DNS

SSL Checker

Enter Domain to Check SSL Certificate:

https://www.dohnutfarms.com/

eck SSL Certificate

Buy Cheap SSl Certificate

tools

m Password Generator Server Headers Checker Port Tester Tool Online Traceroute Test

More Tools

Check Google Page Rank | DMARC Validation Tool | Domain DNS Health Checker

IPv6 Compatibility Checker | SMTP Test | Broken Links Checker

Show More | All Tools

SSL Certificate Examination

Host	dohnutfarms.com
URL	https://dohnutfarms.com
Issued For	dohnutfarms.com
Issued By	Google Trust Services (WR1)
SSL Compression	SSL Compression disabled.
SSL Chain Validation	Successfully validated certificate chain.

ertificate Chain Info

utfarms.com

d For	dohnutfarms.com
d By	Google Trust Services, US (WR1)
Signature Algorithm	RSA-SHA256
Version	2
Valid From	18-Aug-2024 04:24:44 +0000
Valid To	16-Nov-2024 04:24:43 +0000
Validity (Total)	89 days
Validity (Remaining)	40 days
Serial Number	0xEA57192449DCE3830ED3800BA3855C70
Serial Number (Hex)	EA57192449DCE3830ED3800BA3855C70
Hash	**0:** e504b67e934aa7762f782a4b02655b0d **1:** a83ba23a9a0a59dd43289a4a3bbdaf974475ff91 **2:** 05ee24dcf2fd9330f4969e33e597aa3434538c6e96b06e32975138e1c4426aee **3:** 85fe97e2e3ec0d0ecfcc62c81fc0d4f14679f6e85be103301ecc9ce0ec676097c6661c35a9024d7a412d93c4ff75c3fa **4:** 922d29a4d301d9ac4af918a71670fe37d0fc7a6cdfe75fbc3af3e226722559150977785773 8e8f1e64ca97e8b4f452d302085c6bfefedeee1d801
Public Key	Click to View

