国家网络安全宣传周
China Cybersecurity Week

2025 陕西省第十二届国家网络安全宣传周

THE 12TH CHINA CYBERSECURITY WEEK IN SHAANXI PROVINCE

网络安全为人民 · 网络安全靠人民

国家网络安全宣传周
China Cybersecurity Week

12TH

2025年陕西省
第十二届国家网络安全宣传周

THE 12TH CHINA CYBERSECURITY WEEK IN SHAANXI PROVINCE

·网络安全为人民 网络安全靠人民·

前言 PREFACE

2025年国家网络安全宣传周于2025年9月15日-21日举行，主题是“网络安全为人民，网络安全靠人民——以高水平安全守护高质量发展”，全国各省（直辖市、自治区）同步开展。陕西省第十二届国家网络安全宣传周由省委宣传部、省委网信办、省教育厅、省公安厅、省通信管理局、省总工会、共青团陕西省委、省妇女联合会和中国人民银行陕西省分行等九部门联合举办。将深入宣传《网络安全法》《数据安全法》《个人信息保护办法》《关键信息基础设施安全保护条例》等法律法规，《未成年人网络保护条例》《网络暴力信息治理规定》《促进和规范数据跨境流动规定》《互联网政务应用安全管理规定》等政策文件。开展相关宣传活动，编写发放宣传资料，推动媒体、社会团体广泛开展宣传普及、推进关键信息基础设施保护、大数据安全、个人信息保护等工作，通过展览、专题讲座、知识竞赛等多种形式，以及报刊、电台、电视台、网站等传播渠道，普及网络安全知识，提升全社会网络安全意识和防护技能，全面加强网络安全保障体系和能力建设，不断打造网络安全工作新格局。

“没有网络安全就没有国家安全，没有信息化就没有现代化”。网络安全和信息化已经成为事关国家安全、经济社会安全和国家发展的重大战略问题，要求我们必须贯彻以人民为中心的发展思想，本着对社会负责、对人民负责、对国家负责的态度，发展好网信事业、治理好网络空间、守护好这个亿万民众共同的精神家园，让互联网更好地造福人民。

活动介绍

活动时间

2025年9月15日 - 21日

主题日活动

9月16日，校园日
9月17日，电信日
9月18日，法治日
9月19日，金融日
9月20日，青少年日
9月21日，个人信息保护日

举办单位

省委宣传部、省委网信办、省教育厅、省公安厅、
省通信管理局、省总工会、共青团陕西省委、省妇女联合会、
中国人民银行陕西省分行

重要活动

网络安全宣传周开幕式、网络安全博览会、
网络安全专题演讲会、网络安全主题日活动、网络安全进基层、
“网络安全大讲堂”宣讲活动、网络安全线上知识竞答、
网络安全微视频征集

网络安全金句

网络安全对国家安全牵一发而动全身

没有网络安全就没有国家安全，没有信息化就没有现代化

网络安全和信息化是一体之两翼、驱动之双轮

网络空间是亿万民众共同的精神家园

网络安全为人民 网络安全靠人民

网络空间不是“法外之地”

互联网核心技术是我们最大的“命门”

