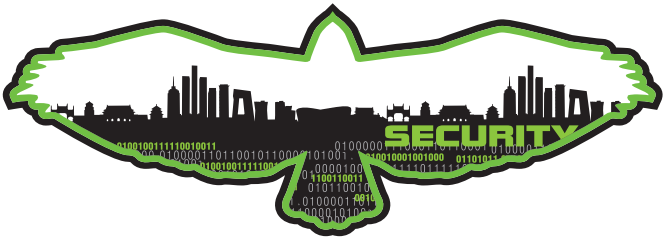


信息安全意识漫谈 2.0

SECURITY COMIC TALK 2.0

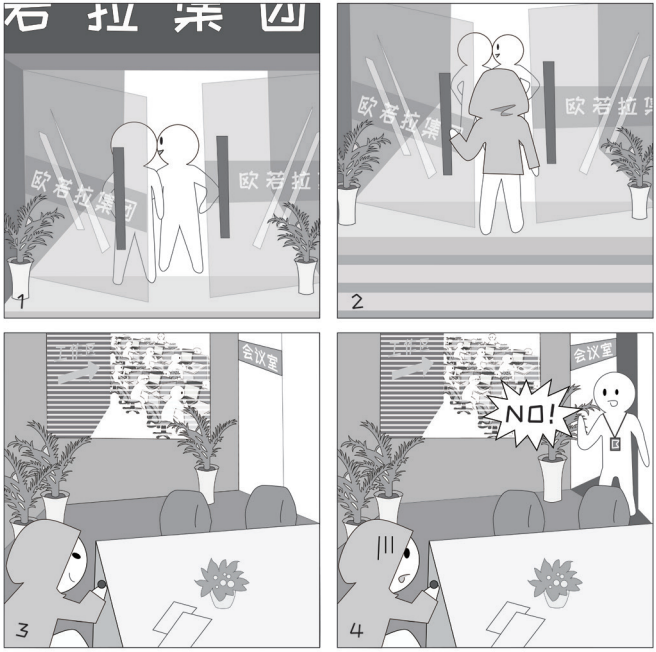
NSFOCUS 绿盟科技

版权声明

目录 CONTENTS

01 办公区域

陌生人进入



案例解析 大门是保护办公区域安全的第一道屏障，可以防范商业间谍或黑客进入工作区后产生的物理风险。然而，在与同事聊天、看手机或有急事时，可能会忘记关门，或忘记确认身后是否有人尾随，因此应在平时养成随手关门的习惯。

