

## 版权声明

1. 《信息安全意识漫谈》作品的著作权人是绿盟科技（英文简称NSFOCUS）。
2. 著作权人将本作品电子版发送于贵公司，只代表授权您本作品的使用权。
3. 被授权使用权的您无论采用什么形式使用本作品的部分或全部内容，都必须充分体现本作品的著作权人。
4. 未经绿盟科技许可，贵公司不得将本作品部分或全部公布于公开媒体或互联网，不得发送给第三方，贵公司的子公司、分公司或下属单位除外。
5. 任何单位或个人不得侵犯本作品著作权，否则绿盟科技保留追究权人法律责任的权利。



THE EXPERT BEHIND GIANTS

## 巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，  
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具  
有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。  
在这些巨人的背后，他们是备受信赖的专家。



# 信息安全意识漫谈

## SECURITY COMIC TALK

 **NSFOCUS** 绿盟科技



# 目录 CONTENTS

---

## 01 办公区域 Office Area

---

陌生人进入	03
会议安全	04
锁屏	05
桌面安全	06
办公区域安全总结	07

---

## 02 WIFI安全 Wi-Fi Security

---

免费WIFI接入	08
私搭WIFI热点	09
WIFI自动连接	10
WIFI万能钥匙	11
WIFI安全总结	12

---

## 03 个人电脑 Personal Computer

---

文件加密存储	13
弱口令	14
密码分级	15
软件下载	16
系统更新	17
文件删除	18
数据备份	19
个人电脑安全总结	20

---

## 04 邮件安全

Email Security

传输加密	21
钓鱼邮件	22
附件病毒	23
恶意链接	24
邮件安全总结	25

## 05 移动办公

Mobile Office

短信链接木马	26
越狱和ROOT	27
二次验证防盗号	28
应用安装	29
SIM卡和SD卡安全	30
手机出售前脱密	31
手机使用安全总结	32
手机丢失后被钓密码	33
手机丢失后处理总结	34

## 06 日常交流

Daily Communication

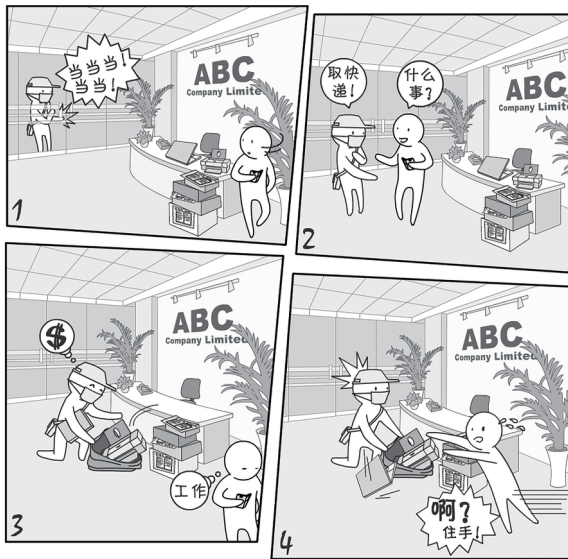
私建工作聊天群	35
敏感资料随意分发	36
代码发布到github	37
外部打印	38
公用共享文件夹使用	39
日常交流总结	40

# 01

## 办公区域

Office Area

### 陌生人进入



- 案例解析 伪装成各种工作人员进行作案也是商业间谍或黑客收集信息的重要方式之一，快递员是写字楼最常见的工作人员，所以也是伪装后最不容易引起注意的角色。另外，也不能排除个别快递人员的职业操守问题。
- 安全建议
  - 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注意随手关门

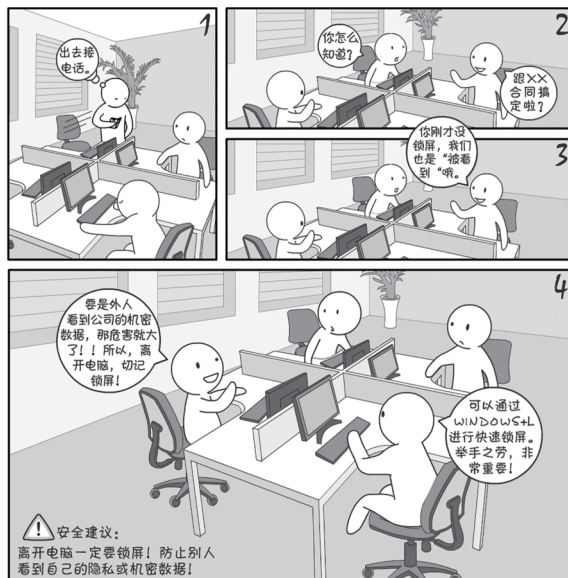
## 会议安全



▣ 案例解析 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经授权知晓的人员，容易带来各种不可预知的后果。

