信息安全意识漫谈

SECURITY COMIC TALK

NSFOCUS绿盟科技

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. 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侵权人法律责任的权利。

目录 CONTENTS

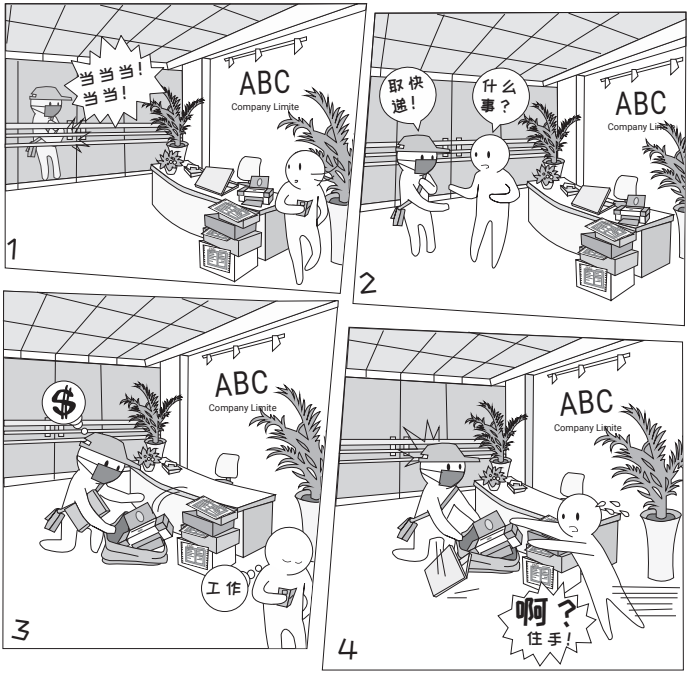
04 邮件安全
Email Security

05 移动办公
Mobile Office

06 日常交流
Daily Communication

01 办公区域

陌生人进入



案例解析 乔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
- 进出大门时注意是否有尾随人员
- 带外人进入要前台登记并全程陪同
- 对于不能自动闭合的大门注意随手关门

01 办公区域

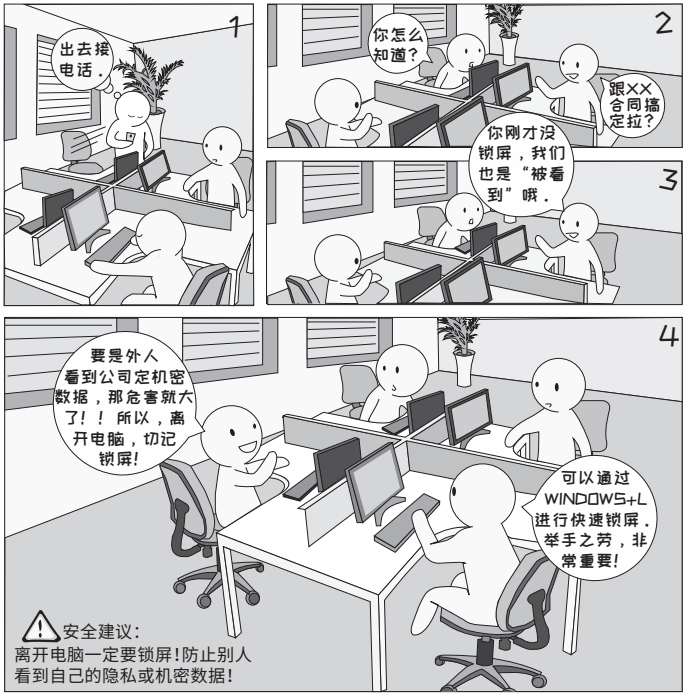
案例解析 利用会议室白板讨论的一般都是一些主要思路、关键结论，这些内容如果泄露给未授权知晓的人员，容易带来各种不可预知的后果。

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

01 办公区域

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，别有用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
- 设置屏保程序，10 分钟内自动启动，勾选“恢复时显示登陆屏幕”

01 办公区域

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
- 桌面不要遗留门禁卡、钥匙、手机等重要物品
- 敏感文件一定要锁到柜子里

01 办公区域

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
- 离开电脑要锁屏，设置自锁十分钟
- 会议过程不拍照，会后谨记擦白板
- 敏感文件柜里锁，钥匙门禁身边留

