**2018国家网络安全宣传周系列动漫①WiFi安全篇**

如今，随着移动终端的兴起和互联网技术的不断进步，那些古老的盗窃、诈骗、骚扰手段也换了新颜。不知道大家有没有意识到，大家每天使用的WiFi，其实并不安全。

是的，你没看错，使用WiFi上网时，我们的个人信息安全或许面临着巨大的风险。

比如，黑客自己搭建一个“山寨WiFi”，取一个与附近WiFi相似的名字，不设登录密码诱导人们连接。使用时，传输的数据就会被黑客监控，个人隐私、账号名和密码等信息，也可以轻易被盗取。其实，不仅是蹭WiFi，不少人还喜欢随时开着手机无线网自动连接功能，这样风险就更大了。

不信？看看下面这几幅漫画，这些危险场景，或许你都曾经置身其中。

* **免费WiFi接入**

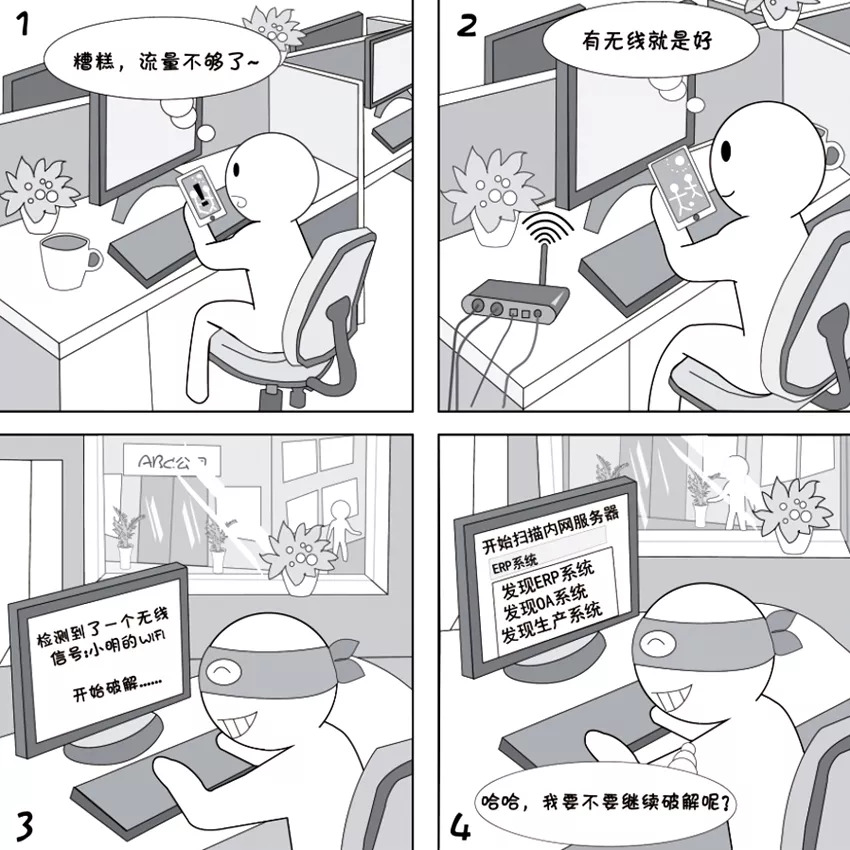


【危险】

不法分子搭建与常用WiFi相同或相近的WiFi，设置空密码或者相同密码吸引公众连接，然后在WiFi路由器上劫持DNS(域名系统)，将用户引入到钓鱼网站获取

【提示】

* 公共场合连接WiFi时请同商家确认好WiFi名称
* 没有密码的公共WiFi慎用
* 使用支付APP时，尽量使用运营商的4G网络
* **私搭WiFi热点**



**【危险】**

无线路由器有较多的安全隐患，比如，之前的WEP认证能很轻易破解。个人架设无线路由器，如果配备不当会导致蹭网或个人资料泄露，在公司使用可能导

**【提示】**

* 在办公网络架设无线路由器必须经过公司批准并进行安全安装
* 认证方式使用安全的WPA2
* 建议隐藏SSID(服务集标识)，绑定接入设备的MAC地址
* WiFi密码必须八位数以上，包含大小写、数字和标点符号，定期修改密码
* **WiFi自动连接**

