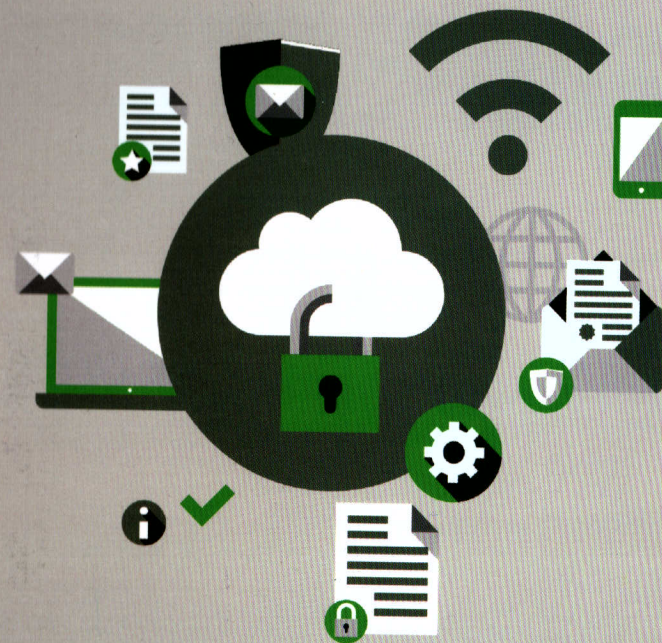


网络安全意识宣传漫谈

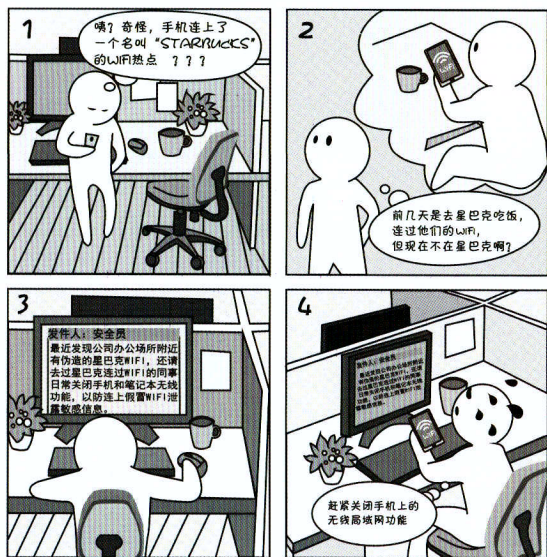
中共龙岩市委网络安全和信息化委员会办公室 宣



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。





案例解析

一些手机在搜索到不是同一个WIFI热点名称相同的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

对于一般的公司来说,外来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

- 各种方案、合同、报告、代码等比较敏感的文件在分发时必须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

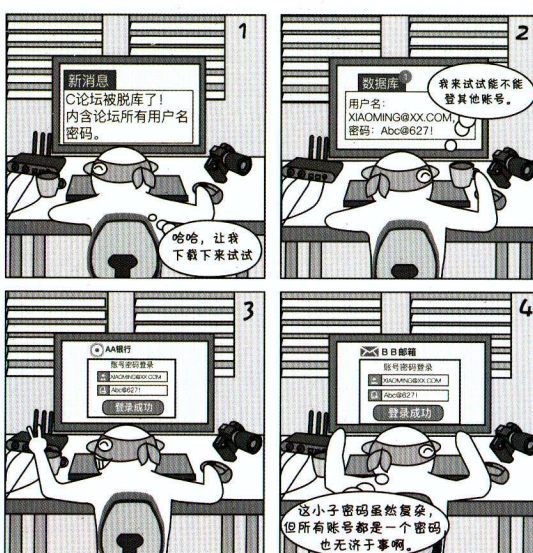


案例解析

利用会议室白板讨论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,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

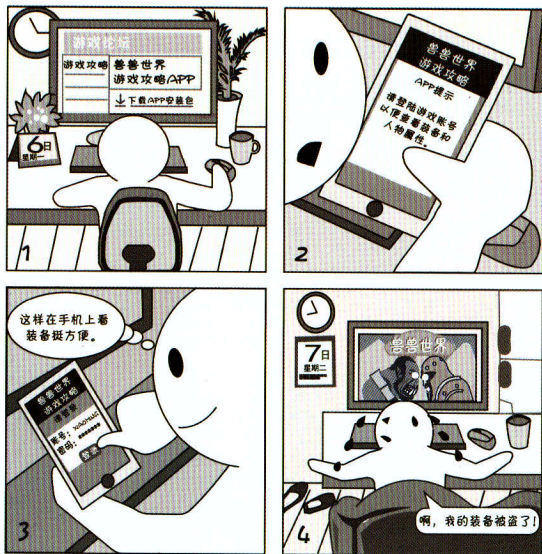


案例解析

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录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
- 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
- 爆发脱库事件时第一时间修改自己的相应级别的账号密码