02 WiFi 安全

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
- 慎用没有密码的公共 WiFi，使用支付 APP 时切换为运营商 4G 网络

02 WiFi 安全

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。
在公司私搭热点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

02 WiFi 安全

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

案例解析 手机上的 WiFi 密码共享类的 APP 在安装后如果设置或使用不当会自动上传你所连接过的 WiFi 密码，包括家里路由器或单位路由器的密码。这些密码一般不会明文给出，但用一些手段可以看到明文的密码。

安全建议

- 建议使用 WiFi 密码共享类 APP 时，手动关闭自动上传功能，不要在此类 APP 界面输入自己单位或家里的 WiFi 密码，以免被自动共享出去

02 WiFi 安全

WiFi 安全总结

WiFi 安全口诀

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

03 个人电脑

文件加密存储

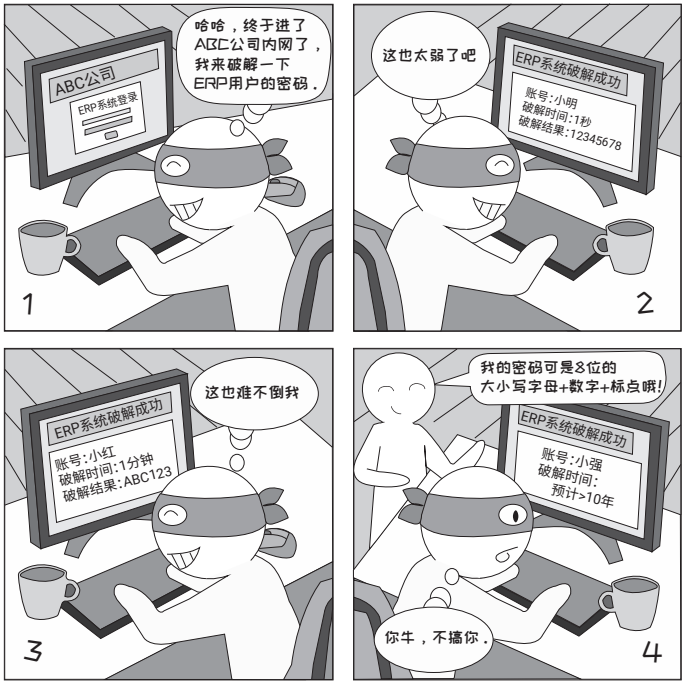
案例解析 文件直接放在硬盘上，电脑丢失后硬盘上文件就可以被直接读取，如果存到加密盘中，就必须输入加密盘密码才能看到其中的文件，有效避免了重要文件泄露。

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

03 个人电脑

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

03 个人电脑

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。

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
- 可以按账号重要程度进行分级，不同级账号设置不同密码
- 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

03 个人电脑

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
  - 查看下载软件的 MD5 值，同官网网站公布的 MD5 值做对比是否一致

03 个人电脑

系统更新

案例解析

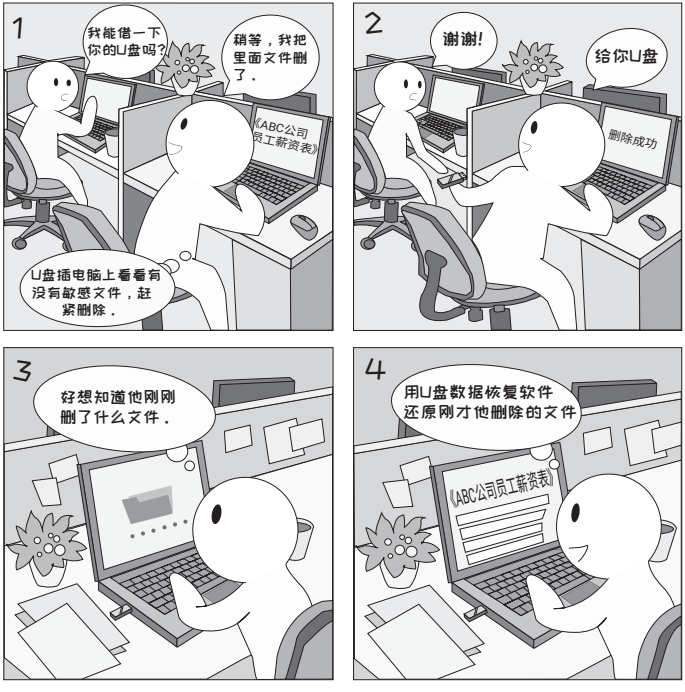
操作系统和软件的安全更新是用来修复可能导致系统被入侵或用户信息泄露的漏洞。如今，挖矿病毒抓住补丁发布后、用户更新前的空窗期，感染未及时更新补丁的电脑将其作为矿机，大量消耗 GPU 或 CPU 资源。