维护网络安全不应有双重标准

中国是网络安全的坚定维护者

共同构建网络空间命运共同体

网络安全法律法规

2017.6.1 起施行 **《中华人民共和国网络安全法》**

旨在保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，对中国网络空间法治化建设具有重要意义。

2020.1.1 起施行 **《中华人民共和国密码法》**

旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，是中国密码领域的综合性、基础性法律。

2021.9.1 起施行 **《中华人民共和国数据安全法》**

旨在规范数据处理活动，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。

2021.9.1 起施行 **《关键信息基础设施安全保护条例》**

旨在建立专门保护制度，明确各方责任，提出保障促进措施，保障关键信息基础设施安全及维护网络安全。

2021.11.1 起施行 **《中华人民共和国个人信息保护法》**

旨在保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用。

2024.1.1 起施行 **《未成年人网络保护条例》**

旨在营造有利于未成年人身心健康的网络环境，保障未成年人合法权益。

2025.1.1 起施行 **《网络数据安全管理条例》**

旨在规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。

日常办公用网规范

1.办公环境安全

纸质文件妥善保管

放在抽屉等不易暴露的位置
打印过程中不离开
及时带走文件
丢弃时用碎纸机销毁

离开时电脑要锁屏

防止办公文件泄密
被误操作或损坏

会议安全防范四种情况

对会议室进行安全检查，防止监控和窃听
确认参会人员身份，防止外部人员混入
重要会议禁止拍照、录音等行为
会后及时清理纸质资料、多媒体设备存档

2.设备安全

U盘使用要查杀

- 个人U盘不插入工作电脑，工作U盘不插入个人电脑
- U盘使用前要先查杀一下，不使用来历不明的U盘
- 禁用计算机的自动运行功能，阻止U盘自动运行

设备维修/报废要检查

- 设备要设置密码、指纹、面部识别等，适当给予查看权限
- 设备替换/报废，设备内信息要清除，可恢复至出厂模式

3.通讯安全

建议使用高级别社交软件

不在开放环境讨论工作细节

重要、敏感文件要加密

注意传输安全

4.移动办公安全

通过零信任或VPN远程接入访问内网资料

免费WI-FI不乱蹭

以免掉入黑客陷阱

防弱口令攻击

案例说

某一单位使用的办公系统及网站管理员登陆采用弱口令，且未采取初次登录必须更改密码或强制所设密码强度等保护措施，导致单位存储的用户个人信息被黑客采取撞库方式窃取，导致大量客户信息泄露。

1.“密码”是怎样被破解的？

如果黑客认识你

- 他可能会直接猜测你的“密码”是你的生日、手机号码等
- 也可能直接进入你的账户，回答你设置的问题用于找回“密码”

如果黑客不认识你

- 常用的策略就是，暴力破解
- 也可能会尝试最常见的“密码”组合，直到成功访问

2.看看你的口令属于哪个等级？

密码：弱	密级：中等	密级：强
abc 仅由小写字母组成	a2c 字母+数字	a2!x 大小写字母+数字+符号
1-6 仅由字符组成	1******8 至少有8个字符	8+ 8个字符以上的长度
年+月+日 名字、生日或其他普通名字	AbC 大小写字母都有	B!gd05 包含合成短语
单词 字典里的单词	@2! 数字+符号	定期换密码
重复旧密码 重复以前用过的密码	不是字典里单词	

3.如何设置安全性更高的“密码”？

6步“密码”设置法！

第1步

不要过短，最好大于8位数

第2步

使用一句话的缩写可以作为基础“密码”
例如:“吃葡萄不吐葡萄皮”的缩写为“cptbtptp”

第3步

加上数字可使基础“密码”更复杂
“密码”增强为“2025cptbtptp”

第4步

加上符号可进行强化
“密码”增强为“2025cptbtptp?”

第5步

使用大小写进一步强化
“密码”增强为“2025CPTbtptp?”

第6步

创建一个规则，在不同的网站使用不同的“密码”
例如:微博+“密码”为“WB2025CPTbtptp?”

4.“密码”使用安全小贴士

不要一码多用，不使用常见单词、名字、纪念日等作为“密码”

重要账户单独设置，重要“密码”要定期更换

注意公共设备登录安全

采用多方验证

不要向任何人透露“密码”

防社工攻击

案例说

黑客冒充单位内部信息部门人员，通过微信添加人事部门工作人员为好友，以统一安装“补丁包”为理由，要求该工作人员下载安装。此“补丁包”实际为远控木马，工作人员安装后，系统被远程控制，单位信息被盗取。

1.社工攻击的常用手段

假冒身份或机构进行欺骗

攻击者会伪装成合法的身份，例如银行、政府机构和公司的工作人员等，通过电子邮件或者短信等方式，诱骗受害者揭露出个人或机构的敏感信息。

钓鱼攻击

攻击者通过电子邮件、短信或者社交网络等媒介发送虚假信息，引诱用户登录到假冒的网站，从而窃取用户的账户和密码等信息。

偷袭攻击

与普通的钓鱼攻击不同，偷袭攻击是一种目的性更强的攻击方式。攻击者会针对某一个特定的个体或组织进行攻击，通过伪造相应的信息获取目标信息。

直接沟通攻击

攻击者通过电话或者面对面的方式直接与受害者联系，利用技巧性的语言或其他手段，混淆受害者的思路，诱骗其泄露敏感信息。

社交工程攻击

攻击者通过社交工具、社交网络等渠道，收集受害者的信息，掌握对方的喜好、兴趣等，再制定个性化攻击计划，诱骗受害者泄露敏感信息。

2.社工攻击如何进行?

