OWASP 中国
The Open Web Application Security Project

安全意识 TOP 10

- 2018

V1.0

目录

目录

关于OWASP中国

OWASP，即，Open Web Application Security Project（开源Web应用安全项目）是一个全球性的、开源的软件安全社区，致力于帮助各企业组织开发、购买和维护可信任的应用软件。

OWASP中国，是OWASP全球组织在中国大陆地区的区域组织。总部设在深圳，并在北京、上海、成都、合肥、大连、南宁等12座城市设有区域性分部。

在OWASP和OWASP中国，您可以找到以下免费和开源的信息：

- 应用软件安全工具和标准；
- 关于应用软件安全测试、安全代码开发和安全代码审查方面的完整书籍；
- 标准的安全控制和安全库；
- 全球各地分会；
- 尖端应用软件安全技术研究；
- 专业的全球会议；
- 邮件列表。

更多信息，请访问：https://www.owasp.org。
更多中文信息，请访问：http://www.owasp.org.cn/。

所有OWASP的工具、文档、论坛和各地分会都是开放的，并对所有致力于改进应用软件安全的人士开放。

我们主张将应用软件安全问题看作是人、过程和技术相融合的问题，因为提供应用软件安全最有效的方法是在应用软件开发过程中对人、过程和技术进行提升。

OWASP和OWASP中国没有商业压力，使得我们能够提供无偏见、实用、低成本的应用软件安全信息。 和许多开源软件项目一样，OWASP和OWASP中国以一种协作、开放的方式制作了许多不同种类的材料。

OWASP基金会是确保项目长期成功的非营利性组织。几乎每一个与OWASP相关的人都是一名志愿者，这包括了OWASP董事会、全球各地分会会长、项目领导和项目成员。

我们期待您的加入！

版权和许可

关于

前言

近年，我国先后颁布和实施了《国家网络空间安全战略》、《国家网络安全法》、《网络产品和服务安全审查办法(征求意见稿)》、《网络安全等级保护条例（征求意见稿）》等一系列关于网络安全保障的法律法规和政策文件，以指导和要求相关网信工作的开展。而随着我国互联网应用的普及，信息安全与网络安全已不仅是国家或企业需面对的问题。社会公众对信息网络的依赖性越强，面临的潜在安全风险也将越高，且极易遭受信息泄露、财产损失等方面的损害。

准确的意识并识别信息安全风险变得越发重要。作为一个具有社会责任感的安全组织，OWASP中国不能坐视普通公众忽视那些常见却又威胁大的安全问题而不顾。

OWASP中国鼓励社会公众使用本《安全意识Top 10》，开始了解日常生活中的信息安全，并从其他已经发生的实际安全事件中学习经验教训，在日常生活中管理安全风险，避免受到信息安全事件的影响。

如您有任何关于本文档的建议或是意见，可通过 project@owasp.org.cn，与我们取得联系。

我们希望本文档可以对您有所帮助！

OWASP S-SDLC项目

本《安全意识Top 10》文档属于由OWASP中国在OWASP全球独立发起并主导的“OWASP S-SDLC项目”中培训部分的一个子项目。

S-SDLC，即，Secure Software Development Life Cycle（软件安全开发生命周期），是一套完整的，面向软件安全开发的安全工程方法。旨在于帮助研发团队在软件产品研发过程中降低安全风险，提升软件安全质量。S-SDLC定义了软件安全开发的流程，以及各个阶段需要进行的安全活动及相应的指南、工具、模板。它包括培训、需求阶段、设计阶段、实现阶段、测试阶段、发布/维护阶段。

有关OWASP S-SDLC项目的更多信息，请访问：
https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project

简介

欢迎

欢迎阅读2018年版《安全意识Top 10》，本版本也是OWASP中国为本项目面向社会公众发布的第一个正式版本。

《安全意识Top 10》基于项目组收集、整理和筛选的近200个典型信息安全事件。这些信息安全事件全部发生在2017年1月至5月和2018年1月至5月两个时间段内。这10类安全意识项是根据对200个安全事件的数据统计分析，并结合了对普遍性、危害性、可控性的一致性评估而形成。

