信息安全24小时

INFOSECURITY AROUND THE CLOCK

NSFOCUS绿盟科技

版权声明

1. 《信息安全24小时》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

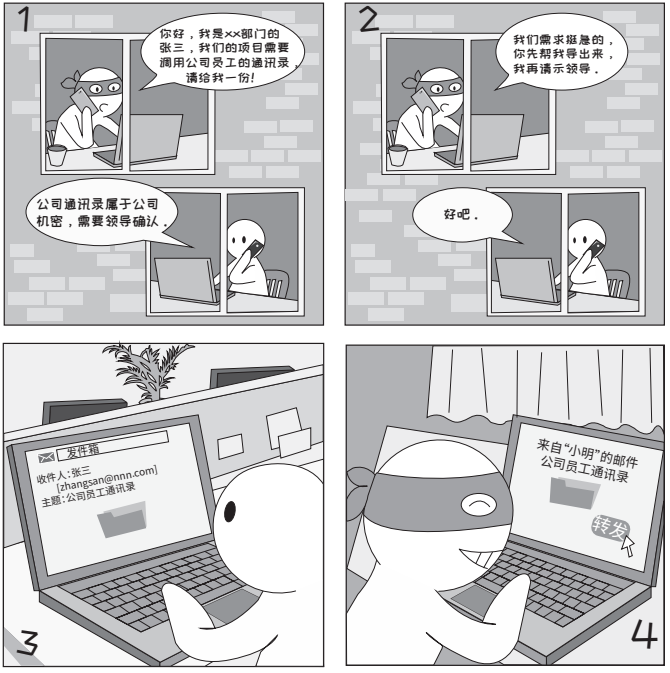
03 移动场所安全
Cyber Security at a Public Place 24

01 办公场所安全

Cyber Security in Office

在现代高速发展的信息网络技术下，信息安全在企业信息化的建设中占有越来越重要的位置。现代信息和网络技术就像一把双刃剑。一方面，企业借助信息系统准确、高效、互联的特性拥有了更大的发展空间；另一方面，企业也不得不关注由此引发的信息安全问题，而办公场所安全是最需要警惕的。

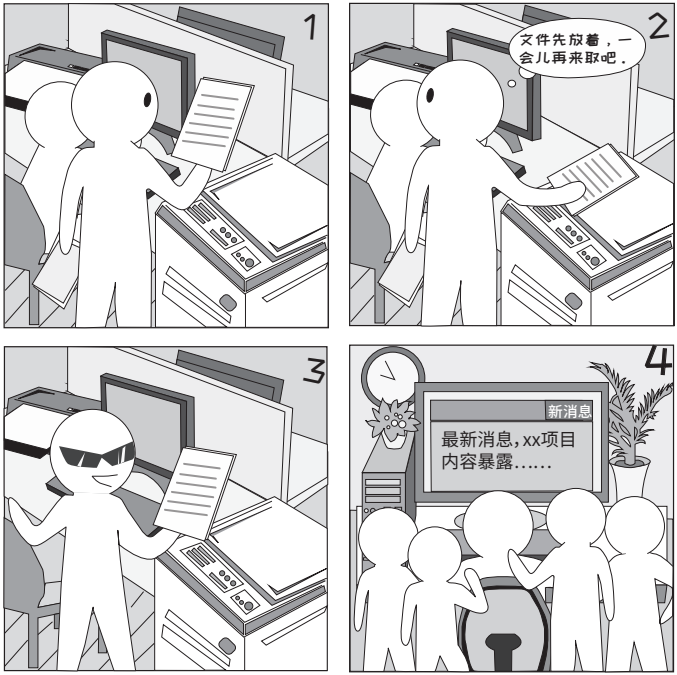
01 办公场所安全



- 案例解析　这个方法的实施需要黑客首先通过搜索引擎或者其他渠道掌握一些内部消息，本案例中黑客在信息收集中打听到公司内的通讯录由办公室保管，小明在处理事件时，也没有按照流程，没有验证对方身份的真实性就把信息给了出去，从而造成信息泄露。
- 安全建议
  - 在接到电话或者邮件索要公司内部资源，比如文档，客户信息等，都要验证其身份，向其领导确认是否存在此人并且要求其按照流程申请资源，不能直接将信息发给对方，以免造成公司内部信息泄露。