目标确认：利用人性的弱点找到人群中容易上当的目标。过分信任他人、同情心泛滥、好奇心爆棚、贪图小利等，这些都是容易被恶意利用的性格特点。

信息收集：未经销毁的票据存根、随处丢弃的快递包裹、网上注册的各种账号、论坛发表的各种言论、朋友圈共享的各种图片，都会导致个人信息泄露。

信任建立：利用各种伪装和欺骗技术与目标建立联系。各种通信软件、美颜软件、声音处理软件让攻击者成功隐藏自己。

陷阱设置：利用各种信息网络技术，采用钓鱼网站、钓鱼短信、诈骗电话、仿冒热点等方式，全方位、多角度进行陷阱设置。

利益获取：通过设置的各种陷阱，攻击者可进行后台流量分析获得用户账号密码，进一步挖掘得到个人或单位秘密，直接获取受骗者的钱财等。

3.个人用户如何防范社工攻击?

- ✔ 如发现了异常情况或接到可疑电话或电子邮件，或是发现个人信息可能被窃取或泄露，应及时向上级或安全团队汇报。
- ✔ 在接收到可疑请求时，要采取切实措施、多维度来核实对方的身份和信息，防止冒充熟人。
- ✔ 对于工作或个人帐户，不要随意提供用户名、密码、银行卡号码等敏感信息。
- ✔ 在日常工作中，保持警觉，切勿轻易点击或下载可疑的链接或文件，避免使用公共无线网络等不安全网络环境，并且定期备份重要数据。

4.单位如何防范社工攻击?

- ✔ 提高工作人员的安全意识：加强辨别社交工程攻击的常见方法，例如钓鱼邮件、Smishing（短信诈骗）、USB 网络攻击等，提高警惕性。
- ✔ 使用多层身份验证技术：使用多种认证因素来确认用户身份，例如密码、指纹、面部识别和硬件令牌等。这样可以防止攻击者使用窃取的凭证或身份信息登录系统。
- ✔ 规范并加强审批流程：设置流程审批制度，并确保流程审批环节必须由特定人员完成，避免在没有得到上级批准的情况下操作单位财务或机密信息。
- ✔ 加强单位内部网络的保护：在单位网络中设置防火墙、反病毒软件和入侵检测系统，及时监测并阻止恶意攻击。

防钓鱼邮件

案例说

某单位的财务主管收到了一封疑似来自领导的电子邮件，请求他尽快给一个供应商付款，并附上一份看似合法的发票。由于该主管此前曾经收到过类似的电子邮件，并没有多想就付款了。然而，这是一封黑客冒充的钓鱼邮件。

1.典型的钓鱼方式

恶意链接或附件

通过钓鱼邮件，引导目标点击或打开恶意链接或附件

冒充领导、朋友

发送恶意链接或恶意指令

仿冒网站

通过仿冒网站，如gogle.com、sinz.com等，获取敏感信息

利用热点事件

通过Email、论坛、博客等网站利用热点事件批量发布恶意软件和链接

利用聊天工具

通过微信、QQ、短信等聊天工具发送恶意链接

含恶意链接的广告

在搜索引擎、中小网站投放含恶意链接的广告

钓鱼邮件是什么？

在诸多的钓鱼手段中，钓鱼邮件颇受关注。钓鱼邮件是指黑客伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件、点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动。

2.如何识别钓鱼邮件

识别发件人地址

钓鱼邮件的发件人地址经常会进行伪造，比如伪造成本单位域名的邮箱账号或者系统管理员账号。

识别收件人地址

如果发现所接收的邮件被群发给单位内大量人员，而这些人员并不是工作常用联系人或同一工作组织内人员，那么就需要警惕，有可能是钓鱼邮件。

识别发件的日期

公务邮件通常接收邮件的时间在工作时间内，如果收到邮件是非工作时间，需要提高警惕。比如，凌晨 3 点钟。

看邮件标题

大量钓鱼邮件主题关键字涉及“系统管理员”“通知”“订单”“采购单”“参会名单”“历届会议回顾”等，收到此类关键词的邮件，需提高警惕。

看正文措辞

对使用“亲爱的用户”、“亲爱的同事”等一些泛化问候的邮件应保持警惕。同时也要对任何制造紧急气氛的邮件提高警惕，如要求“请务必今日下班前完成”，这是让人慌忙中犯错的手段之一。