《安全意识Top 10》的首要目的是教导社会公众，特别是对信息安全意识和知识不了解、不熟悉的社会公众，让他们认识到这些信息安全事件所产生的后果。本文档还提供了防止这些高风险事件发生的基本方法。

鸣谢

感谢互联网安全研究中心对本项目的创建和领导：

- 牵头人：丁子桓
- 参与人（按姓氏拼音排序）：曹传勇、陈香锡、夏天泽、许飞、王颉、邹庆明

感谢广东清远职业技术学院对本项目提供的信息收集整理：

- 指导教师：黄华、郭锡泉、王斌、陈湘辉、刘志成
- 学生团队：郑楷涛、邹俊鹏、陈榕华、陈浩亮、刘梓健、黄绮萍、余远宏、王春前、梁冠雄、黄邵模、马俊明、邹俊杰、孔慧欣、何尧光

互联网安全研究中心（英文Security Zone），是国内知名的独立、开源的互联网安全研究机构，专注于前沿互联网安全技术研究。SecZone秉承创新、融合、开拓的宗旨，不断吸收国内外最新、最专业的安全技术，并创新性运用于国内各个行业，推动国内互联网安全技术的发展。互联网安全研究中心工作范围主要涵盖：OWASP中国运营、CWASP培训运营、CWASP CSSP培训运营、应用安全联盟（ASC）运营、WAF测评服务。

清远职业技术学院成立于2002年，是清远市人民政府举办的综合性公办高等学校。学院现有全日制高职学生1.2万人。学院实施“强师工程”，加强师资队伍建设，现有清远市紧缺适用高层次人才27人，广东省高等职业教育专业领军人才培养对象2人，广东省高等学校优秀青年教师培养计划培养对象3人，广东省扬帆计划培养高层次人才项目1人，清远市重点人才项目“起航计划”项目1项。

扫一扫
关注OWASP中国

Top 10 安全意识 Top 10 —2018

TOP 10	描述
A1-利用漏洞攻击	除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件。
A2-信息泄露事件	因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件。
A3-计算机病毒事件	蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件。
A4-木马事件	蓄意制造、传播特洛伊木马程序，或是因受到特洛伊木马程序影响而导致的信息安全事件。
A5-钓鱼事件	利用欺骗性的计算机网络技术，使用户泄漏重要信息而导致的信息安全事件。
A6-电信诈骗	利用各种渠道取得被害人的信任和注意，实施诈骗行为。
A7-网络设备监视及窃听事件	通过技术手段，利用网络监控或窃听设备，窃取用户个人隐私等而导致的信息安全事件。
A8-网页内嵌恶意代码事件	蓄意制造、传播网页内嵌恶意代码，或是因受到网页内嵌恶意代码影响而导致的信息安全事件。
A9-信息篡改事件	未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件。
A10-信息丢失事件	因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件。

A1 利用漏洞攻击事件

什么是利用漏洞攻击事件？

利用漏洞攻击事件是指除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件。

利用漏洞攻击事件属于网络攻击事件的一种。网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的安全事件。

影响

各种可能的负面后果包括：数据泄露、损坏；未授权访问；植入病毒木马；甚至整个主机被控制等。

普遍性 ★★★★★

危害性 ★★★★★

可控性 ★★★★

典型事件案例

案例#1
支付宝一键克隆

腾讯玄武安全实验室揭露了“应用克隆”漏洞；此漏洞广泛影响安卓系统的手机软件，例如支付宝，用户只要点击短信链接或扫描二维码就可能被克隆，造成财产损失和信息泄露

案例#2
噩梦公式二代

黑客利用 Office 内在的功能（公式编辑器）发起的攻击(“噩梦公式二代”)，打开恶意文档就会中招。此漏洞会趁着用户没打补丁的空挡，在你不知情的情况下控制你的电脑。

案例#3
“WannaCry”勒索病毒

“WannaCry”勒索病毒攻击爆发，国内外多所高校及企业因为漏洞较多，遭遇勒索软件入侵，导致大量电脑文件被加密，被迫支付赎金或无法再使用。

我如何做能避免损害?