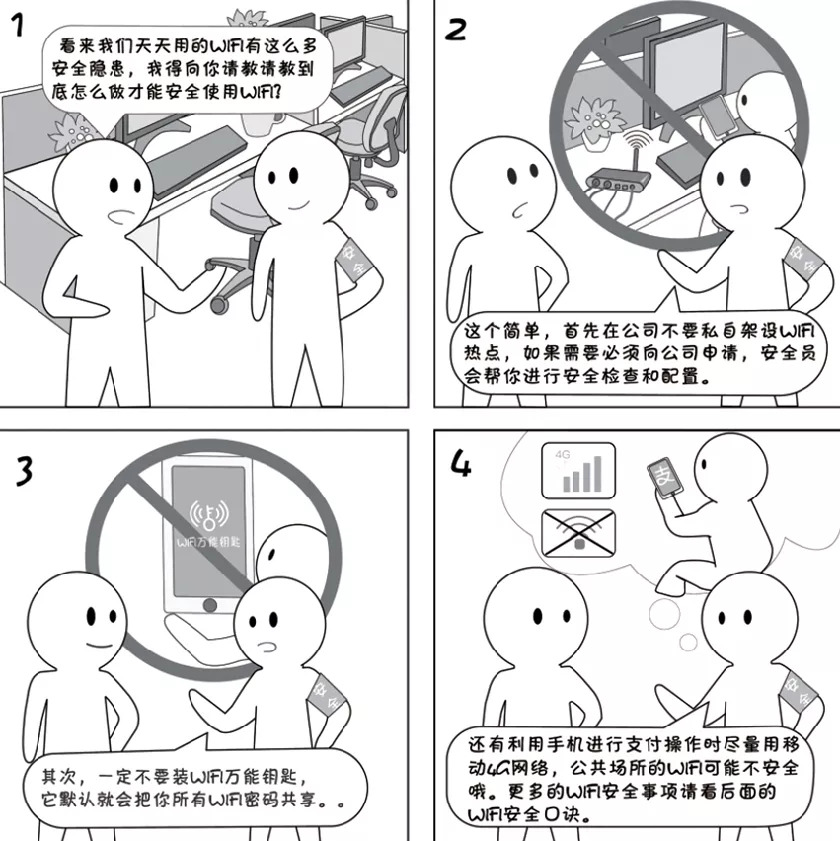


**【危险】**

一些手机在搜索到不是同一个WiFi热点但名称相同的WiFi时，也会自动使用保存的密码连接，这就给黑客以可乘之机。

**【提示】**

* 日常不用WiFi时关闭手机和笔记本电脑的无线局域网功能，以防自动连接恶意WiFi
* 当手机和笔记本连上WiFi后，留意连接到的WiFi热点名称
* **WiFi安全总结**



**<WiFi安全口诀>**

公共场合接WiFi，名称一定确认好

无密WiFi不要连，安全支付用4G

私搭路由要审批，安全设置莫忘记

WiFi不用要关闭，万能钥匙请回避

**【后记】**

万物互联时代，蹭WiFi似乎成为了一项基本“生存技能”，但在享受WiFi带来便利的同时，由于人们普遍缺乏WiFi上网的安全防范意识，逐渐成了各种网络陷阱、钓鱼诈骗的重灾区。WiFi风险主要有两种形式：一是正常WiFi被不法分子入侵，二是不法分子建设假冒可信热点。

为防范这些安全问题，无线网都需要增加基本安全认证和加密功能。包括：

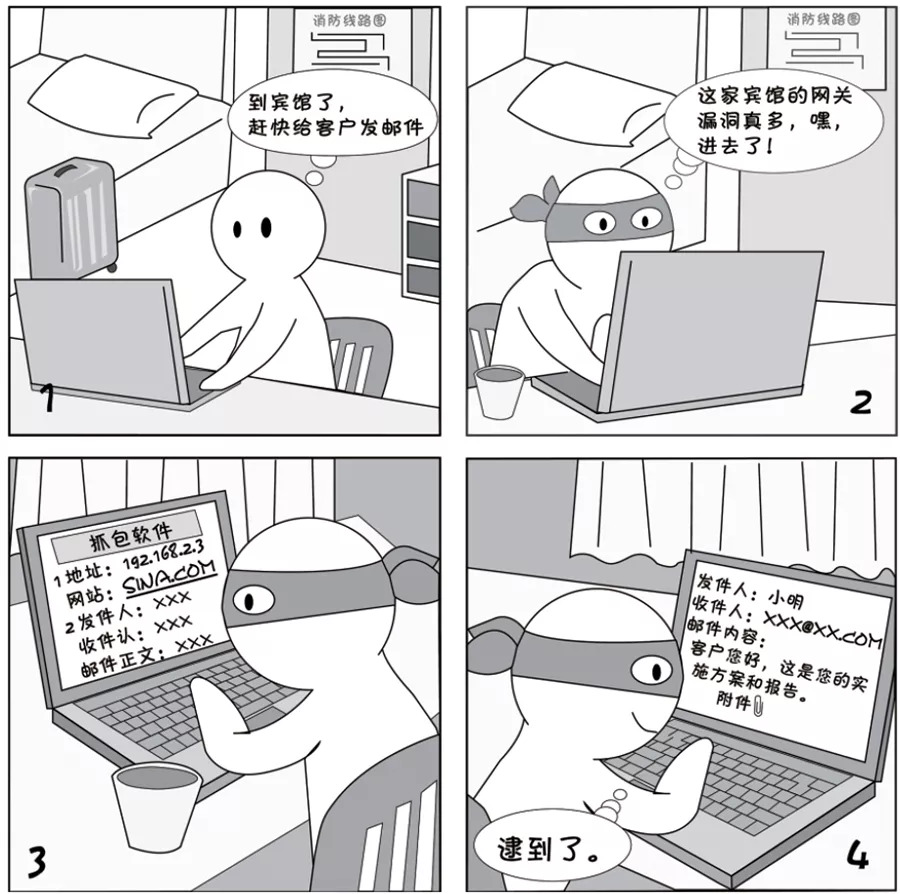
* 1、用户身份认证，防止未经授权访问网络资源；
* 2、数据加密以保护数据完整性和数据传输私密性；
* 3、平时使用要注意固件升级，有漏洞的无线路由器一定要及时打补丁；
* 4、手机端、电脑端都应安装安全软件。