- ▣ 安全建议
- 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



▣ 案例解析 同事之间工作内容、工作性质不同，有权看到的信息内容、信息密级也可能不同。中午吃饭或上洗手间的时间如果不锁屏，同事们不光能看到屏幕内容，别有心的人还会打开电脑中各种文件甚至用U盘拷出。

- ▣ 安全建议
- 短时间离开电脑请按win+L键锁屏
  - 长时间离开电脑建议关机
  - 日常请设置屏保程序，建议在10分钟以内自动启动，并勾选“恢复时显示登录屏幕”，以免离开电脑忘记锁屏。

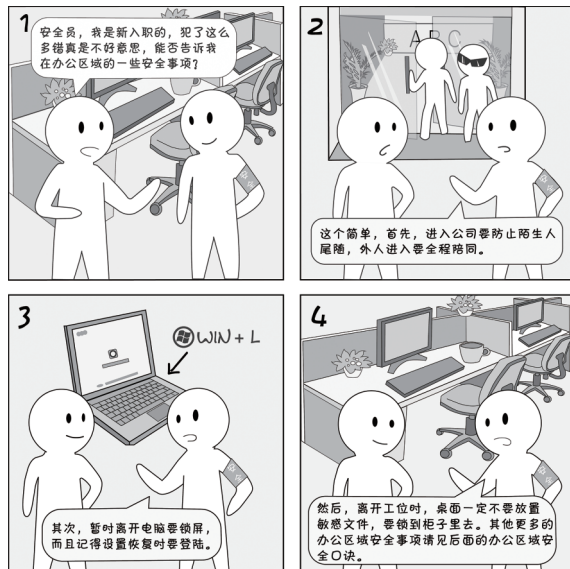
## 桌面安全



■ 案例解析 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情，特别是对于面向公众办公的单位，桌面如果放有敏感文件，很容易被拿手机偷拍或随手带走。

- 安全建议
- 同样要强调电脑要锁屏
  - 敏感文件一定要锁到柜子里
  - 桌面不要遗留门禁卡、钥匙、手机等重要物品

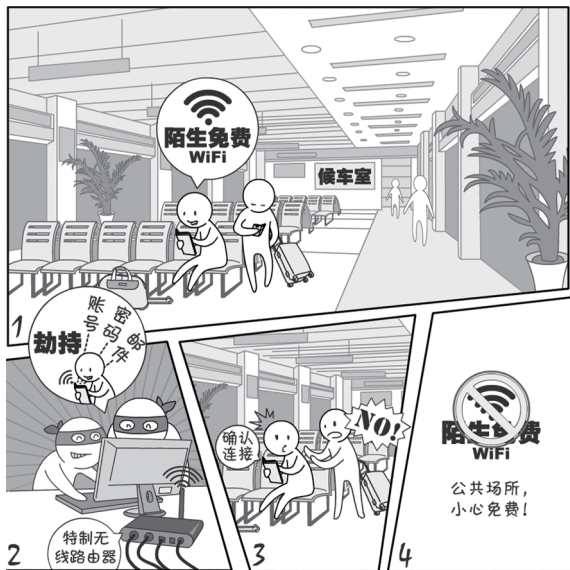
## 办公区域安全总结



## 办公区域安全口诀

- 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；

## 免费WiFi接入



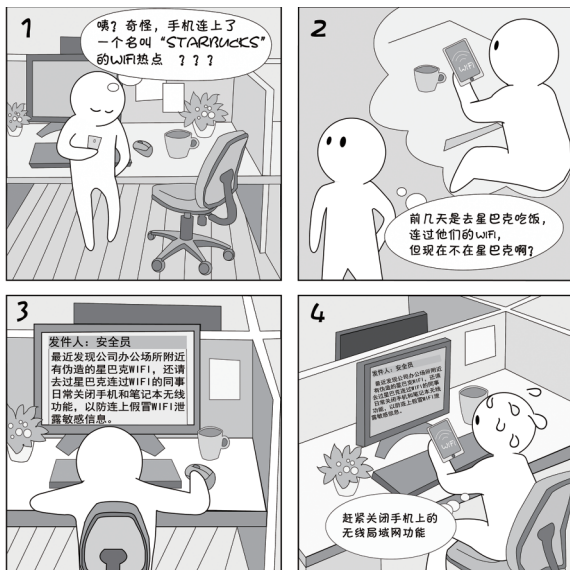
- **案例解析** 不法分子通常会搭建与常用WiFi名相同或相近的WiFi，设置空密码或相同密码吸引公众连接，然后在WiFi路由器上劫持DNS，将你引入到钓鱼网站获取你的账号密码，或者在路由器上监听手机流量，获取明文密码。
- **安全建议**
  - 在公共场合连接WiFi时请同商家仔细确认WiFi名称
  - 没有密码的公共WiFi请慎用
  - 在使用支付APP时请使用运营商4G网络，不要使用公共WiFi