安全建议

- 建议打开操作系统和各种应用的自动安装更新，或选择“有更新时提示”
- 建议关注定期安全更新的发布日期（例如：Windows 是每月第二周的周二），留意更新通告，对于重要的更新第一时间手动安装

03 个人电脑

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，可点击鼠标右键查看
- 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

03 个人电脑

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

03 个人电脑

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

04 邮件安全

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．这个场景容易出现在一些针对性的商业间谍活动中。

安全建议

- 一般在邮件客户端“发送和接收服务器”处勾选 SSL，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

04 邮件安全

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，直接电话向发件人确认

04 邮件安全

附件病毒

- **案例解析**　勒索病毒邮件的主题和正文诱导你打开附件。附件实际为 JS 可执行文件，黑客用压缩包的形式和 .txt 进行伪装。此病毒对文档的加密强度很高，只有付款才能解密。
- **安全建议**
  - 确保自己的邮件客户端禁止访问可执行文件，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
  - 防病毒软件不一定能检测出最新病毒木马，因此不要放松警惕

04 邮件安全

恶意链接

- 案例解析：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挂马页面，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

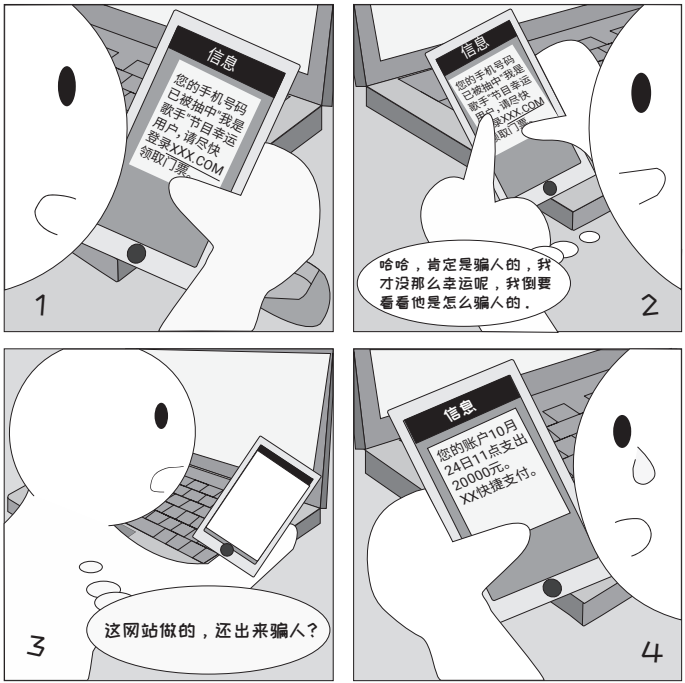
04 邮件安全

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
- 默认浏览器非 IE，陌生链接勿点击
- 各种附件谨慎点，可执行文件风险高
- 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，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，恶意 APP 可以随意读写删除手机文件、监听截获短信和数据流量、后台安装 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

