SSL QUALITY CHECK

TLS and Cypher Report

example.com **SAMPLE STATUS REPORT**

Certificate Information

Common names	example.com
Alternative names	example.com www.example.com

Valid from	Tue, 14 Apr 2020 11:43:16 UTC
Valid until	Mon, 13 Jul 2021 11:43:16 UTC
Key	RSA 2048 bits (e 65537)

Content

Who are sslqualitycheck.com

We are a group of 20 years + experienced webmasters & search engine specialists with a special interest on how google and other search engines work with security issues and the impact it has on visibility within search. Key members of our staff are

- **Peter Loleit**
    - 20+ year within ecommerce management and SEO
    - Ecommerce and Digital Marketing Agency Manager with over 20 years of Digital Marketing and Ecommerce expertise building high growth, high revenue (£4m+) Direct To Consumer (D2C), B2C and Ecommerce businesses across diverse industry sectors including Luxury, Retail (Clothing, Fashion, Furniture) and Travel.
    - Achieved double digit annual growth through E-commerce Technology and Operations and Search Engine Marketing. Deliver End-to-end project management, effective team leadership, leverage marketing and technology skills to deliver tactical and strategic initiatives.

- **Thomas Svensson**
    - 20 + years within web & traffic development
    - Senior Advisor for both national and global B2B and B2C companies as well as for organisations within the public sector on issues regarding online visibility, on-site behaviour and conversion.
    - Affiliated with IHM Business School, teaching courses on ecommerce management and chairman of digital marketing specialist education at IHM Malmö

Services from sslqualitycheck.com

We provide services for

- Consultancy within search engine optimisation and related online security
- Online security checks
- Monitoring of SSL for multiple domains

Who this report is for

This report is for Website Owners and Website Operations Managers with details specific to Website Security and Data Privacy

Google clearly states that functional HTTPS is important and it has been known for a while that not only is this a ranking factor for SEO, it is also a trust and reputation factor for visitors.

https://web.dev/why-https-matters/
https://loganix.com/google-ssl-requirements-seo/

Even if a website does not provide a shopping function, it may well have a user information transfer like contact forms or other communication that requires a level and expectation of privacy.

Poorly implemented HTTPS and HTTP provide **no privacy** to users or customers and **may result** in **data theft** and **damage to business reputation**.

SSL QUALITY CHECK

Investigation Results and Recommended Actions

Key Issues	Status	Action
Mixed Secure and Insecure Content	**PASSED**	No Action Required
Failure to Redirect from HTTP to HTTPS	**PASSED**	No Action Required
Failure to Renew Certification	**PASSED**	No Action Required
Out of Date SSL Protocols	**FAILED**	Remove support for **Insecure TLS 1.0 and TLS 1.1**
Weak Encryption Keys Used	**PASSED**	No Action Required
Weak Encryption Cyphers Used	**FAILED**	Remove **Weak CBC** Cyphers Remove Weak Cyphers use **Intermediate** compatibility configuration for nonEcommerce websites
Insecure Cookie Delivery	**PASSED**	No Action Required
WildCard or Mixed Certificates	**PASSED**	No Action Required

Common Issues of HTTPS Security

Mixed Secure and Insecure Content

Some files images, javascript, css are being served over HTTP. This can be from the site owner or a third party. Browsers will mark the website insecure to users.

Failure to Redirect from HTTP to HTTPS

The HTTPS website has been created but someone forgot to redirect from the legacy HTTP website to HTTPS. Now two websites exist causing duplication in search engines and negating the work on HTTPS

Failure to Renew Certification

Not automatically renewing your certification or poorly implementing renewal and monitoring can downgrade your HTTPS. Problems accrue exponentially the longer the website is insecure, leading to loss of revenue, reputation and trust with customers.

Out of Date SSL Protocols

Out of date or end of life protocols like TLS 1.0 SSL3 can make websites vulnerable to attack and exploitation. Problems accrue exponentially the longer the website is insecure, leading to loss of revenue, reputation and trust with customers. In some circumstance a data breach may lead to large PCI fines that could pose a severe business risk

Weak Encryption Keys Used

Allowing weak encryption keys to be used can make websites vulnerable to interception, attack and exploitation. Problems accrue exponentially the longer the website is insecure, leading to loss of revenue, reputation and trust with customers. In some circumstance a data breach may lead to large PCI fines that could pose a severe business risk

Weak Encryption Cyphers Used

Allowing weak encryption cyphers to be used can make websites vulnerable to interception, attack and exploitation. Problems accrue exponentially the longer the website is insecure, leading to loss of revenue, reputation and trust with customers. In some circumstance a data breach may lead to large PCI fines that could pose a severe business risk

Insecure Cookie Delivery

Serving cookies over HTTP on an HTTPS website can lead to cross site scripting attacks and cross site forgery attacks. In the latter case the customer could be directed to a copy of the website and have their data stolen.

WildCard or Mixed Certificates

Using a wildcard for the domains on a certificate may seem like a time saver in setup. But allowing an SSL connection on any variation of a domain name can increase the risk of proxy or cross site and phishing attacks on your websites. Take the time to define your domains and add them to your certificates.

With the high availability of Lets Encrypt free certificates, if you want to use some domains for infrastructure or scaling, aside from your main website. You

can easily automate a process of high quality certification and setup configuration. Few will need access to the large numbers of subdomains anyway, that wildcarding is supposed to solve.