## 私搭WiFi热点



- **案例解析** 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，如果配置不当，家用最多导致蹭网或个人资料泄露，但在公司使用可能会导致内网被入侵，公司机密、客户资料泄密，后果不堪设想。
- **安全建议**
  - 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检查
  - 认证方式使用安全的WPA2算法
  - 建议隐藏SSID，绑定接入设备的MAC地址
  - WiFi密码必须8位以上，包含大小写、数字和标点符号，定期改密码

## WIFI自动连接



■ 案例解析 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。

- 安全建议
- 日常不用WiFi时关闭手机和笔记本的无线局域网功能，以防自动连接恶意WiFi
  - 当手机或笔记本连接上WiFi后，留意连接到的WiFi热点名称

## WIFI万能钥匙

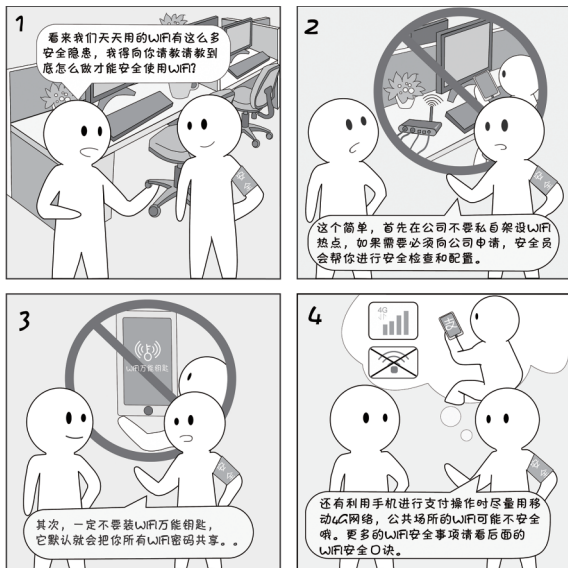


■ 案例解析 手机上的WiFi万能钥匙类的APP在安装时默认设置会自动上传你所连接的WiFi的密码。这些密码一般不会明文给出，只会在连接WiFi时自动输入，但曾爆出漏洞用一个APP能读出检测到WiFi的密码，这样就可以用笔记本接入WiFi使用更强大的攻击工具了。

- 安全建议
- 建议不要使用WiFi万能钥匙类APP
  - 如果必须使用建议关掉自动上传密码功能



## WIFI安全总结



## WIFI安全口诀

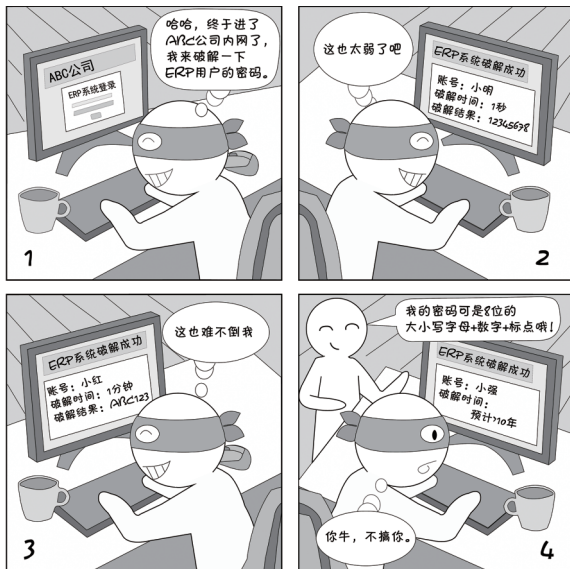
- 公共场合连WIFI，名称一定确认好；
- 无密WIFI不要连，安全支付用4G；
- 私搭路由要审批，安全设置莫忘记；
- WIFI不用要关闭，万能钥匙请回避；

## 文件加密存储



- 案例解析 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载加密盘才能看到其中的文件，就有效避免了重要文件泄密。
- 安全建议
  - 敏感文件建议存放在加密盘中，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Bitlocker或Truecrypt

