

## 应用和网站的安全风险

了解避免应用和网站上的陷阱和风险的一些提示和技巧。

### 1.应用和网站上存在哪些安全风险？

有些应用和网站可能自带安全风险：

- 它们可能包含恶意软件
- 它们的数据存储方法不佳，可能会给您的个人数据带来风险
- 它们可能采取不良的登录流程
- 它们可能会使您暴露在入侵性第三方跟踪程序和 Cookie 之下

恶意应用和网站会给您的个人信息和安全造成重大风险。

### 2.如何避免有风险的应用？

- 从备受认可的正规来源安装应用，例如您手机的应用商店
- 在设备上安装任何应用之前先查看评论并做一番研究
- 注意权限。确保您了解该应用会做什么，并确保您能放心授予该应用所请求的权限

### 3.如何避免有风险的网站？

- 使用安全搜索模式过滤掉含有露骨内容的结果  
这类结果通常包含安全风险，如恶意软件。大多数主要搜索引擎都提供安全搜索模式，例如 Chrome。

- 搜索网站，而不是尝试输入 URL

诈骗网站通常会使用和真实网站相似的 URL，而您的意外输入错误也可能会将您定向到一个充满恶意软件的站点。

- **检查 URL**

确保那正是您想要的网站，避免点击恶意链接。

- **使用 URL 扩展工具检查短链接**

这类扩展工具包括 CheckShortURL 或 Expand URL。

- **确保您访问的网站 URL 中包含“https”**

HTTPS 意味着网站是安全的。如果只有 HTTP，则不够安全。

- **注意来自浏览器的警告**

如果浏览器告诉您该网站不安全，您就应该果断回避

- **考虑网站推广或提供的内容**

对于提供软件或电影免费下载的网站，或者要求您提供个人信息和银行信息（但看起来没必要）的网站，您都应当抱着怀疑的态度。