



信息安全意识漫谈 3.0

SECURITY COMIC TALK 3.0



版权声明

- 1.《信息安全意识漫谈 3.0》作品的著作权人是绿盟科技集团股份有限公司（中文简称：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. 包括贵公司在内的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

安全部分 I

01 物理入侵

BadUSB	01
尾随进入	02
桌面便签	03
躲猫猫	04
安全意识薄弱的特定人群	05
小测试	06

02 Wi-Fi 突破

公用 Wi-Fi 风险	09
私搭 Wi-Fi 热点	10
Wi-Fi 共享软件	11
访客网络与公司网络	12
Wi-Fi 加固建议	13
小测试	14

03 个人隐私保护

不关联就浑身难受	16
不良软件后门	17
物联网设备弱密码 & 漏洞	18
社交软件送货上门	19
人脸信息被滥用	20
填信息抽奖	21
小测试	22

04 办公安全

盗版软件	25
远程控制软件	26
公用密码	27
安全不都是骗人的	28
固定会议密码	29
小测试	30

05 各种钓鱼

简历不一定是简历	34
好奇心害死的不只是猫	35
U 盘不只是 U 盘	36
测试下你的密码弱不弱	37
不要乱扫二维码	38
公网和内网	39
钓鱼漏斗	40
小测试	41

保密部分 II

06 保密义务

国家秘密范围	45
国家秘密标识	46
国家秘密载体	47
泄密行为举报	48

07 泄密防范

微信办公泄密	49
保密审查	50
兼职泄密	51
拍照泄密	52
废品回收	53
境外人员主动接触	54
单位内鬼	55
打印泄密	56



案例解析

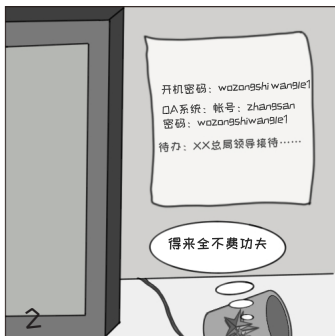
BadUSB 是一种通过重写 U 盘固件伪装成 USB 输入设备（如鼠标、键盘、网卡）用于恶意的 USB 设备，杀毒软件对此类硬件攻击防御效果较差。随意在办公机器上插来源不明的 USB 设备，就会有主机失陷的可能。

安全建议

- 对研发、财务等敏感区域，通过管理和技术性控制措施限制的移动存储设备使用，并定期检查；
- 使用终端安全软件的 U 盘管控和封堵功能，对类似行为进行告警和封堵；
- 加强个人安全意识，不在电脑上使用来源不明的 USB 设备，包括小台灯、数据线等等。



- **案例解析** 大门是保护办公区域安全的第一道屏障，可以防范黑客或商业间谍进入工作区后产生的物理风险。当攻击者进入办公区后，物理安防措施也有一定的缓解效果。
- **安全建议**
- 管理措施要求进入工作区域佩戴工卡，进出大门时应观察是否有人尾随，不能自动闭合的大门随手关门，离开工位锁屏；
 - 对内部区域保持监控和巡检，及时发现和处置可疑人员可疑设备；
 - 快递外卖等行为应在门外进行，外部人员进入办公区需登记并全程陪同。

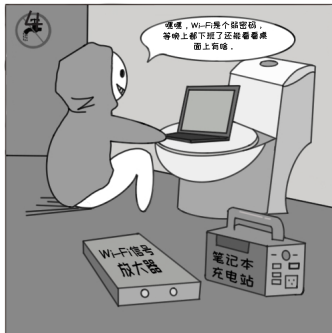
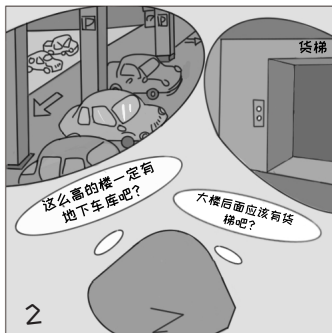


案例解析

安全建议

桌面或便签本记录待办和密码很方便，但很容易被无关人员看到，或在无意间流出，导致信息泄露的风险。

- 管理措施要求桌面不得有记录敏感内容的介质；
- 加强个人安全意识，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；
- 使用 keepass 等密码管理工具管理密码，使用办公软件或手机的备忘录功能记录敏感事项。



- ▣ **案例解析** 绕过保安和隐藏自身的方法有很多，因此要加强门禁管理，让攻击者面对门禁“进不来”，进而加强安全建设，进来之后“带不走”。
- ▣ **安全建议**
- 通过对办公楼和物业人员访谈和了解，发现潜藏的可能进入的方式，采取合适的措施予以防御；
 - 加强办公区域门禁安全建设和管理，让攻击者“进不来”；
 - 加强 Wi-Fi 安全、物理安全教育和建设，让攻击者物理进入后也无法进入内部网络；
 - 对内部区域保持监控和巡检，及时发现和处置可疑人员。



- **案例解析** 除了员工，能够出入办公区域、或对公司有足够了解的第三方人员（如物业保安）往住也容易被利用进行信息获取或攻击。
- **安全建议**

 - 需要对所有有权限进入办公区的人进行安全意识教育；
 - 从管理措施上避免 Wi-Fi 密码分享、纸质敏感文件未处理直接丢弃。

1

办公室突然来了不认识的人，应该怎么做

- A. 不询问，让他自己找要找的人
- B. 不询问，但注意着
- C. 看情况，不忙的时候询问
- D. 主动询问

2

多人一起进入公司大门时，以下说法正确的是

- A. 我不是队伍中最后一个人，门禁安全和我无关
- B. 遇到外卖、快递人员，可以帮其打开公司大门
- C. 人员全部进入后，应核实大门是否关闭
- D. 无需注意一同进入的人员是否是公司同事