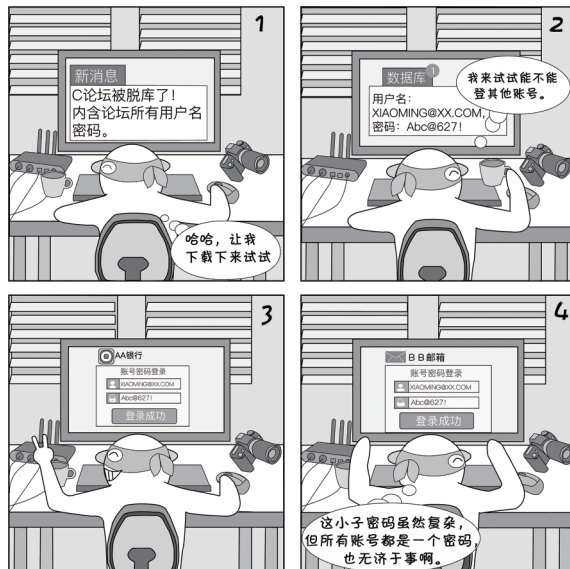
## 弱口令



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

- ▣ 安全建议
- 包含大小写字母，数字和标点符号，位数在8位以上
  - 不能包含名字、生日、手机号或车牌号
  - 定期修改各种密码，如三个月或半年

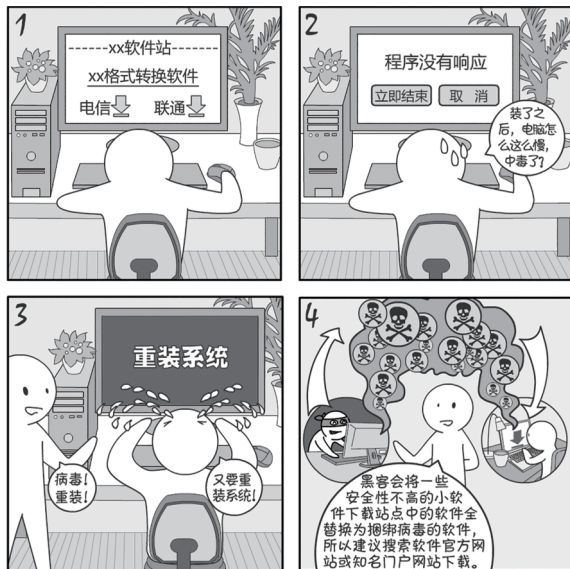
## 密码分级



▣ 案例解析 很多人各网站用户名密码相同，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。

- ▣ 安全建议
- 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

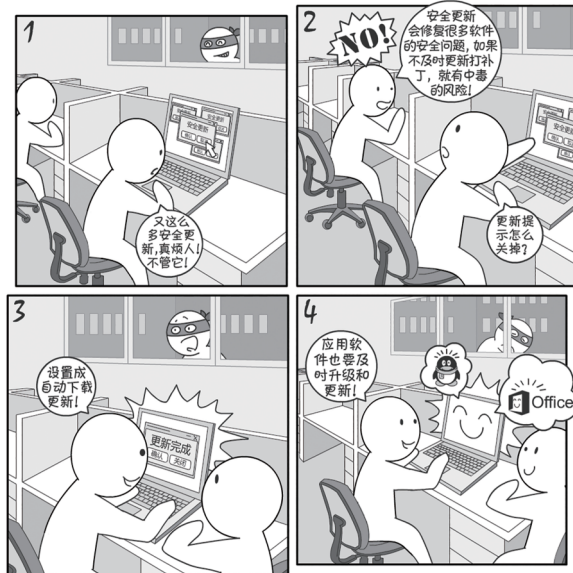
## 软件下载



- ▣ 案例解析 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, 一般都会做成免杀版, 各种主流杀软无法检测到。
- ▣ 安全建议

  - 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

## 系统更新



- ▣ 案例解析 操作系统和软件的安全更新就如同汽车的缺陷召回, 安全更新修复了已知的可能导致系统被入侵或用户信息泄露的的漏洞。更重要的是, 每个更新补丁发布时, 黑客会多方收集漏洞细节和利用方法, 这几天就成为用相应的漏洞进行攻击的高峰期。
- ▣ 安全建议

  - 建议打开操作系统和各种应用的自动安装更新, 或有更新时提示
  - 建议得知漏洞或更新通告后, 了解漏洞详情, 对于重要的更新第一时间手工安装

## 文件删除



- 案例解析 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,其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。
- 安全建议
  - 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
  - 电脑出售或者移交其他人使用,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