05 移动办公

二次验证防盗号

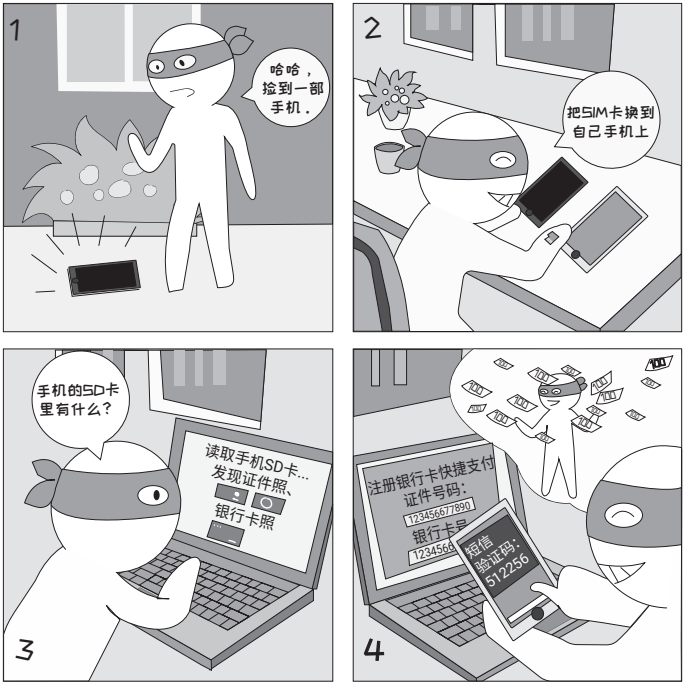
- **案例解析** 用一个密码来保护账号是常用的认证方式，但密码泄露后账号就不保。现在很多手机厂商账号或 APP 账号支持二次验证，当检测到你的账号在其他手机登陆时，会增加一种除了密码外的验证方式，比如短信验证码。
- **安全建议**
  - 关注你的各种重要账号是否开启了二次验证，有些是默认打开，有些是需要人工开启
  - 不要告诉任何人你的短信验证码
  - 换手机号后记得修改二次验证通知的手机号