安装杀毒软件。

安装防火墙。

及时更新电脑的系统补丁。

养成不用电脑时关闭联网的习惯。

A2 信息泄露事件

什么是信息泄露事件？

信息泄露事件是指因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件。

信息泄露事件常见于网络个人信息泄露，包括基本信息、设备信息、账户信息、隐私信息、社会关系信息和网络行为信息等。不法人员利用恶意程序、各类钓鱼和黑客攻击非法获取个人信息，谋取利益。大规模信息泄露事件频发。

影响

各种可能的负面后果包括：个人信息的泄露、人身威胁、财产损失。

普遍性 ★★★★★

危害性 ★★★★★

可控性 ★★★★☆

典型事件案例

案例#1
“晒”机票泄露个人信息

朋友圈晒机票有风险。只要将你的条形码上传至免费解码网，就能知道你姓名和旅程所有信息，并可能导致后面的退票诈骗及其他信息泄露导致的财产损失。

案例#2
滴滴顺风车乘客信息泄露

空姐在郑州航空港区乘坐滴滴顺风车遇害一案引发社会广泛关注。乘客个人信息泄露，造成严重后果。

案例#3
二维码泄露被复制

微商赵女士在网络交易过程中，不法分子以自己支付宝余额不足为借口，提出让赵女士将付款码发给自己扫码付款。收到付款码截图后，不法分子随即进行复制，盗刷了赵女士的银行账户。

我如何做能避免损害?

不在非官方网站填写个人敏感信息。

微信和QQ不加不明身份的好友。

不轻易连接公共场所提供的Wi-Fi以及免费Wi-Fi。

连接不安全的Wi-Fi时不填写任何密码以及敏感信息。

处理照片、车票、快递单等包含个人信息的资料时，一定要遮蔽姓名、卡号和条形码。

A3 计算机病毒事件

什么是计算机病毒事件？

计算机病毒事件是指蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件。

计算机病毒是一个程序、一段可执行代码，类似于生物病毒，具有隐蔽性、感染性、潜伏性、可激发性、破坏性。它们能自身附着在各类文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。随着智能电子设备的使用，影响范围越来越广。计算机病毒已不再局限于传统的台式机和笔记本电脑，移动终端同样也会遭受病毒破坏。

影响

各种可能的负面后果包括：引起终端设备故障、破坏数据、远程操控、个人信息的泄露、未授权的访问、财产损失等。

普遍性	★★★★
危害性	★★★★★
可控性	★★★★☆

典型事件案例

案例#1
“锁机病毒”勒索钱财

锁机生成器病毒，仿冒各类软件诱导用户安装，锁定手机并勒索用户钱财 。

案例#2
“短信拦截马”窃取隐私

“短信拦截马”这个病毒活跃在各大Android平台上，以窃取用户隐私为目的，通过拦截并监视短信，利用盗取的用户信息盗刷银行账户、偷取用户财产。

案例#3
“变脸窃贼”暗扣付费

手机突然收到大量扣费短信息。这是用户手机下载了暗扣类应用（俗称“变脸窃贼”）所致，表面上所需权限正常，其实内含使手机付费接受短信等有害权限。

我如何做能避免损害?


