国家网络安全宣传周
China Cybersecurity Week

网络安全为人民
网络安全靠人民

2023年国家网络安全周
上海地区活动

宣传手册

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

第一部分：序言 PART ONE

网络安全为人民 网络安全靠人民

2023年国家网络安全宣传周上海地区活动

十个“坚持”：中国特色治网之道

坚持党管互联网；**坚持**网信为民；**坚持**走中国特色治网之道；**坚持**统筹发展和安全；**坚持**正能量是总要求、管得住是硬道理、用得好是真本事；**坚持**筑牢国家网络安全屏障；**坚持**发挥信息化驱动引领作用；**坚持**依法管网、依法办网、依法上网；**坚持**推动构建网络空间命运共同体；**坚持**建设忠诚干净担当的网信工作队伍。

——习近平总书记关于网络安全和信息化工作的重要指示

主办单位：中共上海市委网络安全和信息化委员会办公室

第二部分：法律法规 PART TWO

一：数据安全法 数据分类分级保护

法律法规

《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。

Q&A

Q：为什么要做数据分类分级？

A： 数据分类分级是数据安全治理的前提，是数据合规最核心的问题。只有对数据进行有效分类分级，才能避免一刀切的控制方式。在数据安全管理上采用更加精细的措施，使数据在共享使用和安全使用之间获得平衡。科学有效的数据分类分级可以让数据处理者能够根据数据的差异化制定不同的安全保护策略，同时，通过数据分类分级可以进一步明确数据资产，尤其是重要和敏感数据资产的分布和使用状况，以便实施有针对性的保护策略保障数据的安全。数据分类分级不是一成不变的，需要随着业务的变化而不断进行调整优化，以达到识别重要数据、保障数据安全的目的。

业务实践

2022年7月至12月，上海市网信办会同市政府办公厅成立试点工作组，开展数据分类分级、制定重要数据目录试点工作，涉及16家试点单位，形成了一系列工作成果。为推广试点工作经验，2023年上半年，“网信上海”公众号已发布11期成果分享文章。

二： 个人信息保护法 过度收集个人信息

法律法规

《中华人民共和国个人信息保护法》

第五条： 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。

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。

Q&A

Q：开展个人信息处理活动要注意哪些规范要求？

A：处理个人信息应当遵循合法、正当、必要和诚信原则，具有明确、合理的目的并与处理目的直接相关。处理个人信息应当在事先充分告知的前提下取得个人同意，个人信息处理的重要事项发生变更的应当重新向个人告知并取得同意。个人信息处理者不得过度收集个人信息，不得以个人不同意为由拒绝提供产品或者服务。个人有撤回同意的权利，在个人撤回同意后，个人信息处理者应当停止处理或及时删除其个人信息。

业务实践

2023年3月，上海市消保委对上海29家知名度较高的奶茶店、快餐店进行暗访。经调查发现，某网红知名连锁奶茶品牌每收到一笔订单，就可产生87条数据。截至今年3月其累计产生的数据超100亿条。其中，涉及消费者姓名、电话、收货地址经度纬度等敏感个人信息的达6.7亿条。6月，上海市网信办、市市场监管局共同启动“亮剑浦江·消费领域个人信息权益保护专项执法行动”，聚焦餐饮店、停车扫码、少儿学习培训等八个消费场景，重点整治没有隐私政策、利用互联网各种渠道非法买卖公民个人信息等八类问题。

三：网络安全法 网络安全保护义务 网络安全等级保护

法律法规

《中华人民共和国网络安全法》第五十六条：

省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

Q&A

Q：网络运营者不履行安全保护义务需要承担什么责任？

A：网络运营者，是指网络的所有者、管理者和网络服务提供者。网络运营者不履行网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

业务实践

上海市网信办全面履行互联网信息内容、网络和数据安全、个人信息保护等领域监督管理职责，进一步加大执法处罚力度，综合运用执法约谈、责令整改、处置账号、移动应用程序下架、关闭网站、行政罚款、处理责任人等多种手段，依法查处网上各类违法违规行为。据统计，2022年全年共约谈网站平台和自媒体119家，下架移动应用程序342款，关闭违规账号1043个，会同市通信管理部门关闭网站70余家。

四：密码法 密码技术应用

法律法规

《中华人民共和国密码法》

第六条： 国家对密码实行分类管理。

密码分为核心密码、普通密码和商用密码。

第七条： 核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级。

核心密码、普通密码属于国家秘密。密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。

第八条： 商用密码用于保护不属于国家秘密的信息。

公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

Q&A

Q：《密码法》的管理对象有哪些?

