当心！办公室内满是网络陷阱

网管忠告：无论哥在不在江湖，江湖上都不要有任何哥的传说

□据《羊城晚报》

一封邮件可以制造出一个轰动全国白领界的“邮件门”，一个网络帖子可以令你黯然“自动辞职”，你以为只是你与同事的私人点对点聊天，也可以被曝光作为处分，甚至“炒鱿鱼”的“呈堂证供”……网络时代，科技便利了我们的工作流程，然而同时，科技也令世界变得没有边界，甚至没有个人秘密……是的，你知道网络有风险，但你是否知道，所谓的网络风险在职场上会有多大的杀伤力？有朝一日一不留神，这些职场“暗器”的攻击目标也许就是你！

（资料图片）

A

办公室网络陷阱大扫描

水能载舟，亦能覆舟，这个最简单的道理，相信每个白领都知道。不过，谁会想到，日常使用的办公用具，一不小心也会成为危害到自己的“暗器”？科技就是这样，为你带来便利的同时，总会留有各种后门。

办公室没有秘密！这不仅在面对面的现实交流中。网络上，一切都太便利。别说私人日记，你大概已经连订饭、记账这种生活琐事都在网上完成了吧？况且现在各种秘密网、记账网、实名制社交网站大行其道，凡走过必留痕迹，不知不觉中，你在网络上已经留下了太多的“痕迹”。

网线背后有只“眼”，这个说法似乎有些恐怖，不过事实是，至少大家都知道，公司的网络是有专人维护的，也就是说，某些不符合公司规范的网络行为，你以为神不知鬼不觉，实际上却在专业人士的监控之下！

大家也不用听“监控”便“色变”，很简单的道理，比如你利用公司网络下载色情电影或玩网络游戏，别说是否会对公司网络招来病毒这个极大的风险，光是阻碍了公司网络的带宽，就可能会对别人的正常工作文件传输造成影响。所以，对于大部分公司严格规范职员的网络行为，大家应该是没有异议的。只是很多人并不知道，他自以为安全无害的一些网络行为，原来也会成为“暗器”，一不小心就掉入了这个高科技的职场陷阱！

【一级警报】

SNS、微博：真心话大冒险

爱玩“真心话大冒险”是吧？很好，希望你有良好的心理承受能力以及承担风险的能力。因为，代价，可能就是你的饭碗。

关于像开心网、facebook这类SNS实名制社交平台泄露个人资料的巨大危机，早已被大家所知，而微博的即时简短信息发布，甚至曾作为某国警方侦破绑架案的线索。不过，以上这些还不是我们今天所讨论的职场“暗器”。

曾经有一件真人真事，某个白领在客户处见到了一些他认为非常不合理的现象，义愤之下把这个故事写到开心网上。虽然随后他便觉得不妥，10分钟后便自行删帖，但这个帖子已经被熟人转帖，流传了出去。未及，客户跑到公司告状，他只能在公司的“遗憾”下自动辞职。

暗器等级：初级

因为是实名制平台，只要是通过认证的人，都能见到你的白纸黑字，走不掉跑不脱，因此，“侦破”基本上是不需要太多技术含量的，可谓危险性极高。由于此危险性的明显存在，所以大家基本都知道，什么不该放上去，因此陷阱程度反而最低。

【二级警报】

E-mail：收集罪证最方便

私人邮件往来就可以畅所欲言，受到隐私条例保护？别傻了，放在自家枕头底下的信件，你的父母是不能看，不过，在公司的网络中发送的电子邮件，情况恐怕会有些不同。

如果你有留意，有些邮件末尾会附带一份免责声明，表明请不要将私人信息透露在此邮件中，否则有可能造成个人资料泄露等。因为这些是公司的工作邮箱，如果你用于私人用途，恐怕是要视同偷盗公司财产损害公司利益的。由此你也可合理推断，这类工作邮箱是会受到一定监控的。

当然不会有人那么无聊，无端花费精力专门去偷窥你的每封邮件，不过既然是通过公司网络往外发送，“凡走过必有痕迹”。某外企的资深网管告诉记者，这种情况在一些销售型职位尤为敏感。比如公司已怀疑你有某些损害公司利益的不法行为，会事先要求网管人员对你进行重点监测，例如对你的工作邮箱设定某种程序，那么之后你所发的每一封信都会抄送一份给相关领导。不知不觉中，你的“罪证”就被完全收集了。曾有一位销售人员，将自己企业的销售价格私下给了对方企业，殊不知他之前的异常举动已经受到怀疑，当一系列“私通邮件”被列印出来，他也只能无话可说。

