境外间谍盯上贫寒学子

假借捐资助学之名『放长线钓大鱼』

近年来，境外间谍情报机关以“合法掩护非法”“公开掩护秘密”等方式，对我境内人员甚至是青少年实施拉拢渗透策反，手段卑劣、毫无底线。他们往往伪装成青少年身边的“好心人”“热心人”“贴心人”，在目标对象成长、学习、工作过程中施以潜移默化影响，妄图实现为其所用的目的，窃取我国家秘密、危害我国家安全。

一个熟悉的声音

一天，某重点院校大四学生小韦的手机响了。

“L老师，您好！”“小韦你好，最近还好吗？”“挺好，就是时间有点不够用，又得忙毕业论文，还得忙考公的事……”“你看现在的就业形势，啥都不如公务员稳当。考的是老师上次推荐的那个岗位吧？那可是重要部门，你可得加把劲，争取一次上岸，未来肯定前途无量。”“就是那个岗位，老师您放心，我一定全力以赴！”“好！老师等你的好消息。另外，今年的助学款已经打到你卡里了，注意查收。”“好，已经收到了，谢谢老师！您在国外也多保重身体，我这边工作定了马上告诉您。”“好！等你好消息！”

一段迟来的关怀

小韦是来自南方大山里的孤儿，自幼在福利院生活成长。从小学到高中，小韦勤奋学习、一贯品学兼优，后在当地有关部门的帮扶和社会爱心人士的资助下，顺利进入重点院校就读。不同于其他人从小学开始资助，“L老师”是在小韦以全县第一的成绩考上当地最好的高中后，才突然出现，“专程”到小韦的家乡提出要资助的。在与小韦见面后，“L老师”承诺每年资助小韦5000元，直至其大学毕业。此后不久，“L老师”便“移居”国外。

多年来，“L老师”会时不时从国外给小韦打电话，除了例行问候外，还经常向其布置调查问卷任务，让小韦协助开展田野调查、社会信息搜集汇总等工作任务，并额外支付酬劳。

小韦觉得学习之余顺便挣点生活费是一举两得的事情，便一直按照“L老师”的要求完成相关工作任务。

一个正确的抉择

小韦大学毕业后，在公务员考试中一路过关斩将，最终考入心仪的工作单位。他第一时间将这个好消息告诉了“L老师”。在小韦入职后，“L老师”不仅打电话关心问候的频率明显增加，而且经常向小韦打探我经济发展及政策制定方面的内部敏感信息，并以开展研究、撰写报告等名义，要求小韦提供一些涉密数据资料。

小韦一开始出于感恩之心，为“L老师”搜集提供了一些公开资料，但随着“L老师”索要的资料越来越关键敏感，部分内容还涉及国家秘密，有一次甚至直接向小韦提出需要红头涉密文件，小韦愈发觉得不对劲，便婉拒了对方的要求。回想起“L老师”的种种疑点，以及自己入职后接受的反间防谍宣传教育，小韦最终决定向国家安全机关反映“L老师”的情况。

后经国家安全机关查明，“L老师”的真实身份是境外间谍情报机关人员，多年来一直在我境内物色、培养像小韦一样出身贫苦、成绩优秀、具备较好发展前景的青少年，妄图“放长线、钓大鱼”。他们假借“捐资助学”之名，利用受助人员的“报恩”心理，怂恿其报考党政机关、科研院所或参军入伍，借此打入关键核心岗位，进而指挥其非法搜集窃取我内部敏感资料，开展危害我国家安全的间谍窃密活动。

国家安全机关提示

国家安全机关在依法严厉打击惩治间谍违法犯罪活动的同时，将持续加大宣传力度，着力提升全社会反间防谍意识和能力。广大人民群众如发现相关可疑线索，请及时通过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。

弱口令，高风险，速修改！

国家安全部提醒：

生活在数字化时代，网络已成为日常工作学习生活中不可或缺的重要部分，我们在不同的网站注册账号、设置密码，搭建虚拟世界中的私人空间。但如果密码过于简单，如连续数字、电话号码、姓名生日等组合形成的“弱口令”，不仅极易被猜中或破解，还有可能遭到境外黑客攻击，成为网络安全防护中最薄弱的突破口。弱口令的风险不止是造成个人隐私的泄露，更有甚者，会给一些重点涉密部门带来泄密风险。

现身境外论坛的内部数据

国家安全机关工作发现，在某境外论坛上出现我国某企业的内部数据，数据内容包含该企业多个合作客户姓名、身份证号、家庭住址以及手机号码等个人隐私信息，如落入不法分子手中将造成严重安全隐患。经核查，该数据之所以被窃取，是因为企业网络管理员在开展运维测试后，未及时删除测试账号，而该账号恰好具备管理员权限且口令极易猜解，为“admin+连续数字”，成为该企业信息安全维护的一大漏洞，一些客户的数据由此泄露。

频频异地登录的电子邮箱

某单位在其官网公布对外电子邮箱账号用于联络收信，为方便查阅历史邮件，该单位工作人员将所有邮件及附件长期存储于邮箱云空间，未定期进行清理。近期频繁出现异地登录告警，该单位随即向当地国家安全机关反映异常情况。

国家安全机关核查发现，该邮箱为单位公用邮箱，为方便工作人员使用，登录密码为单位对外办公的固话号码且长期未修改，导致邮箱密码被境外黑客猜解，进而邮件数据被窃取。

自动切换视角的监控摄像

某跨境物流公司位于我沿海港口，园区内装有大量摄像头用于监控物流运转情况。该公司员工小李发现，在午休及夜间，摄像头时常自动旋转，寻找并聚焦至停靠、出港的有关船只。小李立即向公司领导汇报，公司同时将此情况向当地国家安全机关报告。

国家安全机关上门查验发现，该公司监控系统的管理员账号密码为出厂默认的弱口令密码，数月前境外黑客开展密码“撞库”攻击，成功登录监控系统，获取了监控系统操控摄像头权限。境外黑客通过高清摄像头监控目标海域情况，给我国家安全带来风险隐患。

国家安全机关提示

数字化时代，有关单位和个人应提高信息安全意识，履行网络安全义务，增强网络防护，避免使用弱口令，防止数据被窃取、泄露，影响国家安全。

使用复杂密码。设置密码长度至少为8位，宜同时包含大小写字母、数字、特殊字符，提高密码的复杂度，不使用设备或账户初始密码及常见的弱口令密码。

定期更改密码。设置复杂密码后，并非一劳永逸，随着时间的推移，密码仍存在被破译的可能性。重要网络信息系统应定期（至少3个月内）进行密码更改，同时要避免数套密码轮换修改。

避免密码串用。在不同平台及系统避免使用相同的密码，防止一个密码泄露后其他系统被“撞库”攻击连带攻破，导致泄密面进一步扩大。

定期检查账户状态。计算机系统及网络账户通常具备安全审计功能，可查询历史异常记录，定期检查日志，及时发现账户异常行为，防止因密码泄露导致内部数据、信息被持续窃取。

加强技术防范措施。反间谍安全防范重点单位应当按照反间谍技术防范的要求和标准，采取相应的技术措施和其他必要措施，加强对要害部门部位、网络设施、信息系统的反间谍技术防范。在信息系统维护过程中若发现可疑的网络间谍线索，请及时通过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众号）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com