**2018国家网络安全宣传周系列动漫②邮件安全篇**

电子邮件，人们几乎天天发、天天收。网络信息化时代，电子邮件已经成为常用通信工具，而且也成了企业内部主要的沟通工具。

然而，邮件安全问题也日益突出，逐渐成为电信诈骗、勒索软件攻击的重灾区。如何让邮件更安全？下面这组漫画，大家可以学习一下。

* **传输加密**



**【现象】**

一些宾馆或公共网络的安全性较差，黑客很容易入侵到其网关设备并监控网络流量，如果收发邮件没有加密，黑客抓到这些数据包后很容易还原出邮件正文和附件。

**【建议】**

* 收发敏感邮件时要确保传输通道是加密的
* WEB邮箱的传输是否加密要看URL（网页地址）是HTTP还是HTTPS，带S说明是加密传输
* 用邮件客户端的加密设置一般为在发送和接收服务器设置处勾选SSL
* **钓鱼附件**

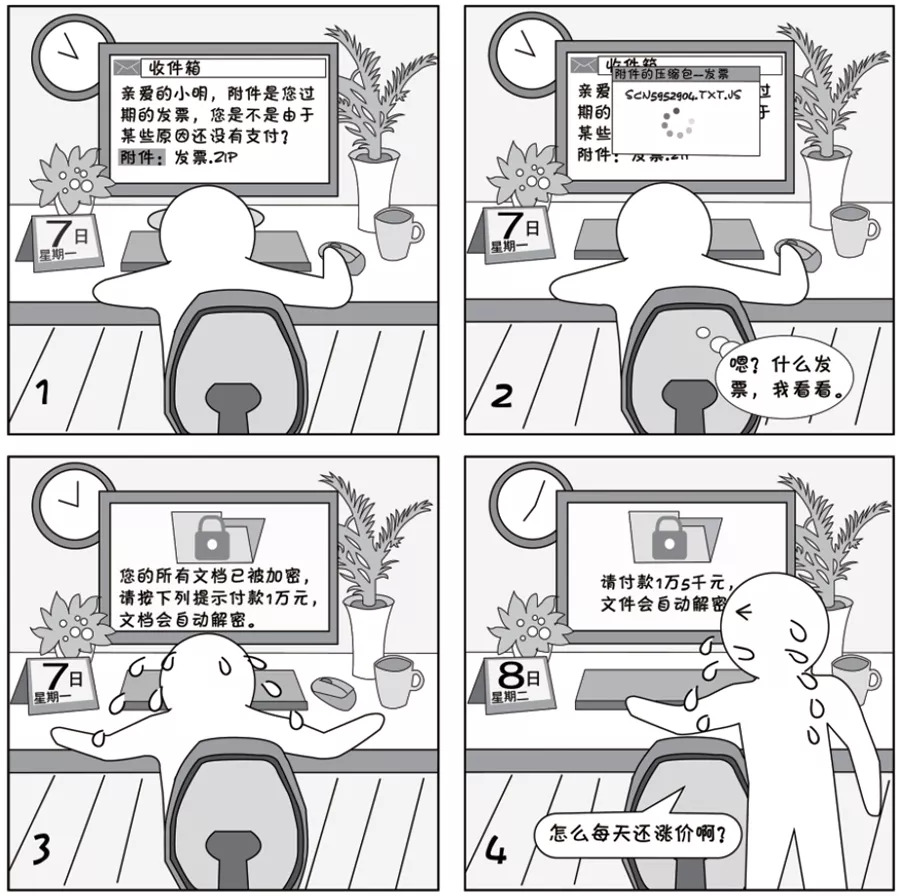


**【现象】**

钓鱼邮件种类繁多，利用邮件骗取回复敏感信息是最简单和常见的钓鱼方式。

**【建议】**

* 望：看邮件发件人地址、签名等信息，是否是你的熟人，是否是系统邮箱，是否是可疑的地址
* 闻：多听周围人的看法，骗子不会骗到所有人
* 问：打电话与相关人员直接确认是最保险的
* 切：懂一些电脑的技术人员可以查一下发件人的真实IP地址、分析一下邮件头内容
* **附件病毒**