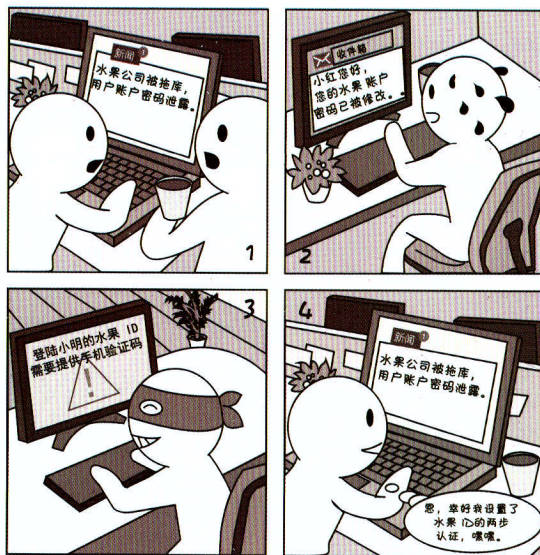


案例解析

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, 各种主流杀毒软件无法检测到。

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

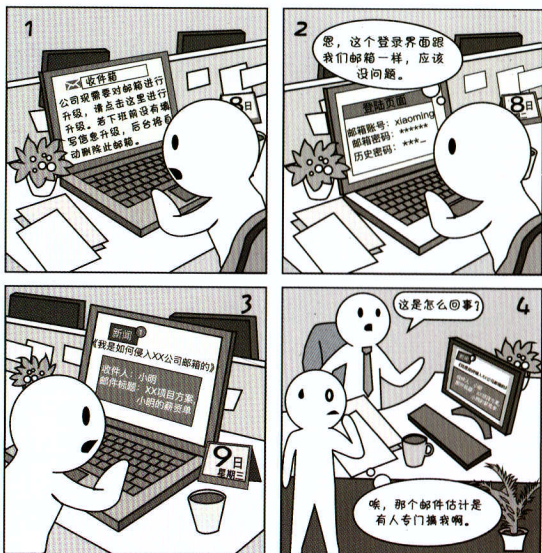


案例解析

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险。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录时, 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

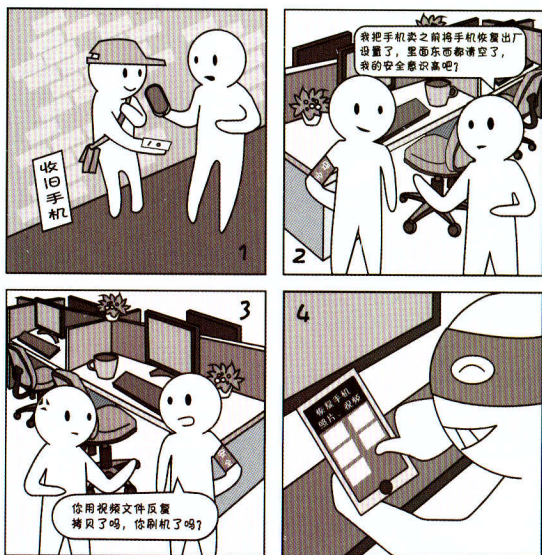


案例解析

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

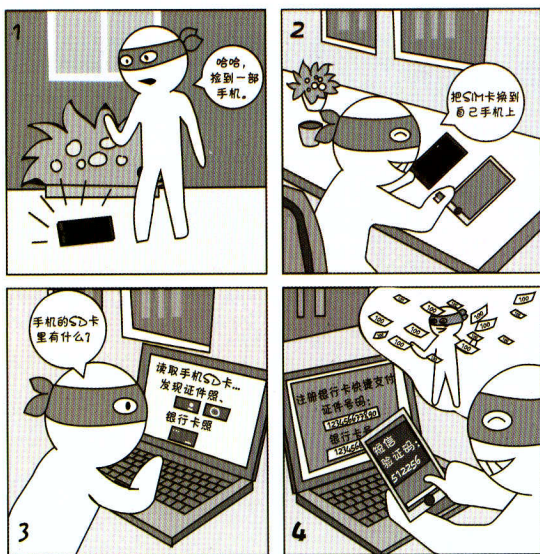


案例解析

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



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上收取验证短信。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

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盘文件刻意拷贝在电脑上

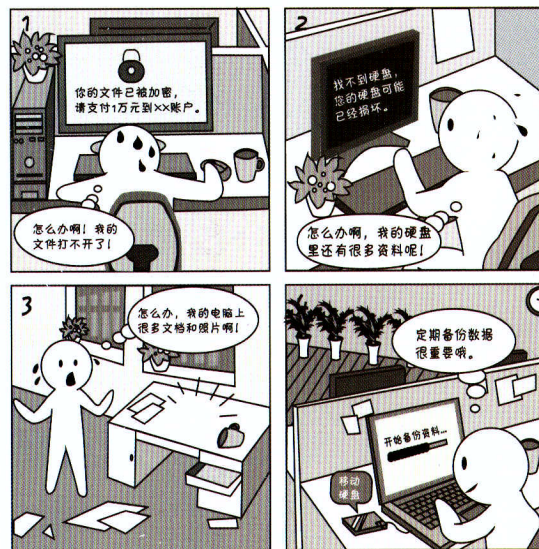


案例解析

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



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