A：作为《密码法》的管理对象，密码包括密码技术、密码产品和密码服务。

密码技术，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术。

密码产品，是指采用密码技术并以加密保护、安全认证的产品，即承载密码技术、实现密码功能的实体。

密码服务，是指基于密码专业技术、技能和设施，为他人提供集成、运营、监理等密码支持和保障的活动，即基于密码技术和产品，实现密码功能，提供密码保障的行为。

业务实践

2022年10月，人力资源社会保障部发布《中华人民共和国职业分类大典（2022年版）》，新增2个密码职业，即密码技术应用员（职业编码4-04-04-06）以及密码工程技术人员（职业编码2-02-38-13），均被标注为数字职业。新职业的发布将有效带动密码职业人才培养评价，促进密码科技创新和产业发展。

五：关键信息基础设施安全保护条例 认定标准

法律法规

《关键信息基础设施安全保护条例》第二条：

关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

Q&A

Q：关键信息基础设施安全保护有哪些基础保障措施?

A：根据《条例》规定，一方面，保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。另一方面，国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

业务实践

2023年5月21日，国家互联网信息办公室网络安全审查办公室依法对美光公司在华销售产品进行了网络安全审查。审查发现，某公司产品存在较严重网络安全问题隐患，对我国关键信息基础设施供应链造成重大安全风险，影响我国国家安全。

网络安全审查办公室依法作出不予通过网络安全审查的结论。按照《网络安全法》等法律法规，我国内关键信息基础设施的运营者应停止采购美光公司产品。

来源：https://mp.weixin.qq.com/s/BEX4nl_S11tZaPZTDCExHQ

六：未成年人保护法 “网络保护”专章

法律法规

《中华人民共和国未成年人保护法》第六十八条：

新闻出版、教育、卫生健康、文化和旅游、网信等部门应当定期开展预防未成年人沉迷网络的宣传教育，监督网络产品和服务提供者履行预防未成年人沉迷网络的义务，指导家庭、学校、社会组织相互配合，采取科学、合理的方式对未成年人沉迷网络进行预防和干预。

Q&A

Q：对未成年人网络成瘾问题，《未成年人保护法》做了哪些要求？

A：针对未成年人网络成瘾的问题，《未成年人保护法》规定，网络相关管理机构要定期开展防沉迷教育，指导家庭、学校采取科学、合理的方式对未成年人沉迷网络进行预防和干预，并明确规定任何组织或者个人不得以侵害未成年人身心健康的方式对未成年人沉迷网络进行干预，要求网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当针对未成年人使用其服务设置相应的时间管理、权限管理、消费管理等功能，提出网络游戏服务提供者不得在每日二十二时至次日八时向未成年人提供网络游戏服务。

业务实践

2023年6月28日，上海市网信办会同市文明办、市检察院、市文旅局执法总队举办“清朗守护·为你而来”上海市未成年人网络保护系列主题发布活动，正式启动“清朗浦江·2023年暑期未成年人网络环境整治”专项行动。重点聚焦有害内容隐形变异、网络欺凌、隔空猥亵、网络诈骗、不良内容、网络沉迷、新技术新应用风险等涉未成年人突出问题，开展集中整治，拦截清理侵害未成年人身心健康的网络信息，全面压缩有害信息隐形变异的生存空间，坚决遏制侵害未成年人权益的违法行为，进一步提升学习类APP、儿童智能设备等专属产品服务信息内容安全标准，有效解决网络沉迷问题，营造有利于未成年人健康安全成长的网络环境。

七：数据出境安全评估办法 事前评估

部门规章

《数据出境安全评估办法》第三条：

数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。

Q&A

Q：哪些情形应当申报数据出境安全评估？

A：《办法》规定了应当申报数据出境安全评估的情形，包括数据处理者向境外提供重要数据、关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息、自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息以及国家网信部门规定的其他需要申报数据出境安全评估的情形。

业务实践

自2022年9月1日起开展数据出境安全评估相关工作，上海网信办已开通电话咨询专线，解答咨询电话近4500通；在官方账号”网信上海“发布实务问答2次；会同重要功能区管委会、重点领域行业主管部门召开数据出境安全评估政策系列宣讲会10余场，面对面服务属地企业近650余家。

