恶意软件

了解如何识别、避免和处理各种设备上的恶意软件。

1.什么是恶意软件?

“恶意软件”是一个涵盖多种不同软件的涵盖性术语，这些软件可能会感染、中断或者未经授权访问设备。

恶意软件可能会感染电脑、手机和平板电脑。以下是一些您可能听说过的恶意软件形式：

- **勒索软件**：可加密文件并锁定用户设备的恶意软件
- **间谍软件**：可收集用户信息的恶意软件
- **广告软件**：常见形式为失控的弹出式广告
- **蠕虫**：自我复制并传播到其他用户设备的一类病毒
- **病毒**：可感染设备并破坏数据和软件的一种恶意软件形式。病毒通过代码自我复制并运行

病毒有哪些类型?

- **木马病毒**：一种广为人知的计算机病毒，通过伪装成正规程序入侵机器。用户被骗安装或下载包含木马病毒的程序
- **浏览器劫持程序**：此类病毒可感染浏览器并更改设置，或将用户重定向到恶意网站
- **宏病毒**：此类病毒可感染 Microsoft Word 中的宏
- **文件型病毒:**此类病毒可感染重要计算机文件并在这些文件中传播

2.如何判断自己的设备是否含有恶意软件?

很遗憾，恶意软件有时不易察觉。但是，您可以通过一些迹象或情况来判断设备上是否含有恶意软件。

您可以安装一个安全软件来扫描您设备上的恶意软件。但是，务必做好研究，确保您下载的是正规的工具！实际上，有些恶意软件会冒充安全软件，欺骗您安装它们。

请注意，有些安全软件可能要花钱购买。不过，它们有不同的价位可供选择，而且许多设备预装了安全软件，因此您可以决定最适合自己的选项。

以下情况有助于您识别潜在恶意软件：

- 设备运行缓慢或总是崩溃
- 您无法关闭或重启设备
- 您的文件丢失
- 您收到意外的错误消息
- 您看到陌生的群发邮件从您的帐户发出
- 您的浏览器开始重定向或运行滞后
- 您不断收到弹出式窗口或过多干扰性广告
- 电池电量消耗过快
- [对于笔记本电脑] 风扇连续运行且噪声很大
- 您在设备上看到一些应用、打开的选项卡或其他东西，但您并没有打开或安装它们

3.如果设备上有恶意软件，该怎么办？

如果您怀疑自己下载了恶意软件，或者怀疑您的电脑已经被恶意软件感染，则检查是否有恶意软件存在，然后直接将它移除。

首先检查并证实您的疑虑很有必要，因为有些恶意软件的迹象实际上可能预示着其他问题。例如，电池电量消耗过快可能只是设备老化的迹象！

但是，如果您确实发现了更大的问题，可以采取以下措施：

- 停止网购或输入帐户密码等操作，直到解决该问题。处理完问题后更改密码
- 如果您的设备已连网，则断开网络连接，以防止恶意软件传播
- 在安全模式下重启设备，以更好地运行安全软件并处理恶意软件感染问题

- **Windows**：重启开始后立即按住 F8 键，然后从菜单中选择安全模式。接着运行安全软件扫描
- **Mac**：重启的同时按下 Shift 键，然后进行安全软件扫描

- 确保您的安全软件是最新的
- 如果您没有安装安全软件，则为您的设备安装一个声誉良好的安全类软件。您可以搜索来自技术评论网站和博客等正规可靠来源的推荐和列表，例如*《纽约时报》下属的产品推荐网站 Wirecutter* (https://www.nytimes.com/wirecutter/)
- 一旦安全软件准备就绪后，在您的设备上运行一次扫描，看看是否存在恶意软件
- 使用安全软件帮助您移除恶意软件
- 对于更严重的感染，您可能需要重装操作系统。访问设备制造商的官方网站，获得如何重装操作系统的指示
- 如果您仍需要帮助，请联系设备的技术支持（这可能属于保修范围）
- 发生恶意软件感染后，更改您的密码并监视您的帐户是否存在欺诈

4.如何避免恶意软件感染?

以下是为保护您的设备远离恶意软件可以采取的一些措施：

- **谨慎安装软件、应用和浏览器扩展程序**

恶意软件可能隐藏其中，因此务必确保您在设备上安装的是声誉良好的正规软件。

- **在您的设备和浏览器上始终保持最新的安全设置**

及时安装操作系统更新、补丁和安全更新。

- **保持警惕**

小心提防网络钓鱼骗局，避免点击或下载来自可疑或未知来源的链接或文件。

- **留意您访问的网站**

不要忽略浏览器发出的不安全站点警告。

- **定期备份您的数据**

此举有助于使数据始终受到保护，并且即使感染恶意软件仍可恢复数据。

- 安装安全软件

使用安全软件监测您的设备，并帮助您阻止、检测和移除恶意软件。

5.制定计划

在下方空白处写下您的计划和想法，看看您可以采取哪些措施避免感染恶意软件：