安装杀毒软件以及防火墙。


定期对计算机或终端设备进行扫描并及时更新杀毒软件的补丁。


使用正版软件，不随意从非官方渠道下载软件或APP（尤其是“破解版“）。


不上不熟悉且引发安全告警的网站。

从非官方网页安装软件或APP时注意核对文件信息。


不轻易点击收到的邮件链接及附件。

A4 木马事件

什么是木马事件？

木马事件是指蓄意制造、传播特洛伊木马程序，或是因受到特洛伊木马程序影响而导致的信息安全事件。

木马程序通常通过一段特定的程序（木马程序）来控制另一台计算机，打开一个或几个端口，攻击者利用这些打开的端口进入电脑系统。隐蔽性是木马的首要特点，木马程序发展到今天，对用户的威胁越来越大，使普通用户很难在中毒后发觉。一旦被木马控制，电脑或智能设备将毫无秘密可言。

影响

各种可能的负面后果包括：远程监控、危害本机信息安全（盗取QQ帐号、游戏帐号甚至银行帐号），将本机作为工具来攻击其他设备等。

普遍性 ★★★★

危害性 ★★★☆

可控性 ★★★★☆

典型事件案例

案例#1
公共充电桩易藏木马

3.15晚会上，安全专家曾把藏身于免费充电桩中的木马病毒揪了出来。通过实验得知，通过使用公共充电桩给手机充电，黑客可控制手机，实现手机中的照片查看、短信发送、窃取手机使用者的验证码，甚至进行消费。

案例#2
短信链接藏木马，银行卡被盗

市民王女士取钱时，发现这张一直锁在家中的银行卡里只剩十多块钱，另外16万元存款莫名消失。原来，王女士的手机曾收到过一条名为“老同学照片”的短信链接，手机中了木马，导致存款被盗。

案例#3
QQ营销病毒，强行添加好友

QQ营销病毒传播感染量高达约15万余台。感染用户电脑后会强行添加QQ好友、QQ群，邀请好友加群并自动发邮件给QQ营销号。

我如何做能避免损害?

安装杀毒软件以及防火墙。

定期对电脑进行扫描并及时更新杀毒软件的补丁。

使用正版软件，不随意从非官方渠道下载应用或APP（尤其是“破解版“）。

不上不熟悉且引发安全告警的网站。

从非官方网页安装APP时注意核对文件信息。

不轻易点击收到的邮件链接及附件。

A5 钓鱼事件

什么是钓鱼事件？

钓鱼事件是指利用欺骗性的计算机网络技术，使用户泄漏重要信息而导致的信息安全事件。

最典型的网络钓鱼攻击通过将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉，并利用这些获取不正当利益。

影响

各种可能的负面后果包括：信息泄露、经济损失等。

普遍性 ★★★★☆

危害性 ★★★★

可控性 ★★★★☆

典型事件案例

案例#1
邮件钓鱼，被骗汇款

西安一外贸公司收到"伪造邮件"，由于没有对收来的邮件进行辨别，向国外供货商汇款，被骗了40多万元。

案例#2
点"微信红包"手机中毒

多位网友遭遇了疑似"微信红包"骗钱的事，点开"微信红包"后不但没有领到钱，手机反而中了"木马病毒"导致账户内的钱被转走。

案例#3
Wi-Fi钓鱼，银行账户被盗

株洲市张女士，在一家商场内发现一个没设密码的Wi-Fi。连接Wi-Fi后，通过手机银行支付方式在淘宝上购买了衣服。随后，手机连续收到短信提醒，其信用卡被盗刷4笔，总金额高达8000多元。

我如何做能避免损害?