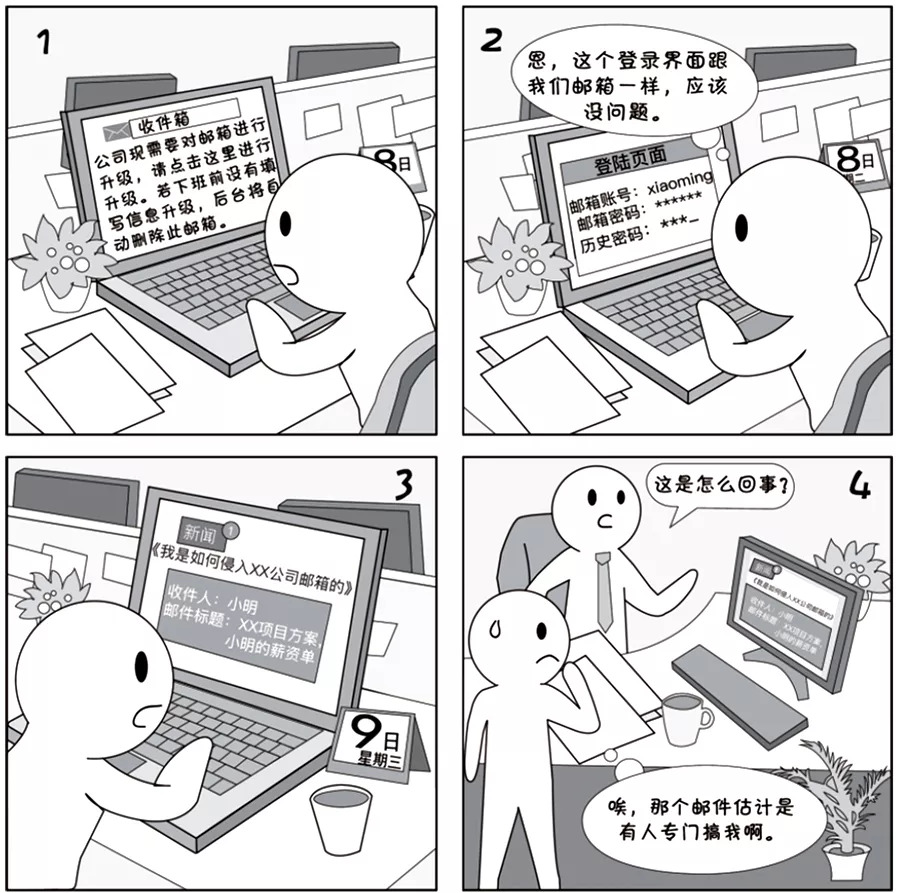


**【现象】**

流行的勒索病毒邮件多为英文邮件，主题和正文诱导用户打开附件。这种病毒对文档的加密强度很高，可以说是无法破解，只有付款才能解密文档。

**【建议】**

* 必须要装但不要完全相信防病毒软件
* 确保自己的邮件客户端禁止访问执行文件，可以自己给自己发一个.exe 后缀的文件测试一下
* 所有类型的文件都可能带病毒，不仅仅是exe/js/bat 为后缀的可执行文件，非可执行文件的利用难度较高，需要利用相关漏洞
* **恶意链接**



**【现象】**

包含链接并链接向钓鱼页面的邮件比较具有迷惑性，因为让受害者看到了与真实登录界面几乎一模一样的网页，受害者就会放低戒心，输入用户名和密码。邮件中的链接也可能直接指向一个挂马页面，打开后直接就会中木马。

