2018 国家网络安全宣传周系列：盘点极易泄露信息的不良习惯

来源:新民晚报

建了聊天群后却不精心管理、对敏感资料随意上传转发、打印资料不注意及时清除存档……殊不知，这些日常场景都可能导致信息的泄露。如果在生活和工作中有下面这些不良习惯，赶紧纠正过来吧。

2018 国家网络安全宣传周系列动漫——日常交流篇

建了聊天群后却不精心管理、对敏感资料随意上传转发、打印资料不注意及时清除存档……殊不知，这些日常场景都可能导致信息的泄露。如果在生活和工作中有下面这些不良习惯，赶紧纠正过来吧。

■私建工作聊天群

【现象】

聊天群在方便沟通的同时，也隐藏着巨大的隐患，比如被盗号后群聊信息泄密、离职后潜伏在工作沟通群里等。

【建议】

◆工作相关聊天群尽量使用单位搭建的、有专人维护的即时通讯服务

◆公共即时通讯平台上的聊天群（如微信、QQ 等），管理员要严格审核加群人员

◆聊天群中尽量不要发送敏感信息和文档，以防无关人员知悉

■敏感资料随意分发

【现象】

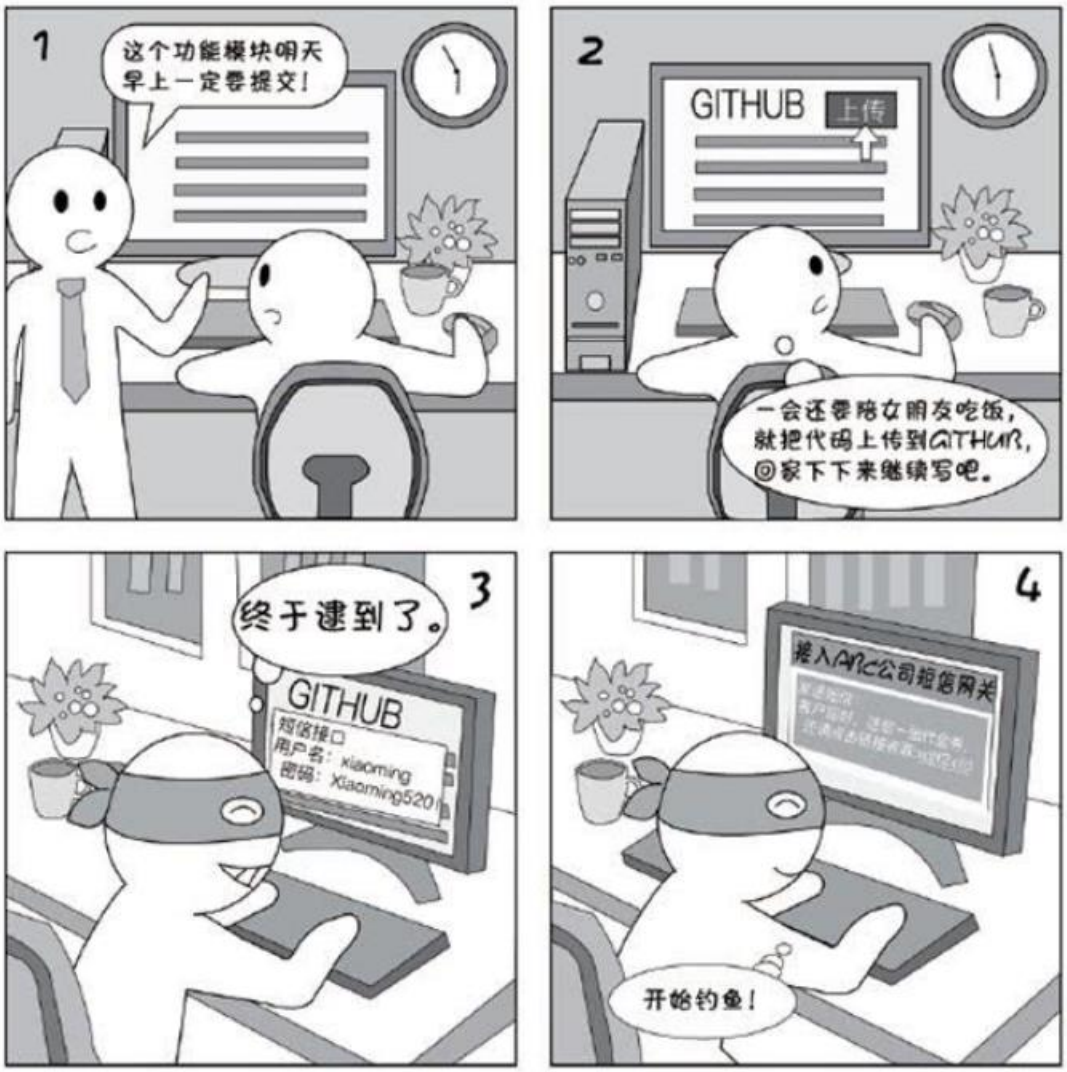
单位各类文档实际上都有授权扩散范围，比如，与客户项目相关的文档均为商业机密，只能在项目组内部扩散，泄露后会给双方带来不良影响。

【建议】

◆方案、合同、报告、代码等较敏感文件在分发时，务必注意密级以及单位授权扩散范围

◆若发现网上有关单位相关的敏感文件，请立即通知单位安全保密人员进行投诉和删除

■代码发布到 github



【现象】

黑客在入侵一个网站或者系统前，会到网上搜索此网站的相关信息，很重要的信息就是代码库，没有安全意识的开发人员会将代码上传公共代码库，黑客会分析代码，找出其中的安全漏洞。