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动修改

05 移动办公

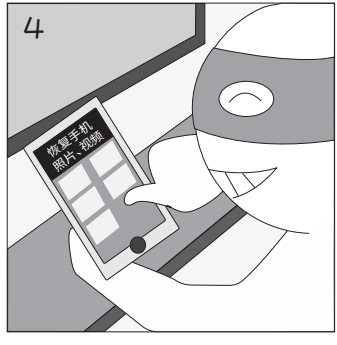
SIM 卡和 SD 卡安全



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



案例解析 手机恢复出厂设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

05 移动办公

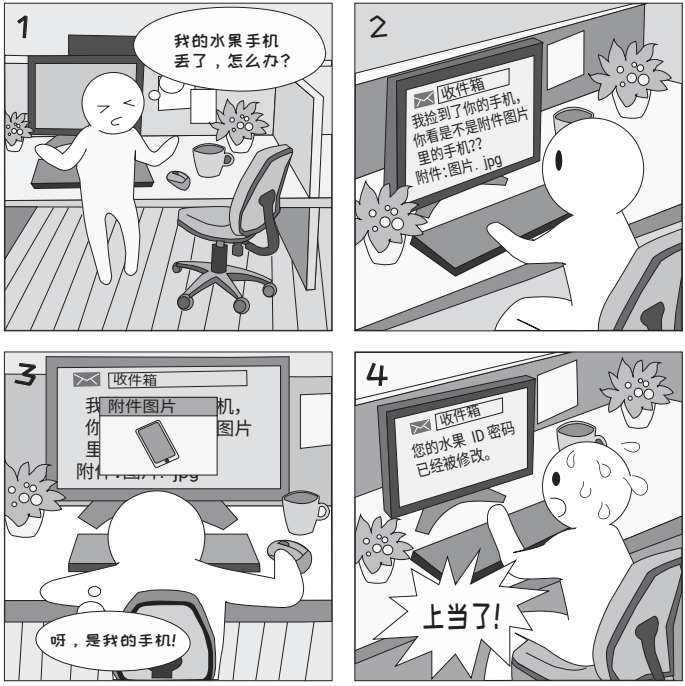
手机使用安全总结

手机日常安全口诀

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

05 移动办公

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

05 移动办公

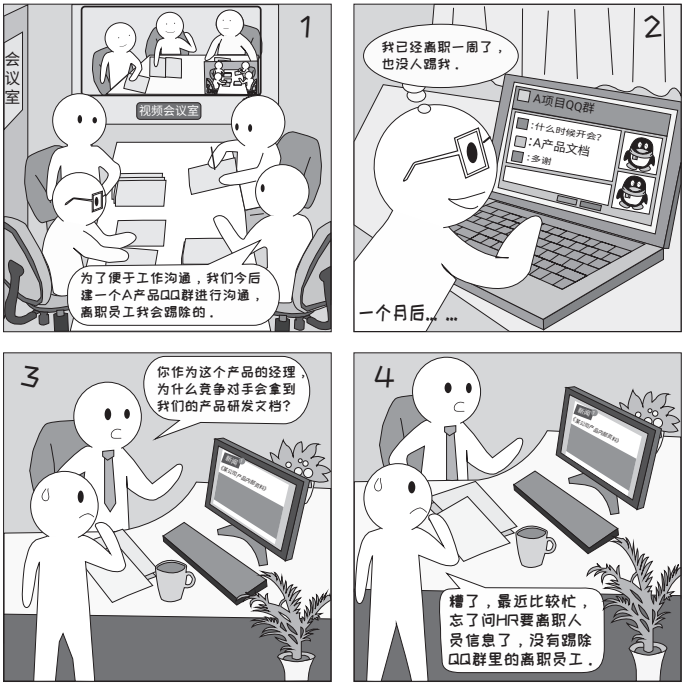
手机丢失后处理总结

手机丢失后安全口诀

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

06 日常交流

私建工作聊天群



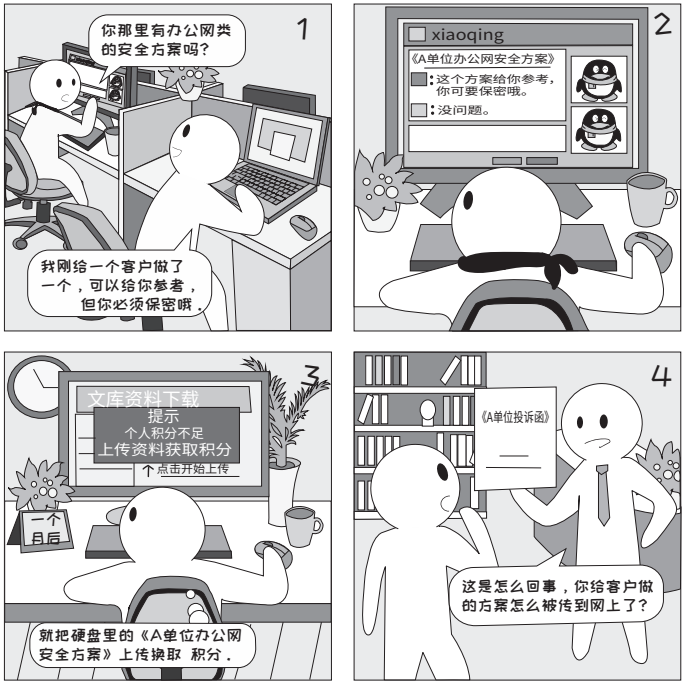
案例解析 聊天群在方便沟通的同时，也隐藏着巨大的隐患，比如冒名进来的不怀好意的人，被盗号后群聊信息泄密，离职后潜伏在工作沟通群中等。

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

06 日常交流

敏感资料随意分发



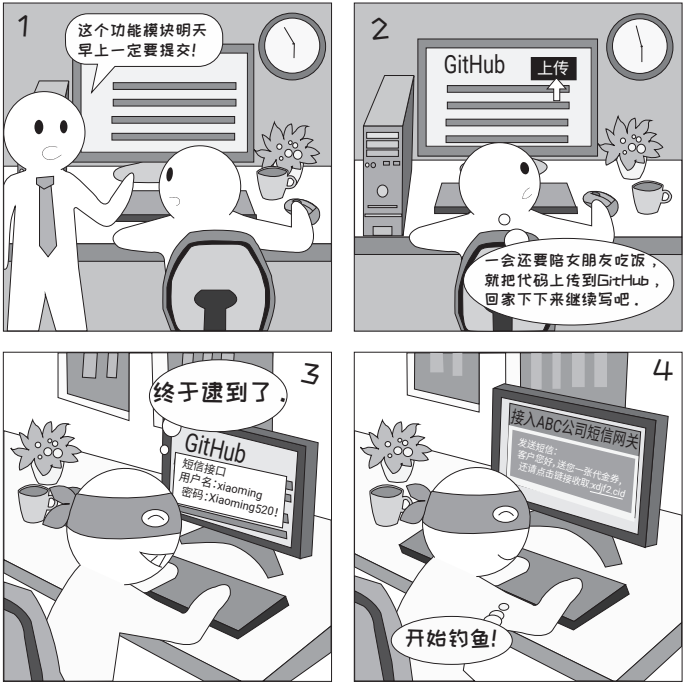
案例解析 单位的各类文档实际上都有授权扩散范围，比如与客户项目相关的文档均为商业机密，只能在项目组内部扩散，泄露后会给双方带来或多或少的不良影响。