**【建议】**

* 遇到索要敏感信息的邮件首先要保持冷静、提高警惕
* 若对邮件所说内容不知情，请勿点击链接，直接电话向发件人确认
* 邮件安全总结



**<邮件安全口诀>**

邮件传输要加密，黑客截获难破译

各种附件谨慎点，可执行文件风险高

默认浏览器非IE，陌生链接勿点击

遇事冷静莫慌张，电话确认是法宝

**2018国家网络安全宣传周系列动漫③个人电脑安全篇**

电脑已经成为人们日常重要的工具之一，但电脑安全防护意识却在大众心目中并不完善，再之，信息安全系统的不完善，很容易成为黑客的攻击目标。

无论是企业，还是个人电脑安全防护，都与人们的很多信息和私有财产有着密不可分的关系，面对互联网的复杂形势，如何防护好电脑数据安全？以下这些漫画场景不妨仔细看看……

* 文件加密存储

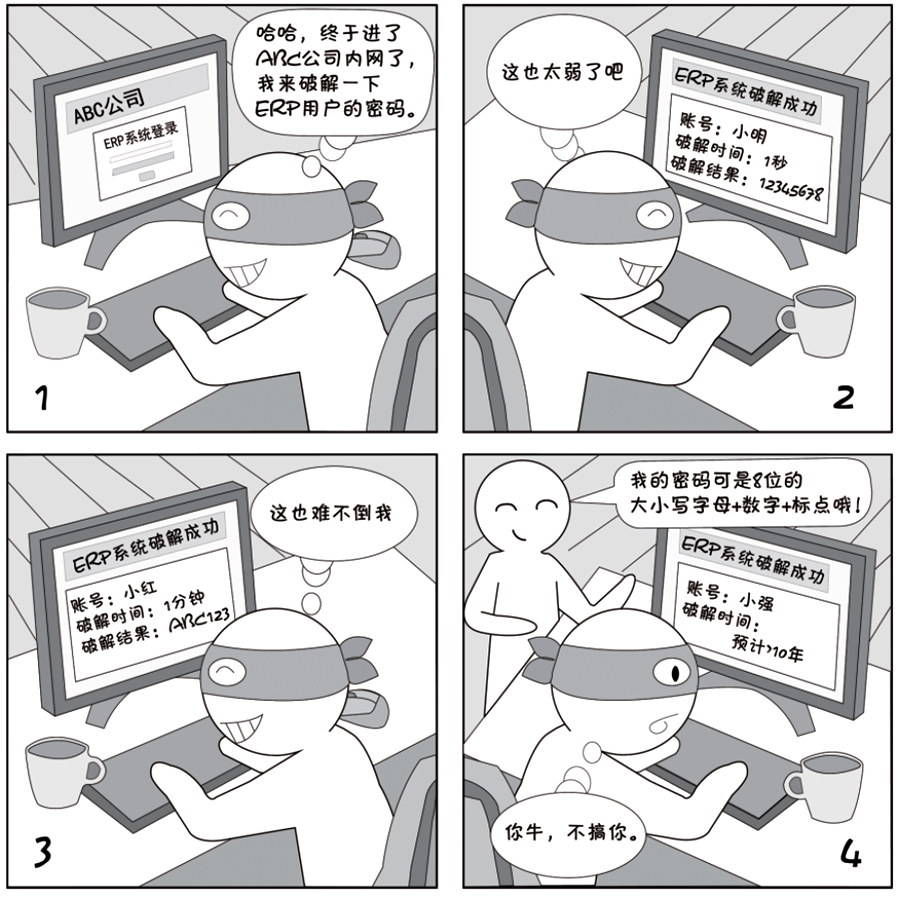


**【现象】**

文件直接放在硬盘上，电脑丢失后硬盘上文件就可以被直接读取，如果存到加密盘中，拿到硬盘后必须输入加密盘密码加密盘才能看到其中的文件，就有效避免了重要文件泄密。

**【建议】**

* 敏感文件建议存放在保密盘中，开机输入密码后加载加密盘
* 邮件中也会有很多敏感信息，Outlook或Foxmail的数据文件也建议放入加密盘
* 加密盘密码一定要设置复杂密码
* 加密盘可以使用微软的Billocker或Truecrypt
* 弱口令