安全建议

- 进出大门时应观察是否有人尾随
- 针对不能自动闭合的大门应注意随手关门
- 收快递、拿外卖应在门外进行
- 外部人员进入工作区需登记并全程陪同

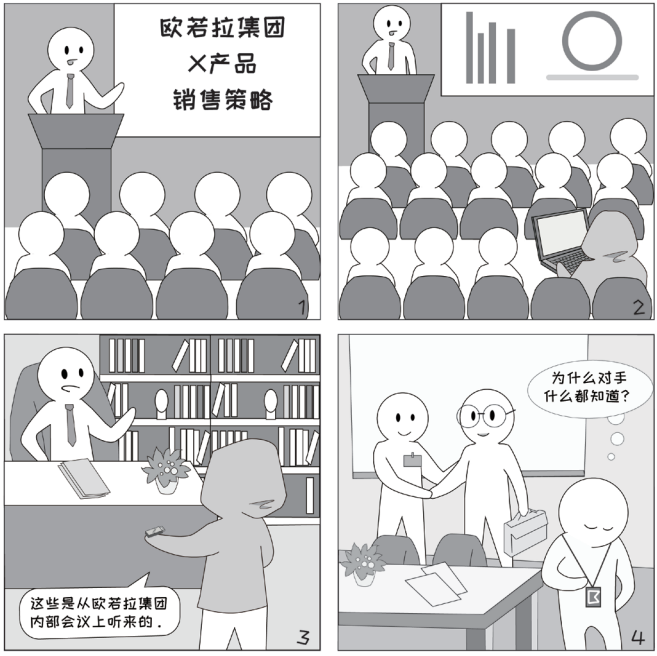
01 办公区域

防窃听

案例解析 随着科技的发展，目前的窃听装置已经能够做得非常小。在一些需要保密的重要场合，应该注意防范窃听风险。

安全建议

- 如有需要，可以选购专业的防窃听检测装置，在重要场合对各个隐蔽位置进行排查，检测电磁波信号或电子设备是否存在，从而判断是否存在窃听风险。

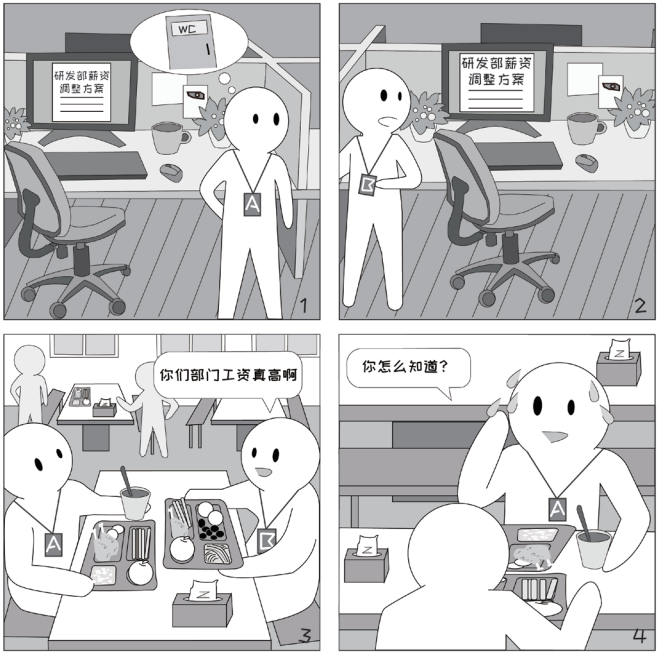


案例解析 在会议召开的过程中，会议组织者应确认在场参会人员，员工也应警惕身边是否有可疑或陌生人员，特别是在进行人数较多的大型会议时。一旦有外部人员混入，就可能会造成信息泄露，从而导致更严重的后果。

安全建议
- 会议组织者应现场确认参会者身份
- 会前叮嘱参会人员保密事项
- 召开重要会议时，应选择隔音、封闭的会议室
- 会后整理会场，确保不遗留资料，并擦除白板

01 办公区域

锁屏



案例解析 在公司中，不同岗位的工作内容、工作性质不同，有权限接触到的信息也各不相同，一些信息在公开披露前需要暂时保密。因此，在离开电脑前，应锁定屏幕，否则就存在被他人看到文件内容、拷走资料等风险。

安全建议
- 如果长时间离开，建议将电脑关闭；
- 在离开电脑前应使用 Win+L 快捷键锁屏；
- 设置屏保自动启动：右击桌面，选择个性化 - 锁屏界面 - 屏幕保护程序设置，选择屏保程序并设置等待时间为 10 分钟以内，同时勾选在恢复时显示登录屏幕。

案例解析 一旦攻击者混进办公区域，桌面就成为他们的首要“狩猎”目标。在攻击者找到敏感文件或重要物品后，可能会对其进行拍照、复制、窃取，造成更大的风险。

安全建议

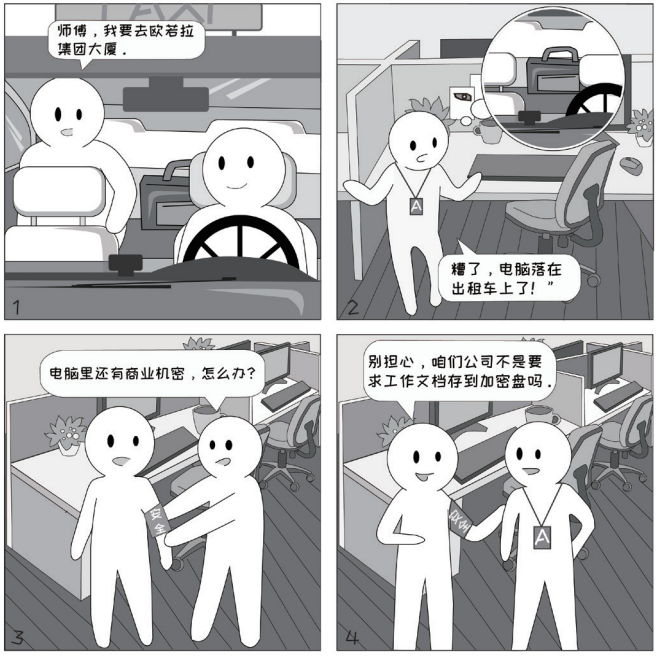
- 如果日常工作涉及敏感文件，应及时将敏感文件放入带锁的抽屉或柜子；
- 避免在桌面上放置敏感文件、存储敏感文件的设备、门禁卡、钥匙、写有密码的便签等物品。

01 办公区域

安全小测试

■ 测测你能不能发现上图存在的安全风险?