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

06 日常交流

代码发布到 GitHub



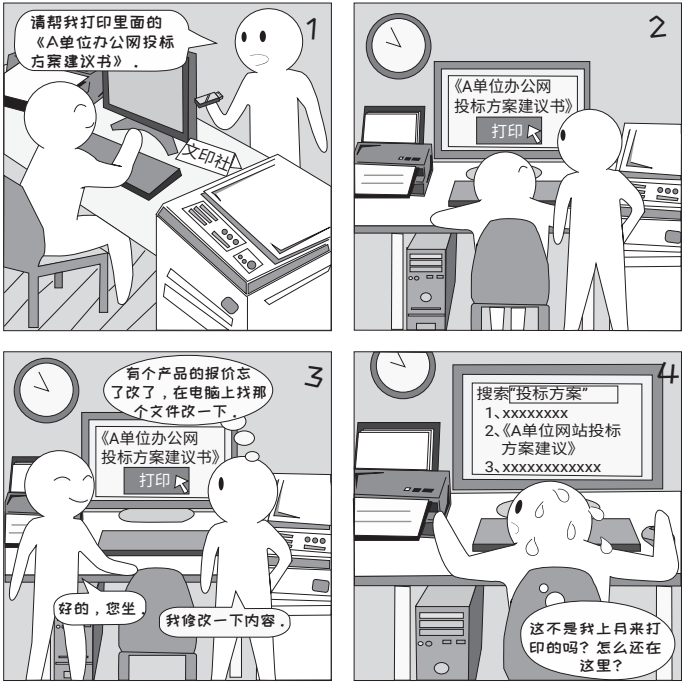
案例解析 黑客在入侵一个网站或系统之前会到网上搜索此网站的相关信息，如果没有安全意识的开发人员将代码上传公共代码库，黑客会分析找出其中的接口账号或安全漏洞。

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

06 日常交流

外部打印



案例解析 打印社的电脑上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

06 日常交流

公用共享文件夹使用

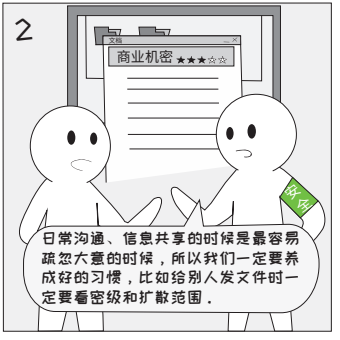
案例解析 公用共享文件夹一般会搜到各个部门各种各样的文档，包含很多敏感文件。敏感文件通常都是共享拷贝后忘了删除和剪切而遗留下来，暴露给侵入内网的黑客或内部恶意人员。

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

06 日常交流

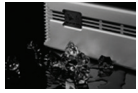
日常交流总结



日常交流安全口诀

- 工作群聊须谨慎，敏感信息私下传
- 敏感资料勿乱发，扩散范围要看准
- 外部打印需谨慎，U 盘打开可打印
- 加群严审莫被骗，关注离职及时踢
- 产品代码莫上网，在家可连 VPN
- 共享目录是方便，敏感文件勿上传











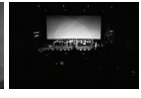
CSA SUMMIT CHINA 201
云安全





2000
INFOCUS
INFORMATION
TECHNOLOGY
CO.,LTD
INFOCUS









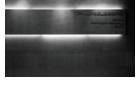
INFOCUS











2000
INFOCUS
INFORMATION
TECHNOLOGY
CO.,LTD
INFOCUS

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。

www.nsfocus.com