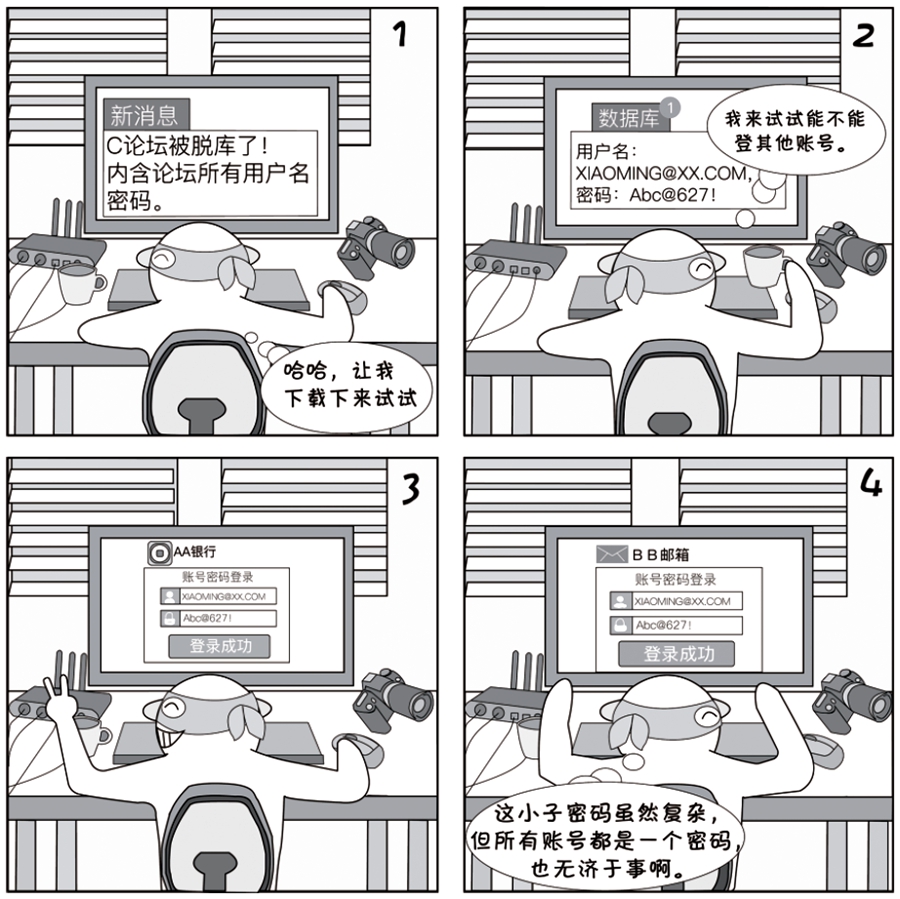


**【现象】**

密码越复杂，破解难度越高，且这个比例是成指数级的，假如说简单的6位数字密码秒破，而8位复杂密码的破解需要20年以上。

**【建议】**

* 包含大小写字母，数字和标点符号，位数在8位以上；
* 不能包含各字、生曰、手机号或车牌号；
* 定期修改各种密码，如三个月或半年；
* 密码分级

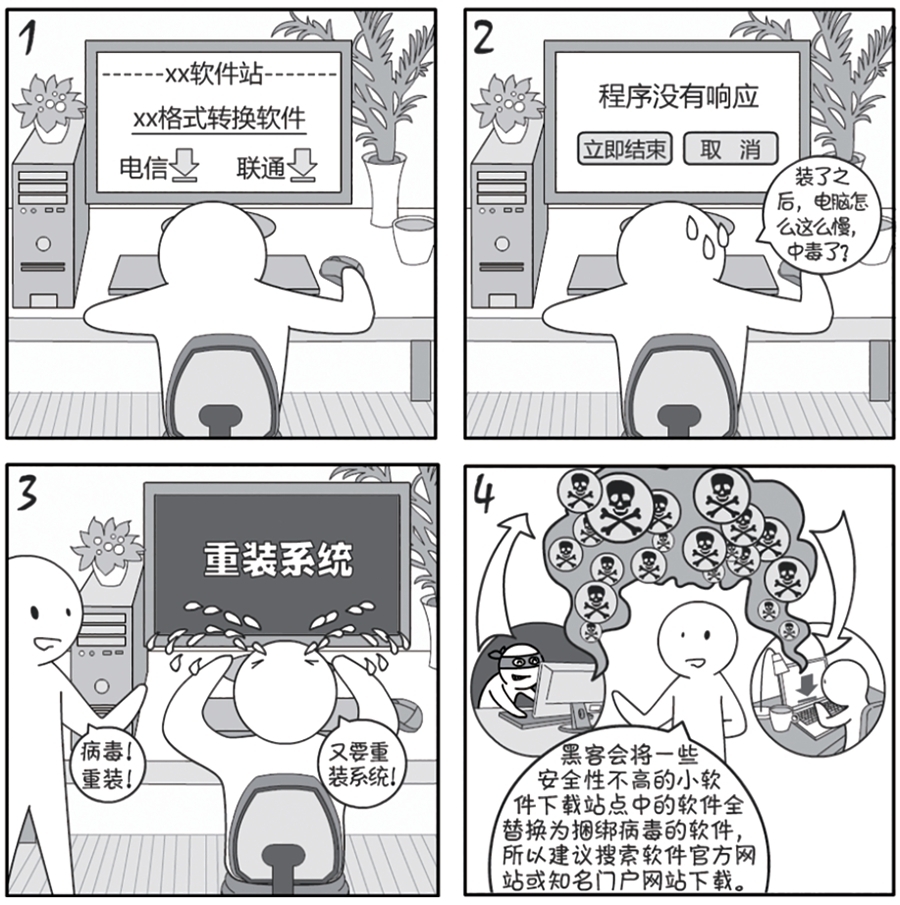


**【现象】**

很多人各个网站的用户名、密码相同，这样黑客用被泄露网站的密码登陆其他网站很有可能会成功。每个网站都设置不同的密码可能不现实，那就可以对密码分级管理。

**【建议】**

* 不同网站/应用的账号设置不同的密码是最安全的
* 也可以按账号重要程度进行分级，不同级账号设置不同密码，同一级账号设置相同或相似密码
* 爆发拖库事件时第一时间修改自己的相应级别的账号密码
* 软件下载

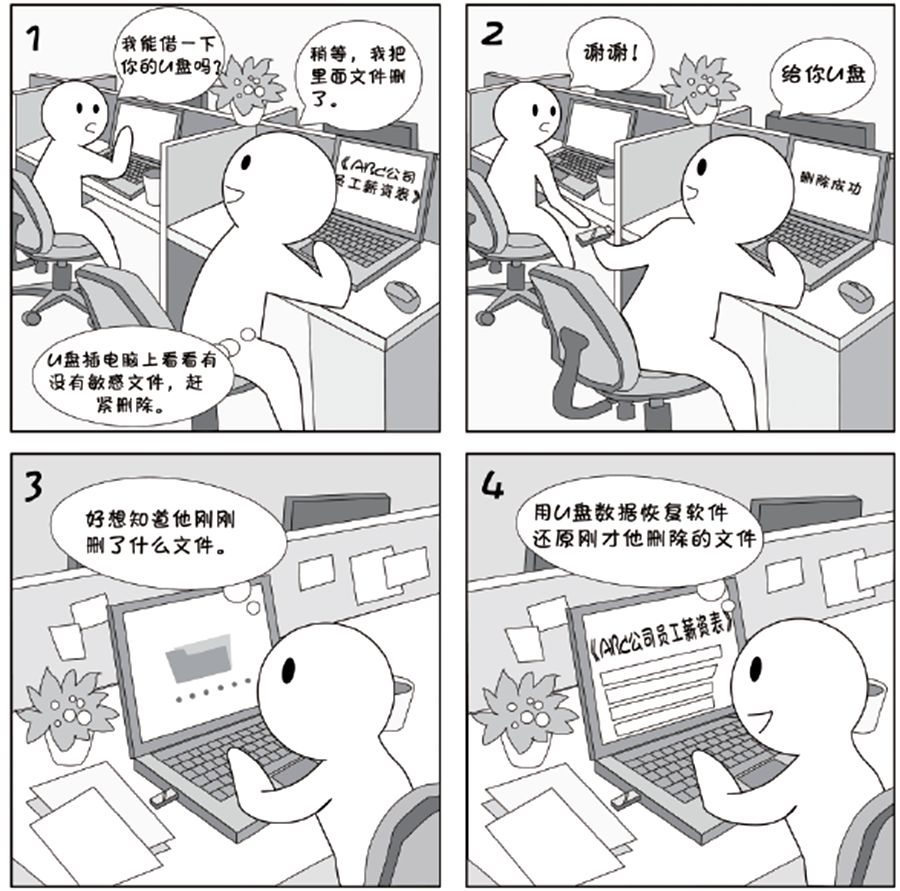


**【想象】**

黑客会入侵一些安全性不高的小软件下载站点，将其中的软件全部替换为捆绑病毒的软件，这些软件安装使用和原版一模一样，但后台就默默运行着病毒木马，各种主流杀软无法检测到。

**【建议】**

* 建议搜索该软件的官方网站，到官方网站下载
* 下载后用MD5工具查看下载软件的MD5值，并同官方网站公布的MD5值做对比，如果不一样则肯定被修改过
* 文件删除



**【现象】**

删除电脑或U盘中的文件时，如果仅点删除按钮或快速格式化，真实并未真正从硬盘或U盘中删除，利用数据恢复软件可轻松恢复出来，清空回收站同样可以恢复。

**【建议】**

* 单个文件彻底删除可利用杀毒软件自带的文件粉碎功能，一般在文件上点鼠标右键可以看到
* 电脑出售或移交其他人使用，删除敏感文件后，同样需要对硬盘脱密，使用脱密工具反复擦写5次以上
* 数据备份

