你的心该有「一道墙」

坚固的保险柜、加密的网络、森严的门禁、层层审批的流程……保密管理工作在多种举措下已日趋完善全面。然而，仍有大量的失泄密案例警示我们，心理层面的漏洞往往成为泄密的“催化剂”，导致保密工作“一失万无”。


资料照片

失泄密背后的心理“暗礁”

无知心理。对保密规定一知半解，对信息的涉密属性缺乏辨识能力，这种因无知心理导致的泄密既荒谬又普遍。比如，不清楚信息的涉密属性就随意拍照留存，使用公共网络传输敏感信息等，都是无知心理状态下的高危操作。

侥幸心理。抱着“仅此一次”“问题不大”“都是为了工作”的想法，在规章制度面前心存侥幸，在原则问题上打折扣，以“下不为例”“这也没出事”自我安慰，然而每一次的“破例”都埋下了风险隐患。

盲从心理。“别人都这么做，我怕什么”，看到别人违规操作不加制止反而效仿，发现保密隐患认为“都这么操作”而置之不理，甚至当作“潜规则”。涉密操作中的盲从心理同样危险，会让小问题变成大漏洞。

炫耀心理。掌握“内部”“劲爆”的信息可能会给人带来莫名的优越感，但是把涉密接触条件当“个人本事”，在社交场合“爆料”“分享”一些工作内容，以此显示自己的“重要性”和“知情权”，打造“消息灵通”人设，殊不知信息扩散如决堤洪水，将造成难以挽回的损失。

冷漠心理。“事不关己高高挂起”“多一事不如少一事”，认为保密是保密部门、领导干部的事，发现他人有违规苗头不愿提醒，看到保密隐患不想报告，认为泄密只是新闻上的案例，跟自己没关系。这种无所谓态度，最终损害的是集体与自己的利益。

靶向施策共筑保密心理防线

要正视保密管理工作中的心理“暗礁”，重视心理因素带来的潜在风险，多措并举，构筑坚固心理防线。

常敲警钟，莫嫌“老生常谈”。系统、定期地开展保密教育，明确保密范围，划分保密责任，用“身边事”警示“身边人”，从根本上消除认知盲区，让“不可为”成为共识。

冷静刹停，管住“一念之差”。严格执行保密规章纪律，划清“一次也不行”的刚性底线，多问自己“这能说吗”“合规吗”，让“禁区”成为涉密操作中的潜意识。

破除侥幸，织密“天罗地网”。建立全流程溯源机制，涉密内容“谁发的找谁”“谁转的找谁”“谁管的找谁”，对违规行为严肃追责，让每则涉密文件、信息的流向实现可控、可查、可溯。

国家安全机关提示

“心中有畏，方能行有所止”。守护国家秘密，人人有责，广大公民尤其是涉密单位工作人员，务必严守保密纪律，切勿使用非涉密信息系统、非涉密信息设备处理、存储任何涉及国家秘密或敏感信息的数据。如发现相关失泄密可疑线索，可通过12339国家安全机关举报受理电话、网络举报平台（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。

炼就火眼金睛，识别问题包裹

截至2025年11月30日，我国快递业务量已突破1800亿件，这个连接千家万户的“小包裹”，正在成为亟需筑牢的国家安全“隐形防线”。今天，我们就一起来辨识那些可能隐藏在包裹中的风险。

“李鬼”包裹：夹带的非法内容。反动宣传品的“变装术”令人防不胜防！看似普通的文化衫，却印着特殊数字组合；表面是贺卡书籍，却夹带着非法内容。这就是典型的“反宣品”伪装，这些非法宣传材料，就像披着羊皮的狼，伪装成“土特产”“小礼品”“活页单”，试图利用你的信任混入快递网络，在潜移默化中危害国家安全。