不轻易点击不认识的人或公司发来的邮件链接，在点开的网页上不轻易输入用户名和密码。

输入前检查网站名是否正确；比如说www.mail.qq.com和www.mail.qq.cn。

上官方及受信任的网站（网站名前有https字样），注意浏览器的安全提醒。

不轻易扫描各种二维码。

A6 电信诈骗

什么是电信诈骗？

电信诈骗是指利用各种渠道取得被害人的信任和注意，实施诈骗行为。

电信诈骗即是虚假信息诈骗，借助于手机、固定电话、网络等通信工具和现代的技术等实施的非接触式的诈骗犯罪。随着网络的发展，可以说是迅速地发展蔓延，给人民群众造成了很大的损失。

影响

各种可能的负面后果包括：财产经济损失、人身伤害等。

普遍性 ★★★★☆

危害性 ★★★★

可控性 ★★★★★

典型事件案例

案例#1
伪装政府机关诈骗

贸易委员会发现了多起伪装成中国大使馆的诈骗电话。犯罪分子伪装成中国大使馆诈骗250万美元。

案例#2
二维码诈骗

李先生收到一条某电商网站的推销短信，通过手机扫描了店主发来的二维码后，进入一个支付界面，输入银行账号和密码后却显示支付失败，之后却发现自己的银行账号被转走10000余元。

案例#3
假账号诈骗

徐玉玉电信诈骗案：诈骗团伙以发放助学金的名义，让徐玉玉转账激活卡片，盗取了9900元学费，最终导致徐玉玉心脏骤停而离世。

我如何做能避免损害？

不要相信任何在电话里提到的公检法部门的侦查、汇款；不要相信网络或传真的“法院传票”。

不要轻易扫描他人的付款二维码需要输入密码账号时，仔细核对支付页面。

在电话中提及转账、汇款、罚款等说法时，一定要通过官网渠道进行二次确认。

不要随便相信中奖信息，尤其是先交“个人所得税”、“公证费”、“转账手续费”等中奖信息。

A7 网络设备监视及窃听事件

什么是网络监视及窃听事件？

网络设备监视及窃听事件是指利用网络监控或窃听设备，获取设备控制权从而窃取用户个人隐私等而导致的信息安全事件。

网络设备监视及窃听事件主要涉及侵犯个人隐私，利用摄像头为代表的物联网设备对政府、企业、个人进行信息窃取。

影响

各种可能的负面后果包括：个人隐私泄露，财产损失、人格利益受损及精神痛苦等。

普及性 ★★★☆

危害性 ★★★★

可控性 ★★★★☆

典型事件案例

案例#1
麦克风窃听

攻击者首先向目标发送钓鱼邮件，恶意程序隐藏 Microsoft Word 文档中，一旦感染目标之后利用恶意程序控制设备的麦克风去记录对话、屏幕截图、文档和密码。

案例#2
监控摄像头直播

某视频直播网站引发热议，在该网站上可以看到全国各地甚至国外的监控摄像头的免费直播，包括街景、餐厅、商店、办公室，甚至市民家中情况。

案例#3
手机摄像头拍照

vivo NEX手机开卖，“隐藏式升降式摄像头”引热议。在QQ浏览器中打开携程网站（APP权限开启），vivoNEX的前置摄像头突然自动升了起来，然后默默“扫描”了一眼再缩回去。

我如何做能避免损害?

不用摄像头的时候，盖住摄像头。

不在摄像头范围内，泄露账户密码等隐私信息。

定期对电脑进行扫描并及时更新杀毒软件的补丁。

A8 网页内嵌恶意代码事件

什么是网页内嵌恶意代码事件？

网页内嵌恶意代码事件是指蓄意制造、传播网页内嵌恶意代码，或是因受到网页内嵌恶意代码影响而导致的信息安全事件。

网页恶意代码(又称“网页病毒”)是利用网页来进行破坏的病毒。当用户登录某些含有网页病毒的网站时，网页病毒便被悄悄激活，这些病毒一旦激活，可以利用系统的一些资源进行破坏。

影响

各种可能的负面后果包括：IE默认搜索引擎被修改、系统启动时弹出广告信息、营销诈骗、信息泄露。

普遍性	★★★☆
危害性	★★★☆
可控性	★★★★☆

典型事件案例

案例#1
知名网站的广告被“挂马攻击”

国内多家知名软件、网站的广告页面遭到病毒团伙的“挂马攻击”只要用户访问该页面，即会触发浏览器漏洞。

案例#2
恶意代码注入合法网站

Websense安全实验室监测到一场大规模恶意代码注入攻击正在不断袭击合法网站，已经有上万个合法网站受到攻击，无数的Web用户受到感染。

案例#3
网站感染按键记录器

WordPress 网站感染了按键记录器。恶意程序会记录密码，以及管理员或访客输入的任何内容。恶意程序除了安装按键记录器还，还安装了挖矿脚本，利用访客的计算机挖掘数字货币。

我如何做能避免损害?

