

“他就是我的理想型，我以为爱情照进了我的现实，但没有想到的是……”小宁坐在审讯椅上，手里攥着沾满泪水的纸巾，泣不成声地说到。近日，国家安全机关破获一起某机关单位工作人员坠入境外间谍情报机关工作人员情感陷阱，利用职务之便为境外窃取、非法提供国家秘密的案件。



资料照片

情为刃，迷心乱

境外间谍情报机关将感情渗透隐藏在正常公务活动下，精准利用部分单身人士的情感需求，构建“完美伴侣”人设，开展猛烈“爱情攻势”。殊不知，虚情假意的关心往往隐藏着处心积虑的窃密陷阱。

小宁博士毕业后入职某机关单

位，因为工作能力突出，多次受到领导表扬。然而，工作上的得意却难掩感情上的失意，原生家庭的不幸、爱情受挫的失落、背井离乡的寂寞，让她的情感世界始终蒙着一层灰色。一次公务活动中，小宁结识了某使馆外籍工作人员，该外籍人员迅速发现小宁情感的空虚，从关心生活到理解共情，逐步走进小宁的内心世界，成为了可以交换“秘密”的亲密伴侣。

多么痛的领悟！ 恋爱脑，

一寸密，一重劫

两人交往期间，该外籍工作人员以关心小宁工作生活为由，多次见面打探其日常工作，从简单的同事关系到办公室的布局再到处理的文件内容，逐步使小宁丧失警惕，泄露了大量敏感重要工作内容。随着交往的深入，小宁发现一旦未提供重要信息，就会遭到“男友”怠慢冷落。但此时

小宁已深陷情网，为维系二人感情，满足对方需求，她铤而走险，刻意打探、收集日常工作中接触到的国家秘密及内部文件，并将其作为每次约会时的“谈资”和感情“筹码”，非法提供给“男友”。

天网恢恢，疏而不漏。国家安全机关及时发现小宁的违法犯罪行为，掌握相关证据后果断收网，及时消除了泄密隐患，有力维护了国家秘密安全。在接受审讯时，小宁才得知，这位“完美男友”实为境外间谍情报机关工作人员，且早已娶妻生子，所谓的“爱情”都是他专业的伪装。但后悔已经来不及了，等待她的将是法律的严惩。

驻心墙，守国门

近年来，境外间谍情报机关利用“感情拉拢”实施间谍犯罪高发频发，当“温柔”被设为陷阱，当“温情”被用来算计，也警示我们真正的感情是真诚和包容，而不是索取和犯罪。广大人民群众特别是党政机关、国防军工、科研院所、高校等单位工作人员务必擦亮双眼、提高警惕，自觉抵制各种诱惑，打消不切实际的幻想，切实增强反间谍意识，筑牢维护国家安全的钢铁长城。

《中华人民共和国反间谍法》规定，参加间谍组织或者接受间谍组织及其代理人的任务，或者投靠间谍组织及其代理人，属于间谍行为。广大人民群众如发现有关可疑线索，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。

你的设备还在“保质期”吗？

办公室的路由器依然闪烁，客厅里的摄像头仍在转动，这些陪伴我们多年的设备，或许早已过了厂商支持的“保质期”，处于无人维护的状态。安全生命周期和设备生命周期的脱节，使得原设备中尚未修复的漏洞暴露，风险隐患也潜滋暗长。

无售后的网络“靶场”

停产设备因厂商终止技术支持服务导致其无法修复自身存在的安全缺陷，其固件、协议栈及应用程序中积累的漏洞永久暴露，如同一个不设防的“靶场”，轻易就能被黑客突破，因此成为境外间谍情报机关重点关注的目标。攻击者可通过自动化扫描工具识别开放端口及服务，利用已知漏洞发起定向攻击，直接获取设备控制权。

摇身一变成“帮凶”

当境外间谍情报机关利用漏洞入侵成功后，这些设备便不再是单纯的“受害者”，反而成了他们的“帮凶”。入侵者会以被控制的设备



资料图片

作为隐匿行动的中转据点，向外部网站或企业服务器发起攻击；还会悄悄扫描内网中的其他联网设备，窃取照片、文件、账号密码等敏感信息。

“小漏洞”演变成“大风险”

单一设备漏洞被突破后，威胁将随攻击深化呈指数级扩散，产生连锁反应。攻击者通过窃取设备存储的敏感数据、劫持设备网络权限

等方式，进一步挖掘内网其他系统的薄弱环节，威胁范围从单台设备逐步蔓延至关联网络、业务系统，甚至影响跨领域基础设施。最终，原本孤立的技术漏洞可能演变为数据泄露、服务瘫痪、生产中断的复合型安全事件，造成难以控制的系统性风险。

国家安全机关提示

面对电子设备“过保”存在的潜在风险，我们要增强安全防护意识，

掌握科学防护方法，筑牢国家安全防线。

给老设备“拆炸弹”，除患清源筑牢根基。定期通过设备官方网站查询路由器、摄像头、网关等联网设备生命周期，若设备已停产且长时间未更新固件，有条件可选用安全性更高的新设备进行替换，切实消除因漏洞暴露形成的“定时炸弹”。

给旧设备“拉闸门”，断链阻敌严守边界。若暂时未更换设备，要实施网络访问最小化原则，配置严格的访问控制权限，尽量使用本地存储替代云端同步，仅开放必要的服务端口，关闭远程连接等敏感服务，阻止设备访问核心业务网络或互联网，有效阻断其成为攻击跳板的可能路径。

给“活”设备“打补丁”，补漏堵缺固若金汤。即便设备未完全停产，也需持续关注厂商发布的固件更新和安全补丁，定期检查更新。对于仍在安全生命周期内但存在漏洞的设备，及时下载并安装修复程序，为设备穿上“防护衣”，防止安全威胁像“滚雪球”般扩散。

（均转自国家安全部微信公号）