识别正文目的

当心对方索要登录密码，一般正规的发件人所发送的邮件是不会索要收件人的邮箱登录账号和密码的，所以在收到邮件后要留意此类要求，避免上当。

识别正文内容

当心邮件内容中需要点击的链接地址，若包含“&redirect”字段，很可能就是钓鱼链接；当心垃圾邮件的“退订”功能，有些垃圾邮件正文中的“退订”按钮可能是虚假的。点击之后可能会收到更多的垃圾邮件，或者被植入恶意代码。可以直接将发件人拉进黑名单，拒收后续邮件。

识别附件内容

当心邮件中的附件信息，不要随便点击下载。诸如Word、Excel、PPT、PDF、RAR等文件都可能植入木马或间谍程序，尤其是附件中直接带有后缀为.exe、.bat的可执行文件，禁止点击。

防漏洞攻击

案例说

黑客利用某单位APP（手机应用程序）安全漏洞，使用技术软件成倍放大存单金额，从中非法获利2800余万元，并非法获取了大量账户信息。

1.什么是漏洞攻击

漏洞，是指信息系统的软件、硬件或通信协议中存在的设计、实现或配置缺陷，从而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。打补丁，就是为了修漏洞。补丁是发现缺陷之后，另外编制的一个修复程序。系统不打补丁，就像家里不关门窗，很容易被入侵。存在漏洞的系统，安全软件也很难有效防护。

漏洞分类

[0day漏洞]

还没有可用补丁的安全漏洞

[Nday漏洞]

已发布了很久，可谓“地球人都知道”的古老漏洞

[1day漏洞]

刚刚公布补丁的漏洞。微软通常在每个月的第二个星期二发布系统补丁，称作Patch Tuesday，但常有黑客根据对补丁的分析而快速发现漏洞所在，称作Exploit Wednesday

2.防范建议

- 软件漏洞普遍，隔三差五发现 → 关注安全提醒，及时排查隐患
- 提示补丁修复，千万别嫌麻烦 → 操作系统、浏览器和其它应用软件，及时打补丁
- 关闭无用服务，卸载没用软件 → 减少暴露途径，提高安全基线
- 禁用危险端口，系统安全改善 → 开启防火墙，设置规则禁止对危险端口的访问

防软件供应链攻击

案例说

某机构多个系统源代码被黑客在暗网上售卖。黑客表示，通过供应链攻击拿到的源代码，而非网络被入侵。

1.供应链安全建设主要面临

- 漏洞处置、管理措施不足
- 责任界限不清晰
- 第三方组件风险
- 不安全的系统配置
- 安全事件通报不及时
- 产品和服务的组成透明性差等
- 脆弱的业务连续性和灾难恢复实践

2.供应链安全如何开始做

采购管理	开发管理	交付和运维管理
制定供应链安全相关的技术措施、管理措施，保证供应商所提供的组件是安全的，比如是否经过源代码检测，是否具备资质认证等。	定期对开源软件进行更新和安全查杀；通过安全威胁分析建模、静态安全测试、动态安全测试、模糊测试等安全机制保障自行软件开发的安全；对于外包软件开发的大阶段进行安全性检测；安全开发时所使用的数据应为非生产数据或脱敏后无法复原的数据，保证数据安全。	软件上线交付前，运营者需要进行渗透测试、漏洞扫描、配置核查等工作；日常运营及时更新软件、建立威胁情报机制、制定安全事件应急响应方案等。

防勒索

案例说

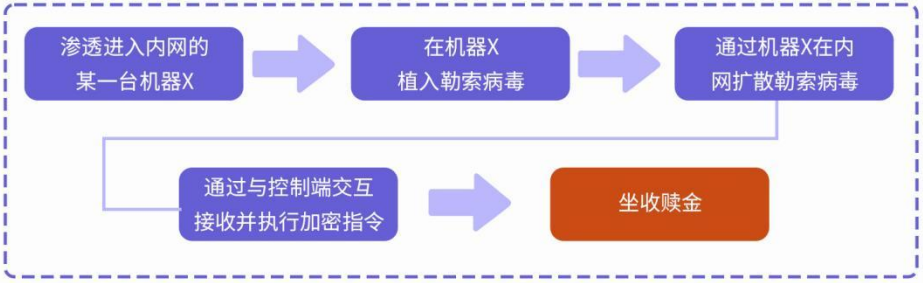
工作人员小李收到一封来自“高层领导”的邮件，声称是重要通知，附带压缩文件。他下载并运行后，电脑被锁定，屏幕上出现要求支付比特币的勒索信息。病毒迅速传播至单位内部网络，导致严重的数据泄露和业务中断。

1.什么是勒索病毒?

