暗战

解码网络深处的博弈

在信息互联互通深度融入日常生活的当下，我们尽享网络带来的便捷与高效，却不曾留意，一场关乎信息安全的无声暗战早已悄然打响。那些潜伏在网络深处、隐藏在日常设备里的窃密风险，正如同无形幽灵，时刻觊觎着我们的信息安全，甚至成为境外间谍情报机关或不法分子的“渗透利器”。广大网民务必提高警惕，擦亮双眼，谨防中招！

国家安全部提醒 谨记防骗“六字诀”

境外间谍情报机关经常瞄准公职人员、企事业单位或相关领域工作人员，精准投放“钓鱼”邮件和短信，企图窃取敏感信息。国家安全部提醒，谨记防骗“六字诀”。

辨：仔细甄别信息来源。官方工作通知一般会通过单位内网、官方微信公众号、官方网页等正规渠道发布，陌生号码、非官方邮箱发送的信息一律提高警惕。

拒：坚决拒绝可疑操作。不点击不明链接、不下载未知附件，不向陌生对象透露个人身份证号、银行卡号、验证码等敏感信息。

核：如有疑问及时核实。对涉及工作对接、资金往来的信息，应通过同事、领导、官方客服等正规途径当面或电话核实，切勿轻信短信邮件内容。

护：做好设备安全防护。工作电脑和手机应安装正版杀毒软件，及时更新系统补丁，必要时可开启双重或多重验证、异常登录报警等功能，避免使用默认弱口令。

守：严守保密工作纪律。公职人员、涉密人员要严格遵守有关法律法规，不在非涉密设备上处理涉密内容，不随意透露工作敏感信息。

报：发现线索及时举报。如发现疑似境外间谍情报机关窃密线索，可通过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。

商旅办公藏陷阱 你的屏幕正被实时直播

到境外出差，您是否会图个方便，直接使用酒店、会议室的公共电脑处理工作？然而，如果设备被提前植入恶意窃密程序，后果将不堪设想。在全国首个以科技安全为主题的“全国国家安全教育基地”，央视记者实地体验，使用一台被“动过手脚”的电脑，究竟有多危险？

在一个模拟宾馆商旅套房的一角，桌子上有一台配置的公共电脑，这台电脑已被提前植入恶意程序，而在它后面屏幕上显示的，就是窃密者那一端看到的界面。用这样一台电脑进行操作，会怎么样呢？

记者看到，键盘上输入的每一个字，在窃密者的屏幕上都能显示出来，而且就连记者输入拼音的过程都是实时显示的。

有人习惯用U盘来存储和传输资料，那么在这台电脑上插入U盘，会发生什么呢？

科技安全馆讲解员陈思介绍，我们现在把外接的U盘口插在这台主机电脑上，当你打开U盘开始处理工作的时候，就会发现，你打开的文件在黑客窃密端也同样被打开，甚至黑客端还可以详细看到所有文件。

陈思表示，不仅黑客可以查看查阅这些文件，还可以把这些内容全部拷走。U盘插入时间越长，它的传输进度，传输的百分比就越多。

小心免费Wi-Fi 背后的窥探

出门在外，连接Wi-Fi已经是日常习惯。一旦不慎接入暗藏陷阱的恶意Wi-Fi，又会面临怎样的安全风险呢？

李先生为了方便上网、节省流量，将手机设置为可自动搜索连接Wi-Fi。一次外出就餐时，他的手机自动连接上了一个没有密码的免费Wi-Fi。

在使用该Wi-Fi期间，他登录了自己的手机网银，并输入了银行卡卡号以及密码，用以查询银行卡账户余额。第二天，李先生就收到一条银行卡被消费了3000元的通知短信，随后又陆续收到银行卡转账和消费的信息。