关注绿盟科技官方微信公众号回复“办公区域”获取答案



案例解析 笔记本的硬盘可以拆卸，一旦笔记本丢失，外部人员可能会拆卸硬盘，从而绕过操作系统密码，直接读取硬盘上的数据。如果将敏感数据保存到加密盘上，就只能在输入密码后才能读取文件，可以有效防止文件泄密。

安全建议
- 敏感文件建议保存到加密盘上，并设置复杂密码；
- 邮箱、即时通信软件中可能包含敏感信息，建议将邮箱的数据文件和聊天记录目录也设置在加密盘中；
- 加密盘可以选用 BitLocker、FileVault 或 VeraCrypt。

02 个人电脑

弱口令

- 案例解析　攻击者通常会使用自动化工具来破解密码，并且可能针对目标公司制一个密码字典。一旦使用弱密码，或使用公司名称、个人姓名等公开信息作为密码，被成功破解的几率就非常大。
- 安全建议
  - 使用高强度的密码，同时混合大写字母、小写字母、数字和特殊符号，长度建议大于 10 位；
  - 密码中不建议包含姓名、生日、手机号码、公司名称等公开信息；
  - 建议定期（例如：每隔 90 天）修改密码。

- **案例解析** 不同系统的安全性各不相同，如果在所有地方都使用相同密码，那么一旦某个地方出现问题，攻击者可能会用获取到的密码尝试登录其他系统。
- **安全建议**
  - 最安全的方式是针对每一个网站或系统设置与众不同的密码；
  - 如果担心忘记，可以先记住一个基础密码，再在后面加上不同网站 / 系统各自的代号，或针对不同重要程度的帐号设置不同密码；
  - 关注网站或系统的相关新闻，一旦发生攻击事件，第一时间对使用此密码的所有位置进行密码修改。

02 个人电脑

软件下载

- **案例解析** 攻击者可能会将恶意程序与正规软件捆绑，并设置恶意程序在后台运行，用户一旦下载使用，很难发现出其中的问题。一旦感染挖矿恶意程序，将会严重耗费电脑的 CPU 或 GPU 资源，造成运行速度缓慢等问题。
- **安全建议**
  - 建议首先搜索软件的官方网站，并从官网下载正版软件；
  - 搜索引擎的结果中可能包含商业推广，因此不要盲目迷信排名靠前的下载地址；
  - 如果无法确认是否为官方原版软件，应使用在线病毒检测平台（如 VirusTotal）进行检测。

案例解析 操作系统和软件会不可避免地出现各类漏洞，而安全更新正是对漏洞的修补。在补丁发布后，攻击者可能会据此反推出漏洞的利用方法，在用户还没来及打补丁的这段时间发动攻击，此前爆发的 WannaCry 勒索病毒就是如此。

安全建议
- 建议开启操作系统和各类应用的自动安装更新功能，或在有更新时弹出提示；
- 补丁发布后，应第一时间进行更新，更新完成后，需确认安装是否成功。

案例解析 在进行文件删除或清空磁盘时，如果仅清空回收站，或者仅使用“快速格式化”功能，由于在磁盘上的数据没有实际被覆盖，因此还可以使用专业工具将其恢复。

安全建议

- 删除单个敏感文件时，建议使用杀毒软件自带的“文件粉碎”功能，一般在文件上点击鼠标右键可以看到；
- 在清除曾经保存过敏感文件的磁盘时，不能仅仅依赖于格式化功能，需使用专业脱密工具，或在格式化后使用其他文件占满整个磁盘并反复多次。

02 个人电脑

安全小测试

■ 测测你能不能发现上图存在的安全风险？

关注绿盟科技官方微信公众号回复“个人电脑”获取答案

03 敏感文件

工作聊天群

案例解析 一些企业使用专门的的工作沟通软件，这些软件通常会接入人事信息，可以保证已离职或外部人员无法加入。但是，如果使用日常生活中的聊天软件，则无法保证人员调整后自动同步，也无法保证用户不添加外部人员进入群组中，会产生一定泄密风险。