01 办公场所安全

纸质文件保护



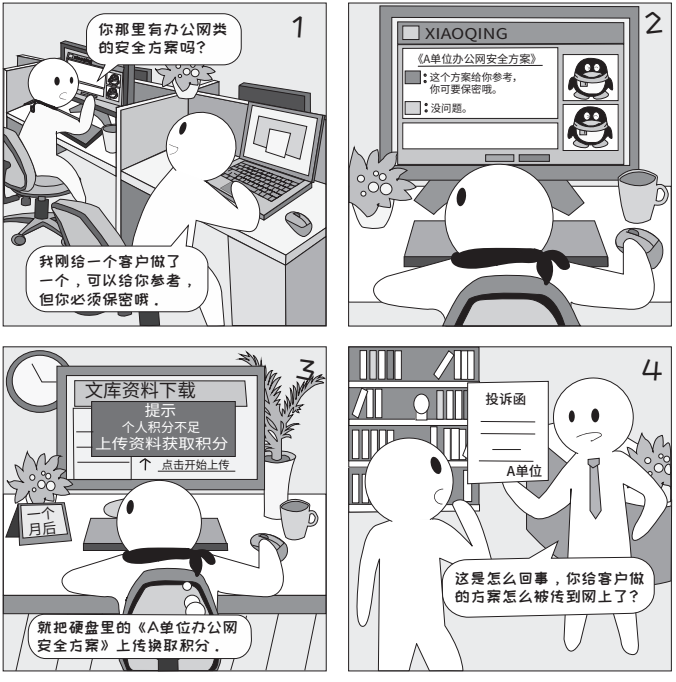
案例解析 办公场所是安全事件的频发地，许多员工认为办公室没有外人，所以不注意办公场所内纸质资料的保护。本案例中小明把未打印完的资料放在打印机旁直接离开，被人看到后带走，造成资料丢失。

安全建议

- 妥善保管纸质资料，不随意乱放；
- 离开座位时，把翻开的纸质资料放到抽屉或文件夹内，不把内容暴露出来；
- 带有公司内部信息的纸质材料，使用完毕后使用碎纸机销毁，不要直接丢掉；
- 在办公室内使用公共打印机时，打印期间不要离开，以免造成文件丢失。

01 办公场所安全

敏感资料保护



案例解析 企业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保密等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，请立即通知单位保密人员进行投诉和删除。

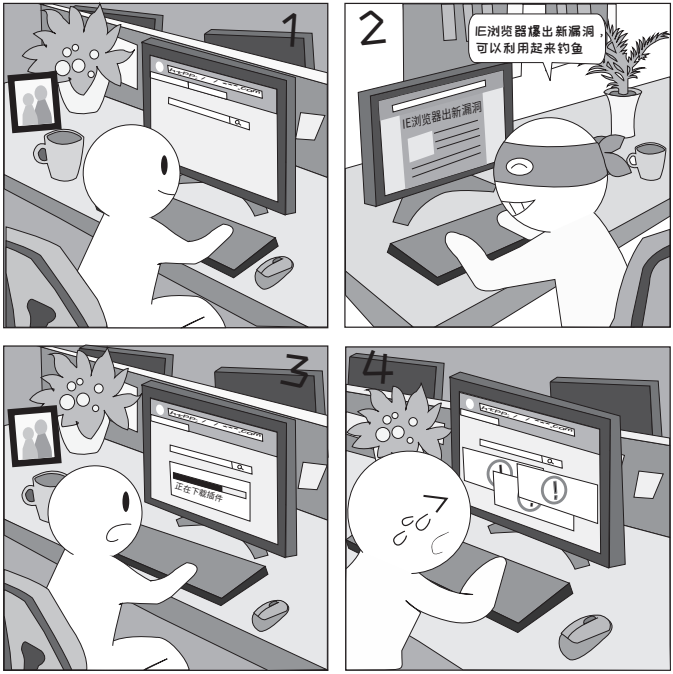
案例解析 密码是个人网络信息安全的钥匙，保护密码安全是保护个人网络信息安全的第一步。

安全建议
- 最好不要直接把密码记录在纸质文件上，一旦文件丢失，个人信息将会被泄露；
- 可以把密码记录存储到加密盘里，电脑配置自动锁屏，可以减小密码丢失的概率。

