YOUR LOGO

Windows系统安全机制与常用设置

2024

申请人：郑冬贤

时间：2024

Catalogue

目录

YOUR LOGO

Part 01

系统安全基础

账户安全

强密码策略

微软建议使用至少12个字符的密码，包含大小写字母、数字和特殊符号，以增强账户安全性。

定期更改密码，避免使用容易被猜测的个人信息作为密码。

多因素认证

启用多因素认证（MFA）可以增加账户安全性，即使密码泄露，攻击者也无法轻易访问账户。

微软账户支持通过手机应用、短信验证码等方式进行多因素认证。

防火墙设置

启用Windows Defender防火墙

Windows Defender防火墙可以监控进出网络流量，阻止未授权访问。

在控制面板中可以找到防火墙设置，确保其始终处于开启状态。

配置防火墙规则

可以自定义防火墙规则，允许或阻止特定程序的网络访问。

对于不熟悉的程序，应保持默认的阻止状态，避免潜在风险。

YOUR LOGO

Part 02

系统更新与补丁管理

保持系统更新

01

定期检查更新

定期检查Windows更新，安装最新的安全补丁和功能改进。可以通过“设置”>“更新和安全”>“Windows更新”来检查和安装更新。

02

自动更新设置

启用自动更新功能，确保系统在检测到新补丁时自动下载并安装。
这有助于及时修复安全漏洞，防止恶意软件利用。

第三方软件更新

01

更新杀毒软件

定期更新杀毒软件，确保病毒库是最新的，可以有效识别和防御新出现的威胁。
大多数杀毒软件都提供自动更新功能。

02

检查软件兼容性

在安装更新前，检查软件是否与当前系统版本兼容，避免更新后出现问题。
可以通过软件官网或用户论坛获取兼容性信息。

YOUR LOGO

Part 03

数据保护与备份

文件加密

使用BitLocker

BitLocker是Windows内置的全磁盘加密工具，可以保护硬盘上的数据不被未授权访问。

在“控制面板”>“系统和安全”>“BitLocker驱动器加密”中启用。

保护敏感数据

对于包含敏感信息的文件，使用文件加密功能，如BitLocker To Go，保护USB设备上的数据。

这可以防止数据在丢失或被盗时被恶意使用。

数据备份策略

定期备份数据

定期备份重要数据到外部硬盘或云存储服务，以防数据丢失或损坏。Windows内置的“文件历史记录”功能可以帮助自动备份文件。

01

验证备份完整性

定期检查备份数据的完整性，确保在需要时可以成功恢复。可以通过恢复测试来验证备份的有效性。

02

YOUR LOGO

Part 04

网络与浏览器安全

安全网络连接

02

避免公共WiFi

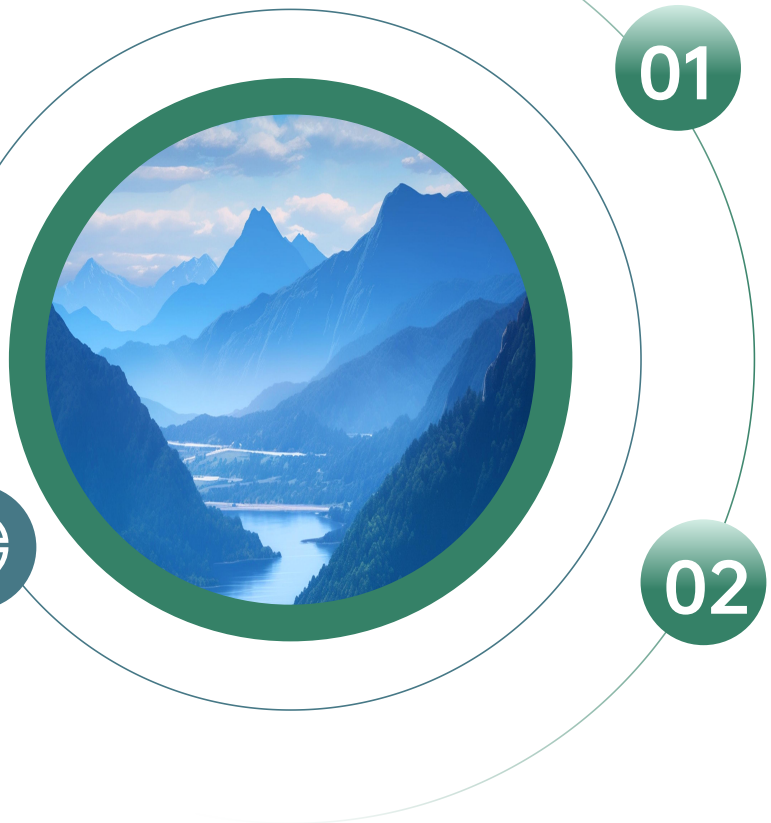
公共WiFi网络可能存在安全风险，避免在此类网络上进行敏感操作，如网上银行。
使用VPN或移动数据连接可以提高安全性。

01

使用VPN

使用虚拟私人网络（VPN）可以加密网络连接，保护数据传输过程中的隐私。
选择信誉良好的VPN服务，并正确配置以确保安全。

浏览器安全设置



01

禁用JavaScript

在不需要时禁用JavaScript可以减少恶意网站攻击的风险。

可以在浏览器设置中找到JavaScript选项并禁用。

02

安装广告拦截插件

安装广告拦截插件可以减少恶意广告和跟踪器，提高浏览安全性。

插件如uBlock Origin可以有效拦截广告和跟踪器。

YOUR LOGO

Part 05

应用程序与服务安全

应用程序权限管理

一

限制应用程序权限

仅授予应用程序必要的权限，避免过度授权可能导致的安全风险。

在“设置”>“隐私”中管理应用程序权限。

审查新安装应用

在安装新应用程序前，审查其权限请求和用户评价，确保其安全性和可靠性。

避免从不可信来源下载和安装软件。

服务账户安全

POWERPOINT DESIGN

使用本地账户而非管理员账户

避免使用管理员账户进行日常操作，以减少恶意软件获得高权限的风险。

创建一个标准用户账户用于日常操作，仅在必要时使用管理员账户。

定期审查账户权限

定期审查账户权限，移除不再需要的权限，减少潜在的安全风险。

可以通过“计算机管理”>“本地用户和组”来管理账户权限。

YOUR LOGO

谢谢大家

2024

申请人：郑冬贤

时间：2024