THE NATIONAL CYBERSECURITY SOCIETY

# DNS SECURITY

## Did you know?

- √ DNSSEC adds a digital signature to an IP address
- √ DNSEC ensures the authenticity of the source domain
- √ Quad9 provides DNSSEC for free
- √ DOS - is defined as Denial of Service - meaning your customers cannot reach your site

## What is DNS and DNS Security?

The Internet depends on a secure domain name system (DNS) to deliver websites and other services to users around the world. The system translates Internet addresses like Wikipedia.org into a numerical Internet Protocol address. Wikipedia translates to 91.198.174.192

A secure DNS is critical in the delivery of valid content about your business on the Internet. DNS Security is an extension - an added feature you can add to your website hosting services to ensure your website visitors are provided valid and secure content about your business.

## FACT 1: DNS SECURITY

Domain Name System Security Extensions (DNSSEC) adds a digital signature to a domain name's DNS to determine the authenticity of the source domain name. This service is available through many domain name registrars, such as Bluehost and GoDaddy. To obtain this extension as part of your hosting agreement, you will need to opt-in. The benefit of this service is to ensure your users are connecting to the actual address for the domain name. If the source cannot be validated, the request is discarded.

## FACT 2: COMMON SECURITY THREATS

1. **DNS spoofing/cache poisoning**: a hacker tries to introduce false DNS data into the DNS resolver cache* system. This attack will cause the website’s traffic to be re-directed to a location of the attacker’s choice. The redirected site may look similar to the original site, but the attacker will use the site to collect sensitive user information. The redirected site may also

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.

# DNSSEC continued...

display inappropriate content. The result may cause harm to a business.

* *DNS resolver cache is a temporary database in a computer's operating system that contains the records of recent website visits. This system is place to enable faster Internet browsing.*

**2. Non-existent domain (NXDOMAIN) attack:** This attack involves a flood of bogus website requests sent to a DNS server. The volume of these requests will prevent legitimate requests from getting through. The result will be a denial of service attack.

**3. Phantom domain attack:** This attack involves a number of phantom domain servers which are set up to respond to website requests either slowly or not at all. When the DNS resolver is inundated with these requests, the result will be either a long time before a site can be accessed or denial-of-service.

**4. Random subdomain attack:** This attack involves a heavy volume of queries being sent to random, non-existent subdomains for a particular site. The attack will cause a denial-of-service which prevents the website from being accessed.

These types of attacks are what drove the government in partnership with the private sector, to develop DNS SEC.

## FACT 3: OTHER WAYS TO PROTECT YOUR WEBSITE

When domains are registered (e.g. Wikipedia.org), the domain registrar will require both an administrative and technical contact. It is essential that this registration information be kept up to date. If one of the addresses belongs to a disgruntled employee who leaves the company, the employee may use this as a way to redirect the site to a malicious location. In addition, if a free email address (Gmail, yahoo, etc.) was used for a contact person and that address was taken over by someone else, they could redirect your DNS to a different location. Some hackers will actively look for when a website may expire. When this occurs, a person may commandeer the site -- they could replicate what it looked like and redirect the site to a different location.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.

# DNSSEC continued...

## REFERENCES:

- https://securityintelligence.com/the-past-present-and-future-of-dns-security/
- http://info.infoblox.com/WW_FY17_PS_EB_PPC-DNSCoreITSecurity?ss=google&st=dns%20security&gclid=CjwKCAjw0ujYBRBDEiwAn7BKt0RLZmITxdZo-4MbhqQEtthlQmU9uA0eQCzucAc4nkNmllEmy8CV2BoCot4QAvD_BwE
- https://searchsecurity.techtarget.com/feature/DNS-Security-Defending-the-Domain-Name-System
- https://www.cloudflare.com/learning/dns/dns-security/

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
**web@thencss.org** or visit us at the link below.