01 办公场所安全

软件下载

- **案例解析** 下载到非正版软件后，软件可能会绑有木马程序，盗取用户账号和密码，并在运行时读取用户在软件中存储的内容，造成不同程度的机密泄露。
- **安全建议**
  - 建议去官方网站下载软件；
  - 下载后用 MD5 工具查看下载软件的 MD5 值，并和官网工具的 MD5 值做对比，如果不一样则肯定被修改过；
  - 保证杀毒软件版本为最新版本。



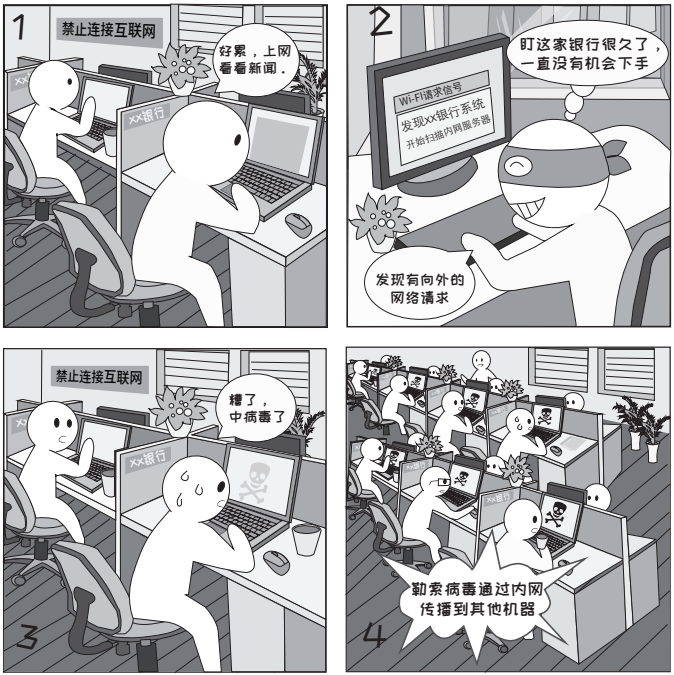
案例解析 IE 浏览器的安全性相对偏低，黑客常常会利用 IE 的漏洞进行钓鱼攻击、数据窃取等操作。如果使用低版本的 IE，部分漏洞未修复，更容易遭到黑客攻击。

安全建议

- 建议使用安全性更高的浏览器 Firefox、Chrome 等；
- 养成好的上网习惯，尽量不在网页中保存账号、密码；
- 访问外部资源时，尽量使用非 IE 内核的浏览器；
- 及时升级系统和软件版本，避免由于低版本漏洞造成信息泄露。

01 办公场所安全

内网违规外连



案例解析 黑客通过 IP 监控到公司出口流量，然后做 DNS 劫持让小明在访问某个网页的时候自动下载木马程序，病毒传染到办公室其他电脑上。

安全建议

- 根据单位规定，禁止连接外网的网络坚决不能连接；

同样需要注意的是，外来电脑禁止连接内部网络。

01 办公场所安全

不明 U 盘使用

案例解析 不明来源的移动设备容易携带木马病毒，携带病毒的设备插入电脑后，可通过多种方式传播，造成电脑文件丢失、系统无法启动等问题。

安全建议

- 建议不要直接把不明来源的存储设备连接到办公电脑上，以免造成数据丢失；
- 电脑关闭系统“自动播放”功能，打开“设置”“设备”“自动播放”，选择“关闭”；
- 插入 U 盘后先用杀毒软件进行扫描。

01 办公场所安全

邮件弱密码

案例解析 邮件密码强度是邮件安全中关键的一环，用户经常由于设置弱密码导致被黑客轻松破解，从而泄露个人数据。设置密码的方法请参考安全建议。

安全建议

- 设置一个复杂度高又好记得密码，例如 : 给我涨工资吧 ! Ge1wzgzb !
- 密码定期更新，一般建议三个月更新一次密码 ;
- 多个账户使用不同的密码。

01 办公场所安全

病毒处理

案例解析 在使用电脑时，如果发现电脑运行缓慢、自动弹出奇怪的网页，更严重的有系统内文件无故消失、运行应用程序无反应、后台有可疑程序运行等现象，说明可能已经中病毒了，应及时联系技术人员处理。