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApuPK0aredxuzvytjjbmD
```

HkF8lUEEqZNohrpBYLRyzyMPEc7PK7mK5uQYI+qeB2H0jX521wE/9N2UGRO1b0Ik
wou1e0o5GhA/tvd0MzaW2i63RYXURE0QbGGZZNnxE5yNNkrSkragGZffDjXNKEod
qKf7lqBj5aGcg/VLcQ6ibk8xs7CXUzrfvq1NzeUyCCx6gfPrcKbqMoWHi3K7qLPr
MfeP1eqZrXdNYK4hSW/RZ7ZOko9zxd5+/pvrrpz2auhbyzSeSPc0SbTR6AEmbOsX
jw/2q531L0WbgVNCD8stjuv3fHBjM2IJO5pSIuMH6/pXsWl7qdebsWNXoI7mlBG7
zQIDAQAB
-----END PUBLIC KEY-----

PEM Click to View

WR1

Issued For	Google Trust Services, US (WR1)
d By	Google Trust Services LLC, US (GTS Root R1)
ature rithm	RSA-SHA256
on	2
From	13-Dec-2023 09:00:00 +0000
To	20-Feb-2029 14:00:00 +0000
Validity (Total)	1895 days
Validity (Remaining)	1597 days
Serial Number	169943283142817666033504407772870502567
Serial Number (Hex)	7FD9E2C2D2048A0474B627A26D0868A7
Hash	**0:** 94fa897766a23adace0e09666c7cffb3 **1:** 41f091692f3b70803bd1fd77e92963d113718cd2 **2:** b10b6f00e609509e8700f6d34687a2bfce38ea05a8fdf1cdc40c3a2a0d0d0e45 **3:** d7bda1f1e03eefffc2e6e27e6f9513e3920d33e38493287ccf5ced43b8665faaf2d8e05801994085eb3efffb6b40a0d1 **4:** 06c9763b4917a81b9801fdbc26db8ea360e7d7ac6bf863524354787ac766a29f3fddf9fe9830185ee8810fd5087e1b8559714ca8c6de940b514
Public Key	Click to View
PEM	Click to View

GTS Root R1

Issued For	Google Trust Services LLC, US (GTS Root R1)
Issued By	GlobalSign nv-sa, BE (GlobalSign Root CA)
Signature Algorithm	RSA-SHA256

Version	2
Valid From	19-Jun-2020 00:00:42 +0000
Valid To	28-Jan-2028 00:00:42 +0000
Validity (Total)	2778 days
Validity (Remaining)	1208 days
Serial Number	159159747900478145820483398898491642637
ber	77BD0D6CDB36F91AEA210FC4F058D30D
	0: 3682b6c0eb81959e4b4458dfbb65d4f7
	1: 08745487e891c19e3078c1f2a07e452950ef36f6
	2: 3ee0278df71fa3c125c4cd487f01d774694e6fc57e0cd94c24efd769133918e5
	3: ffe2999f8250213d239a57e9e17a826ca1b5bb243ff2713f2a14a1796f387964b0d3101a7871323db8e4e408c0b5301a
	4: 7c883c258b8de73481d66121df53d0997a7c3b06e0e709688ffb1efd18b36cb5435f41528c7e64d6d888b2272817aed10c4a44220e01f384502
Public Key	Click to View
PEM	Click to View

SSL Certificate Checker

SSL certificate lookup verifies the SSL certificate of provided host or domain and checks the validity of SSL and the issue date, expiry date, and many more parameters.

What is an SSL cert checker?

The SSL certificate checker (Secure Sockets Layer certificate checker) is a tool that checks and verifies the proper installation of an SSL certificate on the web server. The SSL checker online verifies the SSL certificate and ensures the certificate is valid, trusted, and functioning correctly.

To check the SSL certificate, perform the following steps.

- Open the tool: SSL Cert Checker.
- Enter the URL in the space provided for that purpose and click the "Check SSL Certificate" button.
- The tool will process your query and provide the results, including common name, server type, issuer, validity, certificate chaining, and additional certificate details.

What is an SSL?

SSL is an acronym for Secure Sockets Layer. It's a standard security technology that establishes a secure web server and browser connection.

SSL connection ensures that the data transferred remains private. The SSL is also called TLS (Transport Layer Security).

SSL certificate is what enables the website to move from HTTP to HTTPS. An SSL is the data file hosted on the website origin server, making SSL/TLS encryption possible. It has a key pair: a public and a private key. These keys work together to create an encrypted connection. The certificate also contains "subject," which is the identity of the certificate/website owner.

Why do I need an SSL certificate?

An increase in cyber security threats led to an emphasis on user security. A study by pewresearch.org shows that 68% of internet users believe current laws are insufficient to protect their rights.

Therefore, in 2014, the search engine giant Google announced HTTPS as a ranking signal. Today, if you want your website to look legitimate and trustworthy. Want to boost sales, revenue, and customer loyalty, and rank higher in SERPs? You must have an SSL certificate installed on your website.

are selling something online or allowing users/customers to create an account on your website, an SSL certificate helps protect mers' information.

ollowing reasons why every web owner should serve each website over HTTPS.

dentity: SSL certificate gives verification to any website. This authentication plays an essential role in online security. Website erification is the same as verifying social media accounts. However, the SSL certificate does not allow any other website to nake a fake version of yours. That enables the users to differentiate between genuine and counterfeit websites, helping them ilter explicit fraudulent sites.

erformance: Modern SSL can improve page load time. SSL enables HTTPS/2, making the website two times faster without having any changes in the codebase. As per Google, page speed is an essential factor in user experience, and it directly influences the conversion rate. The study showed that pages that loaded in 2.4 seconds had a 1.9% conversion rate.

- **Search ranking boost:** For Google, the user is the boss, and for the user, privacy protection matters. Google gives priority to those websites in its SERPs that are served over HTTPS.
- **Security:** The majority of internet users believe that current laws are not enough to protect their privacy on the internet. Therefore, they are always afraid of sharing their information, like their credit card or other personal information, on the internet. SSL establishes an encrypted link between server and client, typically between the web server (website) and the browser. It guarantees nobody can snoop on users' data.
- **Trust:** With a padlock icon in the browser's address bar, encrypting traffic with SSL improves visitors' trust. It also ensures that third parties, including hackers and online thieves, cannot access the data.
- **Regulatory compliance:** SSL is a critical component in PCI compliance. Generally, SSL certificates come with a full 256-bit encryption key, which is impossible for hackers to crack. Therefore, there is no possibility of sensitive data getting leaked. Considering the heavily-armed protection SSL certificates provide, it wouldn't be wrong to call it the backbone of PCI DSS.

Note: PCI DSS stands for Payment Card Industry Data Security Standard.

How to get an SSL certificate?

To get an SSL certificate.

- Create a certificate signing request (CSR) on the server. That process creates a key pair: public and private keys on your server.
- The CSR data file you send to the SSL Certificate issuer (Certificate Authority or CA) contains the public key.
- The SSL Certificate issuer uses the CSR data file to create a data structure to match your private key. The CA never sees the private key.
- On receiving the SSL certificate, install it on your server. The instructions for installing and testing your SSL certificate will differ depending on your server.

The browsers have a pre-installed list of trusted CAs, known as the Trusted Root CA store. Anyone can create the certificate, but the browsers depend on the certificates from the organizations mentioned in their list of trusted CAs.

However, to be a Certificate Authority and be part of the Trusted Root CA store, a company necessarily comply with and be audited against authentication and security standards practiced by the browsers.

By addressing the CAA record in the domain's DNS records, one can restrict which CA (Certificate Authority) is authorized to issue digital credentials for your domain. From DNS lookup, you can get information about public policy regarding issuing digital

certificates for the domain.

How does the SSL certificate create a secure connection?

Communication over SSL always begins with an SSL handshake. The SSL handshake is asymmetric cryptography, which allows the web browser to verify the web server by getting the public key. It creates a secure connection before any beginning of data transfer.

- When the browser connects with the web server secured with SSL, it sends the SSL version numbers, cipher settings, session-specific data, and other information the web server needs to communicate with the client using SSL.
- In response, the web server sends a copy of its SSL certificate, including the server's SSL version number, cipher settings, session-specific data, and public key.
- The browser checks the certificate against the pre-installed list of trusted CAs. It also filters out that the certificate is unexpired and unrevoked, and its common name is valid for the website it connects to.
- If the browser trusts the certificate, it uses the server's public key to create and send back an encrypted symmetric session key.
- On receiving the encrypted symmetric session key, the server decrypts it using its private key and sends a response encrypted with the session key to start an encrypted session.
- Now the server and browser encrypt all transmitted data with the session key.

ıy certificate SSL or TLS?

SL certificate has always been used for secure and encrypted data transmission. Each time when a new version was released, he version number was altered. However, when the version was updated from SSLv3.0 to SSLv4.0, it was renamed TLSv1.0. TLS successor to SSL.

Looking for more Cyber Security tools on DNS Checker? Why do not you try our Encrypt Password Online, Strong Password Generator, and Password Strength Checker? All the Cyber Security tools are top-notch and free!