八：生成式人工智能服务管理暂行办法 生成内容进行标识

部门规章

《生成式人工智能服务管理暂行办法》

第九条：提供者应当依法承担网络信息内容生产者责任，履行网络信息安全义务。涉及个人信息的，依法承担个人信息处理者责任，履行个人信息保护义务。

提供者应当与注册其服务的生成式人工智能服务使用者（以下称使用者）签订服务协议，明确双方权利义务。

第十二条：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。

Q&A

Q：《生成式人工智能服务管理暂行办法》的适用范围是什么？

A：《生成式人工智能服务管理暂行办法》规定，利用生成式人工智能技术向中华人民共和国境内公众提供生成文本、图片、音频、视频等内容的服务，适用本办法。

业务实践

2023年8月15日，《生成式人工智能服务管理暂行办法》正式施行。当日，上海市网信办面向各相关企业、机构召开宣贯培训会，会上对办法的出台背景、技术发展与治理、服务规范与合规义务、监督检查和法律责任、合规义务等开展了详细宣贯，回应企业关切，指导企业合规发展生成式人工智能业务。

九：汽车数据安全管理若干规定（试行）汽车数据安全管理情况报送

部门规章

《汽车数据安全管理若干规定（试行）》

第十条：汽车数据处理者开展重要数据处理活动，应当按照规定开展风险评估，并向省、自治区、直辖市网信部门和有关部门报送风险评估报告。

第十三条：汽车数据处理者开展重要数据处理活动，应当在每年十二月十五日前向省、自治区、直辖市网信部门和有关部门报送以下年度汽车数据安全管理情况：

（一）汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式；

（二）处理汽车数据的种类、规模、目的和必要性；

（三）汽车数据的安全防护和管理措施，包括保存地点、期限等；

（四）向境内第三方提供汽车数据情况；

（五）汽车数据安全事件和处置情况；

（六）汽车数据相关的用户投诉和处理情况；

（七）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全管理情况。

Q&A

Q：什么是汽车数据、汽车数据处理、汽车数据处理者？

A：规定所称汽车数据，包括汽车设计、生产、销售、使用、运维等过程中的涉及个人信息数据和重要数据。
汽车数据处理，包括汽车数据的收集、存储、使用、加工、传输、提供、公开等。
汽车数据处理者，是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

业务实践

为规范汽车数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，促进汽车数据合理开发利用，根据《汽车数据安全管理若干规定（试行）》，上海市网信办每年组织开展年度汽车数据安全管理情况报送工作。报送范围是注册地为上海的开展重要数据处理活动的汽车数据处理者，包括汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等。

十：《互联网直播服务管理规定》 网络生态

规范性文件

《互联网直播服务管理规定》第三条：

提供互联网直播服务，应当遵守法律法规，坚持正确导向，大力弘扬社会主义核心价值观，培育积极健康、向上向善的网络文化，维护良好网络生态，维护国家利益和公共利益，为广大网民特别是青少年成长营造风清气正的网络空间。

Q&A

Q：网络直播有哪些禁区？

A：不得利用直播从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人合法权益、传播淫秽色情等法律法规禁止的活动，不得利用互联网直播服务制作、复制、发布、传播法律法规禁止的信息内容。

业务实践

2023年5月8日，网信部门针对某直播平台存在的色情、低俗等严重生态问题，派出工作组进驻该平台开展为期1个月的集中整改督导。对此，该平台表示，将积极配合工作组的检查和指导，认真按照监管要求深入开展内容整改等工作。

第三部分：网络安全防范指南 PART THREE

一、木马病毒“钓鱼”邮件

不明邮件不打开 警惕病毒和木马

犯罪分子将木马病毒包装成正常邮件中的链接或附件，恶意欺诈受害者。在受害者下载软件或是接收邮件时，将病毒木马植入手机或电脑，破坏或篡改用户数据和个人信息。

典型案例

2023年6月12日，四川省某公司财务人员王先生收到一条关于增值税发票的陌生电子邮件。王先生未察觉到异常，随之在电脑上点击邮件链接、并下载了一个压缩包，解压之后却发现只有一串英文字母，此时，王先生以为只是有人发送了“错误”的发票，便没有将此事放在心上。没想到数天后，王先生的“老板”在微信上发来消息，要求其向某公司账户进行大额资金转账，见对方头像、姓名与自己老板的一模一样，王先生并未对其身份产生怀疑，在没有通过电话进行核实的情况下，先后向对方提供的对公账户转账470余万元，事后才惊觉被骗。