3

如何对计算机进行锁屏

- A. 同时按住 Windows logo 键和 S 键
- B. 同时按住 Windows logo 键和 L 键
- C. 单击 Windows 左下角的【开始】按钮 -> 单击【注销】按钮 -> 单击【切换用户】或【锁定】按钮
- D. 同时按住 Ctrl 键、Alt 键和 Del 键，再点击【锁定计算机】按钮

4

APT 攻击目的是为了获取某个组织的重要信息，有针对性的进行的一系列攻击行为。一般来说 APT 侵入企业的途径有

- A. 基于互联网恶意软件的感染，如网络钓鱼
- B. 物理恶意软件的感染，如 U 盘
- C. 外部威胁，如漏洞应用
- D. 内部威胁，如恶意的员工等

5

以下不正确的操作是

- A. 当公司出现陌生人时应主动询问，确认身份
- B. 进出门禁控制场所时应随手关门，防止他人尾随
- C. 不需要的敏感文件应进行粉碎，不能随意抛弃
- D. 会议过后，白板上书写内容可以由保洁人员清除按钮

6

信息安全最大的威胁是

- A. 木马病毒、蠕虫病毒等恶意代码
- B. 信息安全部门不作为
- C. 人员普遍缺乏安全意识
- D. 信息安全产品和设备不够先进

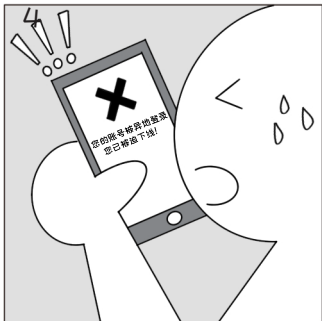
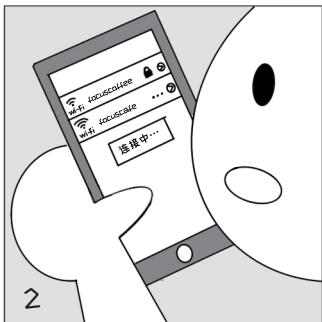
7

当您准备登录电脑系统时,有人在您的旁边看着您,您将如何

- A. 在键盘上故意假输入一些字符,以防止被偷看
- B. 友好的提示对方避让一下,不要看您的机密
- C. 不理会对方面,相信对方是友善和正直的
- D. 凶狠地示意对方走开,并报告这人可疑



关注绿盟科技官方微信公众号回复“物理入侵”获取答案



- **案例解析** 在公共场所，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**
- 在公共场所连接 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；
 - 在不需要使用 Wi-Fi 和蓝牙时，将手机的 Wi-Fi、蓝牙功能关闭。



- **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。



- **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** 通过访客网络功能，可以为访客建立一个独立的上网环境，使用单独的上网密钥，防止私有网络数据信息的泄露，从而进一步保证内网安全。
- **安全建议**
- 建议实现办公网和访客网的隔离，并对办公网做 SSID 隐藏；
 - 尽量为办公网进入添加二次认证逻辑，防止仅通过密码就能进入内部网络。

1

Wi-Fi 密码使用 8 位以上大小写 + 特殊字符，提高字典破解难度；

2

定期修改无线 AP 的 SSID 标识（即 Wi-Fi 名）或密码；

3

不要使用 Wi-Fi 共享软件；

4

使用选择规模较大、具有良好声誉的品牌的 Wi-Fi 设备，并关注厂商升级公告更新设备；

5

可以使用关闭 SSID 广播（如此设置后需要输入 Wi-Fi 名才能连接），MAC 地址白名单（如此设置后需要在管理页面绑定允许连接的设备）等方式，防止外部连接；

6

敏感网络如内网 Wi-Fi，建议使用二次认证机制进行保护。

1

下列关于无线网的使用情况中哪些是【不安全】的

- A. 手机、PAD 通过 USB 线连接电脑，通过公司网络上网
- B. 笔记本电脑通过软件架设 Wi-Fi 热点，供手机、PAD 上网
- C. 电脑 USB 口插入随身 Wi-Fi 类外设架设 Wi-Fi 热点，供手机、PAD 上网
- D. 移动设备使用 Wi-Fi 共享软件破解 Wi-Fi

2

你在一家酒店开会时，需要发送一封紧急的邮件，你带着公司配备的智能手机，可是酒店里的 3G 网络信号不好，你扫描到一个开放式的无线网络接入点，便打算通过无线网络传输邮件，这种做法正确吗

- A. 不正确，开放式的无线接入不安全
- B. 正确，开放式的无线接入点是安全的
- C. 正确，因为邮件很重要
- D. 不正确，开放式的无线网络很慢，邮件会等很久

3

你收到一条 10086 发来的短信，短信内容是这样的：

“尊敬的用户，您好。您的手机号码实名认证不通过，请到 XXXX 网站进行实名制验证，否则您的手机号码将会在 24 小时之内被停机”，请问，这可能是遇到了什么情况

- A. 手机号码没有实名制认证
- B. 实名制消息与本人信息不对称，没有被审核通过
- C. 手机号码之前被其他人使用过
- D. 伪基站诈骗 /Wi-Fi 探针诈骗