安全建议

- 进行工作相关交流时，建议优先使用企业指定的工作沟通软件；
- 如果需要使用聊天软件（例如：QQ、微信）建群，管理员应该做好群组成员维护，禁止非管理员成员邀请其他用户入群，及时请出离职人员；
- 敏感信息和重要文档建议优先选择邮件发送或单点发送，避免直接发送到外部群里。

03 敏感文件

文档分发

案例解析 工作中的各类文档都有授权扩散范围，应该严格按照此范围进行文档的分发，避免将敏感资料分发到外部，从而造成信息泄露，或产生其他不良影响。

安全建议

- 在编制文档时应首先明确密级，在分发文档时应严格按照密级所对应的扩散范围进行；
- 一旦发现外部存在公司相关的敏感文件，请立即通知公司的安全保密人员进行处理。

- **案例解析** 一旦产品或业务系统的代码公开到网络上，将会在很大程度上帮助攻击者发现产品或业务系统存在的漏洞，从而开展有针对性的攻击。除此之外，竞争对手在看到代码后，也有可能会进行抄袭，从而降低产品的竞争力。
- **安全建议**
  - 工作相关代码建议上传至企业指定的代码管理平台，并注意设置权限，不得公开发布到代码共享平台，不能在网盘、云盘等未经企业允许的第三方平台上保存；
  - 将重要系统的代码带离工作场所前，需经企业同意，并做好防护措施，在代码使用完毕后确保彻底删除。

03 敏感文件

外部打印

案例解析 打印店每天都会处理大量文档，可能不会及时清除主机上已经打印过的文档。并且，一些打印店可能会允许顾客自行在电脑上找到文件并打印，这样就产生了文档泄密的安全风险，造成外部人员可以轻松拷贝在打印店电脑上的任意文件。

安全建议

- 在外部打印时，建议直接在 U 盘中打开文件并打印，不要拷贝到打印店的电脑上；
- 如果有条件，可以使用防拷贝 U 盘，能有效防范文件被复制到本地的风险。

03 敏感文件

共享文件夹

案例解析 为方便局域网中文件传递，往往会设置一些公用的共享文件夹。在这些文件夹中，可能包含一些传递后未及时删除的敏感文件，这些文件会暴露给侵入内网的黑客或内部恶意人员，造成信息泄露的风险。

安全建议

- 尽量避免利用共享文件夹分享敏感文件；
- 共享服务器的管理员可以设置定期自动清理共享文件夹。

03 敏感文件

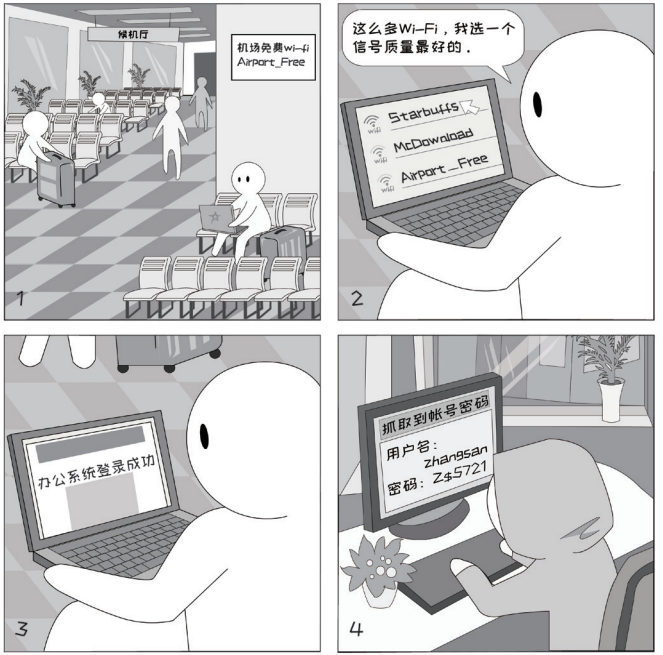
安全小测试

■ 测测你能不能发现上图存在的安全风险?