安装杀毒软件以及防火墙。

定期对电脑进行扫描并及时更新杀毒软件的补丁。

不上不熟悉以及引发安全警报的网站。

A9 信息篡改事件

什么是信息篡改事件？

信息篡改事件是指在未经授权的情况下，将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件。

信息篡改事件通常体现在网页、商务数据、金融数据、个人信息等保存在数据库中的资料被人为修改，从中牟利，例如数据篡改、网页篡改等。攻击者获取受害网站权限或个人信息的方法都很常见，包括SQL注入和口令盗取，其中最常见的就是文件包含漏洞。

影响

各种可能的负面后果包括：访问控制失效、个人信息泄露、财产损失。

普遍性 ★★★☆

危害性 ★★★★☆

可控性 ★★★

典型事件案例

案例#1
银行存款被篡改

俄罗斯一安全公司实验室介绍了他们的一些调查结果，表明一个或多个黑客群体针对至少 140 家银行和组织进行了这种攻击，旨在盗取凭证和金钱。

案例#2
政府网站被篡改

江苏警方奔赴马来西亚打掉一个由四人组成的黑客团伙，个别政府网站遭黑客非法侵入，会被链接到境外的赌博网站。

案例#3
虚拟货币客户端被篡改

Myetherwallet（MEW）是网络上最受欢迎的以太坊钱包客户端，很不幸其在北京时间4月24日晚9点遭受DNS劫持攻击。许多用户报告缺失资金，造成经济损失。

我如何做能避免损害?

重要信息和有价值的资料应定期备份。

不要把存款、股票等有价证券放在同一个平台。

A10 信息丢失事件

什么是信息丢失事件

信息丢失事件是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件。

此类事件多由于服务端被攻击或人为失误造成，会在一定程度上影响公众生活。

影响

各种可能的负面后果包括：财产经济损失等。

普遍性 ★★★

危害性 ★★★☆

可控性 ★★★☆

典型事件案例

案例#1
误操作，移动用户数据丢失

因华为误操作导致广西80万移动用户数据丢失一事，华为已经被中国移动处以5亿罚款，同时中国移动已经展开全国范围的系统大排查。

案例#2
苹果手机读取权限漏洞

苹果macOS系统曾经被曝光允许任何人通过客人账户获得该设备的所有读取权限。不过好在苹果及时做出了补救措施。但事情没过多久，又有一位用户发现了类似的漏洞。

案例#3
数据库被删除数据，以备份勒索

数据库被黑并遭勒索，犯罪分子利用数据库配置漏洞进行未授权访问、拷贝、删除数据库内容，并以备份数据威胁受害者、索要赎金。

我如何做能避免损害?