关注绿盟科技官方微信公众号回复“Wi-Fi 突破”获取答案



案例解析

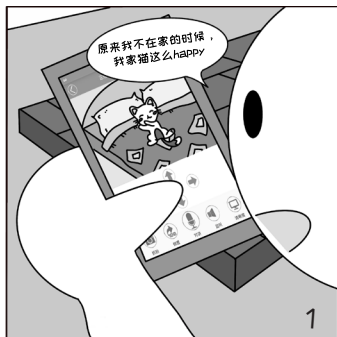
安全建议

网站服务提供商基于各种目的，喜欢让用户关联其他即时通讯方式、招聘网站、社交软件等，当关联过多的信息时，就有可能造成个人隐私泄露。

- 对于第三方服务，不关联或仅关联部分不敏感的个人信息，避免个人信息泄露；
- 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，并在个人资料处尽量不填写，或选择性填写个人真实信息，以防范潜在的泄露风险。



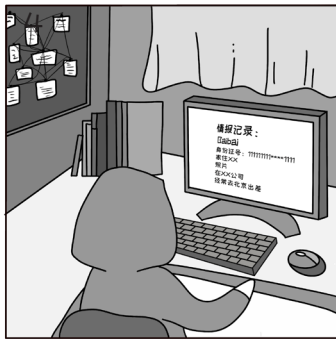
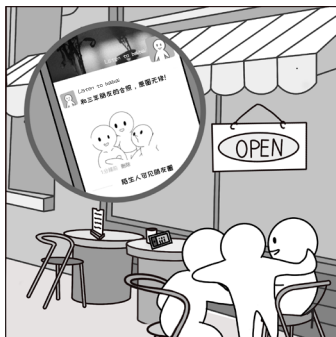
- **案例解析** 非法软件往往会默认开启许多权限，并大量收集本地信息，用来出售隐私数据，甚至进行勒索。
- **安全建议**
- 不要在手机上下载非法软件和来源不明的 APP，避免安全问题和隐私泄露问题；
 - 在手机上也要定期系统升级、安装杀毒软件、定期杀毒；
 - 被敲诈勒索时，请第一时间报案联系警方处理，避免扩大损失。



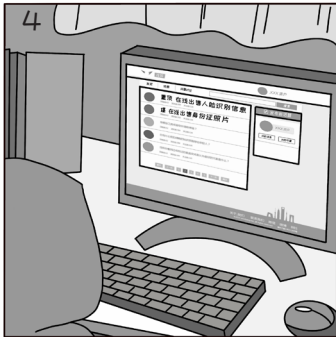
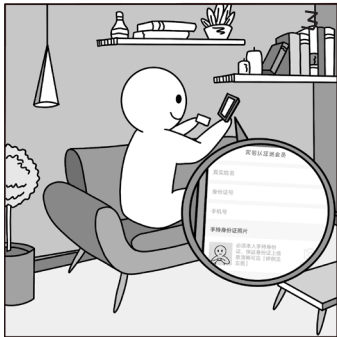
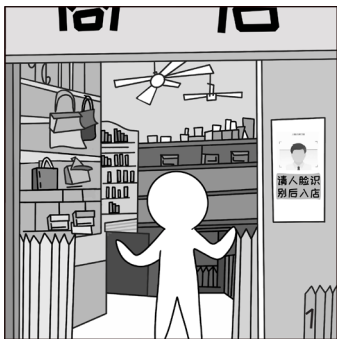
案例解析 安全建议

家用摄像头等物联网设备，默认状态下常常存在默认密码。较早的物联网设备甚至可能有各类漏洞，可能会被攻击者轻易破解利用。

- 物联网设备接入家庭局域网时，注意关闭网络对外共享功能，如有默认密码需要及时修改；
- 尽量购买规模较大、具有良好声誉的厂商的物联网产品，并及时根据厂商售后提示对物联网设备进行升级；
- 如果发现个人物联网设备记录的个人隐私的数据（如录像）出现在互联网，请及时联系警方与厂商处理。



- **案例解析** 社交软件中发布的信息，往往包含个人真实生活的写照。分享之余更要注意个人隐私的保护。
- **安全建议**
- 设置朋友圈、QQ空间等平台“仅好友可见”“仅可见三天内动态”，不要对外公开；
 - 在微博等社交平台，不要发布包含个人可识别信息的图文，包括姓名、地址、身份证号、公司岗位等。



案例解析

身份证照片、没有标注用途的身份证复印件、人脸识别信息等个人隐私数据，有可能因软件漏洞、内部恶意员工等途径被不法分子收集，滥用进行账号注册、贷款、诈骗等违法活动。

安全建议

- 对服务商非必要使用人脸识别的场景，消费者有权向有关部门举报，不同意接受人脸识别；
- 身份证照片与原件要谨慎保存，不要轻易泄露和发送给别人；
- 使用身份证复印件时，最好在复印件上标注用途，避免被不法分子滥用；
- 对要求同时使用身份证和人脸信息进行核查的场景，一定要谨慎确认，或使用替代服务，避免给个人带来损失。