安全建议

- 断网，防止病毒扩散；
- 备份文件，防止电脑被锁或文件丢失的情况发生；
- 联系技术部门进行杀毒或重装系统等操作。

01 办公场所安全

涉密文件保护

案例解析 涉密文件是公司内部重要文件，必须从技术、管理等方面制定确保文件安全的策略，禁止扫描文档，是为了防止文件直接暴露在公网上，存在可能泄密的隐患。

安全建议

- 禁止把涉密文档分享给非相关人员；
- 禁止把涉密文档放在个人办公电脑上；
- 禁止通过非涉密网传输涉密文件。

01 办公场所安全

涉密意识提升

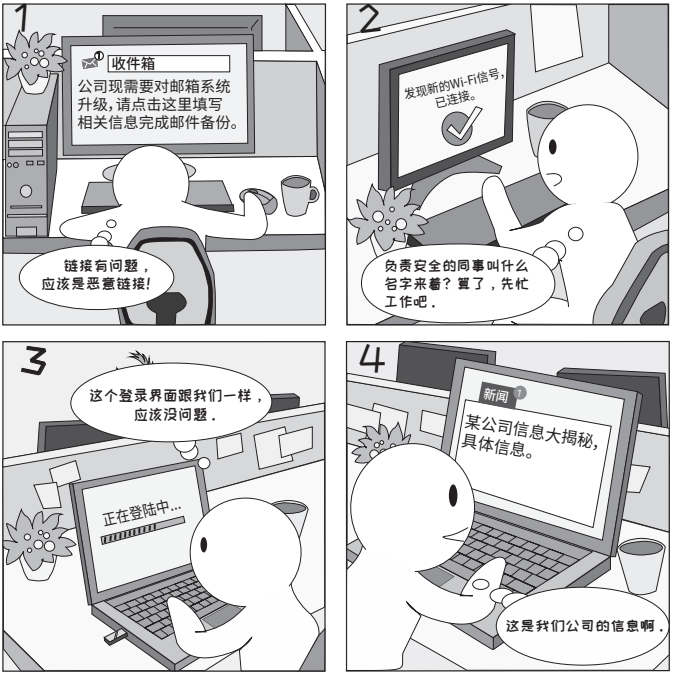
案例解析 有涉密室的企业，禁止携带一切录像设备进入，不按照规定管理和使用涉密计算机造成泄密事件的，将依法依规追究责任。

安全建议

- 涉密室内禁止携带一切录像设备；
- 涉密室内电脑禁止连接公网，只能使用专用网络；
- 涉密文件使用完毕后整理并放回密码保险柜。

01 办公场所安全

熟知上报流程



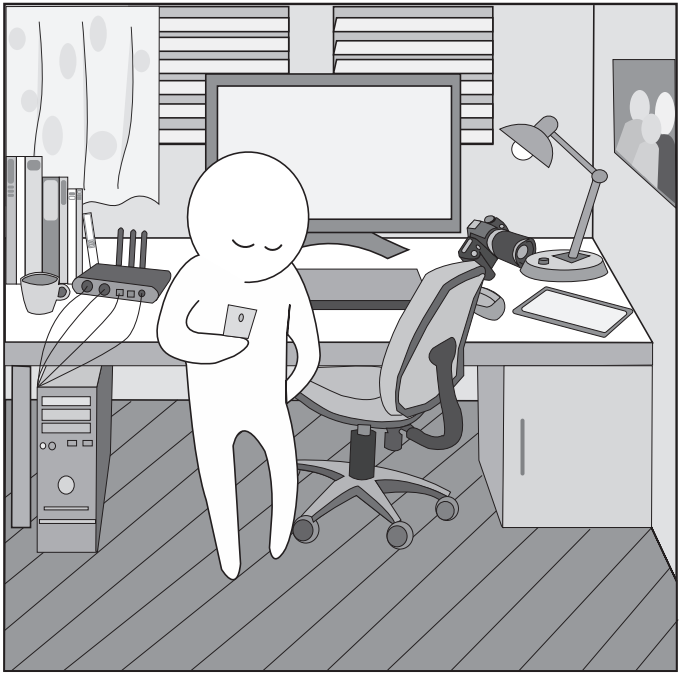
案例解析 小明在发现邮件中隐藏恶意链接时，并没有引起足够的重视，导致其他员工落入圈套，这个案例告诫我们在遇到可疑邮件或其他可疑事件的时候要及时上报相关负责部门，避免发生安全事件。

安全建议

- 熟悉上报流程，清楚公司哪个部门负责公司信息安全，这样即使忘了某个同事的电话，也可以联系到相关负责人。

02 家庭网络安全

Cyber Security at Home



- 物联网、云计算、移动互联网等新技术的发展，使得手机、平板电脑、PC 普及到家家户户，由于网络的发展，许多工作已经可以在家里完成，而且交流和协作也不是问题。不过家庭办公也有太多的信息安全问题，导致个人乃至企业蒙受损失。

