常见数据泄露隐患及防范常识

【摘 要】本文介绍了常见的数据泄露及数据窃取场景、途径及手段，并结合近几年出现的典型案例，分析了办公、生活两种场景下常见的数据窃取与数据泄露风险隐患及防范常识，以期为公众提高信息安全防护素养提供借鉴。

【关键词】数据泄露 数据窃取 风险隐患

1 引言

大数据、云计算、物联网、人工智能等新技术的迅猛发展和广泛应用，为我们带来工作便利的同时，数据泄露与数据窃取渠道、手段也更加多样，安全风险持续加大。一方面，不法分子通过网络攻击重要部门窃取数据的活动越发猖獗；另一方面，国家秘密、工作秘密、个人隐私正面临着极大的数据泄露风险。

2 常见的数据泄露方式

近年来，数据泄露、窃取事件频频发生，从案发情况来看，导致数据安全隐患增加的原因主要有以下 3 种。

（1）数据窃取：数据窃取一般指外部人员利用技术手段主动窃取数据，或策反内部人员协助其达到窃取数据的目的。常见的数据窃取手段，如网络钓鱼、利用信息系统存在的配置缺陷或安全漏洞、结构化查询语言（SQL）注入攻击、植入间谍软件等，都是通过非法入侵他人系统窃取数据。

（2）数据泄露：数据泄露主要指因人员保密意识薄弱、疏忽大意造成数据泄露。此外，部分人员出于经济利益或报复情绪等原因，将敏感数据故意泄露或售卖。

（3）数据丢失：数据丢失一般指因数据发布或传输流程存在缺陷、数据存储介质丢失、维修或处置失误、不完善的数据定级制度及授权访问机制失控导致的敏感数据泄露。

3 办公场景中的数据泄露隐患及防范常识

近年来，手机、平板、电脑及其配备设备逐步成为辅助办公的重要手段，强大的功能丰富了数据获取、上传、存储、传输的途径，随之而来的数据泄露事件频繁发生，最常见的原因无外乎“为图省事”“事多疏忽”“事出紧急”等。

本节从移动存储设备、无线通信及网上办公等方面分析了办公场景中常见的信息泄露隐患，并提出对应的防范措施。

3.1 移动存储设备存在的安全隐患及防范常识

移动设备作为电子信息传递的载体之一，因其体积小巧、便于携带、存储容量大、价格低廉等优势被人们广泛使用，但移动存储设备使用不当导致的信息泄露事件也频繁发生。据统计，移动存储设备交叉使用造成的数据泄露占比达一半以上，让人细思极恐。

移动存储设备在使用过程中，极易被植入“摆渡”“轮渡”等木马病毒程序，这些病毒的传播过程类似于生物病毒传播过程。当移动存储设备插入一台被植入木马的计算机后，其就成为

病毒携带者，一旦将该设备接入内网计算机，就会导致内网计算机感染木马病毒。当该移动存储设备再次连接联网计算机时，木马病毒会非常隐蔽地将窃取的数据发送给窃取者，造成数据泄露。另外，公私混用、管理困难、设备丢失等，也成为移动存储设备潜藏的安全威胁。

为防止移动存储设备泄露数据，切实保障数据安全，严禁在涉密领域和非涉密领域混用移动存储设备；定期查杀病毒、木马等恶意代码，防止其蔓延传播；严禁将已报废的涉密移动存储介质转为非涉密载体继续使用，并对已报废的涉密移动存储介质要进行彻底销毁；对移动存储设备中的数据进行加密、备份，防止设备丢失后数据被窃取。

3.2 无线通信中存在的安全隐患及防范常识

随着无线通信技术的迅速发展，无线键盘、鼠标、智能穿戴设备等得到广泛应用。相较于传统的有线连接方式，无线设备没有繁杂的线缆，不仅方便携带，更不会因距离限制人们使用。但是无线连接设备在受到人们的喜爱的同时，也引起了不法分子的兴趣，逐渐成为不法分子窃取数据的重要途径。

由于无线通信信号是在空间中自由传播的，无论是移动通信、卫星通信，还是微波通信等，任何人都可以通过相应的接收装置接收到通信信号，并经处理后还原通信内容。因此，从传输媒介的角度来看，无线通信系统是一个开放式系统，其安全保密隐患比有线通信更为突出。常见的无线通信窃密风险主要有空中

监听、定位追踪、重放攻击、注入攻击、信号截取、木马病毒攻击等。通过在无线设备中嵌入木马模块，或截获无线设备发出的未加密的信号，即可达到窃取数据的目的；定位追踪会导致手机等移动终端持有者暴露自己的位置，造成位置泄露；木马病毒会远程隐蔽开启手机等移动终端的通话功能，窃听用户周围环境语音信息。这样无线设备便成了“贴身间谍”，安全隐患极高。

为防范风险，不要随意接受他人赠送的无线设备，如需使用，通过正规渠道如官方网站购买；不使用无线设备处理涉密文件或敏感文件；不将无线设备带入涉密（重要）会议或活动场所；不在通信中涉及国家秘密、工作秘密。