■ **案例解析** 当下制作抽奖 H5、小程序的门槛极低，且一般没有公证方或公证方约束力很弱，不法分子也常常会打着如此旗号去诱导用户填写个人信息。

■ **安全建议**

- 天下没有免费的午餐，遇到需要填写个人信息的场景请三思并谨慎填写；
- 对个人信息分类分级，身份证号、家庭地址、健康状况等信息不要透露给无关第三方；
- 不要信任非可信第三方所说的“保证不泄密”。

1

社交网站中个人隐私泄露的形式一般有

- A. 引导用户填写隐私信息
- B. 诱骗用户填写隐私信息
- C. 数据挖掘
- D. 以上都是

2

确认丢失笔记本电脑中保存的重要资料，若是涉及设备登录密码这类敏感信息，应在第一时间

- A. 关闭相关设备
- B. 登录到这些设备
- C. 找到丢失的重要资料的备份数据
- D. 更改所有设备密码

3

淘宝、京东、新浪这些网站有很高的安全性，我们存储在其中账号密码是不会被泄露的

- A. 正确
- B. 错误

4

小强接到电话，对方称他的快递没有及时领取，请联系 XXXX 电话，小强拨打该电话后提供自己的私人信息后，对方告知小强并没有快递。过了一个月之后，小强的多个账号都无法登陆。在这个事件当中，请问小强最有可能遇到了什么情况

- A. 快递信息错误而已，小强网站账号丢失与快递这件事情无关
- B. 小强遭遇了社会工程学诈骗，得到小强的信息从而反推出各种网站的账号密码
- C. 小强遭到了电话诈骗，想欺骗小强财产
- D. 小强的多个网站账号使用了弱口令，所以被盗

5

即时通讯安全防护建议正确的是

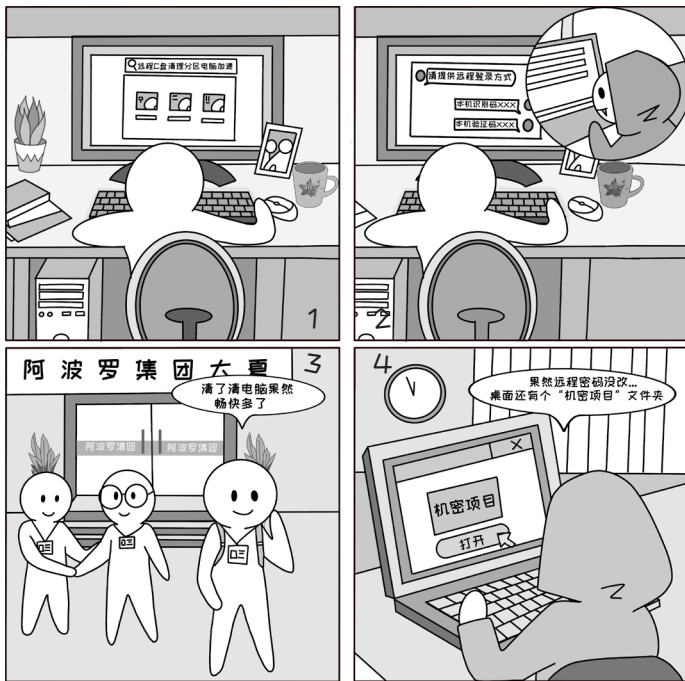
- A. 对微博进行相应安全配置：账号设置 - 隐私安全、账号安全
- B. 接受带有广告、测试等性质的微博要有警惕之心，不要贪图小便宜随意点击来历不明的链接
- C. 可在任意公共电脑或移动终端登录
- D. 不发布虚假信息、不造谣、不传谣、不发表不当言论



关注绿盟科技官方微信公众号回复“个人隐私保护”获取答案



- **案例解析** 攻击者可能会将恶意程序与正规软件捆绑，用户一旦下载使用，很难发现出其中的问题。极有可能造成主机挖矿卡顿、文件被勒索、泄密等情况，使用破解版软件还有一定法律风险。
- **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，不要盲目迷信排名靠前的下载地址；
 - 在下载后，可以使用工具计算文件的哈希值，并与官方提供的值比对，如果不一致则应停止安装；
 - 在电脑本地运行安全软件，并不要随意关闭，确实需要安装的，建议虚拟机尝试安装；使用盗版软件也会给使用者个人及公司带来法律风险。



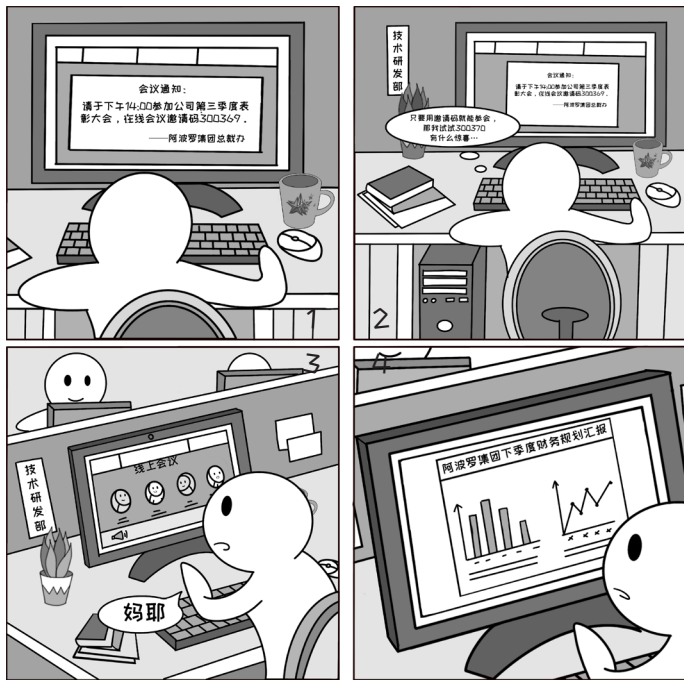
- **案例解析** 为了方便，许多人经常把远程控制软件设为固定验证码，但在别人远程支持之后未更换密码，就会对个人电脑和企业内网带来威胁。
- **安全建议**
- 在公司内部对远程控制软件做一定管理限制措施；
 - 个人在接受第三方远程支持后，及时更改验证码；
 - 尽量使用官方来源正版远程控制软件，避免下载到被动过手脚的软件；
 - 如无远程需求，下班后记得关闭个人电脑，断开网络连接。