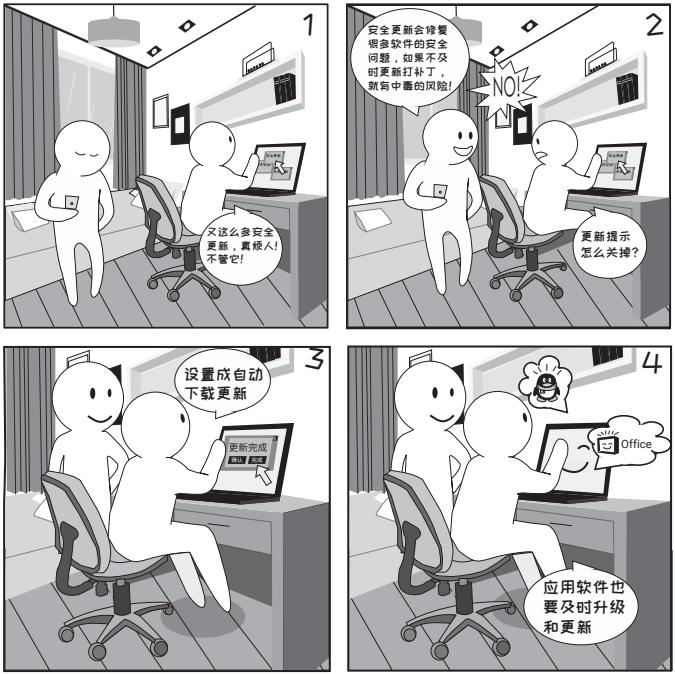
案例解析 家用路由器要设置相关的安全策略，防止给黑客提供入侵的机会；设置路由器安全时，只设置无线密码是不够的，还需要更多相关安全设置。

安全建议

- 修改路由器后台的默认账号及密码；
- 选用安全的加密方式，设置高复杂度的无线密码，同时可以选择隐藏 SSID 来避免被他人搜索到；
- 建议添加已知设备的 MAC 地址，开启无线 MAC 地址过滤功能，就算密码泄露，别人也无法连接路由器。

02 家庭网络安全

及时安装补丁



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全更新，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。

02 家庭网络安全

安装安全软件

案例解析 病毒传播方式有很多，除了捆绑在软件中之外，还有移动设备传播、网络传播、文件传播等方式。如果内网中的一台电脑被攻破，整个网络内的设备都有可能受到影响，从而导致文件丢失、信息泄漏等后果。安装安全软件，可以为电脑的保护增加一道屏障。

安全建议

- 安装防病毒软件；
- 及时升级、及时更新病毒库。

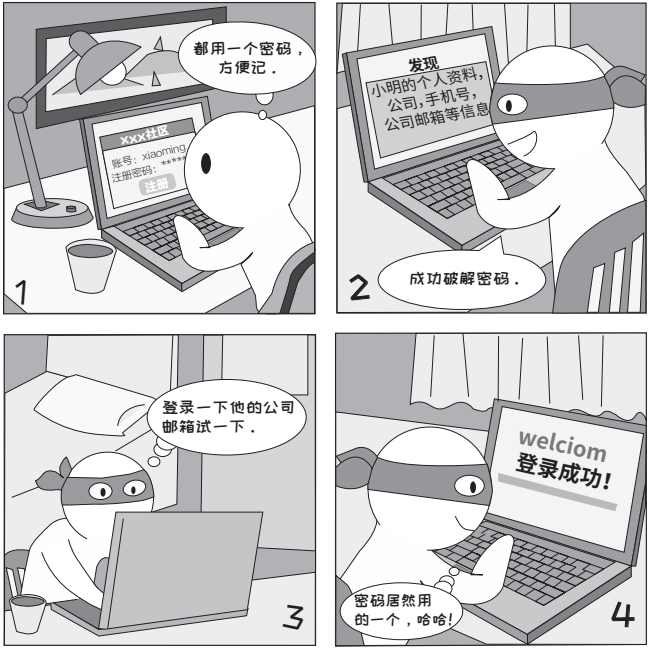
02 家庭网络安全

开启防火墙

案例解析 防火墙是个人计算机和网络之间的一道安全屏障，防火墙的一个重要作用是可以阻断内部程序向外发送数据，从而防止木马进驻用户系统时自由向外发送用户个人数据，防火墙可以有效地防止常见木马对信息的盗取。同时也对从外向内的访问起到一定阻隔的作用。