重要信息和有价值的资料应定期备份。

定期对电脑进行扫描并及时更新杀毒软件的补丁

措施

现在就启动您的安全措施

类别	初级措施	高级措施
系统安装	✓ 安装最新版正版操作系统； ✓ 启用系统防火墙； ✓ 安装系统补丁； ✓ 一定要设密码（用户名/密码）； ✓ 安装杀毒软件，用杀毒软件做全盘扫描。	✓ 取消非必要授权； ✓ 设备自带防护等级设置为“高”。
数据保护	✓ 定期备份文件； ✓ 使用office的加密功能保护文档。	✓ 多因子验证。
正确使用密码	✓ 不使用已知不安全密码或常见密码； ✓ 最好不要名字、生日、电话号码等； ✓ 不要一个密码通用所有帐号； ✓ 设置的密码一定要让自己记住。	✓ 密码应该不少于8个字符； ✓ 同时包含多种类型的字符。
第三方软件管理	✓ 每种功能的软件尽量选择自己熟悉的一种安装，不要重复安装； ✓ 尽量选择规模较大的软件公司出品的第三方软件； ✓ 使用正版的第三方软件； ✓ 发现第三方软件提示要更新时，请尽快安装。	✓ 随时关注相关软件的官方网站，发现最新版本及时安装； ✓ 确认长时间不需要使用的软件请尽快卸。
邮件安全	✓ 如果你不能确认你的邮件是合法并安全的，不要发送； ✓ 不要打开陌生人发来的邮件附件，也不要点击邮件中的链接； ✓ 不要轻易在网站上留你的公司邮箱或重要私人邮箱； ✓ 如果留取你的邮件地址不是获取服务所必需的，不要留取自己的邮件地址。	✓ 通过邮件发送公司机密/敏感信息、个人隐私信息、或信用卡数据等，此类数据需要保护，即加密后才能发送； ✓ 创建不重要的邮件帐号，用于一些网站注册和邮件列表。
无线安全	✓ 区分在家登陆和公共场合的登陆； ✓ 不要使用不受信的无线网络，使用公有的无线网络传输隐私信息时一定要加密传输； ✓ 最好把WiFi连接设置为手动。	✓ 如果不使用无线，带无线功能的笔记本和手机设备在工作区域应该关闭无线功能，避免攻击者通过设备的无线接入内网。
智能终端安全	✓ 不要随意将移动终端连接到内部网络的设备上，哪怕仅仅是充电； ✓ 不要随便安装不受信的app； ✓ 不用电脑时，一定要关机； ✓ 合理处置旧手机。	✓ 移动终端上存储的隐私信息尽可能的加密存储。
移动存储介质	✓ 不使用未知来源的移动存储介质； ✓ 使用移动存储介质时，先进行扫描杀毒； ✓ 请尽量避免工作移动存储介质和私人的移动存储介质交叉使用。	✓ 对于安全要求较高的设备，应该仅允许使用特定的移动存储介质； ✓ 敏感信息如果要存储在移动介质上，请加密后再存储，并妥善保管该介质。
购物安全	✓ 建议在大型的网购平台进行网购，不要轻易相信各种打着打折，优惠的旗号。	✓ 在登录购物网站时要核实网站的域名是否正确。审慎点击商家从即时通讯工具上发送的支付链接。
隐私安全	✓ 要在身份证复印件上加添加用途备注； ✓ 不要随意在各种网站上留个人信息； ✓ 在留取个人信息前仔细阅读网站的隐私保护声明； ✓ 不要总把私人账号随意借给别人使用； ✓ 平时不要习惯乱用他人的电脑登陆； ✓ 登录账号输入密码的时候注意周围是否有人盯着你的输入； ✓ 重要的账号在公共场所登陆后要注意退出； ✓ 妥善处置快递单、车票、购物小票等包含个人信息的单据； ✓ 不在微博、群聊中透露个人信息； ✓ 慎重参加网上调查活动。	✓ 安全意识、使用习惯是首要。
预防诈骗	✓ 不要轻易相信别人，尤其是在网络中； ✓ 不要随意点击别人发过来的网页链接，尤其是在邮件和即时通讯软件中； ✓ 能够自己输入的网址尽量自己输入，而不要直接点击发过来的链接； ✓ 邮件中涉及到修改密码的链接不要轻易点击； ✓ 在网络上涉及银行卡有关的操作一定要慎重，要仔细查看相关网站的信息（证书、域名等）； ✓ 管理员一般不会询问用户的密码，不管在何种场合下（邮件、论坛等）。	✓ 安全意识、使用习惯是首要。