- **案例解析** 撞库是黑客通过收集互联网已泄露的用户和密码信息，生成对应的字典表，尝试批量登陆其他网站。通用密码极容易收到撞库攻击的威胁。
- **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。



- **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，在用户还没来得及及升级更新的这段时间发动攻击，此前爆发的各类挖矿勒索病毒大多是如此。
- **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 安全建议

视频会议仅通过邀请码、链接、简单验证码等形式登入的情况，无法有效确认和控制参会人的身份和行为，因此存在录屏、拍照、无关人员参会导致的泄密风险。

- 使用会议号 + 强密码的形式申请在线会议；
- 会议发起人在会前通知时应将会议号和密码仅发放给需要参加的同事，并告知会议纪律；
- 对于敏感会议，会议发起人在会议开始前应再次强调会议纪律，并在会议确保自带录屏功能关闭，使用带多排水印功能的视频会议；
- 要求参会人必须实名登录，不得将登录凭据发送给其他人员，不允许其他人员未经允许线下旁听。

1

关于下列下载软件的行为，哪些存在感染挖矿木马风险

- A. 从“绿色破解园”网站下载绿色版的 Adobe Reader 软件
- B. 从“超爱破解”论坛下载某网友上传 Windows 系统和 Office 软件的破解工具
- C. 从火狐官网下载最新版本的 Firefox 浏览器
- D. 淘宝购买某软件的激活版本，再从商家提供的百度网盘下载软件和破解工具

2

手机丢失后必做的事包括

- A. 手机丢失后，应第一时间挂失 SIM 卡，挂失关联了该手机号的支付宝、银行卡等重要账
- B. 利用手机自身的功能，锁定或者擦除丢失手机中的数据
- C. 将手机丢失的情况告知亲朋好友，提醒他们注意防范虚假信息的诈骗
- D. 注意防范钓鱼短信、邮件等，骗取你的 ID 账号密码和个人信息

3

发现同事电脑中毒该怎么办

- A. 不关我事，继续办公
- B. 协助同事查找问题
- C. 及时报告给信息安全人员
- D. 用 U 盘把同事电脑里面资料拷到自己电脑里面

4

下列哪些使用密码的行为是【不正确】的

- A. 小刘为自己设置了一个仅包含大写字母和特殊字符的密码
- B. 小张为防止遗忘，将全部工作用到的密码写在一张 A4 纸上，并将其藏于显示器下方
- C. 老李自 2012 年入职以来，一直使用着一个长达 16 位的复杂密码
- D. 大牛为提升工作效率，使用浏览器默认的“密码记住”功能，在访问系统网页时自动填写用户名和密码

5

关于差旅过程中的安全，下列哪些说法是正确的

- A. 在公共交通工具上与同伴沟通或打电话时，应注意不要让陌生人听到无意间透露的敏感商业信息，比如投标报价、方案细节等
- B. 使用客户单位或酒店的网上网发送内部使用级及以上的邮件附件时加密
- C. 出宾馆房间时，把电脑留在房间中
- D. 内部使用级及以上级别的文档放在加密盘里，以防笔记本电脑丢失后被直接读取硬盘资料

6

下列哪些情况会给公司带来安全隐患

- A. 外部技术支持人员私自接入信息内网
- B. 使用无线键盘处理涉密以及敏感信息
- C. 某业务系统数据库审计功能未开启
- D. 为方便将开发测试环境和业务系统运行环境置于同一机房

7

关于 U 盘的使用，哪个是不安全的操作

- A. 安装杀毒软件，防止 U 盘携带病毒侵入计算机
- B. 使用陌生人的 U 盘进行重要文件传输
- C. 个人 U 盘传输资料前可先进行格式化，防止 U 盘中有遗留病毒
- D. 不随意使用捡拾的 U 盘



