DNSSEC

保障您的域名安全

当您登录网站输入个人信息时，
您有多肯定您的信息是安全的？
使用 DNSSEC 能让您对此更有信心。

很少有技术能比 DNS 对互联网运营更重要。在网络活动日益成为我们工作、生活和学习一部分的同时，域名系统安全扩展（通常被称为 DNSSEC）让用户对网络活动产生了更大的信心。DNSSEC 的作用就像域名数据的防篡改包装，有助于确保您与正确的网站或服务进行通信。

DNSSEC 的作用就像域名数据的防篡改包装，有助于确保您与正确的网站或服务进行通信。

终有一日，DNSSEC 验证将会植入操作系统，成为网络基础架构的标准配置。

什么是 DNSSEC？

在连接到某个网站之前，您的浏览器将使用 DNS 获取您所选网站的 IP 地址。但是，攻击者有可能拦截您的 DNS 查询，并提供虚假信息，这些信息可能引向一个假网站，而您可能在此网站上提供个人信息（例如，您以为这就是某银行的网站）。DNSSEC 确保您得到的信息与域名持有人发布的完全相同。

DNSSEC 提供了额外的安全级别，让您的浏览器可以检查，以确保 DNS 信息未被修改。虽然无法消除所有威胁（任何东西都做不到这一点），但它提供了提升数据安全性所需的构件，既包括 DNS，也包括基于 DNSSEC 技术的应用程序和服务。例如，DNSSEC 启用 DANE 协议，该协议可向用于电子商务的 TLS/SSL 证书提供更高的信任等级和安全性，使访问网站和服务变得更安全。

还要注意的是，DNSSEC 不仅可部署到网页，还可用于任何其他互联网服务或协议。DNSSEC 在电子邮件（SMTP）、即时消息（IM）和语音 IP 电话（VoIP）应用程序上已有一些有趣的用途。

关于互联网协会。

互联网协会是世界上深受信赖、独立的互联网信息来源和思想领袖。凭借其原则性的远景和深厚的技术基础，互联网协会推动用户、公司、政府和其他组织之间就互联网政策、技术和未来发展进行开放性的对话。互联网协会与世界各地的会员以及分会密切合作，致力于推动面向所有人的互联网的继续演变和发展。

您要做的事：为您的域名部署 DNSSEC。

使用 DNSSEC 签署您的域名涉及两个组件：

1. 您的域名注册商需要能够接受“授权签名者（Delegation Signer, DS）”记录，而且可以将这些记录发送到顶级域名（TLD）（如.com、.org 或.net）。
2. 运营托管您域名的 DNS 域名服务器的 DNS 托管提供商必须支持 DNSSEC 且能够签署（以及重新签署）您的 DNS 区域文件。

有些注册商可能会为您执行这两种功能。其他时候，您域名的 DNS 记录可能会在其他提供商托管，或者您可能在自己的 DNS 服务器上托管您的域名。

您要做的事：使用 DNSSEC。

作为最终用户，您有多个可确保您在使用 DNSSEC 的选择：

- 您的本地 DNS 解析器（从您的 ISP 或您的本地网络）可以执行“DNSSEC 验证”，并自动阻止带有错误 DNSSEC 签名的网站。
- 或者，您也可以在本地计算机上安装验证 DNS 解析器。
- 您可以将 DNSSEC 支持直接添加至网页浏览器。

终有一日，DNSSEC 验证将植入操作系统，成为网络基础架构的标准配置，但在此之前，如果您精通技术且对安全性感兴趣，您可以采取上面这些措施。

获取帮助。

互联网协会 Deploy360 计划提供现实世界的 DNSSEC、IPv6 和其他部署信息。Deploy360 架设了 IETF 标准进程与全球运营社区最终采纳这些标准之间的桥梁。Deploy360 制定并推广易于理解的资源，负责实施新技术和标准（如 IPv6 和 DNSSEC）的 IT 专业人员可根据这些资源迅速采取行动。

敬请访问 www.internetsociety.org/deploy360/dnssec 了解详情，包括有助于您开始使用 DNSSEC 的“基础知识”页面和具体项目。