【建议】

◆网站、系统或产品代码建议利用单位同意的 SVN 服务器保存

◆在家办公可通过单位的 VPN 链接到开发机上，不可利用网盘、代码库进行共享

◆重要系统的代码用 U 盘拷贝需经单位同意并做好保护措施，使用完毕彻底删除

■外部打印

【现象】

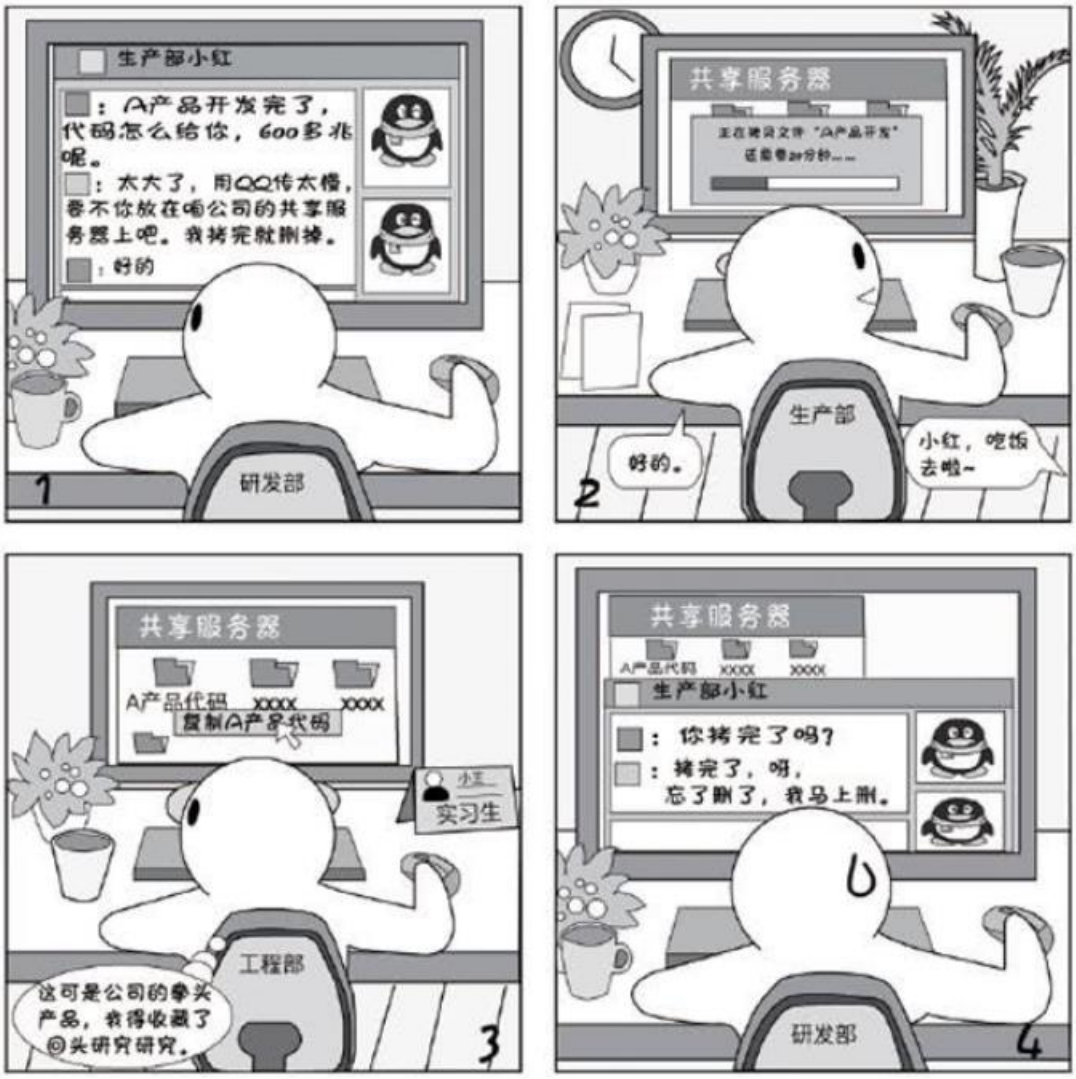
打印社的电脑上一般都保存很多已打印的文档，打印社可能不会定期清除，并且客户随意拷贝没有限制，很容易泄露敏感文件。

【建议】

◆外部打印时务必在 U 盘上打开并打印，不要拷贝到打印社电脑上

◆也可以用防拷贝盘，可防止将 U 盘文件拷贝到电脑上

■公用共享文件夹使用



【现象】

公共共享文件夹一般会搜到各部门文档，其中包含很多敏感文件。敏感文件通常都是共享拷贝后，忘了删除和剪切而遗留下来的，容易暴露给侵入内网的黑客或内部恶意人员。

【建议】

◆敏感文件尽可能不利用公用共享文件夹，因为即使删除后也可在服务器上恢复

◆共享服务器管理员可设置定期自动清理共享文件夹

■安全总结

工作群聊须谨慎，敏感信息私下传；

加群严审莫被骗，关注离职及时清；

敏感资料勿乱发，扩散范围要看准；

产品代码莫上网，在家可连 VPN；

外部打印需注意，U 盘打开可打印；

共享目录虽方便，敏感文件忌上传。