关注绿盟科技官方微信公众号回复“办公安全”获取答案

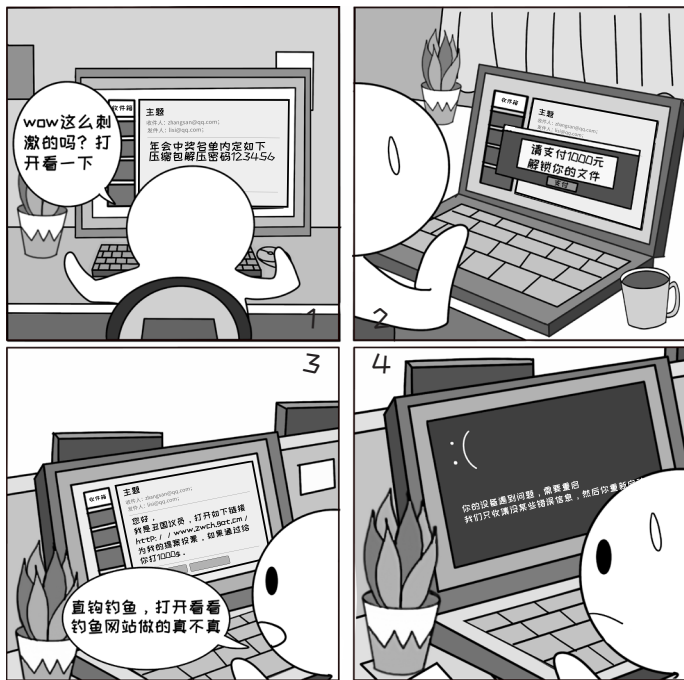


案例解析

安全建议

由于扁平化招聘和内推模式的普及，除了 HR，许多其他岗位人员也会日常接触简历。利用简历为场景的钓鱼也屡见不鲜。

- 规范招聘流程，如禁止使用即时通讯工具与外部人员获取简历，并警惕钓鱼邮件；
- 对于即时通讯软件接受的附件，同钓鱼邮件一样，可执行文件（exe、bat、dll、sys、vbs 等）一定不要打开，文档/PDF 文件确认发送人、理由符合常理且不开启宏，在有杀毒软件的情况下谨慎打开；
- 对于即时通讯、短信中的可疑链接和分享，不确定是正常行为一定不要打开；
- 使用终端安全软件，及时监测与响应；
- 对于邮件收到的附件，一定要判断清楚是图片带超链接还是真实的附件。



- **案例解析** 当前利用好奇心钓鱼的场景十分常见。且常常会利用一些浏览器漏洞，使受害者访问恶意钓鱼链接即执行恶意代码，进而攻陷计算机；或通过加密文档/压缩包绕过钓鱼邮件网关，诱导用户打开。
- **安全建议**
- 警惕一切诱导打开链接、加密文档和压缩包的行为，对标题党邮件需要格外留意；
 - 尽量使用规模较大、具有良好声誉的厂商的浏览器、文档阅读器，并及时打补丁升级，避免被漏洞影响；
 - 使用钓鱼邮件网关类产品，对风险及时监测、阻断与响应。

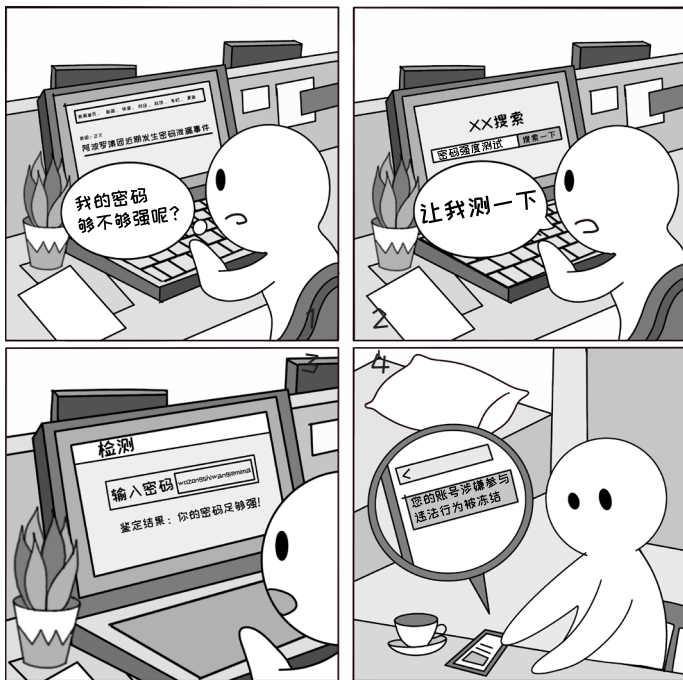


案例解析

除了投放 Bad USB，使用类似方式进行主动钓鱼当前十分常见。

安全建议

- 对研发、财务等敏感区域，通过管理和技术性控制措施限制移动存储设备的使用，并定期检查；
- 使用终端安全软件的 U 盘管控和封堵功能，对类似行为进行告警和封堵；
- 加强个人安全意识，不在电脑上使用来源不明的 USB 设备。



- **案例解析** 当下数据泄露事件频发，有许多同学想要测试下密码是否泄漏，但有许多黑客也会借此心理尝试收集用户密码。
- **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；
 - 尽量不要使用测试密码强度的工具或网站上传本人密码，避免密码被泄露。

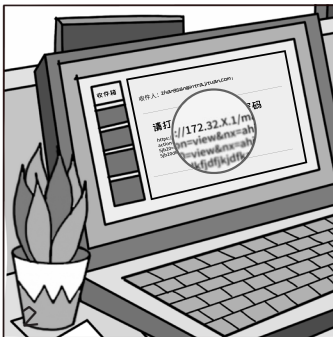
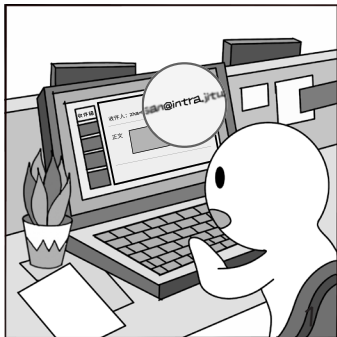