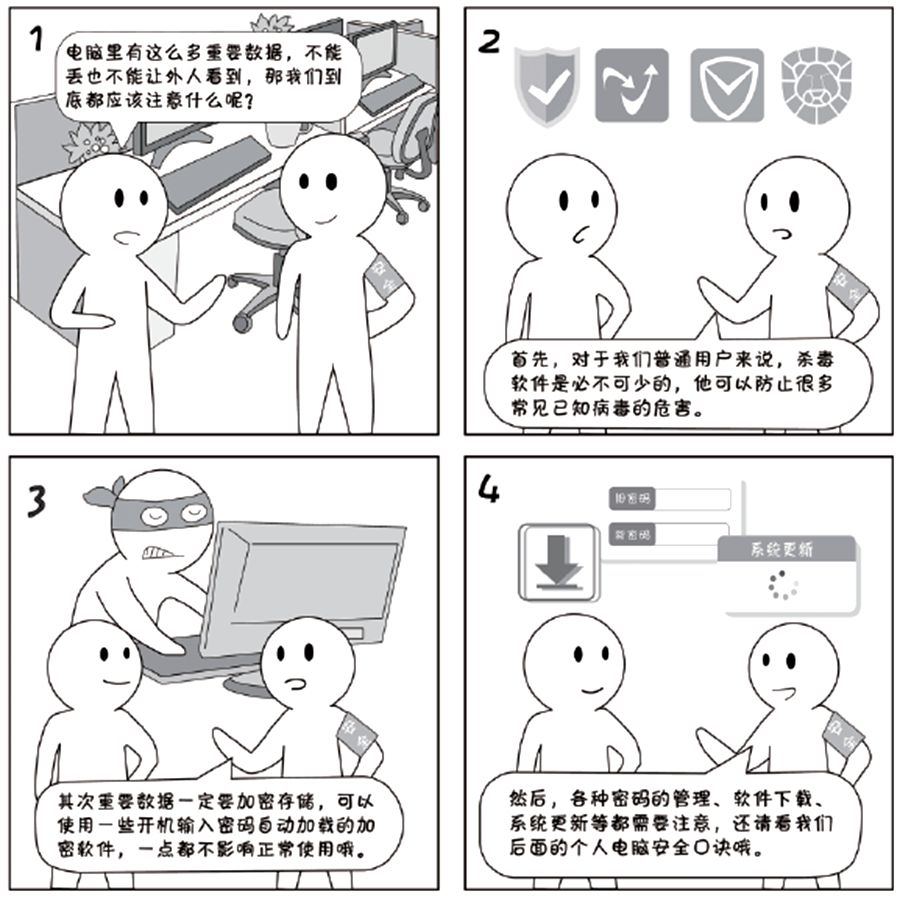


**【现象】**

有很多原因可能导致硬盘上的文件丢失或不可用，比如硬盘日久老化故障，电脑掉电硬盘故障，电脑中病毒将文件都加密，甚至电脑丢失等，所以，日常需要注意重要数据的备份。

**【建议】**

* 个人电脑上的重要数据要定期备份到备份服务器或移动硬盘
* 备份时，注意数据要加密，建议使用加密盘，备份整个加密盘原始文件
* 个人电脑安全总结



**<安全口诀>**

敏感文件要加密，邮件文件莫忘记

软件请到官网下，MD5要对比

文件删除要彻底，硬盘移交须脱密

密码设置要复杂，分级忘记又好记

系统补丁及时打，不怕黑客常惦记

数据备份要定期，备份文件须加密

# 2018国家网络安全宣传周系列动漫④办公区域安全篇

办公区域内常常涉及不少所在单位的各类私密信息，出门忘记关电脑、开完会没有擦黑板、会议室被安装窃听系统……这些都可能成为导致办公区域信息泄露的重要隐患。怎么防护办公区域内的信息安全？看完这些漫画场景，以后可千万别再大意了。

* **陌生人进入**



　　【现象】

　　乔装成各种工作人员作案是商业间谍或黑客收集信息的重要方式之一。

**【建议】**

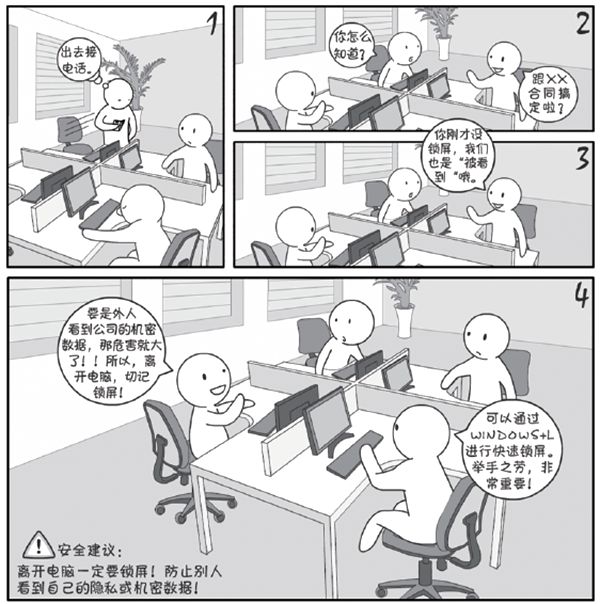
* + - 收取快递在门外进行
    - 带外人进入要前台登记并全程陪同
    - 进出大门时注意是否有尾随人员
    - 对于不能自动闭合的大门要注意随手关门
* **会议安全**