防范指南

1.谨慎点击不明来源邮件的链接

2.使用杀毒软件，定期查杀木马

3.涉及转账业务、敏感信息时要多方求证

二、网络交友陷阱

**网络交友别轻信
莫把骗局当爱情**

在互联网上，不法分子打着交友名义，通过培养感情获取信任，以此骗取受害者金钱。

典型案例

2020年6月，高某与被害人刘先生通过在一起玩某大型网络枪战游戏而相识，在线上聊天互动过程中，高某编造了虚假身份信息，并隐瞒自己真实的婚姻状态，与刘先生建立“恋爱”关系。2020年7月至2021年6月间，高某以家人看病、同事随礼等虚假理由向刘先生索要钱款，刘先生先后向其转账共计人民币22万余元，高某将绝大部分钱款肆意挥霍于某网络平台上。2023年2月25日，高某被民警抓获归案，到案后向办案机关交代了自己的犯罪事实。

防范指南

1.不轻信通过网络认识的陌生人，对其身份及时核实

2.网络交友若涉及金钱转账、博彩赚钱等行为，应提高警惕、立刻拉黑

3.如果发现被骗，一定要保存好银行流水、对方账号等相关证据，及时报警求助

三、智能网联车安全

**车联技术智能化
安全防护需强化**

智能网联车是车联网与智能技术的有机结合。随着智能网联车应用范围变广，也面临着远程攻击、恶意控制、隐私保护、数据安全等方面的安全问题。

典型案例

2022年5月6日，一位汽车博主发布了一条视频，该博主在行车记录仪的界面内可以看到同样拥有该品牌汽车的车主用户列表，点击任意一个用户，就能够加载其行车记录仪的画面，这引发了网友关于智能网联车用户隐私泄露的讨论。事后，该汽车品牌做出回应，称该功能属于车队出行、车路协同系统的组成部分，出厂时默认关闭，需用户确认才能开启。事发后第二天，该功能被该汽车品牌关闭。

防范指南

1.购买智能汽车的消费者要注意个人信息的录入与授权

2.涉及智能汽车的企业应该按相关法律保护客户隐私，提升车联网安全防护能力

四、“伪装”共享充电宝

共享充电需谨慎
警惕意识要常有

不法分子恶意投放植入木马病毒的共享充电宝，欺骗受害者用其充电，以盗取个人信息。

典型案例

2020年12月19日，广州市民陈女士租用了商场里不明品牌的共享充电宝，充电大概半个小时之后，就接到某陌生男子电话，对方竟清楚地知道她的银行卡还剩多少贷款没还。对方声称，如果陈女士不马上还贷款的话，会影响她明年的信用额度。该男子要求陈女士按照他的提示把五千元汇至其指定账户。陈女士转账以后，对方便把她拉黑了，陈女士随后马上报警。警方表示，此类“不明”充电宝里很可能安装了一些木马程序，会窃取手机信息。

防范指南

1.使用共享充电宝时，当手机出现是否“信任”提示时，请保持警惕

2.选择正规品牌的共享充电宝，不随意使用无品牌充电宝

3.安装手机安全防护软件，以防御恶意程序攻击

五、虚假二维码陷阱

不扫不明二维码
天上不会掉馅饼

诈骗者通过中奖信息、资源分享等幌子吸引受害者扫描虚假的二维码，从而盗取其敏感数据或金钱。

典型案例

2023年7月，家住上海市民孙女士收到了一个陌生快递，快递盒内有一个手机支架，一份落款为“某宝联盟”的邀请函，和一张带有二维码的刮奖券。孙女士刮开奖券后，发现自己中了10元红包和当季水果。扫描刮奖券上的二维码后，孙女士被所谓的“客服”拉进一个聊天群，领取了红包及水果后，群主开始在群里派发刷单任务。孙女士第一次尝试了充值300元的任务，获利450元；等第二、三笔刷单任务做完，已经充值了7000多元，却迟迟没有收到返利，孙女士才意识到自己被骗。