案例解析

二维码制作的技术门槛较低，由此也来了安全隐患，许多不法分子会把自动下载病毒、垃圾软件、勒索病毒的链接生成二维码，诱导用户扫描。微信辅助二维码同样是诱导用户扫描的重灾区，使用自己账号帮助别人信任背书进行“微信辅助”，在被辅助的微信涉及违法案件的情况下，也会给自己带来损失。

安全建议

- 不明二维码不要乱扫，尽量通过官方渠道获取相关二维码信息；
- 扫码后，下拉查看网址是否有异常；
- 安装手机安全软件，发现风险时第一时间监测、阻断与响应；
- 付款时尽量让对方扫付款码，或与商家确认后再主动扫码。



案例解析

许多企业会同时使用内部邮箱与外部邮箱，个人会本能地更相信内网邮箱的邮件。针对此场景，获取一个内部账号作为“内鬼”进行钓鱼往往非常有效。此外，利用用户对内网私有地址的不熟悉，进而构造含有IP钓鱼链接，也会使被攻击者误以为打开的是内网的链接，也是一种攻击场景。

安全建议

- 识别清楚局域网地址，172/192 开头不一定是内网 IP：
 - A 类地址：10.0.0.0 ~ 10.255.255.255；
 - B 类地址：172.16.0.0 ~ 172.31.255.255；
 - C 类地址：192.168.0.0 ~ 192.168.255.255；
- 攻击不一定是外部发起的，对内网邮箱和外网邮箱，应该在防护上采取相同的策略，安全意识上同等对待。

1.认识发件人且邮箱地址正确

2.发件人身份与目的相匹配

3.邮件内容时间符合常理

4.未要求点击仿冒 / 可疑链接 / 下载可疑附件

5.未要求进行敏感操作

钓鱼邮件筛查漏斗

5个步骤，轻松防范钓鱼风险

1

下列哪种表述是【不正确】的

- A. 勒索软件非常猖獗，因此公网主机一定要及时安装补丁，但内网主机通常不需要
- B. 邮件中如果出现未知链接，可以尝试点击，一旦发现网页存在异常，只要及时关闭即可避免安全风险
- C. 在收到陌生地址发来的邮件后，警惕以邮件附件形式发送的 exe 可执行文件，仅可以放心打开邮件中附带的 Word、Excel 文档
- D. 我国法律规定，公民有配合国家机关工作的义务，因此在收到公检法发来的邮件后，应当第一时间按照要求配合工作

2

如果你手上有一个 A 部门发给你的文件，B 部门员工问你要这个文件，你需要怎么做

- A. 直接发给 B 部门员工
- B. 让 B 部门员工直接找 A 部门

3

针对钓鱼邮件，下列哪个描述中【不正确】的是

- A. 由于内网邮箱不会接收到钓鱼邮件，因此我们特别需要注意对外网邮箱收到的邮件进行甄别
- B. 只要发件人邮箱地址是正确的，就可以排除风险，放心打开邮件附件
- C. 在收到包含 .rtf 类型附件的邮件后，应提高警惕，谨慎打开
- D. 为了避免对同事的工作造成打扰，应尽量避免与发件人电话二次确认邮件是否真实

4

在使用便携式设备（例如 U 盘）时，怎么保证数据安全

- A. 关闭自动播放
- B. U 盘先杀毒后打开
- C. 不随意外借设备
- D. 不在不可信的设备上使用 U 盘

5

下面那种方法发送敏感信息邮件时能更有效保证邮件安全

- A. 正常发送
- B. 以附件形式发送
- C. 附件加密发送，正文中说明密码
- D. 加密发送，密码通过其他渠道发送

6

如果员工小王问你要你手上的某个文档，之前没给他发过这类文档，哪个做法是不正确的

- A. 查一下公司部门相关要求，看这个文档的扩散范围是否包含小王
- B. 不能确定这个文档的扩散范围，咨询信息安全经理；
- C. 你觉得应该没问题，就发给小王，并告知要保密
- D. 询问直接上级的意见
- E. 如果你知道这个文档的编写部门，让小王直接找这个部门索要

7

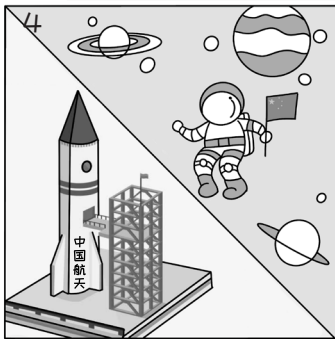
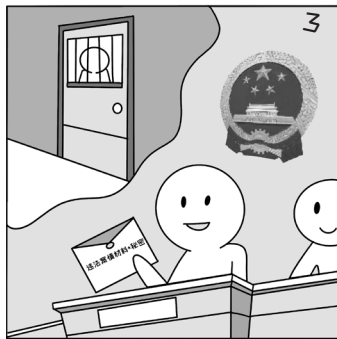
在某电子商务网站购物时，卖家突然说交易出现异常，并推荐非平台官方的客服电话或即时通讯号码。

以下最恰当的做法是

- A. 直接和推荐的客服人员联系
- B. 如果对方是信用比较好的卖家，可以相信
- C. 通过电子商务官网上寻找正规的客服电话或联系方式，并进行核实
- D. 如果对方是经常交易的老卖家，可以相信