暗器等级：中级

一般而言，加密的网页接收邮件是比较安全的，不过并不是所有邮件都是加密的。更何况，如果使用公司工作邮箱，你更要清楚，请不要利用公司资源做不法之事，否则后果自负。

有人认为电子邮件应该类同于信件的隐私保护，我只能告诉你，对此国内已经有案例判决，供你参考。曾有白领群发公司邮件，收集同事性骚扰证据，结果被判“擅自利用单位的设备、网络，散布非工作内容言论，处理个人争端，采用的方式是不当的，会扰乱工作秩序，损害单位利益。其行为严重违反用人单位的规章制度，公司解除劳动合同并无不当”。

当然，这个级别的监控技术含量较高，需要视公司的网络监测设定程度与网络管理设备而定。

【三级警报】

MSN、QQ：集中八卦，集中危机

传统的办公室八卦地，排行榜上的第一名，应该是茶水间与后楼梯之争。闲人多的地方口水杂，像《志明与春娇》那样，在后楼梯抽烟从而相识相恋的桥段，也就是办公室八卦地这个事实的浪漫版的进化版。现在，八卦阵地当然已经转移。点对点的即时通讯工具，也就是白领们早已离不开的MSN、QQ，已经成为第一八卦集中地。

点对点地讲八卦发牢骚，就不怕隔墙有耳被茶水间阿姨偷听了去？你未免也太放心了！

是的，现在许多点对点即时沟通工具都已经加过密，比如QQ。有的虽未加密，不过你也可以通过外挂加密插件，原则上保证了别人无法随便“破解”你的聊天记录。不过别忘了当你使用公司配备的工作电脑，你的聊天记录都会被储存在本地硬盘上。基本上，本地硬盘上的资料调阅，对于最普通的网管，这都是一项入门技术了。更何况，绝大部分企业为了网络安全需要，都安装了企X通等各种网络管理软件，你的所有网络通联记录，会在一定期限内被保存。虽然不会被无关人员轻易调阅，不过如果以为在MSN上窃窃私语就无人知晓，这种想法只能说是“无知者无畏”了。

暗器等级：高级

此暗器的伤害程度在于，在你自以为安全的环境下，放松警戒，信口开河，结果可能大大出乎你的意料！原来你以为只存在两个人之间的点对点交流，旁边还有第三只眼。

B

网管忠告：公器私用就是最大陷阱

这么看来，网管就是那个恐怖的间谍，掌握着所有人的秘密？事情没有那么严重！

不同的公司对于自身的网络安全设定不同，投入的设备也不同。不过，即便是高度安全戒备的企业，网管们也不至于有事没事就去你的硬盘里逛逛，看看你的聊天记录。

网管们通常的工作只是维护整体网络安全。一位外企网络主管说，他的网络监控，只是每天看看从公司连出的最热门前10位访问地址是哪里，看看有没有人的电脑突然发出几百个连接请求，这种不是中毒就是在非法下载的行为，要及时处理免得阻碍公司网络正常运行。

“事实上，那个恐怖的职场间谍，就是你自己！如果你不公器私用，不违反网络使用规范，哪里会有那么多的陷阱呢？”

安全贴士

❶ 加密是基本！

尽管这有点治标不治本。有的即时通讯工具如QQ，本身已经加密，而像MSN等则未被加密，若担心被网管之外的别人偷偷窃取相关资讯，可以自行下载一个外挂加密插件。

❷ 学会分辨邮件的安全程度。

网页接收邮件比起用软件接收，安全性较高。若网址开头为“https://”，则为加密邮件；若只是普通的“http://”则未被加密。

❸ 可以利用系统自带的防火墙，在电脑中设置不允许共享本地硬盘。

不过这个权限也要根据公司的统一电脑权限设置，不少公司的普通职员电脑并没有权限进行此操作。

❹ 最彻底的防御，就是放弃！

不要公器私用，不要利用公司资源，发布任何对自己有危险的信息。做到“无论哥在不在江湖，江湖上都不要有任何哥的传说”，这才是最彻底的安全之道。