更衣室安装人脸识别设备与维护公共安全无关，督促商家就更衣室内安装人脸摄像头问题进行了整改，并对其运营主体进行了警告的行政处罚。经普法宣传，企业已认识到违法违规问题，将单独与用户签订授权人脸信息收集协议，并将在更衣室禁用人脸识别设备，改用发放芯片手环用于开柜。

第三部分 防范指南

（2）问题分析

部分体育场馆、培训机构、商场超市等经营场景以办理业务、提升服务质量等名义要求消费者接受人脸识别技术验证个人身份，既没有向个人告知处理敏感个人信息的必要性，取得个人的单独同意，也没有对收集的敏感个人信息采取严格保护措施，进行个人信息保护影响评估。

（3）法律法规

《中华人民共和国个人信息保护法》第二十六条规定：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。

（4）防范指南

1.商家或平台增强个人信息保护法律意识，不违法违规滥用人脸识别设备。

2.个人应提高警惕，增强隐私保护意识，使用前仔细阅读隐私政策和使用协议。

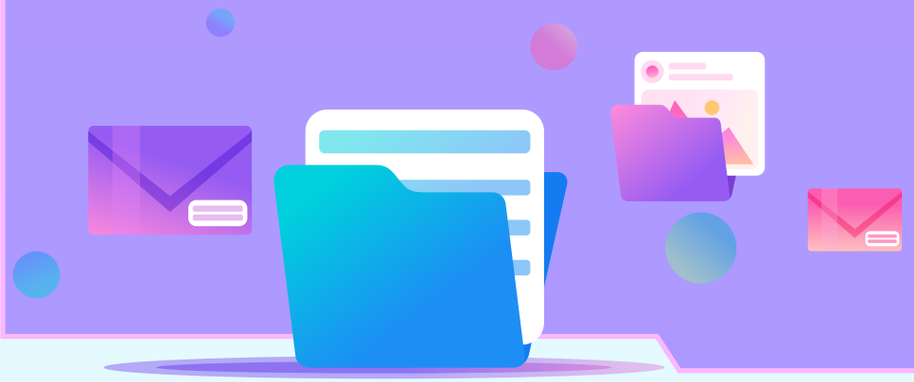
3.发现商家或平台存在侵害用户隐私的行为，及时举报，捍卫权利。

深度合成AI换脸

——保持警惕，确认核实，减少信息泄露

（1）典型案例

黄先生报警称其亲戚范先生收到一个与黄先生相同账号昵称和背景头像的“黄先生”好友验证信息，在通过之后，“黄先生”开启了视频通话，画面里正是黄先生本人在村里的场景，之后“黄先生”提出要向范先生借钱，范先生感觉这与黄先生日常的行为风格不符，便手机电话与黄先生，进行确认，最后核实发现是人像，声音，场景完全一致的AI视频仿冒行为。



（2）问题分析

不法分子通过搜集目标人物的亲友视频、照片、音频等素材，利用深度伪造技术生成逼真的AI换脸视频，合成音效模仿声音，以此冒充身份。

（3）法律法规

《互联网信息服务深度合成管理规定》第六条规定：任何组织和个人不得利用深度合成服务制作、复制、发布、传播法律、行政法规禁止的信息，不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等法律、行政法规禁止的活动。

（4）防范指南

1.提高技术认知，了解AI换脸等深度伪造技术的原理和可能的诈骗手段。

2.观察视频细节，注意观察视频中的人物是否有不自然的表情或动作，要求对方做一些特定的面部运动，如侧脸转向、面部遮挡、捏鼻子等，以辨识AI换脸的可能性。

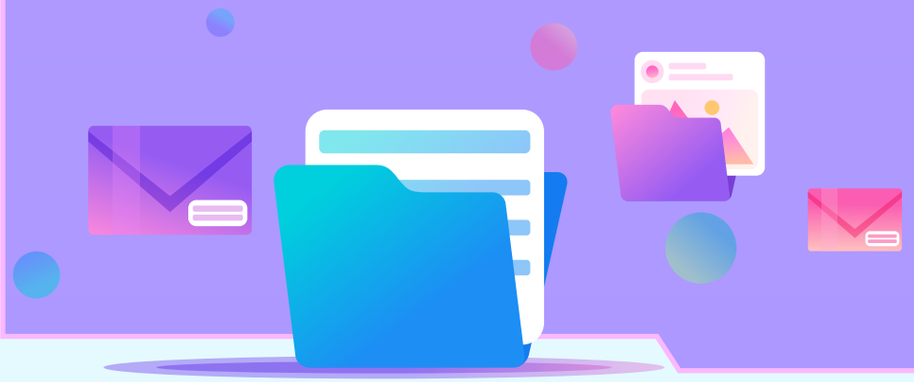
3.在未知来电时，先了解对方信息再开口，减少不必要的信息泄露。

网络暴力行为

——防范抵制举报，维护良好网络环境

（1）典型案例

王某某、林某某等人因不满法院判决结果，在网上多次发布恶意编辑制作的视频帖文，非法收集并公开发布多名法官个人信息，通过电话“轰炸”辱骂法官，引发网民炒作攻击，严重危害社会秩序。目前，王某某等人已被公安机关依法采取刑事强制措施，案件正在进一步侦办中。



（2）问题分析

近年来网络暴力违法事件频发，网络暴力信息泛滥，致使部分当事人“社会性死亡”甚至精神失常、自杀，严重扰乱网络秩序、破坏网络生态，造成恶劣社会影响。

网络暴力信息，是指通过网络以文本、图像、音频、视频等形式对个人集中发布的，含有侮辱谩骂、造谣诽谤、煽动仇恨、威逼胁迫、侵犯隐私，以及影响身心健康的指责嘲讽、贬低歧视等内容的违法和不良信息。

（3）法律法规

《网络暴力信息治理规定》第十条规定：任何组织和个人不得制作、复制、发布、传播涉网络暴力违法信息，应当防范和抵制制作、复制、发布、传播涉网络暴力不良信息。任何组织和个人不得利用网络暴力事件实施蹭炒热度、推广引流等营销炒作行为，不得通过批量注册或者操纵用户账号等形式组织制作、复制、发布、传播网络暴力信息。

（4）防范指南

1.理智判断，不主动发起或跟风评论、转发、传播网络暴力信息。

2.发现网络暴力事件，积极向平台举报相关行为。

3.平台及时处置涉网络暴力违规和不良信息及相关账号，引导用户文明互动、理性表达。

4.遭遇网络暴力时，保持冷静，收集证据，积极寻求平台保护，必要时可向法院起诉。