DOMAIN NAME SYSTEM SECURITY EXTENSIONS

HELP SECURE DNS INFORMATION YOU SEND VIA THE INTERNET

Domain Name System Security Extensions (DNSSEC) allow registrants to **digitally sign** information they put into the Domain Name System (DNS). This protects consumers by ensuring DNS data that has been corrupted, either accidentally or maliciously, doesn't reach them.

TIMELINE

1980

When the DNS was designed, security was not a focus. Attackers could **compromise your DNS messages** and **redirect your messages to another location** on the Internet instead of to the one you requested.

1990

The DNS technical community created the definitive solution to this problem – DNSSEC. DNSSEC strengthens authentication in the DNS using digital signatures based on **public key cryptography.**

DNSSEC IN ACTION

Two sides of DNSSEC must be enabled for it to work.

Registrants, who are responsible for publishing DNS information, must **ensure their DNS data is DNSSEC–signed.**

Network operators need to **enable DNSSEC validation on their resolvers** that handle DNS lookups for users.

BENEFITS OF DEPLOYING DNSSEC

Helps to protect the Internet, end users, companies, organizations, and governments.

Decreases vulnerability to attacks.

Fosters innovation. DNSSEC verifies and protects DNS data, which enables data to be trusted in applications beyond the DNS.

ENCOURAGE YOUR NETWORK OPERATORS TO ENABLE DNSSEC

ICANN

FOR MORE INFORMATION ON DNSSEC, VISIT:

http://go.icann.org/OCTOpublications
http://go.icann.org/DNSSEC

Designed by ICANN Communications | May 2020