Cybersecurity
Awareness

网络安全意识科普手册

每天培养一个网安小习惯

CONTENTS.

目录

01

AI使用安全

选择正版AI应用

通过官方渠道下载AI应用程序；

打开AI网站时，应针对网址进行多方面验证

避免分享敏感信息

避免在使用AI的过程中分享敏感信息，如公司内部私密文档、设计图纸以及敏感数据等

使用匿名身份交流

使用匿名或虚拟身份与AI进行交流，尽量减少个人信息的暴露

管理隐私设置

定期检查所使用AI应用的隐私设置，确保只分享必要的信息

谨慎判断AI生产的内容

对AI提供的内容和建议保持怀疑态度，尤其是在做出重要决策时，避免盲目相信AI的建议

设置强密码和多因子认证

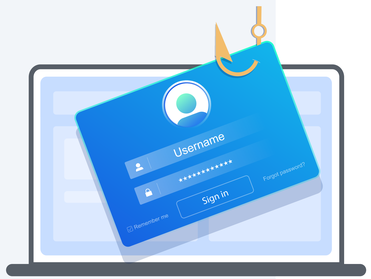
为AI账户设置强密码，并采用多方式登录验证，增加账户安全性

及时更新软件

确保所使用的AI应用保持最新版本，所购买的AI相关设备及时安装安全更新

02

钓鱼防范



警惕邮件钓鱼

1. 不浏览被安全软件提示为恶意的站点
2. 不打开来历不明的文档，以及带有图片、文件夹、文档、音视频等图标的文件
3. 不安装来历不明的软件、外挂、浏览器插件等，不打开被安全软件标记为恶意的文件
4. 不点击未经核实来源邮件内的任何链接
5. 不输入账号、密码信息等到未经核实的邮件中，重要邮件需二次电话确认
6. 安装终端安全防护软件以防御木马病毒攻击

警惕社工钓鱼

1. 安装杀毒软件并开启实时查杀功能
2. 不打开任何未经验证人员发送的文件
3. 不轻信陌生人、「熟人」聊天内容，拒绝任何来自陌生人的在线帮助
4. 社交软件中不轻易同意陌生人的好友请求，不添加任何不认识的陌生人
5. 不轻信陌生人、「熟人」来电或短信，如：申请添加好友，询问同事信息，索要验证码等
6. 谨慎处理主题为「紧急」、「中奖」「XX到期」「优惠打折」「扫码进群」等信息的邮件、短信或二维码
7. 不在微信、QQ、微博、论坛等社交应用上发布本单位敏感信息，透露个人及单位信息
8. 对办公电脑敏感数据进行加密处理
9. 不在公共场合交流和处理敏感信息

03

病毒防范

防范银狐病毒

1. 在官方网站下载日常使用工具
2. 不打开未经核实的附件内容
3. 不点击社交软件聊天中任何未经核实的链接，警惕聊天软件中的异常命名文件，尤其是各类以文档格式命名的exe文件

防范破坏性病毒

1. 增强安全意识，做好数据备份
2. 部署终端安全软件定期查杀
3. 养成良好上网习惯，谨慎下载网络文件数据，拒绝来历不明的移动介质
4. 遭遇破坏性病毒建议第一时间断开网络避免文件被删除、破坏等问题从而引起更大损失

防范勒索病毒

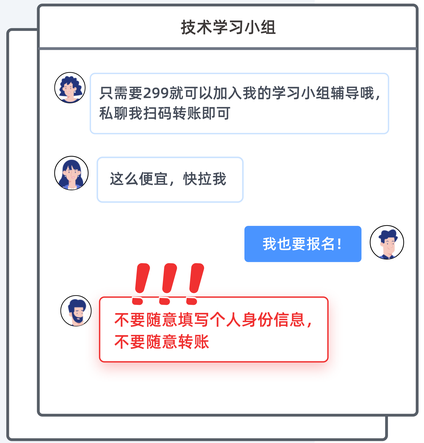
1. 定期备份业务系统数据，多点异地存储
2. 部署终端安全防护软件，并开启自动处置功能
3. 增强相关人员信息安全意识，定期开展网络安全意识培训
4. 使用强密码和多因素身份验证来保护远程访问凭据，并定期更换密码
5. 加强组织内部网络安全管理，如网络隔离、访问控制、资产管理、漏洞排查等
6. 避免将业务远程方式直接暴露在公网。如需要远程访问，可考虑使用零信任等其他安全的访问方式

防范挖矿木马病毒

1. 及时更新系统补丁，预防漏洞攻击
2. 不浏览被安全软件提示为恶意的站点
3. 不打开来历不明的文档，以及带有图片、文件夹、文档、音视频等图标的文件
4. 不安装来历不明软件、外挂、浏览器插件等，不打开被安全软件标记为恶意的文件
5. 安装终端安全防护软件以防御木马病毒攻击