关注绿盟科技官方微信公众号回复“敏感文件”获取答案

04 Wi-Fi 安全

钓鱼 Wi-Fi



案例解析 在餐厅、商场、火车站、机场等公众场所，通常都部署了免费的 Wi-Fi。然而，攻击者可能会创建一个有迷惑性的 Wi-Fi 热点，一旦不注意连接到这些恶意热点，可能会导致信息泄露、流量劫持等一系列风险。

安全建议

- 在公众场所连接 Wi-Fi 前，应留意周围的提示，接入官方提供的网络；
- 在处理敏感信息或进行移动支付时，尽量不要使用公用网络，最好使用 4G/5G。

案例解析 Wi-Fi 信号具有一定的覆盖范围，不仅在工作区域内可以连接，甚至在办公楼附近也可以接入。员工私自搭建的 Wi-Fi 加密方式通常较弱，一旦被攻击者成功破解，可能会导致攻击者直接访问内网的风险。

安全建议

- 在办公区域，使用公司提供的网络接入方式，不要自行搭建个人热点，不要使用“Wi-Fi 分享器”等设备；
- 如确有需要，在架设无线路由器前必须经过公司批准，并进行安全检查，Wi-Fi 应使用安全算法、设置复杂密码、保证密码定期更改。

04 Wi-Fi 安全

Wi-Fi 密码共享

- **案例解析** 一些 Wi-Fi 密码共享类 APP 会在安装后自动上传所有已经连接过的 Wi-Fi 密码，其中很可能也包含家庭、工作单位的密码。一旦攻击者使用这类工具，也可以轻而易举地连接到家庭或工作单位的内部网络。

- **安全建议**
  - 尽量避免使用 Wi-Fi 密码共享类 APP；
  - 如果需要使用，建议首先关闭自动上传密码功能。

案例解析 目前，有些广告公司会在公共场所部署“Wi-Fi 探针”，当用户手机开启 Wi-Fi 功能时，探针盒子可以自动识别到手机的 MAC 地址、RSSI 值等信息，从而掌握用户的行为轨迹。如果将这些信息与企业自有数据或第三方数据进行匹配，可能会关联到用户的设备 ID 和手机号码，再据此进行有针对性的推广。

安全建议

- 在不需要使用 Wi-Fi 和蓝牙时，将手机的 Wi-Fi、蓝牙功能关闭；
- 使用手机安全软件，根据数据库中保存的记录，对潜在的推销电话进行拦截。

04 Wi-Fi 安全

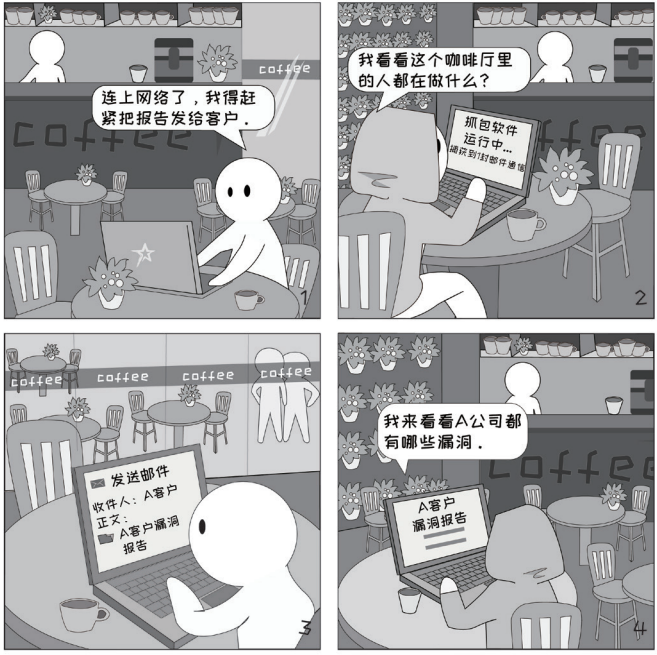
安全小测试

■ 测测你能不能发现上图存在的安全风险?