- 案例解析 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。
- 安全建议
  - 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

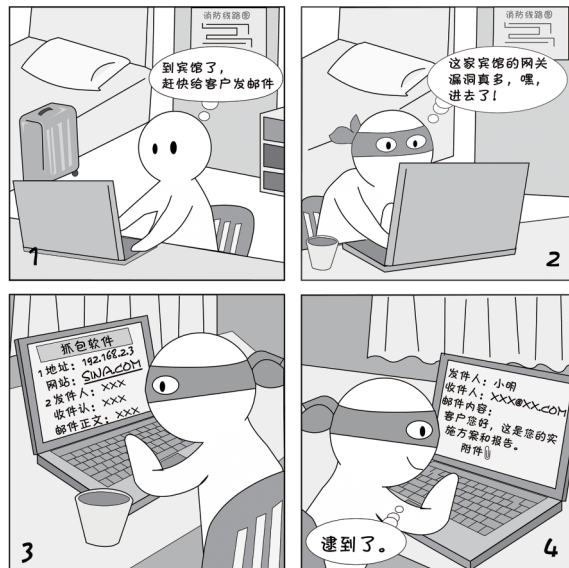
## 个人电脑安全总结



## 个人电脑安全口诀

- 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，分级安全又好记；
- 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。

## 传输加密



- 案例解析 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。这个场景易出现在一些针对性的商业间谍活动中。
- 安全建议
  - 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

## 钓鱼邮件

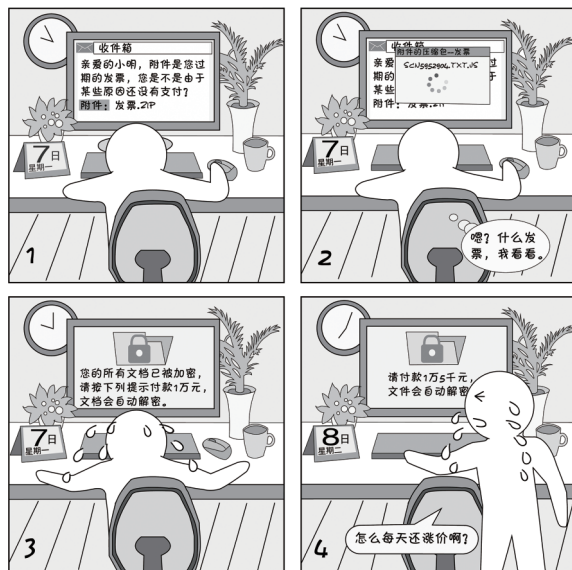


▣ 案例解析 钓鱼邮件种类繁多, 利用邮件骗取回复敏感信息是最简单和常见的钓鱼方式。这种邮件都自称是领导或网站管理, 看到这种邮件一般会头脑发热, 精神紧张, 很容易不假思索就按要求回复了。

▣ 安全建议

- 遇到索要敏感信息的邮件首先要保持冷静、提高警惕。
- 如果对邮件所说内容不知情, 请勿点击链接或回复, 直接电话向发件人代表的人员确认。

## 附件病毒

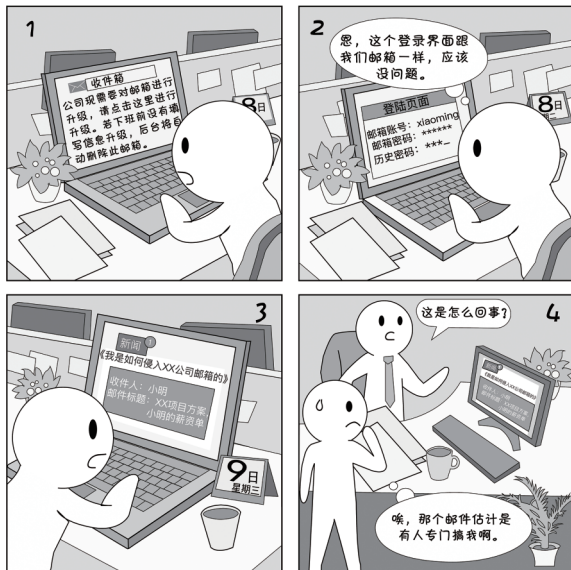


▣ 案例解析 勒索病毒邮件一般是英文邮件, 主题和正文诱导你打开附件。附件是压缩包, 因为病毒文件是js后缀的可执行文件, 文件名还用了.txt来伪装成安全的文本文件。此病毒对文档的加密强度很高, 只有付款才能解密文档。

