小心掉进隐秘的『陷阱』

网恋交友、网络求职……

是志趣相投的“网友”？
是亲密无间的“恋人”？
是关怀备至的“朋友”？
是能解燃眉之急的“热心人”？
又或许，这些都只是“他们”设下的甜蜜“陷阱”……

网恋的诱惑，也许是危险的黑手

位于我国南方某滨海城市的大二学生小刘通过交友软件结识了一名自称“小敏”的“小姐姐”，经过几天的交谈，两人关系迅速升温。其间，“贴心”的“小敏”主动给小刘介绍了一份杂志社兼职工作，内容为到所在地港口拍摄游客和游艇照，每次可获数百元报酬。小刘想着既能赚外快又能博取“小敏”芳心，可谓是一举两得，于是欣然答应，先后两次拍摄了景区海边、游艇照片发给“小敏”，并按时收到了约定酬劳。之后，“小敏”进一步要求小刘到指定地点拍摄我军舰停靠和进出港情况，并要求其改用境外通讯软件，使用“暗语”联系。在双方多次“合作”后，对方为小刘购买了拍摄用的手机、电瓶车，还为其解决靠近军事基地的租房费用。

实际上小刘已经意识到了对方的间谍身份，但还是财迷心窍、心存侥幸。法网恢恢，疏而不漏，国家安全机关很快发现并依法制止了小刘的不法行为。鉴于小刘的违法行为被及时制止，尚未造成严重危害，国家安全机关依法未追究其刑事责任，但小刘自己的学习和生活还是受到了严重影响。

高薪的offer，可能是潜藏的骗局

临近毕业季，某高校学生小王通过手机求职软件投放了求职信息。不久，一家调查公司的“张总”联系了他。起初“张总”以海洋环境调查为名，要求小王为其拍摄海边游艇、船舶情况，并支付高额报酬。后来，逐渐引导小王前往军事敏感区域拍摄军机军舰情况。这一要求引起小王的怀疑和警觉，他立即停止和对方的联系，在老师的陪同下拨通了12339国家安全机关举报受理电话。

经证实，“张总”确系境外某间谍情报机关人员。事后，国家安全机关对小王的主动举报行为给予表彰、奖励，相关事件经媒体公开报道，在全社会引起广泛影响。

国家安全机关提示

境外间谍情报机关人员可能以交友“恋爱”、网络求职等行为方式，以收集文献资料、发放调查问卷、拍摄风景建筑之类为名目，以丰厚的酬金为诱饵，采取“漫天撒网，重点捕鱼”的战术，诱使涉世未深的青年群体为其搜集、窃取情报。一旦“上钩”，境外间谍情报机关就会采取威胁、利诱、讹诈等手段施加控制，难以轻易脱身。

国家安全，需要你我共同守护。如发现他人通过各种渠道收集涉密、敏感信息的可疑情况，请通过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反映，或直接向当地国家安全机关进行举报。（以上案例根据真实案件改编，人物均为化名）

想“钓”我？没门！

今天，网络平台早已成为人们工作生活的重要工具，普遍使用的电子邮箱也成了境外间谍情报机关网络窃密的重点目标。他们将我党政机关、涉密单位计算机网络作为窃密主渠道，“钓鱼”邮件便是他们实施网络攻击的惯用手法。

“钓鱼”邮件是什么？

“钓鱼”邮件是一种常见的网络攻击手段。攻击者通常会伪造发件人地址和邮箱账号，诱使目标用户点击恶意链接或下载恶意文件，窃取用户凭证和数据资料等敏感信息，甚至入侵控制相关终端设备。

常见手法有哪些？

境外间谍情报机关会预先搭建一个与目标电子邮箱高度相似的邮箱登录界面，并伪装成邮件服务商，向指定用户发送虚假的“高风险账户警告信息”邮件。待目标对象点击后，“高仿”登录界面便会弹出，账号密码一旦输入，便会被境外间谍掌握。

案例一：假扮官方实施欺诈

2021年，我国某涉密军工企业工作人员收到了一封伪装成邮件服务商警告信息的“钓鱼”邮件，受诱导点击后导致工作邮箱账户密码泄露。境外间谍情报机关通过该密码登录其电子邮箱，窃取了大量敏感工作资料。

境外间谍情报机关会预先搜集、分析相关电子邮箱用户信息，筛选出有价值的目标，并根据其关注的热点事件、工作事项或个人事务，“定制化”设计邮件标题、内容，以降低目标对“钓鱼”邮件的防范心理，诱使其下载恶意攻击性文件，实现“精准”窃密。

案例二：个性定制精准窃密

2019年，某市政府部门工作电子邮箱收到一封伪装成某县委办发来的电子邮件，附件为“干部年度考核审批”。工作人员出于对辖区机关单位的信任，未加核实便点击了邮件内伪装成附件的攻击性文件，造成邮箱中的内部资料被窃。

境外间谍情报机关还会利用盗取的个人账号进行窃密，通过“黑”进目标对象的电子邮箱或社交软件，向其好友、联系人等发送可能感兴趣的“钓鱼”邮件，利用其好友、联系人“不设防”的心理，达到窃取敏感信息或诱使下载恶意攻击性文件的目的。

案例三：窃取账号冒充身份

2020年，境外间谍情报机关预先控制了某地党校教授的邮箱，利用其教授身份向邮箱中的联系人发送主题为“某全会精神深度解析”的邮件，相关收件人点击查看后导致多个邮箱资料被窃。

防范应对怎么办？

网络“钓鱼”作为境外间谍情报机关实施网络攻击窃密的主要手段之一，有着成本低廉、手法隐蔽、危害性强的特点。在当前网络窃密多发高发的态势下，我们在工作生活中要时刻保持警惕，提高防范应对能力。

增强安全意识。随着网络“钓鱼”方式不断更新，我们要学习应知应会网络安全知识，增强网络安全风险意识，善于识别网络攻击手段，避免“咬饵上钩”。

提高甄别能力。我们在工作生活中要注意甄别虚假信息，对于无法确定来源、疑似仿冒、索要账号密码等可疑邮件，不要轻易点击或打开其中的附件、链接，避免进入恶意链接或下载恶意文件。

完善安防举措。个人应设置具有较高安全性的登录密码并定期更新，配置并使用二次认证、异常登录报警等安全防护功能。相关单位要强化网络安防措施，启用有效的安全防护策略。同时，应安装并及时更新计算机、手机等终端杀毒软件，定期进行全盘体检杀毒，不给网络窃密者以可乘之机。

国家安全机关提示

没有网络安全就没有国家安全。公民若发现通过网络“钓鱼”邮件进行窃密活动的可疑情况，应及时拨打12339国家安全机关举报受理电话，或登录互联网举报平台（www.12339.gov.cn），或通过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