间谍“套路”识破春招里的“情报试纸”

春回大地，生机盎然。春季招聘正是毕业生追逐职业梦想、开启人生新篇的关键时期。然而，有的“光鲜”岗位、“优厚”薪资，看似是人生进阶的捷径，背后可能隐藏着境外间谍情报机关精心布下的陷阱。在此提醒，广大毕业生在求职路上，要识破这些别有用心的“套路”，守护个人前程与国家安全。

“居家办公”画大饼，需警惕！

“远程居家办公，日薪800元，只需整理行业数据即可”“时间自由，参与课题研究，轻松躺赚”……这些诱人的招聘信息，可能是境外间谍情报机关精心设计的诱饵。

春招期间，境外间谍情报机关可能伪装成正规企业、调研机构等，发布“市场调研”“课题研究”等居家办公岗位，以远高于市场价的薪酬，招募求职学生开展收集窃取敏感信息等非法活动。求职学生请牢记：

拒利诱。对待遇远超行业标准的薪资承诺需保持警惕，理智辨别“高薪低门槛”“高回报易入门”等可疑岗位。

查资质。通过官方渠道多方核实用人单位资质，警惕来历不明、经营范围模糊的“可疑公司”。

辨真伪。对“重点课题”“重大合作项目”等招聘标签加强辨识，拒绝不明用人单位提出的信息采集、数据搜集等要求，避免落入“巧立名目”的陷阱。

“补充资料”无底洞，勿轻信！

“请提供详细实习资料”“填写完善项目内容，上传技术参数”……这些看似招聘单位常规的资料补充，可能是境外间谍情报机关的“情报试纸”。

春招季，招聘单位可能需要求职人员补充资料、完善简历，但若强制要求提供曾参与的军工单位、涉密科研院所等实习经历，或以核实、佐证等名义索要曾接触过的敏感数据，就有可能是境外间谍情报机关布下的“局中局”。求职学生请牢记：

不轻信。警惕无缘由地补充资料、提供信息等异常要求，求职时辨识对方真实意图。

不涉密。投递简历时不填写参与涉密项目经历、涉密单位实习经历等，避免透露此前接触过的敏感信息。

不侥幸。若察觉招聘单位及招聘人员有刺探敏感信息等可疑情况，应立即向国家安全机关举报。

“校友熟人”套近乎，要核实！

“我是你导师的校友，在某国际机构任职”“学长内推，只需带来实验室的数据即可”……这些看似亲切的熟人内推及介绍，可能是境外间谍情报机关“众里寻他”的惯用手法。

境外间谍情报机关深谙“人情攻势”，可能以校友、前辈等关系为伪装，主动靠近应聘学生，使其放松警惕，进而开展针对性的拉拢渗透。求职学生请牢记：

擦亮眼。对突然示好、过度热情的陌生前辈等需保持距离、审慎接触，警惕别有用心的拉拢渗透。

慎交往。求职中，应提高安全防范意识，与背景不明的招聘人员沟通交流时，不随意透露个人隐私、不轻信陌生邀约，遇到可疑情况及时核实、理智拒绝。

守底线。求职内推、资源交流走正规渠道，即使亲友相托，也应守住底线，不因人情往来放弃保密原则。

青年朋友们都对未来的职业发展充满期许，但不能让别有用心之人有机可乘。在这个充满机遇的春招季，广大毕业生若在求职中发现可疑人员渗透窃密等线索，可及时通过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。

军事机密泄露竟是因为它？

近日，某国发生一起因智能穿戴设备导致的军事机密泄露事件，引发全球关注。当时该国某重要军事装备正在执行任务，一名军官跑步时佩戴的智能运动手表持续记录并公开了高精度GPS数据，致使该军事装备实时位置等重要敏感信息泄露，给该国国防安全造成难以弥补的重大损失，也让智能穿戴设备的泄密风险再次走入人们的视线。

