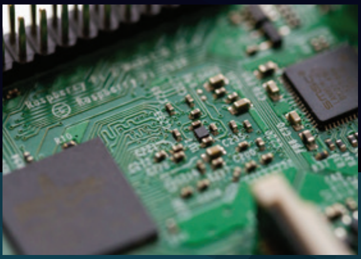
Internet Society

DNSSEC: Securing Your Domain Names



Few technologies are more critical to the Internet than the Domain Name System (DNS). DNS Security Extensions — commonly known as DNSSEC — allow users to have more confidence in our online activities at work, home, and school.

DNSSEC acts like tamper-proof packaging for domain name data, helping to ensure that you are communicating with the correct website or service.

What is DNSSEC?

Before you connect to a website, your browser uses the DNS to retrieve an IP address for the website you've chosen. However, it is possible for an attacker to intercept your DNS query and provide false information that would lead to a fake website where you could potentially provide personal information (for example, what you think is a bank website). DNSSEC ensures that you get exactly the information the domain name owner publishes.

DNSSEC provides a level of additional security so that your browser can check to make sure the DNS information has not been modified. It does not address all threats (nothing does), but it provides a building block for providing additional data security, and not just within the DNS, but also within the applications and services that are built on it. For example, DNSSEC enables usage of the DANE protocol, which can add a higher level of trust and security to TLS/SSL certificates for e-commerce and secure access to sites and services.

DNSSEC is not only for the Web, but can be used by any other Internet service or protocol. There are already interesting uses of DNSSEC with email (SMTP), instant messaging (IM), and voice over IP (VoIP) applications.

When you log on to a website and enter personal information, how certain are you that your information is secure? Using DNSSEC can help you to be more confident of that.

Do Your Part: Deploy DNSSEC on Your Domain Name(s).

Signing your domain with DNSSEC involves two components:

1. The registrar of your domain name needs to be able to accept "Delegation Signer (DS)" records and be able to send those to the Top Level Domain (TLD) (like .com, .org, or .net).
2. The DNS hosting provider who operates the DNS name servers for your domain must support DNSSEC and be able to sign (and re-sign) your DNS zone files. Some registrars may perform both roles for you. Other times, the DNS records for your domain might be hosted at another provider — or you might host them yourself on your own DNS servers.

Do Your Part: Use DNSSEC.

As an end user, you have several options to ensure you're using DNSSEC:

- Your local DNS resolver (from your ISP or your local network) may perform "DNSSEC validation" and automatically block sites with incorrect DNSSEC signatures.
- Alternatively, you can install a validating DNS resolver on your local computer.
- You can add DNSSEC support directly into a web browser.

Eventually, DNSSEC validation will be built into operating systems and will be a standard piece of network infrastructure, but until then, these are steps you can take if you're technically adept and interested in security.

Get Help.

The Internet Society provides real-world DNSSEC, IPv6, and other deployment information, bridging the gap between the IETF standards process and final adoption of those standards by the global operations community.

Visit https://www.internetsociety.org/deploy360/dnssec/ for more information.