安全建议

- 建议开启计算机防火墙，一般不要关闭；
- 设置防火墙的端口规则，除允许必要的端口外，其他的尽量全部禁止掉。



- 案例解析　很多人各网站用户名密码相同，这样黑客利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
  - 不同网站或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。

确认网站域名

案例解析 在网络上挂钓鱼网站是黑客盗取用户数据和实施诈骗的常用手段。黑客利用的是大多数用户对网站错误的概念：长得一样就是该网站；认准是不是钓鱼网站的关键是要检查网站的网址。

安全建议

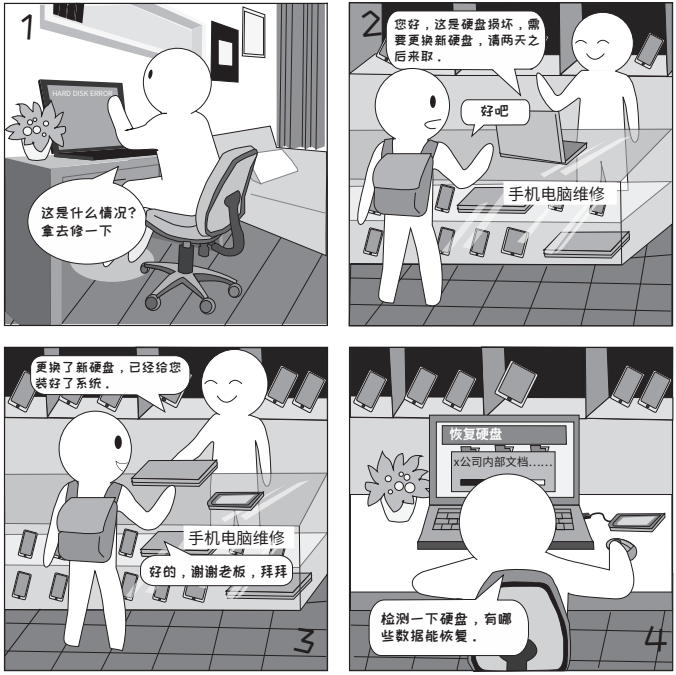
- 网上购物时，检查网址是否有误；比如水果官网是 www.shuiguo.com，访问的网站是 www.shuiguox.com，那这个网站就是钓鱼网站；
- 可以使用错误的用户名和密码尝试，一般的钓鱼网站不会验证用户名及密码，可借此判断该网站是否为钓鱼网站；
- 检查网站使用的是否是 https 协议。

文件上传网盘

案例解析 把客户资料等公司内部文档上传至公共网盘存在泄密风险，由于网盘本身可能存在漏洞，如果网盘提供商被黑客入侵或者数据泄露，就会给公司造成损失。其实敏感资料放在第三方之后，就已经不是自己可控的了。