在科技安全馆里，记者实地体验了电脑接入恶意Wi-Fi后的真实风险。科技安全馆讲解员陈思介绍，当需要连接Wi-Fi的时候，我们下意识可能会选择免费Wi-Fi，其实这个做法是有风险的。点击连接，你在电脑上看不出它有任何破绽，但是我们看一下黑客窃密端，当你连的那一瞬间，你的电脑就完全被掌控了。可以看到在黑客窃密端已完全同步了你的电脑。比如我们打开文档，写上会议纪要时，黑客窃密端也可以显示，甚至能显示键盘的打字画面。

手机也是一样。当连上恶意Wi-Fi后，不仅会被实时监控，还可能被暗中植入恶意程序，在不知情情况下被远程操控，给个人财产和社会公共安全带来威胁。那么如何进行有效防范？

一是关闭设备的“自动连接Wi-Fi”功能，防止手机在用户不知情情况下连入恶意网络。如果确实需要连接公共Wi-Fi，可以在连接前向场所工作人员确认，连接到的是真实可靠的Wi-Fi。

二是在公共Wi-Fi环境下，不要登录隐私敏感账号，不要进行网上转账、输入银行卡密码等高风险操作。同时要安装并及时更新防护软件，可以有效防止恶意软件攻击，保护设备安全。

“云端”不是“保险箱” 便捷背后有风险

近年来，随着网络“云”功能不断普及，“云端”数据也被境外间谍情报机关盯上，像邮箱、云盘一旦被攻破，究竟会有多危险？

科技安全馆讲解员陈思介绍，我们现在演示的是邮箱失密的风险，在被植入木马病毒的电脑上打开邮箱，我们看到已经登录完成了，实时同步的，还有黑客监控端的画面，你可以看到每一封邮件都已经完成了传输，所以它的窃取是同步实时的。

陈思说，我们再来演示一下云盘的窃密，当我们打开登录账号密码的时候，可以同步看到云盘当中的内容，涉密文件也被黑客窃密端所看到，它也可以进行传输，而且可以拷走这些文件。

无论是邮件收发，还是云端存储，看似高效便捷的线上办公，一旦疏于防范，就会成为失泄密的“重灾区”。

近年来，国家保密行政管理部门公布了多起违规云存储国家秘密的案例，相关责任人在未经保密审查的情况下，将涉密资料上传至网络，事后均依纪依法受到严肃问责处理。比如，某省直单位工作人员李某，利用自己的网盘私自保存机密级涉密资料。

面对云存储账户易遭非法网络攻击等风险，平时使用互联网处理个人事务时，需从操作层面加强安全防护。“涉密不上网、上网不涉密”是底线，一定不要通过互联网上传、存储、处理涉密信息，也尽量不要把个人隐私或敏感信息上传至云端或邮箱。

不少用户会选择将照片、通信录、数据等信息定期自动备份到云端，建议通过手动方式，有选择地对相关数据进行备份。出门在外，尽量使用自己的办公设备，同时要安装并及时更新防护软件。

警惕无线键鼠 三大窃密套路

国家安全部近日发布提醒，指出无线键盘、鼠标等设备在带来便利的同时，也可能成为失泄密的“隐形通道”。

空中信号“裸奔传输”：部分产品为节省成本，采用不加密的无线协议，导致每一次按键和点击，都以明文形式在空气中传播。攻击者使用普通USB射频接收器，即可截获并还原输入内容。

恶意设备“潜伏接入”：攻击者可改造无线接收器，将其变为“硬件木马”。一旦插入涉密或关键计算机，它便能伪装成合法设备，为攻击者打开远程控制和数据窃取的“后门”。

休眠状态“暗度陈仓”：设备从休眠状态唤醒并重新配对时存在安全漏洞。攻击者可能伪造配对信号，诱使你的鼠标与其设备配对，从而截获后续输入信息。此攻击隐蔽性强，用户难以察觉。

