我被控制了，「不是我操作的」

为了方便在家也能登录实验室电脑处理数据，有人安装了远程控制软件；为了赶上项目进度，有人将远程控制工具接入内网环境进行操作。远程控制在提供便捷的同时，也带来了更大的安全保密隐患。

资料图片

警惕潜藏“窃密通道”

远程控制软件是一种允许用户通过网络从一个地方远程操作另一台计算机的程序，通常集远程桌面、远程开机、远程管理、内网穿透于一体，在远程运维、远程协助等场景中应用广泛。远程控制软件本身并非恶意程序，但可能因为安全漏洞、恶意操纵和不规范使用而造成风险。

随意下载不明软件。个别用户出于免费或便捷的考虑，可能会选择下载一些来源不明的小众远程控制软件。这类软件没有正规安全资质，缺少加密防护机制，攻击者可通过在软件中预先植入木马“后门”，在安装阶段即引入窃密程序，静默抓取设备内的文件、聊天记录、浏览痕迹等信息，持续向外传输数据，实现隐形窃密。

非必要开放高权限。个别用户为图便利，在远程控制时，默认开放全部设备权限，且全程不监督操作过程。攻击者可通过漏洞破解设备密码，长期在后台潜伏，持续拷贝、篡改、窃取信息。更危险的是，多数远程控制软件只要完成设备绑定、登录授权，即便单次远程连接断开，后台权限依然保留，造成长期隐患。

小心开启“方便之门”

远程控制泄密隐蔽性强，大多不会留下明显操作痕迹。被发现时，可能已造成隐私曝光、财产损失、工作泄密等严重后果。广大网民特别是涉密单位工作人员要提高警惕、规范选用。

支持官方严选。在选用远程控制工具时，建议注意其来源的合规性与可靠性，尽可能选用官方正版软件。这类软件在安全性上更有保障，能有效降低数据外泄风险。

做好“物理隔离”。严禁在涉密计算机、涉密服务器、涉密存储设备上安装远程控制软件，不以“临时调试”“远程协助”等为由在涉密终端上开放远程桌面功能或开启远程登录端口。

定期开展排查。定期检查设备安装软件、后台授权列表，一旦发现陌生远程控制工具、未知授权记录，应立即卸载、关闭权限，修改设备密码，并查杀病毒。必要时，可留存证据，并向有关部门报告。

（摘自5月31日微信公众号“国家安全部”）

“马上回来”就没事？

日常办公时，大家难免都会遇到因临时性事务短暂离开工位的情况，短则几分钟，长则数小时。有的人抱着“马上就回来”的心态，在短暂离开期间对涉密材料、办公区域疏于管理，看似问题不大，实则暗藏失泄密风险。

麻痹大意造成失泄密

国家保密部门披露案件显示，某部门工作人员取回涉密文件后，随意摊放在桌子上，其间多次离开办公室。一外来办事人员趁办公室无人，顺手将桌上的涉密文件拿起翻阅，并使用其办公室的复印机复印三份后将原件放回原位。案件发生后有关部门第一时间进行处理，相关人员受到严肃党纪政纪处分。

某央企一名副总经理刘某在阅办涉密文件过程中，未落实保密管理规定，阅看完毕后未将装有涉密文件的传阅盒锁入保密柜中。其间刘某多次离开办公室，均未锁闭房门，导致涉密文件丢失。经核实，丢失文件属于国家秘密，相关责任人受到严肃处理。

离开工位要做四件事

广大涉密岗位工作人员，临时离开工位时要做好这四件事：

清桌面。临时离开工位时，要清理桌面、收拢涉密资料，杜绝文件外露、载体乱放，防止无关人员随意窥视涉密内容。

关屏幕。临时离开工位时，涉密电脑要及时锁屏，杜绝无防护运行。同时，应定期更换密码，规范涉密计算机使用管理，避免涉密信息外泄。

锁柜门。临时离开工位时，应将涉密文件、物品及时存入保密柜，做到“入柜即落锁”。

锁好门。若办公室内无人，应及时锁闭办公室门，杜绝无关人员随意进出、逗留观望，严禁外来人员独自留在办公区域。

国家安全机关提示

“马上回来”不是放松保密的借口，广大涉密岗位工作人员要养成日常保密的好习惯，做到人离桌清、屏闭、柜锁、门严。如发现危害国家安全的有关可疑线索，可通过12339国家安全机关举报受理电话、网络举报受理平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

（摘自5月29日微信公众号“国家安全部”）

“数据犯罪”知多少

人工智能、物联网、大模型等前沿科技正重构着人类社会的运行逻辑。与此同时，数据安全面临的风险与日俱增。

数据窃取花样多

国家安全机关工作发现，境外间谍情报机关往往通过“买”“聘”“诱”“骗”等方式开展数据窃取，对我国家安全构成严重威胁。

“买”

他们可能通过向境内相关人员有偿咨询、打包购买等方式，获得相关行业领域数据。

“聘”

他们可能招聘航空、船舶等爱好者作为“志愿者”，通过在特定区域架设专门设备，非法搜集、获取我航空、船舶、高铁、气象等重点领域信号数据。

“诱”

他们可能通过代理公司，向我境内相关行业领域推广其技术和设备，诱导上传关键数据。

“骗”

他们可能以小利诱骗境内人员进行精确定位、图像拍摄，并标注上传我敏感地理坐标信息。

“数据犯罪”有哪些

近年来，我国出台《数据安全法》等法律法规，构筑起维护国家数据安全的法治体系。特别是《刑法》明确了涉及数据安全的犯罪行为及其刑罚，为打击数据安全犯罪提供了强有力的法律保障。

跨境非法传输数据

为间谍组织及其代理人提供对方需要的数据资料，且明知对方是间谍组织及其代理人，还向其提供需要的数据资料的，适用《刑法》规定的“间谍罪”。跨境传输数据，属于国家秘密或情报的，适用《刑法》“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”。

跨境传输数据，不属于国家秘密或情报，但被鉴定为商业秘密的，适用《刑法》规定的“为境外窃取、刺探、收买、非法提供商业秘密罪”。

境内非法采集、传输数据

持有、传输的数据资料、信息经鉴定为国家秘密的，适用《刑法》规定的“非法获取国家秘密罪”“非法持有国家绝密、机密文件、资料、物品罪”。

未获取国家秘密，但在搜集信息或展开调查过程中使用法定的窃听、窃密设备的，适用《刑法》规定的“非法使用窃听、窃照专用器材罪”。通过技术手段非法侵入计算机信息系统获取数据的，适用《刑法》规定的“非法侵入计算机信息系统罪”“非法获取计算机信息系统数据罪”。

以窃取或其他方法获取，向他人出售、提供公民个人信息，情节严重的，适用《刑法》规定的“侵犯公民个人信息罪”。（摘自5月30日微信公众号“国家安全部”）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com