

## 分析 URL

了解 URL 的分析策略，避免使用不安全或有风险的 URL。

### 1.URL 有哪些组成部分？

要分析统一资源定位符 (URL)，您应当了解 URL 由哪些不同的部分组成以及您对其指向的内容应有的预期。让我们来看看一个 URL 示例：<https://www.microsoft.com/en-us/>

示例	URL 组成部分	说明和定义	风险因素
https	协议	协议描述浏览器从 URL 获取信息的方式。	这里的关键是寻找“https”字样或安全协议。带有“http”的 URL 未加保护，因而存在风险。
www.microsoft.com	域名	域名是网站的名称和类型。域名由二级域名和顶级域名组成。  在本例中，二级域名为“www.microsoft”，顶级域名为“.com”，表明这是一个商业站点。	域名是骗子可以用来隐藏或欺骗用户的地方。  例如，骗子可以利用一个有安全风险的顶级域名搭配一个受信任的二级域名来蒙骗用户。例如，“www.microsoft.xyz”
/en-us/	路径	路径表明您将在网站上访问的特定页面或资源。本例中的路径表明我们将访问 Microsoft 网站的美国英语版。	骗子可能会在文件路径中加入跟踪程序或奇怪的符号。  请注意，骗子可能会使用简短 URL，例如 bit.ly，来隐藏 URL 路径的可疑性质。

## 2.如何分析 URL 并判断其是否安全?

分析 URL 时需要注意几点。

### 协议

- 留意协议：切记确认“https”或安全协议。如果您看到的不是 https 协议，则查找您看到的协议并确定其是否安全，在确认安全之前不要点击该链接。

### 域名和路径

- 留意域名和路径中所包含的细节：寻找细微的拼写错误、不常见的顶级域名或古怪的符号等。这些通常是 URL 有风险或不安全的迹象。
- 留意整个域名：骗子通常会在看似可信的域名中加入额外的、可疑的元素。不要被域名中的可信元素所欺骗，而要留意整个域名，确保完整域名是可靠的。
- 记住，顶级域名总是放在最后：域名的顺序是二级域名在前，顶级域名在后，也就是说，顶级域名是路径之前出现的最后元素。骗子常常使用看似可靠的二级域名来欺骗用户。务必留意协议（“https”）和正斜杠符号（“/”）之间的每一个元素。
- 查询简短或自定义的 **URL**：要缩短一个 URL 或自定义一个电子邮件链接非常容易。在点击它们之前，请先用工具（见下文）检查这类 URL。简短 URL 可能成为骗子隐藏恶意链接的绝佳方式！

以下是一些有风险的 URL 的示例，引用了虚构的名校 Hudson University（哈德逊大学）：

### **Hudsonuniversity.edulogin.com**

在这个例子中，真正的顶级域名是“.com”，骗子将域名融入路径中企图蒙骗用户。正规版本应该如下：`hudsonuniversity.edu/login`

### **Hudsoununiversity.edu**

在这个例子中，Hudson 一词被错误拼写成了“Hudsoun”。这是骗子的惯用伎俩，意图让用户点击乍一看没问题的虚假链接。

### **[http://hudsonuniversity.edu.student\\_login%.ie](http://hudsonuniversity.edu.student_login%.ie)**

这个例子中包含很多问题！首先，这个链接使用了不安全的 http 协议。其次，这里的域名实际上是“student\_login%.ie”，而不是“hudsonuniversity.edu”。记住，顶级域名总是放在最后！最后，这个域名包含一些奇怪的符号，可能预示着这是一个不安全的 URL。

## 3.如何检查 URL?

您可以使用许多工具和资源来检查 URL。

**信誉检查器：**这类网站可以用来检查 URL 或 IP 地址的信誉，如果是可疑或恶意地址，则会向您提出警告。

<https://www.urlvoid.com/>

<https://www.virustotal.com/gui/home/url>

**URL 扩展器和 IP 查询：**这些工具可用于检查简短 URL 或 IP 地址。记住，简短 URL 常被用来隐藏恶意 URL。

<https://checkshorturl.com/>

<https://www.expandurl.net/>

<https://www.ipvoid.com/>

**沙盒。**在您点击一个 URL 之前，可以先利用沙盒网站对其进行扫描和分析

# NYC Digital Safety

## Privacy & Security

---

<https://urlscan.io/>

最后，大多数浏览器的自带安全功能会在访问恶意 URL 时向您发出警告。万一您不小心点击了不该点击的 URL，请留意这些警告！

请浏览以上的链接，继续练习 URL 分析，测试自己能否判断它们是否可靠以及为什么！