“无声”暗战：小心流通的“秘密”。看似普通的文件，内容却夹带私货。境外间谍情报机关人员常将“秘密”“机密”文件伪装成商业合同，或将地质勘探数据加密后刻录成光盘或其他电子存储载体混入普通包裹。在破获的某境外间谍案中，境外间谍情报机关人员正是通过快递渠道进行涉密文件的非法传输。

谍器暗渡：伪装的间谍工具。微型摄像机伪装成纽扣、窃听器藏在玩具里、GPS追踪器嵌入行李箱把手……这些专业的间谍设备，近年查获量较之前不断增长。某快递网点发现寄件人要求“能够避开监控飞行”的无人机包裹，经执法人员检查，在其机舱内藏有微型探测设备，该设备可实时传输5公里范围内的电磁信号数据。

生物危机：物种的非法出入。一些往来境外的快递、包裹，成为生物流通的“秘密通道”。某口岸在截获的活体甲虫体内，一次性就检查出3种境外输入的病原体。某次专项行动中查获伪装成“茶叶”出口的稀有药材种子，经检测发现其DNA序列与某国家级保护区特有物种高度相似，一旦流失，将对我生态平衡和生物安全造成威胁。

国家安全机关提示

维护寄递安全是全体从业人员、企业和监管部门的共同责任，要严格落实收寄验视、实名收递、过机安检三项安全制度。如发现可能存在危害国家安全的违禁物品、可疑人员或者行为，可通过12339国家安全机关举报受理电话、网络举报平台（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。

热点不能随意蹭！

公共Wi-Fi，如同数字生活中的便捷桥梁，让我们能随时随地接入网络世界，处理公务、联络亲友、休闲娱乐。然而这座看似平坦的桥梁之下，却可能暗藏着数据窃取与网络攻击的汹涌暗流。

为何公共Wi-Fi不能随意连接

恶意Wi-Fi窃密

个别境外间谍情报机关会在特定区域（如政府机关周边、涉密单位附近）设置恶意Wi-Fi，一旦公职人员、特别是涉密人员不慎连接，其设备内的敏感信息、通讯录、邮件往来等可能会被全程监控，甚至造成国家秘密泄露。

网络攻击跳板

不安全的公共Wi-Fi是黑客攻击的重要渠道。用户设备在连接此类Wi-Fi后，可能被暗中植入恶意程序，在不知情情况下被远程操控，给个人财产和社会公共安全带来威胁。

认知操纵画像

连接不安全公共Wi-Fi时产生的浏览记录、位置信息、输入内容等个人数据，容易被别有用心者非法收集分析，用于构建用户画像、识别群体倾向，攻击者可借此精准投放虚假信息、煽动对立情绪，长期侵蚀社会共识与主流价值观，对社会稳定和意识形态安全构成潜在威胁。

如何有效防范？请牢记以下核心原则

关闭自动连接功能

关闭设备的“自动连接Wi-Fi”功能，防止手机在用户不知情情况下连入恶意网络。在连接公共Wi-Fi前，请主动向场所工作人员核实、确认，确保连接到的是真实可靠的Wi-Fi。

避免进行敏感操作

在公共Wi-Fi环境下，不要登录隐私敏感账号，请勿进行网上转账、输入银行卡密码等高风险操作。尽量避免使用公共Wi-Fi处理涉及个人隐私等敏感事务。

安装更新防护软件

安装并及时更新防护软件，可以有效防止恶意软件攻击，保护设备安全。此外，使用虚拟私人网络等加密手段，让网络流量通过加密通道传输，也能有效防止用户数据被攻击者窃取。

国家安全机关提示

广大公民应自觉提升网络安全意识，不随意连接未知热点、不进行敏感操作、不点击可疑链接，筑牢个人防护屏障，净化网络空间环境，共同守护国家安全。如发现任何利用网络实施的间谍行为或可疑线索，请立即通过12339国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或直接向当地国家安全机关进行举报。

（均转自国家安全部微信公号）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com