关注绿盟科技官方微信公众号回复“Wi-Fi 安全”获取答案

05 邮件安全

传输加密



案例解析 在一些外部的 Wi-Fi 网络中，可能会有攻击者对流量进行监测。因此，在使用 Outlook、Foxmail 等邮件客户端，或者在外使用网页版邮箱时，应该选择加密的收件 / 发件端口或 HTTPS 协议，从而防止攻击者截获邮件正文和附件。

安全建议

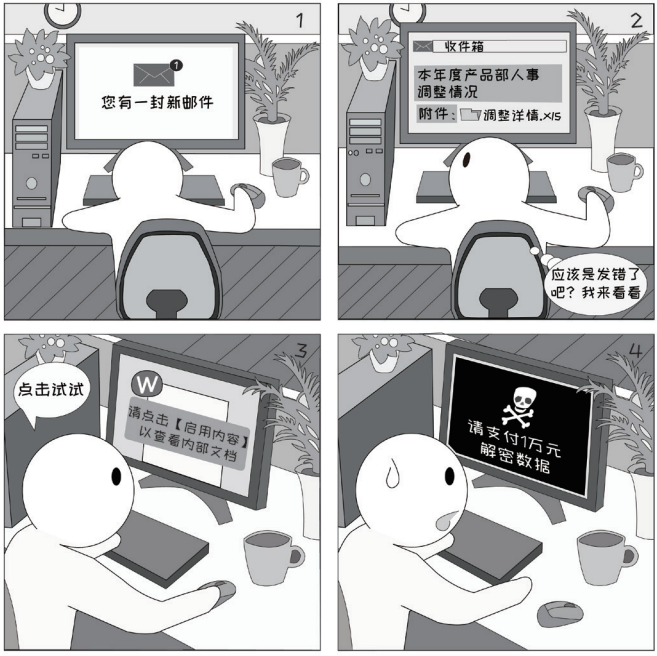
- 收发邮件过程中，应确保传输通道加密；
- 针对 Web邮箱，应确认网页协议为 HTTPS，否则存在风险；
- 针对邮箱客户端，应确认收件、发件均使用安全的 SSL（TLS）端口，默认的 SMTP 和 POP3端口可能存在风险。

案例解析 所谓社会工程学，就是利用人的一些弱点发起攻击。而利用邮件骗取回复敏感信息，是最常见的一种社会工程学方式。特别是看到带有“尽快回复”、“请及时反馈”字样的邮件，更容易放松警惕，本能地按照要求给对方回复过去。

安全建议
- 在收到各类邮件时，都要首先核对发件人是否正确，提高警惕；
- 如果发现邮件存在不合常理的地方，应该首先通过其他沟通方式向发件人本人进行确认。

05 邮件安全

附件病毒



案例解析 随着勒索病毒的不断进化，目前勒索病毒已经发展到针对特定国家、特定行业开展攻击。并且，为防止反病毒软件的查杀，一些病毒可能不再以 exe 文件形式存在，而是隐藏在 Office 文档中。

安全建议

- 在收到可疑邮件后，应避免打开其附件文件；
- 在 Office 中，应避免启用宏和 ActiveX 功能，特别应该避免为外部文件启用上述功能；
- 在收到外部发来的邮件附件时，应首先使用反病毒软件查杀病毒。

05 邮件安全

恶意链接

- **案例解析** 随着攻击的不断升级，攻击者可能会制作专门针对某公司业务的钓鱼邮件，以此增强迷惑性。同时，为增强可信度，攻击者还可能会仿冒一个与公司高度相似的网站，诱导员工在上面输入用户名和密码，这些内容会实时提交给攻击者。
- **安全建议**
  - 收到包含链接的邮件时，应确认链接是否与邮件正文所描述的系统一致；
  - 在访问业务系统时，建议通过浏览器中预先保存的书签点击进入，不推荐点击外部发来的链接；
  - 特别是手机丢失时，谨防邮箱内收到的“查找手机位置”的邮件。