▣ 安全建议

- 确保自己的邮件客户端禁止方可执行文件, 可以自己给自己发一个.exe后缀的文件测试一下
- 要认为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。
- 虽然你必须要装防病毒软件, 但不要完全相信防病毒软件。

## 恶意链接



- 案例分析 包含链接并链接到钓鱼页面的邮件比较具有迷惑性，因为让受害者看到了和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木马页面，打开后直接就会中木马。
- 安全建议
  - 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，直接电话向发件人代表的人员确认。
  - 设置默认浏览器为非IE内核浏览器，因为IE内核浏览器可被利用漏洞相对较多

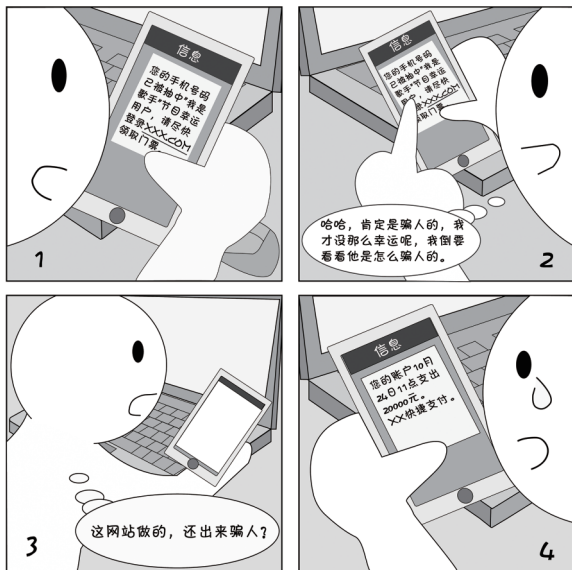
## 邮件安全总结



## 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。

## 短信链接木马



- 案例解析** 这个案例虽说也是短信开始，骗到钱结束，但跟普通的电信诈骗不同的是利用了恶意链接和挂马页面，科技含量非常高。手机中木马后，黑客通过在后台监听截获短信验证码的方式，结合其他途径已经获取的身份证、银行卡信息，注册了受害人的银行卡快捷支付。
- 安全建议**
  - 及时根据系统提示升级手机系统和APP，减少挂马页面可利用的漏洞
  - 手机中安装安全软件
  - 不要点击任何短信中的链接

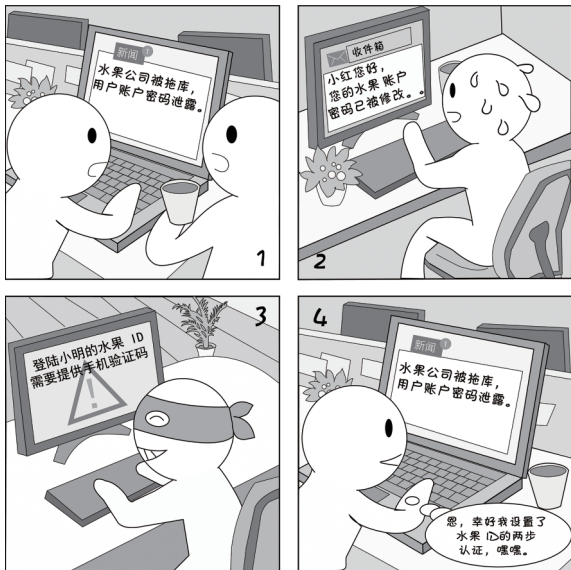
## 越狱和ROOT



- 案例解析** 安卓的ROOT和苹果的越狱都是使普通的APP获取手机最高权限，这样恶意的APP可以随意读写删除手机文件、监听截获短信和数据流量、后台随意安装其他APP等，也使得手机在打开挂马页面时更容易中木马。有些木马甚至可以自行对手机进行ROOT操作。
- 安全建议**
  - 非专业人员或爱好者切勿越狱或ROOT
  - 安装安全防护软件，并在官方市场下载应用