防范指南

1.不贪图小便宜，不扫描来历不明的二维码

2.需扫描二维码付款时，要确认缴费渠道是否正规

3.警惕恶意转账投资、刷单等骗局

六、企业信息泄露

主体责任落实好
数据泄露隐患少

企业因业务需求，收集大量个人信息，但由于自身网络安全系统不完善或是为了获利故意造成的信息泄露。

典型案例

某大型国际信托有限公司项目经理，利用任职便利，采取“撞库”等方式获取某银行个人征信系统用户名和口令，通过其所属国际信托有限公司与该银行之间进行专线互联的终端机，数次非法登陆该用户个人征信系统，查询并下载保存他人征信报告共计100份。

防范指南

1.企业开展数据处理活动时应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取处置措施

2.企业发生数据安全事件时，应当按照规定及时告知用户并向有关主管部门报告

七、网络暴力行为

网络暴力危害大
不评不转不参与

基于互联网，对受害者进行侮辱、诽谤等，并对当事人的隐私权、人身安全权及其正常生活造成威胁或不良影响的行为。

典型案例

2022年，郑同学拿着某高校的研究生录取通知书，希望给正在病床上的爷爷一个惊喜。她将这一幕拍成照片和视频发到社交平台上，照片里的她留着粉色中长发。谈及染头发的初衷，她说希望毕业照上的自己是明媚而鲜艳的，但这一帖子却引发了网友各种谣言，污蔑郑同学从事不正当职业、质疑她学历的真实性，对她进行网络暴力。令人心痛的是，郑同学被网络暴力逼至轻生。

防范指南

1.积极举报网络暴力行为，理智上网

2.不清楚事件原委时，不跟风评论转发，保持互相尊重

3.在遭遇网络暴力时，应保持情绪稳定，收集好证据后可向法院起诉

八、账号密码盗取

密码设置要复杂
不同账号有区分

骗子通过钓鱼网站、木马病毒、密码破解器等不同手段获取受害者密码，受害者密码越简单，风险越大。

典型案例

2020年5月至2021年11月，被告人张某在某社交平台购买了大量的个人邮箱账号及密码，利用这些个人信息，通过某游戏平台扫号器撞库盗取公民的某游戏平台游戏账号和密码，出售其盗取的某游戏平台账号、密码，从中获利。经鉴定，张某出售Steam账号113笔，共计收入人民币30829元。

防范指南

1.密码设置可以增加符号或大小写字母，密码越复杂，安全性越高

2.建议不同平台设置差别化的账号密码，增强账户安全性

九、人工智能AI诈骗

防人工智能诈骗
保个人信息安全

犯罪分子利用人工智能技术合成受害者熟人或亲人的声音、图像或视频，以获取受害者信任，从而诈骗金钱。

典型案例

2023年4月20日中午，郭先生的好友突然通过微信视频联系他，自己的朋友在外地竞标，需要430万保证金，且需要公对公账户过账，想要借郭先生公司的账户走账。基于对好友的信任，以及通过视频聊天、随之轻信对方身份，在走账环节，郭先生在未核实430万是否到账之前，就将钱款转至对方提供的银行账户。之后，郭先生拨打好友电话，才知被骗。骗子通过AI智能换脸和拟声技术，佯装好友对他实施了诈骗。

防范指南

1.不过度公开人脸、指纹等个人生物信息

2.若涉及大额汇款等业务，务必多方面核验对方身份

3.提高安全防范意识，如受骗应及时报警

十、网络购物陷阱

网络购物要谨慎
陌生渠道不转账

骗子通过虚假购物链接、折扣活动、客服售后等不同形式的诈骗手段盗取受害者个人信息或是骗取其金钱。

典型案例

2023年7月2日，王女士的弟媳李女士在某网络平台购物后申请退货，很快便有自称是平台客服人员致电李女士，要求其缴纳保证金后方能退款。李女士因自己的手机软件设置受限，便借用王女士的手机根据“客服”要求下载某会议助手软件，并向“客服”提供王女士的银行卡号、身份证，发送银行卡验证码。很快，王女士的手机收到短信提醒：其在农业银行卡中的30余万元存款已从定期转为活期，看到短信的王女士大惊失色，意识到可能遭遇网购骗局，情急下报警求助。最终在警察帮助下冻结了银行卡。

防范指南

1.不在非官方的平台或链接中填写个人信息

2.警惕不通过官方购物平台、私下联系客户的客服人员

3.谨慎将银行卡、验证码等敏感信息提供给可疑客服人员