05 邮件安全

安全小测试

■ 测测你能不能发现上图存在的安全风险？

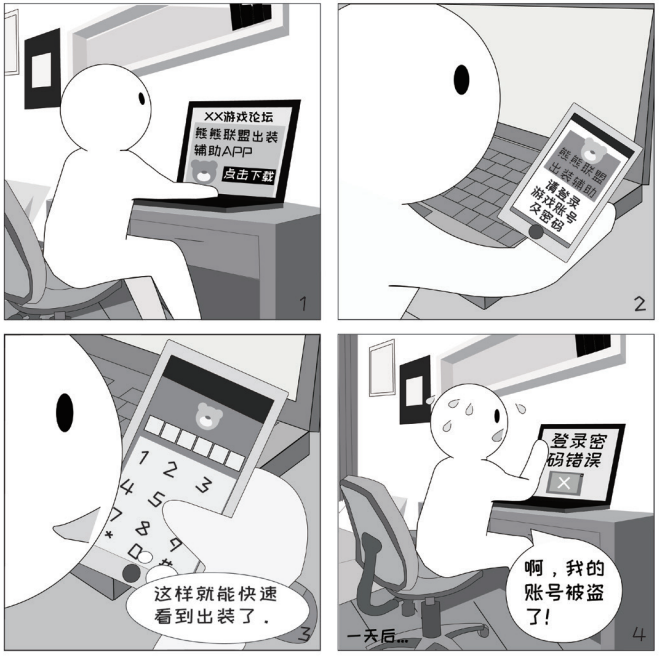
关注绿盟科技官方微信公众号回复“邮件安全”获取答案

案例解析 案例中，攻击者正是通过短信的方式，引诱用户点开链接，从而导致感染木马。一些用户收到此类短信后，会抱着“只要我不填写就没事”的心态，而这种认识是不正确的。点击恶意链接后，可能会自动在后台下载恶意软件，也可能立即在手机上运行恶意代码。

安全建议
- 在收到可疑短信后，不要点击短信中的链接；
- 在手机中安装移动安全软件，防范此类短信诈骗风险；
- 及时更新手机系统版本，防止攻击者利用此类漏洞感染手机。

案例解析 攻击者常常会利用病毒木马、暴力破解、撞库等方式，来获取用户的帐号并尝试登录。为了防范这种风险，越来越多的平台都开始支持“双因素认证”，即在登录时除验证密码之外，还验证另外的一个信息。

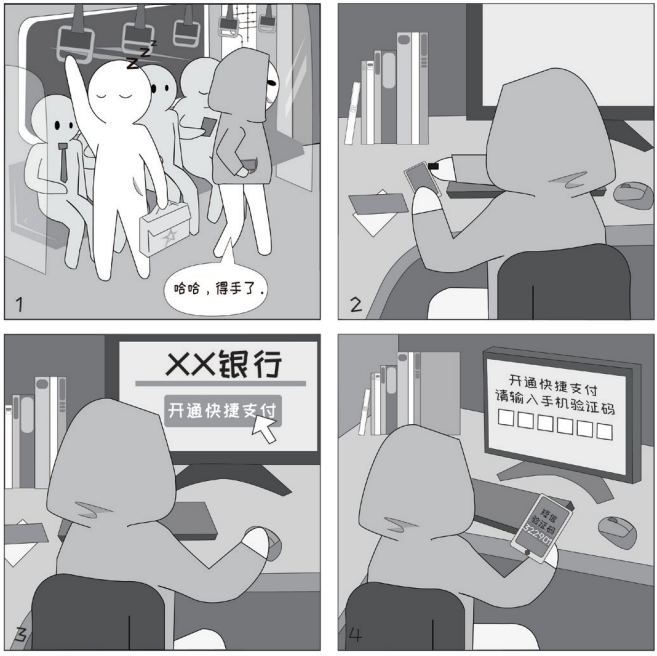
安全建议
- 针对比较重要的平台，应该开启双因素认证，可以绑定常用的手机；
- 手机上收到的验证码，在绝大多数情况下都不需要提供给其他任何人，需要注意保密；
- 在更换手机后，应该及时更改收验证码的手机号，以免无法正常登录。



案例解析 随着智能手机的普及，各类 APP 接连涌现，其中也不乏出现了一些存在恶意行为的应用程序。并且，由于每天都要审核大量 APP 上架，应用商店平台也难免会出现一两只“漏网之鱼”，这时就需要用户格外加强安全意识。

安全建议

- 下载 APP 时，请从官方认证的应用商店中下载，或前往应用程序的官网扫码下载；
- 在下载游戏辅助、系统优化、手机安全、身份信息管理类型的 APP 时，由于这些 APP 通常需要较高权限，因此需谨慎选择信誉较好的产品，并从官方途径下载。



案例解析 目前，许多平台都会使用短信验证码的方式进行用户身份的验证。一旦手机丢失后，如果没有对 SIM 卡及时进行挂失，就给了攻击者可趁之机。除了收取验证码之外，攻击者还可能会拨打亲友电话进行诈骗。

安全建议
- 在丢失手机后，应及时拨打运营商电话远程挂失 SIM 卡；
- 为 SIM 卡设置 PIN 密码，在重启手机或更换手机后，必须输入 PIN 码才能使用 SIM 卡。