04

个人信息安全



网上交易安全

1. 不与他人共享过多个人信息
2. 安装最新的防病毒软件和防火墙
3. 使用安全的网络，避免使用公共无线网络
4. 避免点击未知来源的链接或下载未知来源的文件
5. 使用强密码并定期更改密码，且不要在多个网站使用相同的密码
6. 确保访问的是已知的、受信任、使用了安全加密技术（SSL）的网站
7. 使用安全的支付方式：勿盲目转账，勿进行不可信的第三方交易

移动手机安全

1. 安装杀毒软件并定期进行病毒查杀
2. 从官方应用商店下载应用程序
3. 及时更新手机系统和应用程序
4. 不随意连接公共Wi-Fi
5. 不点击来自陌生人的链接，以免下载恶意软件或遭受网络钓鱼攻击
6. 不轻易授权应用程序访问个人信息
7. 定期备份手机数据

群聊安全管理

1. 明确群内行为规范，禁止发布敏感信息和不当言论
2. 群管理需要明确群内成员身份信息，定期清理群内无关人员
3. 不在群内分享个人敏感信息，如身份证号、地址、电话号码等
4. 禁止群内传播任何未经确认的信息和文件
5. 对于病毒样本等可疑文件，加密压缩后再单独发送给信息安全人员
6. 建议关闭聊天软件自动下载功能，待确认文件无异常后再下载

04

个人信息安全

互联网软件下载

1. 通过官方网站或正规应用商店下载软件，避免使用第三方网站
2. 仔细阅读参考用户评论评分
3. 拒绝不良诱惑，请勿下载擦边软件、播放器等未知软件
4. 针对下载的文件先进行病毒查杀再运行
5. 部署终端杀毒软件并定期进行全盘查杀
6. 保持操作系统和软件更新
7. 限制软件访问权限
8. 定期备份终端重要数据

个人数据安全管理

1. 数据传输
   - 针对需传输的敏感文件进行可信加密处理
   - 不使用公共网络（如商场等公共场所Wi-Fi等）传输敏感信息

2. 数据存放
   - 定期进行数据加密备份（如使用加密压缩备份数据）
   - 使用多个存储设备存储敏感数据
   - 定期更新并检查备份文件完整性

3. 数据销毁
   - 使用专业的硬盘粉碎机进行硬盘物理粉碎
   - 使用消磁机对硬盘消磁处理
   - 使用专用的数据擦除软件进行数据删除
   - 对存储介质进行完全格式化并重置系统
   - 先对需销毁数据进行加密，然后销毁数据，最后将加密密钥进行销毁

05

IT安全

预防网页篡改

1. 定期备份网站数据，异地存储
2. 使用安全的网站托管服务，定期检查服务器安全设置，版本更新情况
3. 使用网络安全设备和软件以检测和防御恶意攻击者入侵网站
4. 加强用户认证和授权机制，限制用户对网站内容的修改权限
5. 增强管理人员安全意识，定期开展网络安全意识培训
6. 提升网站内容的实时监测能力，定期开展专项检查

FRP代理使用安全

1. 对使用FRP工具的人员进行安全意识培训，了解FRP的安全风险和使用规范，避免因使用不当而导致安全问题
2. 限制使用人员和范围，发现未授权用户需要及时阻断并定位人员要求整改
3. 使用时开启加密传输，限制访问IP、设置强访问密码等
4. 定期从可信来源更新FRP工具的版本，以保证工具本身的安全

05
IT安全

企业数据安全管理

1. 数据传输

- 使用安全的网络链接，优先选择HTTPS、VPN等加密连接方式
- 在数据传输过程中使用多因素认证，增加安全层级

2. 数据存放

- 加强访问控制，严格设置访问权限
- 使用AES等强加密算法对存储的数据进行加密
- 定期备份数据，并将备份存储在安全的、异地的存储介质上
- 启用日志记录和监控，及时发现和响应异常访问和操作

3. 数据销毁

- 设置数据的有效期，到期自动删除/覆盖
- 建立严格的数据销毁审批流程，确保数据销毁得到正确授权和记录
- 对数据销毁过程进行监督并进行记录，以备审计和回溯

防范debug敏感信息泄露

1. 关闭debug模式
   在生产环境中，应该关闭debug模式，以避免敏感信息泄露
2. 设置用户访问白名单
   限制用户的访问范围，单位可以更好地控制其数据和资源，并减少数据泄露和其他安全漏洞的风险
3. 加强安全意识培训
   加强员工安全意识培训，提高他们对安全漏洞的识别和处理能力，避免安全事件的发生
4. 定期检查
   定期对系统进行漏洞扫描或渗透测试，及时发现和修复安全漏洞，以保障系统的安全性

安全使用激活工具

1. 尽量使用正版软件，支持开发者并享受完整的功能和服务
2. 如果预算有限，可以寻找免费或开源的替代软件
3. 若必须使用激活工具，务必从可信来源获取，并做好安全防护
4. 部署终端防护软件，阻止用户安装使用未知来源的激活工具