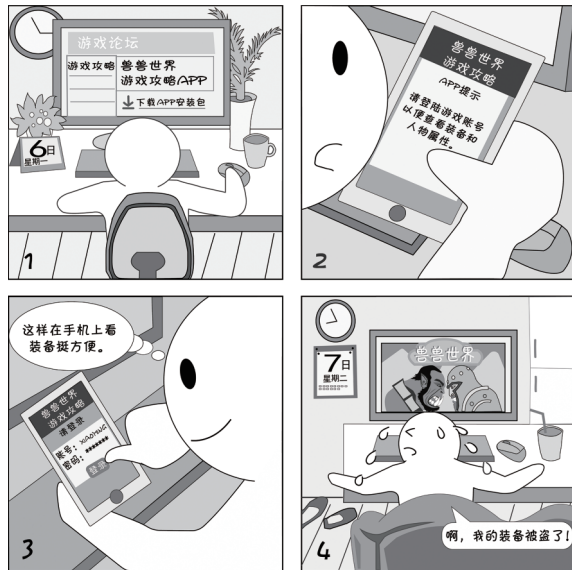


## 二次验证防盗号



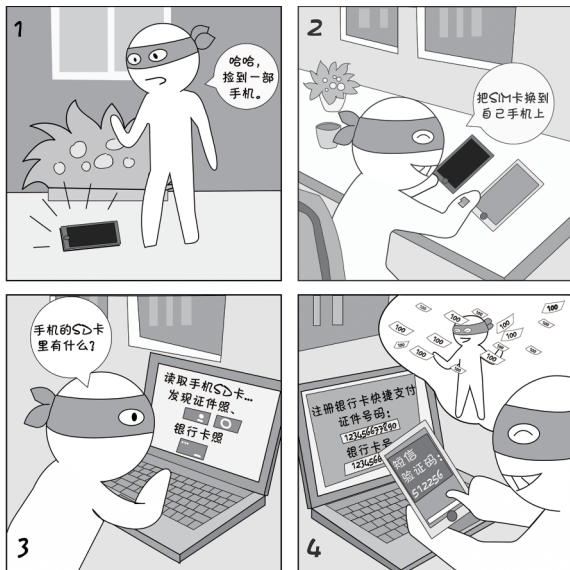
- **案例解析** 用一个密码来保护账号是常用的认证方式, 但密码泄露后账号就不保。现在很多手机厂商账号或APP账号支持二次验证, 当检测到你的账号在其他手机登陆时, 会增加一种除了密码外的验证方式, 比如短信验证码。
- **安全建议**
  - 关注你的各种重要账号是否开启了二次验证, 有些是默认打开, 有些是需要人工开启
  - 不要告诉任何人你的短信验证码
  - 换手机号后记得修改二次验证通知的手机号

## 应用安装



- **案例解析** 目前手机APP应用市场多如牛毛, 各市场对上架APP的审核力度不一, 有些市场安全性不够还被黑客入侵, 将正常APP替换为恶意APP。
- **安全建议**
  - 下载应用务必到手机操作系统官方应用商店下载, 或到应用的官网扫码下载
  - 安装应用时谨慎选择应用所需的权限, 后期若影响使用提示权限不足还可手工修改

## SIM卡和SD卡安全



■ 案例解析 手机丢失后如果不及时挂失SIM卡，黑客可轻易取出换到另一部手机里收取验证短信。注册银行卡的快捷支付只需要证件号码、银行卡号和短信验证码。

- 安全建议
  - 为SIM卡设置PIN码，手机重启或更换手机后必须输入PIN码才能使用这个号码
  - 手机或SD卡上不要存储敏感信息，比如身份证照片、银行卡照片、工作文档，以免手机丢失后被不法分子利用

## 手机出售前脱密



■ 案例解析 手机恢复出厂设置只是把系统文件简单还原、用户数据简单删除，在手机内部存储芯片上并未彻底删除，就如同我们在电脑上删除文件一样。

- 安全建议
  - 手机出售前除了恢复出厂设置外，还需要用大的视频文件反复拷贝删除几次
  - 技术宅可以用非原厂ROM刷机，这样可以清除可能遗留的原厂账号信息