3.3 网上办公潜在的安全隐患及防范常识

近年来，随着智能手机的全面普及和移动网络的广泛覆盖，使用移动终端进行在线办公的单位呈现跨越式增长，加之新冠疫情的影响，移动办公需求显著提升。但用手机拍摄、即时通讯工具传输敏感文件时有发生，通过手机图文识别程序转换敏感文件屡见不鲜，使用互联网网盘、邮箱存储、处理敏感文件屡禁不止，互联网移动办公已然成为数据泄露、数据窃取的“高发地”。

对此，建议提高日常保密防范意识，坚持“上网不涉密、涉密不上网”，严禁在连接互联网的计算机或手机上存储、处理国家秘密、工作秘密；不使用微信、微博、短信、邮件、云盘、网盘等互联网途径存储、处理、传输国家秘密、工作秘密；不得在涉密场所使用手机进行视频通话、拍照、上网、录音和录像；居

家办公期间办理涉密公务，必须在能够确保安全保密的场所进行；涉密文件、涉密计算机、涉密光盘、涉密U盘、涉密移动硬盘等涉密载体和涉密存储介质严禁带回家中使用；不在普通电话通话中谈论涉及国家秘密、工作秘密的事，不与家人谈论涉密事项。

4 日常生活中的数据泄露隐患及防范常识

现如今，我国移动互联进程持续加快，生活中的数据窃取、数据泄露事件时有发生，防不住的数据窃取、止不住的意外泄露，已成为网络时代的安全风暴，认清安全保密风险隐患，并采取措施防范数据泄露刻不容缓。

4.1 即时通讯类社交媒体数据泄露及防范常识

当前，即时通讯类社交媒体走进千家万户，抖音、快手、小红书、微信朋友圈等更是成为当下“网民”分享生活的重要途径，深受人们的喜爱。据统计，社交网络的用户每天会分享约30亿张照片。

就在前段时间，一段关于“照片定位”的视频引爆社交网络，视频中的网络大神通过分析照片中的信息推理出拍摄者的所在位置。在赞叹其高超技术之外，这样的游戏实际上也提醒我们，在网络上随意发布的照片信息十分容易被追踪，如果每张照片的发布算作一次隐私的泄露，那这样的情况将每天发生上亿次。因此，在社交平台上意外泄露数据逐渐成为信息泄露的一大风险隐患，在个人社交媒体上分享的生活照、传递的信息及发布的图片

很有可能就成为黑客手中的工具，对单位、企业及个人的敏感信息造成严重威胁。

对此，应注意不在网上“晒”隐私类信息，如出生日期、火车票、飞机票、个人位置、度假计划、孩子照片及姓名、工作相关信息等。如果发现个人信息已经被泄露，可以向互联网管理部门、工商部门等行业管理部门和相关机构投诉举报。另外，建议关闭社交媒体软件中位置显示、“摇一摇”“搜一搜”等可能泄露个人信息的功能；非必要不建立聊天群组等，如需建立，落实审批建群、规范群名、建档备查、验证成员身份等工作。

4.2 钓鱼攻击导致的数据泄露风险及防范常识

钓鱼攻击指通过给攻击目标发送包含恶意网站网址的邮件，通过诱导访问网站来获取目标的个人信息或密码等，从而盗取数据资产。钓鱼攻击最常见的方式是钓鱼邮件，攻击者通过使用伪造的邮件地址，假冒银行、电商、社交网络等引诱用户点击附件或链接，并在虚假的网站上诱导用户输入账号、口令等数据，从而获取用户个人信息或数据资产。随着人们安全防范意识的提升，钓鱼攻击形式变得更加隐蔽，手机红包钓鱼、无线 Wi-Fi 入侵劫持等方式让人防不胜防。

面对更有迷惑性的攻击方式，我们要主动学习、了解常见钓鱼攻击知识与关键特征，慎重点击“可疑”链接，格外警惕任何涉及个人敏感信息的操作，及时识别并避开钓鱼陷阱。针对邮件钓鱼，点击前应仔细检查发件人的邮件地址及邮件内容是否存在

可疑之处，并注意附件内容；针对通讯、短信钓鱼，建议尽量避免接听来自“未知号码”的呼叫，并及时使用应用程序显示来电、屏蔽未知电话号码的短信内容；针对 Wi-Fi 孪生钓鱼，在连接热点时注意手机警告，不贸然使用不熟悉的网络热点；为防止克隆网站钓鱼，建议直接访问相关软件或与电商客服沟通，需格外警惕以“商品促销或折扣”为主题的链接。

5 结语

综上所述，我国科学技术的迅猛发展及广泛应用推动着信息数据安全管理工作越来越规范，然而，国家秘密、工作秘密及个人隐私的安全问题仍然时有发生。因此，持续加大信息数据保护力度，提升人们安全防范意识迫在眉睫。

（原载于《保密科学技术》杂志 2023 年 4 月刊）

（来源：国家保密局 http://www.gjbmj.gov.cn/n1/2024/0711/c411145-40275876.html）