【现象】

　　利用会议室白板讨论的，一般都是一些主要思路、关键结论，这些内容如果泄露给未授权知晓的人员，很容易带来各种不可预知的后果。【建议】

* 注意选择较隔音的会议室
* 开会期间拉上窗帘或百叶窗
* 会前叮嘱参会人员保密事项，不允许拍照、录音，甚至不能带手机入场
* 会后整理会场，不遗留文件，注意擦白板
* **锁屏**



　　【现象】

同事之间工作内容、工作性质不同，有权看到信息密级也可能不同。工作期间短暂离开工位时，如果电脑屏幕没有关闭，别有用心的人还会打开电脑各种文件，甚至用U盘拷出。

【建议】

* 短时间离开时按win+L键锁屏电脑
* 长时间离开电脑建议关机
* 日常设置屏保程序，并勾选“恢复时显示登录屏幕”，以免离开时忘记锁屏
* **桌面安全**

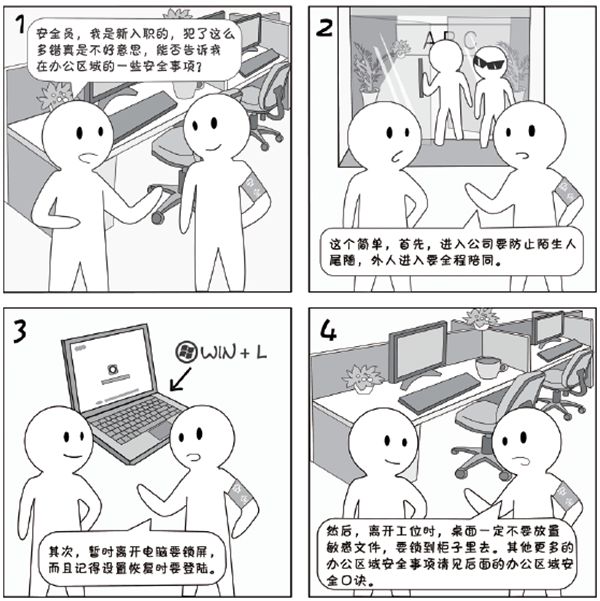


　　【现象】

对于一般的公司来说，外人进入办公区域并不是一件很难的事，特别是对于面向公众办公的单位，桌面如果放有敏感文件，很容易被对方用手机偷拍或随手带走。

　　【建议】

* 再次强调，注意给电脑锁屏
* 敏感文件一定要锁在柜子里
* 桌面不要遗留门禁卡、钥匙、手机等重要物品
* **安全总结**



<安全口诀>

进出大门防尾随，收发快递在门口；

会议过程不拍照，会后谨记擦白板；

离开电脑要锁屏，设置自锁十分钟；

敏感文件柜里锁，钥匙门禁身边留。

# 2018国家网络安全宣传周系列动漫⑤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**

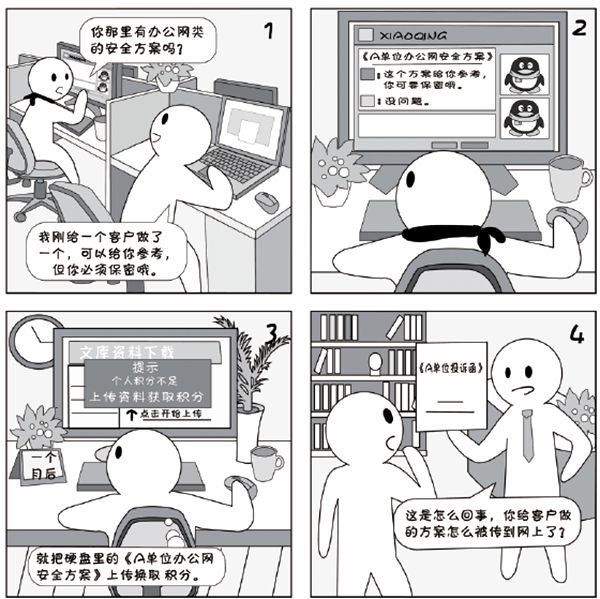


【现象】

　　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**

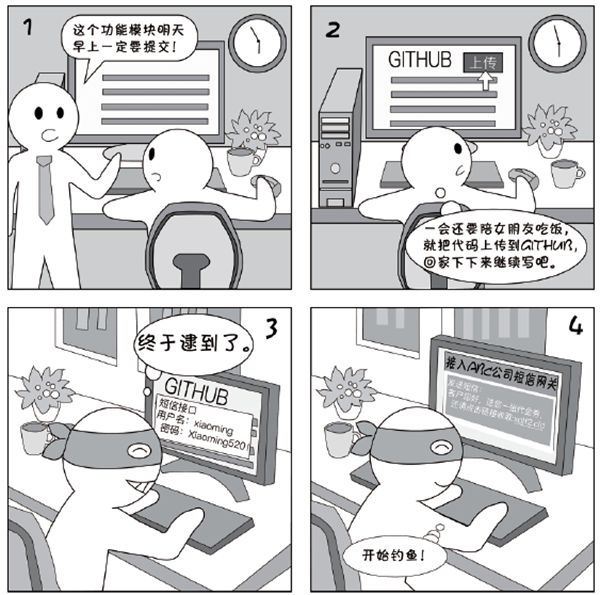


【现象】

　　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**



<安全口诀>

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。