如何防范无线键盘、鼠标泄密？购买时需认准支持AES等高级加密技术的产品，避免使用“免驱即插”的无名品牌。定期检查并更新键盘鼠标固件及电脑驱动程序，以修复已知的安全漏洞。

处理涉密或敏感信息时，应优先使用有线键鼠，从物理上杜绝无线信号外泄。离开工位时，务必关闭键盘鼠标电源开关或直接拔掉USB接收器，防范“休眠劫持”等攻击。定期清理蓝牙设备列表，删除陌生或闲置设备，在不使用时关闭蓝牙功能。

国安部：谨防深度伪造魔改陷阱

近日，国家安全部发文：谨防深度伪造魔改陷阱。生成式人工智能技术的突破性进展，正推动AI视频制作加速普及，在提升创作效率、活化历史记忆等方面展现出巨大潜能，成为数字时代的内容生产利器。但技术若被恶意用于金融欺诈、谣言制造、间谍窃密等非法活动，将侵害公民合法权益，甚至扰乱社会秩序、危害国家安全。

伪造权威，动摇公信力：境外间谍情报机关、各种敌对势力可能利用深度伪造技术，捏造虚假言论、伪造公务人员不当视频、炮制虚假政策画面，以此制造社会恐慌、撕裂舆论、抹黑国家形象。

精准诈骗，侵害公私财产：不法分子可能利用深度伪造克隆亲友、客服等声音面容，实施冒充转账、虚假投资、仿冒官方渠道诈骗等非法活动。更有甚者，企图通过伪造企业公告、专家言论，引发市场波动。

信息泄露，危害数据安全：不法分子可能利用深度伪造人脸、声纹等生物特征，突破身份认证、权限校验等核心数据防护机制，造成账号被盗、后台入侵、敏感数据批量泄露，甚至引发关键信息基础设施安全系统失控等重大安全事件，对数据安全造成危害。

国家安全机关提示，《互联网信息服务深度合成管理规定》明确，任何组织和个人不得利用深度合成服务从事危害国家安全和利益、损害国家形象、侵害社会公共利益、扰乱经济和社会秩序、侵犯他人合法权益等活动。具有舆论属性、社会动员能力的深度合成服务，必须依法备案、内容审核、实名管理、合成标识，禁止删除篡改标识；严禁未经授权使用人脸、人声等生物识别信息进行恶意编辑。

境外黑客组织通过 搜索引擎漏洞窃取数据

国家安全机关工作发现，有不法分子通过给搜索结果添加恶意模块等方式，大肆开展站点权限获取、敏感文件资料窃取等非法活动，威胁国家安全。

案例显示，某企业员工通过搜索引擎搜索某类常用运维软件时，不慎进入境外黑客组织“精心制作”的虚假页面，下载并运行了带有恶意程序的软件，导致计算机中敏感数据被窃取。

经查，该企业承担了多家重要单位信息系统和网站的建设运维工作，境外黑客组织非法获取了网站登录凭证等信息，并尝试非法访问我重要单位信息系统和网站后台，企图窃取我内部敏感资料与数据。所幸，国家安全机关及时发现并消除隐患。

国家安全机关提示，只需养成几个好习惯，就能大幅降低风险。

认准身份信息：搜索引擎排名不等于安全认证，在查看搜索结果时，还要注意核对网址信息。正规网站通常以“https”开头，浏览器地址栏会显示安全锁图标，域名简洁规范，不会出现杂乱字符、错误拼写。

警惕免费陷阱：“破解版”“绿色版”“去广告版”这类软件往往是恶意链接的重灾区，尽量不要点击，如需下载软件，最好是手动输入官方网址，进入正确安全的官方网站进行下载。

保持免疫防护：保持设备系统和杀毒软件更新，开启实时监控，及时更新浏览器、操作系统和各类软件补丁。在遇到页面强制跳转、频繁弹窗、异常请求权限时，立即关闭退出，不做任何点击操作。

综合央视、北京青年报、国家安全部公号