勒索病毒主要以邮件、程序木马、网页挂马的形式进行传播，利用各种非对称加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。勒索病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。

勒索病毒文件一旦进入本地，就会自动运行。接下来，勒索病毒利用本地的互联网访问权限连接至黑客的C&C服务器，进而上传本机信息并下载加密公钥，利用加密公钥对文件进行加密。除了拥有解密私钥的攻击者本人，其他人几乎不可能解密。加密完成后，通常还会修改壁纸，在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。勒索病毒变种非常快，对常规的杀毒软件都具有免疫性。攻击的样本以exe、js、wsf、vbe等类型为主，对常规依靠特征检测的安全产品是一个极大的挑战。

勒索过程如下:



2.常见的处置方法

某台主机在感染勒索病毒后，除了自身会被加密，勒索病毒往往还会利用这台主机去攻击同一局域网内的其他主机，所以当发现一台主机已被感染，应尽快采取响应措施，以下基础措施即使不是专业的人员也可以进行操作，以尽可能减少损失。

Step1

隔离中毒主机

物理隔离
断网，拔掉网线或禁用网卡，笔记本也要禁用无线网络。

逻辑隔离
访问控制:
可以由防火墙等设备来设置，禁止已感染主机与其他主机相互访问。

关闭端口:
视情况关闭135、139、445、3389等端口，避免漏洞攻击传播或RDP（远程桌面服务）被利用。
关闭端口可参考:
https://jingyan.baidu.com/article295430f1e84daa0c7e00501e.html
修改密码：尽快修改被感染主机与同一局域网内的其他主机的密码。

尤其是默认管理员（Windows下的Administrator、Linux下的root）密码，密码长度不少于8个字符，至少包含以下四类字符的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名等。

Step2

排查其他主机

隔离已感染主机后，应尽快排查业务系统与备份系统是否受到影响，确定病毒影响范围，准备事后恢复。

如果存在备份系统且备份系统是安全的，就可以将损失降到最低，也可以最快的恢复业务。

Step3

主机加固

主机感染病毒一般都是由未修复的系统漏洞、未修复的应用漏洞或者弱口令导致，所以在已知局域网内已有主机感染并将之隔离后，应检测其他主机是否有上述的问题存在。

系统漏洞可以使用免费的安全软件检测并打补丁。

检测后根据修复建议处理、联系应用提供商获取漏洞修复方案，或采用其他方式修复。

弱口令应立即修改，密码长度不少于8个字符，至少包含以下四类字符中的三类：大小写字母、数字、特殊符号，不能是人名、计算机名、用户名等。

防挖矿

案例说

某部门的一名网络管理员李某，利用职务之便，在单位服务器上私自安装了挖矿软件，试图通过挖取比特币等加密货币获利。由于挖矿软件需要消耗大量的计算资源和电力，李某的行为很快导致了单位网络性能的严重下降，导致日常办公受影响并且增加了翻倍的电费支出。

1.什么是挖矿

随着互联网经济的高速发展，通过数字货币获得高暴利的同时也为各行各业带来了更多的风险，虚拟货币“挖矿”本质是利用计算机的设备资源（如算力、带宽、硬盘存储等）去解决复杂数学运算的一个过程，从而产生基于区块链技术的去中心化虚拟货币的行为，产生的虚拟货币以比特币和以太坊为主。为了确保尽可能快地计算出问题答案，从而获取虚拟货币奖励，参与“挖矿”的“矿工”们需要投入尽可能多的算力资源，因此获取控制尽可能多的“矿机”成为增加“挖矿”收益的一个主要手段，因此挖矿病毒因为其隐蔽性和蔓延性已经成为了全球最主要网络安全威胁之一。