数据失守 挑战加剧

当前，各类商业APP通过获取用户的位置信息、终端设备、使用习惯等广告标识数据，能够精准构建用户画像，进而有效提升用户黏性和市场转化率。但部分商业公司大批量、长时段、全方位收集用户信息，可能会增加信息泄露风险。如果这些数据被别有用心之人加以分析，就会给国家安全带来威胁。

特殊身份暴露

境外间谍情报机关可能将智能穿戴设备数据，作为渗透策反的突破口，通过抓取各类数据，精准锁定涉密人员、公职人员、科研从业者等目标，直接危害国家安全。

涉密信息外泄

智能穿戴设备会持续采集位置、环境等数据，若在军事管理区、涉密科研院所、党政机关办公区等敏感区域使用，极易泄露涉密敏感信息。

隐私安全失守

智能穿戴设备采集的家庭住址、日常通勤、健康数据、消费轨迹等隐私信息，一旦被不法分子窃取，可能危害个人财产安全与人身安全。

多维防护 防患未然

智能穿戴设备本是便利生活的助手，但使用不当就会带来风险。我们要在享受科技便利的同时，绷紧安全之弦、守住保密底线。

严控使用场景，敏感区域“慎触碰”。

涉密人员及敏感岗位人员，要安全规范使用智能穿戴设备，避免运动轨迹标记出敏感坐标，危害国家安全。

严控权限开关，“精打细算”给权限。

定期审查智能穿戴设备的APP权限，遵循“最小必要”原则，对多数应用“仅在使用期间允许”定位，最小化运动日记、轨迹图的被访问权限，彻底关闭公开访问通道。

严控数据分享，织牢信息“防护网”。

审慎对待每一次运动成果分享，清除地理位置信息。注册时使用虚拟身份信息，不填写真实姓名、家庭住址、工作单位等隐私数据。定期删除APP内以及云端存储的运动历史记录、位置轨迹信息。

（均转自国家安全部微信公众号）

警惕“舌尖”上的泄密

餐桌并非“真空区”，谈笑亦有“红线纪”。身处涉密岗位的工作人员，一言一行都要格外注意。国家安全机关工作发现，有别有用心之人紧盯餐桌饭局，设圈布局、套取信息。面对间谍窃密活动，涉密岗位工作人员须时刻保持清醒，筑牢“舌尖”上的保密防线。

常见“舌尖”泄密情形

话题泛化失边界。个别涉密岗位工作人员在人员复杂的聚餐场景中，受恭维吹捧、酒精麻痹等因素影响，放松了对话题尺度的把控，为彰显自身工作价值或满足虚荣心，将工作内容作为闲聊谈资，随意谈论涉密项目进展、内部工作部署等敏感信息，造成国家秘密泄露。

刻意诱导入圈套。境外间谍情报机关人员可能假借联谊、请教、招商之名设宴款待，在推杯换盏间嘘寒问暖、拉近距离，进而旁敲侧击了解涉密敏感项目情况，步步深入套取涉密信息。

环境布设藏隐患。境外间谍情报机关人员可能在宴请环境中布设窃密网络，以提供方便为由，诱导涉密岗位工作人员携带涉密存储介质、涉密信息设备进入饭局，或诱导其通过该网络处理、传输敏感信息，借此窃取敏感信息数据。

筑牢“舌尖”保密防线

《保守国家秘密法》明确规定，禁止在私人交往和通信中涉及国家秘密。涉密岗位工作人员须将保密纪律内化于心、外化于行，认清餐桌泄密风险，坚决守好言谈边界。

赴宴之前严把关。不参加可能影响公正执行公务的宴请，不接受管理服务对象或利益相关方的吃请，不参加身份不明、背景不清的聚会。

开口之前先三思。不随意谈论国家秘密、工作秘密和内部情况，不随意谈论未公开政策、核心数据、人事安排等单位内部敏感事项。

风险苗头早报告。面对他人打探、诱导、拉拢时，要态度鲜明，敢于说“不”。发现可疑情况，要及时向所在单位报告，或通过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举报。

责任编辑/王睿卿 E-mail:fzbfyzk@126.com