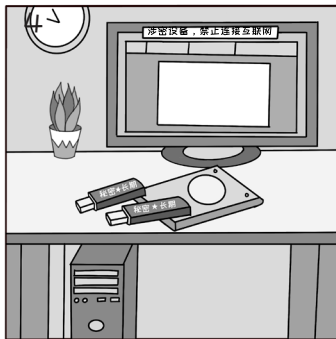
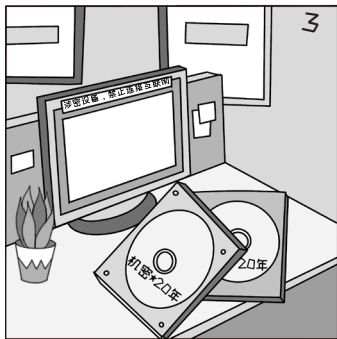
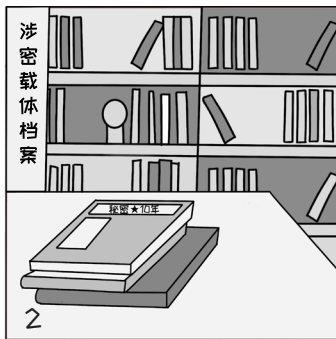
关注绿盟科技官方微信公众号回复“各种钓鱼”获取答案



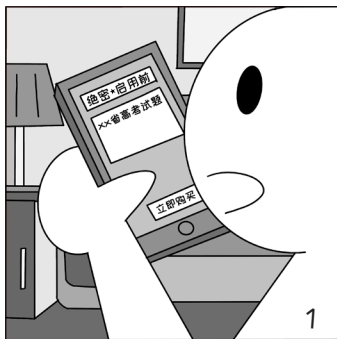
- 国家秘密定义：关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉。



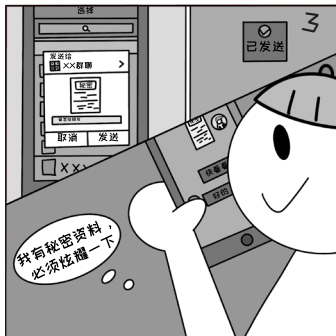
- 国家秘密从高到低，分为绝密、机密、秘密，三个等级；国家秘密标识的格式是【密级★保密期限】，如机密★20年。普通商密文档不可使用国家秘密标识。



- 国家秘密载体：以文字、数据、符号、图形、图像、声音等方式记载国家秘密信息的纸介质、光介质、电磁介质等各类物品。



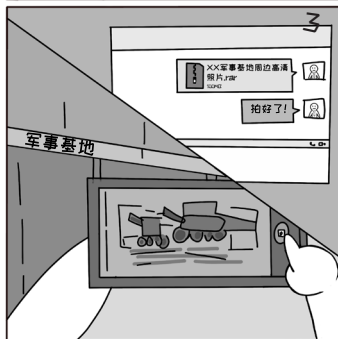
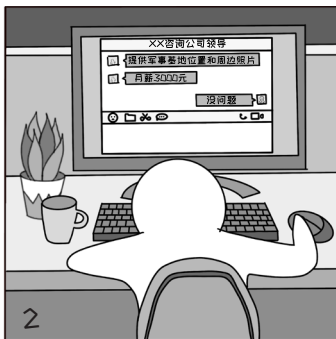
- 只要是泄露后可能损害国家在政治、经济、国防、外交等领域安全和利益的秘密事项，都属于国家秘密，不管您是通过什么途径知道的，都必须严格保密。发现泄露国家秘密的行为，应该第一时间举报。



■ 不得私自复制、记录、存储、拍摄国家秘密信息，更不可私自发送。

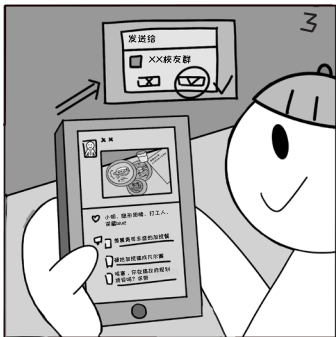


- 依据国家保密事项范围，要对拟公开发布的信息是否涉及国家秘密进行宣传报道前的保密审查审批。



■ 警惕间谍机构以商业调查、调研咨询等名义，向公民套取国家秘密信息。

今天加班餐好丰盛，拍一张。



- 使用和保管国家秘密文档应当严格执行国家保密管理规定。如果发现国家秘密信息外泄，应该第一时间提醒和举报，而不得再行传播。



- 涉及国家秘密的文档应交由保密管理机构统一销毁。废旧工作文件销毁或出售前，要注意清点核对，避免有涉密或敏感文档混杂其中。



- 间谍人士会通过拉近关系、给好处、卖人情等方式，接近目标人士，套取国家秘密。我们在日常工作生活中，尤其在境外活动以及与境外人员的交往中，更要特别注意防范。



- 内部人员、工作同事也有可能被渗透或策反。工作中如果发现可疑行为，应当勇于制止，及时上报。



- 打印、制作涉密文档需要在保密设备上进行。黑客可能长期控制目标公司附近打印店电脑权限，窃取核心机密文档。如果单位内部不具备条件，可到具有涉密载体制作资质的单位进行打印。严禁在普通打印店打印涉密文档。

黑客可能长期控制目标公司附近打印店电脑权限，窃取核心机密文档。涉密打印最好公司自备打印设备人员，离线作业。



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、金融、运营商、能源、交通、企业、教科文卫等行业用户和各类型企业用户，
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