安全建议

- 建议不要使用网盘存储重要文件，如客户资料，内部文档等；
- 如果要使用网盘分享文件，建议先对文件加密压缩。

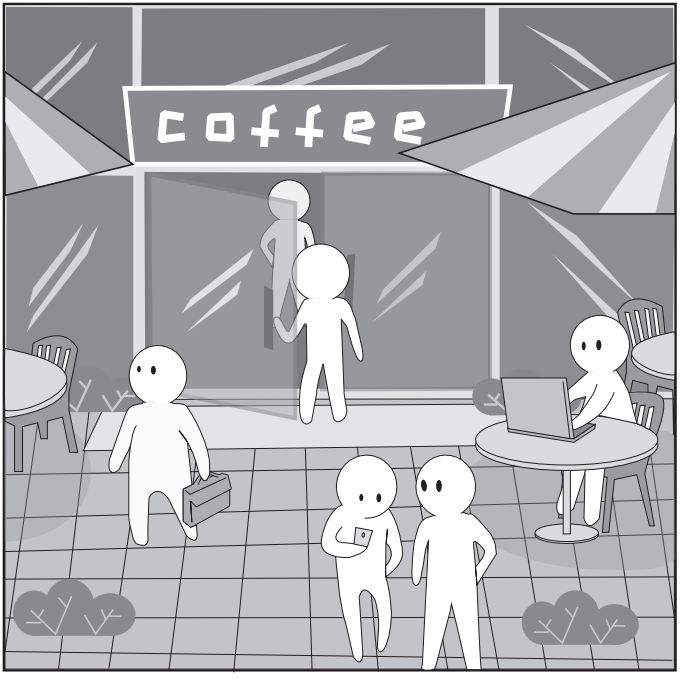


案例解析 旧的硬盘虽然已经损坏，但是还包含个人数据，如果被人拿走并通过工具进行数据恢复，就可能会造成个人隐私泄露。

安全建议
- 更换硬盘后，旧的硬盘不要随意丢弃，最好是妥善保管或者是物理销毁；
- 个人电脑数据定期备份，防止硬盘损坏，造成重要数据丢失。

03 移动场所安全

Cyber Security at a Public Place



- 信息安全意识就是人们头脑中建立起来的信息化工作必须安全的观念，也就是人们在信息化工作中对各种各样有可能对信息本身或信息所处的介质造成损害的外在条件的一种戒备和警觉的心理状态。

- 案例解析：黑客首先在地铁站等人流较大的地方布置伪基站，另一方面通过运营商的其他业务申请让真正的运营商向手机号发送 usim 卡号，小明收到 usim 卡号后，不加思索就直接将 usim 卡号发到黑客手中，使黑客掌握关键信息。
- 安全建议：
  - 对于索要个人信息的短信，可以忽略或者拨打官方联系方式询问事由，不要直接回拨电话；
  - 陌生短信中包含的链接中可能含有木马病毒，如果打开链接，就会导致手机感染病毒。

03 移动场所安全

扫二维码

案例解析 二维码应用广泛，但其安全性一直无法保障，如果扫描到一个携带木马病毒的二维码，手机就可能会中病毒。

安全建议

- 在扫描公共二维码时，先确定二维码是否有被替换或者覆盖的痕迹；
- 建议使用手机防护软件扫描二维码，预览扫描结果，提前检测；
- 尽量不要扫描陌生人发来的二维码。

03 移动场所安全

公众信息发布

案例解析 在日常生活中，员工在社交平台使用公司名称散播有损公司形象的消息，会给公司造成负面影响，同时给黑客社工收集信息增加一个渠道。

安全建议

- 未经公司授权，员工不得以官方名义注册社交平台账号；
- 个人账号上不得发布公司官方信息；
- 员工不能以公司名义建群或组织活动。

- 案例解析

现在任何智能手机拍照，都含有 exif 参数，它包括光圈、快门、ISO、白平衡、日期时间，当手机 GPS 打开的时候还会有位置信息；黑客通过你的位置信息推理出生活习惯后，可能会造成人身伤害或财产损失等问题。

- 安全建议
  - 关闭手机定位功能，苹果手机照片定位关闭路径：设置 -> 隐私 -> 定位服务 -> 相机 -> 永不（安卓手机操作类似）；
  - 另外不少美颜相机也自带定位功能，是在下载完软件后，疯狂点“允许”就默默开启了。

03 移动场所安全

警惕免费 Wi-Fi

案例解析 在手机上接收和处理工作邮件时，需要注意连接的网络是否安全，如果连接到黑客搭建的无线网络，黑客会通过监控数据包获取用户数据。

安全建议

- 注意手机网络使用安全，没有密码的 Wi-Fi 请慎用；
- 注意物理设备安全，防止因为手机丢失造成数据泄露。

案例解析 文件放到移动存储上，U 盘丢失后硬盘上的文件就可以被直接读取，如果对 U 盘加密，即使被别人捡到 U 盘，也需要输入密码才能看到其中的文件，就有效避免了文件泄露。

安全建议

- 建议使用 Windows 自带的 BitLocker 工具，右键点击 U 盘分区，选择“启用 BitLocker”，选择“密码解锁驱动器”，即可进行相应设置。

03 移动场所安全

Wi-Fi 自动连接

案例解析 一些手机在搜索到不是同一个 Wi-Fi 热点但名称相同的 Wi-Fi 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 Wi-Fi 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 Wi-Fi;
- 在手动连接前，应留意 Wi-Fi 的热点名称，避免手机或笔记本连接到假冒的热点。