缩短计算资源设备的使用寿命：参与“挖矿”的设备，CPU、GPU、存储等长期处于高负荷运转状态，加速设备老化，并缩短设备的使用寿命。

浪费能源，增加电费支出：挖矿木马会加大计算设备的功耗，产生巨大能源消耗加大碳排放量，导致单位电力资源的消耗，还可能被增加惩罚性电价。

降低单位的生产效率：挖矿行为会导致计算资源设备的性能严重下降，影响业务系统正常运行，甚至导致业务中断或者崩溃，造成巨大的经济损失。

留置后门，衍生僵尸网络：失陷主机感染挖矿病毒后，会成为黑客控制的僵尸主机，成为内网横向攻击的跳板机，或者释放勒索软件索要赎金、导致数据安全事件。

违背国家能源战略：挖矿程序和挖矿木马会严重占据主机算力资源，干扰正常业务运营，同时消耗大量的电力，与国家能源战略、碳中和战略背道而驰。

2.常见的处置方法

Step1
查看进程

一般“挖矿”进程在运行时对CPU的占用率很高。可以查看当前运行的进程来看是否有CPU占用率较高的进程。

Step2
查看安全日志

如果病毒未干净的清理掉日志，可以在一些安全日志中找到踪迹。通过安全日志发现可疑的登录ip，进而继续寻找到病毒。

Step3
查看历史命令

如果历史命令未被清除，那么历史命令中也许有一些蛛丝马迹。通过历史命令找到下载样本，执行样本的指令。

Step4
查看定时脚本

如果挖矿病毒需要定时启动，那么在计划任务或定时脚本里面也会有一些信息可查。

1.提高网络安全意识

不使用不明来历的U盘、移动硬盘等存储设备、不要点击来源不明的邮件以及附件、不要下载来源不明的破解软件、不接入公共网络也不允许内部网络接入来历不明外网设备

2.安装杀毒软件

更新病毒库
进行杀毒

3.避免弱口令

避免使用弱口令
避免多个系统
使用同一口令

4.关闭应用服务

关闭Windows共享服务、远程桌面控制等不必要的服务

5.应用安装

不要安装不认识的、具有风险的应用；安装应用尽量到正规应用商店下载

数据防泄露

案例说

王某是某单位工作人员，她将大量人员的个人信息上传到公共网盘，以便查询。谁料网盘被攻击，被黑客成功获取了这些未加密的文档，包括大量人员的姓名、地址、电话号码、邮箱地址等敏感信息，并进行恶意攻击和诈骗，造成了严重的损失。

1.数据泄露的常见途径包括

网络攻击

如黑客利用钓鱼、勒索软件、分布式拒绝服务（DDOS）等攻击手段窃取敏感数据。

内外部人员泄露

如部分内部人员或外部人员可能出于个人利益、疏忽或报复心理，泄露单位的敏感数据。

数据存储不当

如数据未经过加密、备份或访问控制，导致数据违规存储或是设备丢失、损坏，导致的数据泄露。

单位监管不足

如单位缺乏严格的数据安全政策和流程，导致数据丢失。

数据的不当共享

如在与第三方共享数据时，没有严格的协议和访问控制，导致数据滥用或泄露。

2.数据保护小贴士

个人数据保护贴士

- 利用计算机的计划任务功能，定期自动备份
- 对备份进行加密，并存储在安全的、干燥的、隔离的物理空间
- 常测试你的备份，确保可以在需要的时候成功恢复数据
- 通过设置社交媒体信息访问权限保护个人信息
- 通过邮件或电话提供个人信息，尤其是医疗、金融类的敏感信息用虚化、模拟处理等方式隐藏敏感信息

单位数据保护贴士

- 最小化收集个人可识别信息，按需尽量最短保留这些信息
- 通过制定政策、开展培训引导工作人员正确保护数据
- 对于传输和存储的敏感数据进行加密
- 远程访问单位网络和特权访问系统时，通过多种方式认证
- 使用密码或PIN保护视频会议，只有受邀请者才能访问
- 使用虚化、模拟处理等方式隐藏单位敏感信息

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

举办单位

省委宣传部 省委网信办 省教育厅 省公安厅
省通信管理局 省总工会 共青团陕西省委
省妇女联合会 中国人民银行陕西省分行