国安部：警惕境外间谍窃密，这些日常场景别忽视

近年来，境外间谍机构通过隐蔽手段窃取国内涉密信息、商业机密及个人隐私的情况频发。国安部近期发布通告，明确要求公众提高防范意识，重点警惕伪装成商务合作、学术交流、技术服务的境外人员。以下从风险识别、应对策略及法律后果三方面展开说明。

境外间谍窃密常见手段有哪些？

境外情报机构主要采用三类窃密方式：技术渗透、人员策反和物理窃取。技术渗透方面，通过发送含木马病毒的钓鱼邮件（如伪造的政府文件或企业招标通知），诱导目标点击后植入窃听程序；人员策反则利用高薪聘请、学术合作等名义，逐步获取涉密人员信任；物理窃取常见于更换办公设备电池、窃听手机信号或植入微型摄像头。

日常场景中如何识别潜在风险？

1. 网络交互：收到标有特殊后缀的邮件（如`.gov.cn`或`.ac.cn`非官方域名），或要求提供密码、验证码的陌生链接，需立即隔离处理。

2. 商务接触：境外机构以"联合研发"名义要求调取企业数据库，或频繁索要员工身份证件复印件，存在信息泄露风险。

3. 设备异常：办公电脑频繁弹出境外IP地址的弹窗广告，或手机在无网络环境下自动连接未知Wi-Fi热点，可能被植入窃听模块。

| 风险场景 | 典型特征 | 应对措施 |

|---|---|---|

| 邮件钓鱼 | 邮件签名含非官方联系方式 | 使用企业级邮件网关过滤 |

| 设备替换 | 办公设备电池仓有未知胶水痕迹 | 立即断开设备电源并报修 |

| 社交工程 | 伪装成客户索要内部图纸 | 审批流程需增加双人复核环节 |

防范措施应如何具体落实？

1. 技术防护：对涉密设备安装国产加密软件，定期进行内存检测（建议使用`360企业版`安全扫描工具）。

2. 流程管控：建立"三不原则"——不随意安装境外U盘、不泄露验证码、不点击陌生链接。

3. 人员培训：每季度开展反间谍演练，重点培训财务、IT部门等敏感岗位人员。

法律后果与责任划分需注意什么？

根据《反间谍法》第二十七条，非法获取、出售或提供国家秘密的，可处三年以上十年以下有期徒刑

；情节特别严重的，最高可判处无期徒刑。2022年某外资企业员工因向境外传递军工企业生产数据，被依法判处有期徒刑七年并处罚金200万元。

FAQ：

1. 如何判断手机是否被植入窃听设备？

答：使用专业频谱分析仪检测2.4GHz频段异常信号，或送专业机构进行拆解检测。

2. 发现可疑情况后应如何上报？

答：立即拨打国安部举报专线12339，或通过"国家反间谍"APP提交证据。

3. 普通公民泄露个人隐私会承担法律责任吗？

答：若造成严重后果（如被境外机构利用从事危害国家安全活动），根据《刑法》第一百一十一条，可追究刑事责任。