03 移动场所安全

Wi-Fi 钓鱼

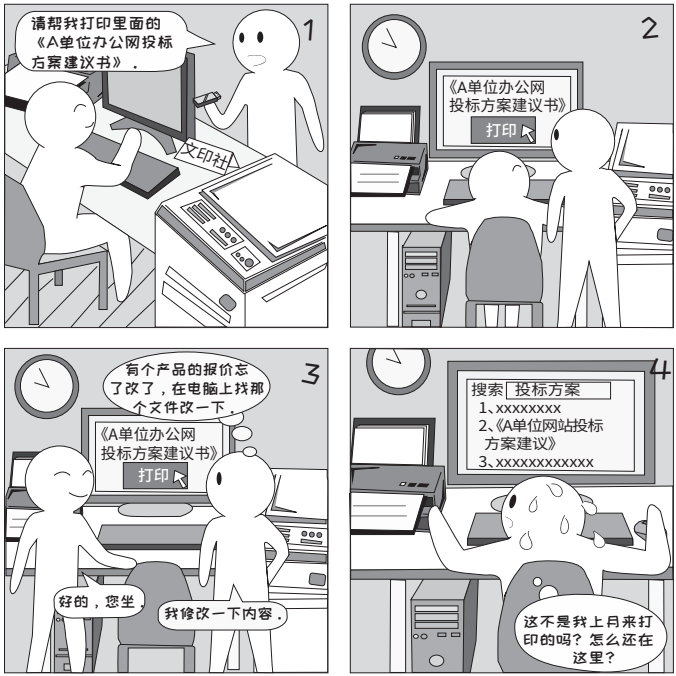
案例解析 手机上的 Wi-Fi 密码共享 APP 在安装后默认设置会自动上传你所连接的 Wi-Fi 密码，这些密码一般不会明文给出，只会在连接 Wi-Fi 时自动输入，但曾曝出漏洞用一个 APP 能读出检测到 Wi-Fi 的密码，这样就可以用笔记本接入 Wi-Fi 使用更强大的攻击工具了。

安全建议

- 建议不要使用 Wi-Fi 密码共享 APP;
- 如果必须使用建议关掉自动上传密码功能。

03 移动场所安全

外部打印



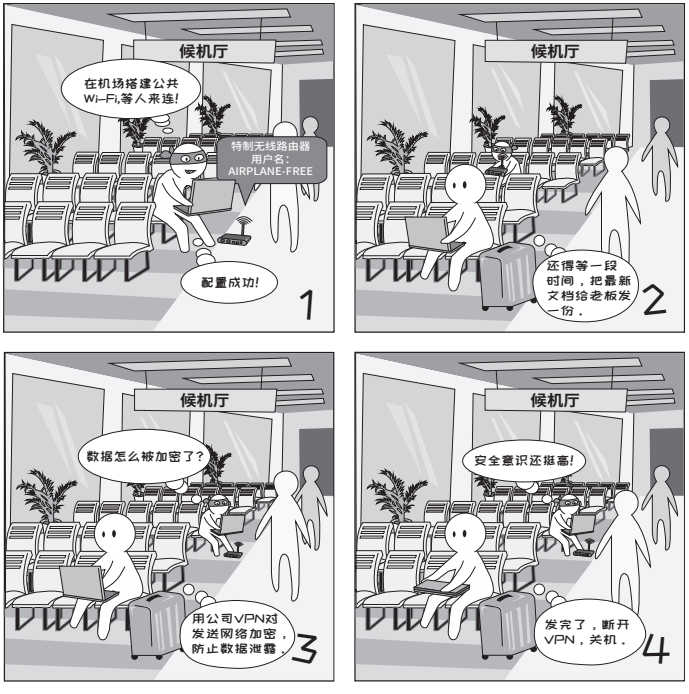
案例解析 打印社的电脑上一般都保存有很多已打印的文档，打印社并无动力定期清除，并且客户随意拷贝没有限制，是一个很容易泄露敏感文件的场景。

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。

03 移动场所安全

VPN 使用



- **案例解析**　出差或者在外办公时，经常会用到外网发送机密数据，如果不注意就会被黑客劫持，造成数据泄露；案例中小明虽然连上了黑客搭建的无线 Wi-Fi，但由于使用 VPN，使网络访问加密，阻挡黑客劫持数据。
- **安全建议**
  - 如果公司有 VPN，尽量使用 VPN 发送和接收办公文件；
  - 配置邮件 ssl 加密传输；
  - 通过外网发送文件时，可先对文件加密，这样可大大减少数据丢失的概率。

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