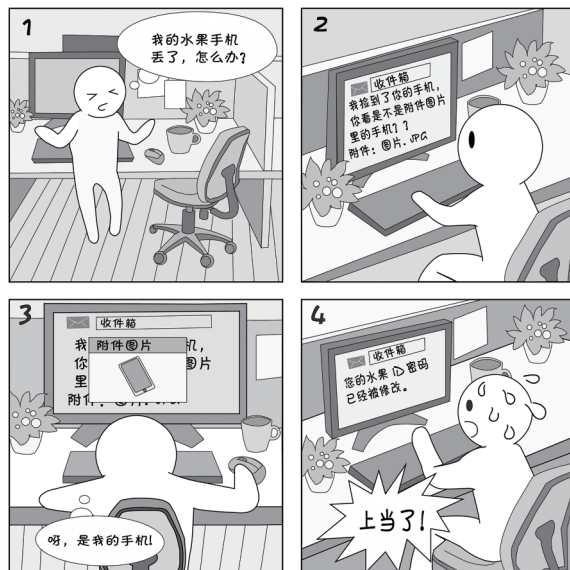
## 手机使用安全总结



## 手机日常安全口诀

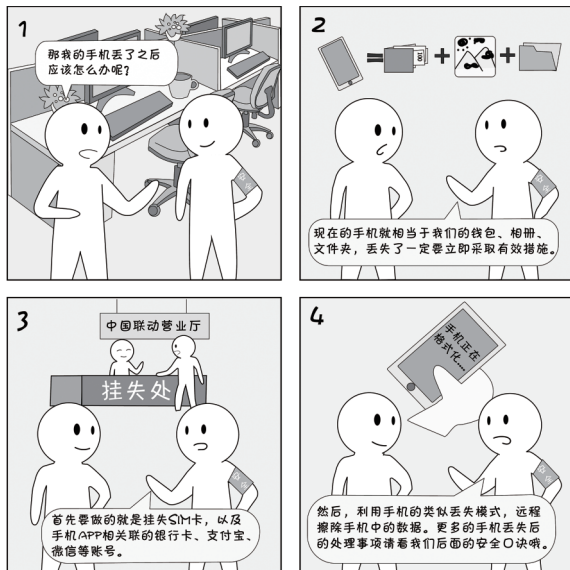
- 系统和应用勤升级，短信链接勿点击；
- 安全软件要安装，越狱ROOT隐患多；
- 二次验证一开启，密码泄露不着急；
- 应用下载到官方，后台权限谨慎选；
- SIM卡要加PIN码，敏感信息莫留存；
- 手机出售要重置，视频文件刷几次；
- 远程擦除要设置，手机丢失一键清。

## 手机丢失后被钓密码



- 案例解析 不法分子在得到丢失的IPHONE后，因为没有你的APPLE ID密码，无法解锁手机，因此会想尽办法得到或修改你的密码，比如如果你的APPLE账号是QQ邮箱，就会给你QQ邮箱发钓鱼链接，获取浏览器COOKIE，即可登录你的QQ邮箱重置密码。
- 安全建议
  - 手机丢失后若收到捡到你手机的邮件，切勿点击任何链接、图片或附件

## 手机丢失后处理总结



## 手机丢失后安全口诀

- 手机丢失莫着急,挂失SIM卡排第一;
- 支付账号要挂失,被盗报警要牢记;
- 远程锁定或擦除,重要APP要改密;
- 钓鱼邮件要防范,告知亲朋防诈骗。

## 私建工作聊天群



- 案例解析 聊天群在方便沟通的同时,也隐藏着巨大的隐患,比如冒名进来的不怀好意的人,被盗号后群聊信息泄密,离职后潜伏在工作沟通群中等。
- 安全建议
  - 工作相关聊天群尽量使用单位搭建的有专人进行人员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)中,管理员要严格审核加群人员,并及时踢出离职或离开项目组人员
  - 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



- 案例解析 单位的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或多或少的不良影响。
- 安全建议
  - 各种方案、合同、报告、代码等比较敏感的文件在分发时务必注意密级以及单位授权的扩散范围
  - 若发现网上有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



- 案例解析 黑客在入侵一个网站或系统之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接口账号或安全漏洞。
- 安全建议
  - 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连接到开发机上进行，不可利用网盘、代码库进行共享
  - 重要系统的代码用U盘拷贝需要经过单位同意并做好保护措施，使用完毕彻底删除

## 外部打印



▣ 案例解析 打印社的电脑上一一般都保存有很多已打印的文档，打印社并无动力定期清除，并且客户随意拷贝没有限制，是一个很容易泄露敏感文件的场景。

- ▣ 安全建议
- 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
  - 有条件的可以用防拷贝U盘，可以防止将U盘文件刻意拷贝到电脑上

## 公用共享文件夹使用



▣ 案例解析 公共共享文件夹一般会搜到各个部门各种各样的文档，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，暴露给侵入内网的黑客或内部恶意人员。

- ▣ 安全建议
- 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以在服务器上恢复
  - 共享服务器管理员可以设置定期自动清理共享文件夹

## 日常交流总结



## 日常交流安全口诀

- 工作群聊须谨慎，敏感信息私下传； ■ 加群严审查，关注离职及时踢；
- 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；
- 外部打印需谨慎，U盘打开可打印； ■ 共享目录是方便，敏感文件勿上传。