- **案例解析** 在注销手机号后，一般间隔 6 个月左右，运营商就会重新发放已经注销的老号码。如果前一个用户没有及时将老号码绑定的支付软件、银行卡、应用程序解绑，新用户在拿到号码后，就很可能通过短信验证码的方式成功登录，从而产生风险。

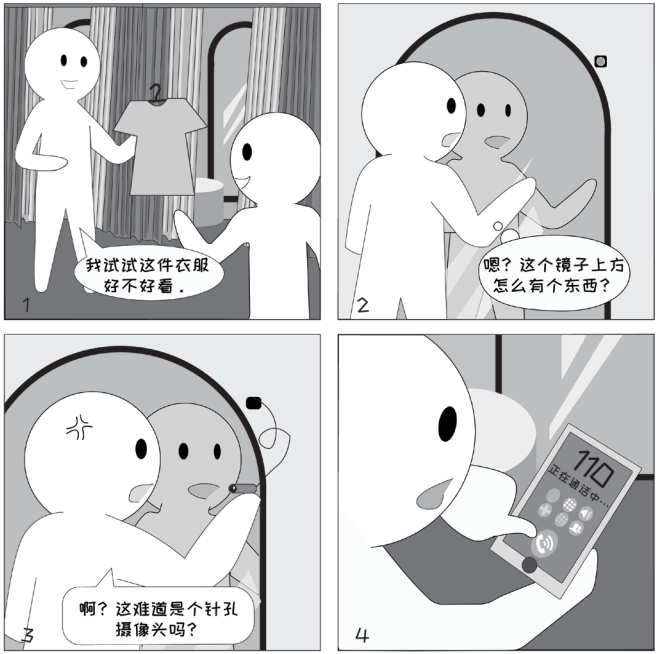
- **安全建议**
  - 在换号前，务必修改银行卡、支付软件、常用应用程序绑定的手机号码；
  - 注销手机号后，如果发现有平台未更换预留号码，通常可以通过联系人工客服的方式，在验证身份信息后进行修改。

■ 测测你能不能发现上图存在的安全风险？

关注绿盟科技官方微信公众号回复“移动安全”获取答案

07 隐私保护

防偷拍



案例解析

近段时间以来，偷拍事件接连发生，不法人员集中在酒店、卫生间、试衣间等位置安装针孔摄像头，对个人隐私造成严重威胁。

安全建议

- 针孔摄像头耗电大，通常需持续供电，应优先排查电源插座、电器等位置是否异常；
- 建议首先推断出最可能被偷拍的地点，然后重点检查这些位置的周边是否存在可疑物品；
- 如有需要，可以选购专业的防偷拍检测装置，通过发出特殊红光或探测电磁波信号的方式排查是否可能存在针孔摄像头。

案例解析 为了保证安全性，在安装或首次打开 APP 的过程中，通常会弹出提示要求用户授予权限。如果用户忽略了这个地方，在没有仔细查看的情况下直接点击同意，那么很容易会产生未经同意擅自获取通讯录、擅自发送短信、擅自录音等风险。

安全建议
- 在应用程序安装或首次打开时，认真阅读 APP 要求的权限，仅授予必要的权限；
- 后续使用过程中，如果发现有权限未开启，还可以通过系统设置中手动开启。

07 隐私保护

帐号注册

案例解析 在网站上注册用户时，通常都会要求填写一些资料，而一些不良网站运营者为谋取私利，可能会将用户信息打包出售，这也就造成了个人信息的泄露。

安全建议

- 为保护个人安全，应该尽量选择规模较大、具有良好声誉的网站平台上进行用户注册；
- 针对一些规模较小、无法确定其安全性的网站，可以使用“一次性邮箱”、“临时手机号码”等服务进行注册，并在资料处适当填写虚构的信息，以防范潜在的泄露风险。

07 隐私保护

案例解析 一些小程序看起来是游戏，但实际上在运行时会要求获取用户信息，这部分信息会提供给营销机构，从而开展广告推广等活动，需要大家提高警惕。

安全建议

- 在小程序的详情界面中，通常可以查看到当前授予的权限，针对其中的一些敏感权限可以手动进行关闭。

07 隐私保护

安全小测试

■ 测测你能不能发现上图存在的安全风险?

关注绿盟科技官方微信公众号回复“隐私保护”获取答案

NSFOCUS

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