

# Why HTTPS Is Essential to the Future of Your Website

Raising the standards of trust: Chrome and Firefox are the first browsers to take an HTTPS-first approach. Here's how to get your website ready.



# Table of Contents

- 1 Introduction
- 2 How Chrome and Firefox Have Changed
- 2 Why Is the Internet Moving to a "Secure by Default" Model?
- 3 The Value of Advanced Website Security
- 5 Types of SSL/TLS Certificates
- 6 SSL/TLS Certificate Solutions from DigiCert
- 7 Sources

## Introduction

Deploying HTTPS on your website with a valid SSL/TLS certificate for your domain has long been a security best practice for website owners, whether you own one domain or dozens, and whether you process transactions or not. SSL/TLS provides a measure of trust for your users and customers, especially when your certificate is issued by a reputable Internet security company, known as a Certificate Authority (CA).

Over the last few years, the need for security has grown—due to the expanded role of the internet and the amount of sensitive data that is exchanged online, and due to rising expectations of almost every major technology company.

SSL is now a precondition for the modern web. Browsers have already begun giving preferential treatment to HTTPS. New web technologies, which unlock performance benefits and rich functionality, require HTTPS. Now, the latest changes to the Google Chrome and Firefox browsers are making SSL/TLS certificates more important than ever before. In fact, for many companies, having an SSL/TLS certificate will be vital to continued business operations.

From July 2018, Chrome labels pages as “Not Secure” if they do not provide a secure connection via HTTPS with a valid SSL certificate. This warning will appear clearly in the address bar—and could have a significant impact on your site traffic and user engagement.

Chrome is not the only browser discouraging use of the unencrypted and insecure HTTP protocol. Firefox displays a broken lock icon (with a red strike-through) in the address bar when a page containing a password field does not have an HTTPS connection, in addition to an in-form warning.<sup>2</sup> This feature was added to Firefox in 2017, and like Google Chrome, it is expected that warnings and negative indicators for HTTP pages will be expanded. Safari also added a similar warning in early 2018.<sup>3</sup>

Regardless of the type of content and business size, all websites need to be using HTTPS (the secure version of the HTTP protocol which uses SSL/TLS to provide an authenticated and encrypted connection). In addition to ensuring visitor privacy, websites deploying HTTPS will also enjoy higher search engine rankings, have the ability to leverage HTTP/2 performance enhancements, and be able to prevent third-party content injection (such as ads inserted by an ISP or Wi-Fi hotspot), resulting in a better user experience.

The solution for e-commerce merchants is straightforward: Encrypt your website by procuring an SSL/TLS certificate that meets users' high expectations for privacy and lets visitors know your site is safe. Visitors who feel that your site is secure



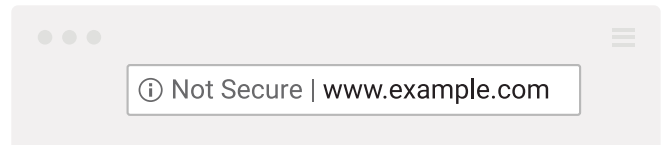
are less likely to bounce from your site or abandon their carts, which translates into more sales and higher revenue for your business.

But there are many ways to accomplish this task, and not all of them are created equal. This paper provides more detail on the many new internet standards and browser changes which are requiring HTTPS, explores the value of advanced website security for online merchants and their customers, and outlines the features to look for in an SSL/TLS certificate.

## How Chrome and Firefox Have Changed

Chrome and Firefox have been leading the way when it comes to user security. Both browsers have made major changes to their UI (user interface) in support a paradigm shift that the web is undergoing. These have come in the form of both positive reinforcement for secure pages (HTTPS), and negative reinforcement for insecure pages (HTTP).

But the current browser warnings for unsecure password and credit card fields are only the first steps. From July 2018, Chrome labels pages as "Not Secure"<sup>4</sup> This warning will appear prominently in the address bar to the left of the URL. Chrome is leading the way with this change, but all major browsers, and other platforms like Apple's iOS and Android will follow the "HTTPS Everywhere" approach. Secure connections, provided by HTTPS/SSL have become the norm—tablestakes for doing business online—and unencrypted sites will be the glaring exceptions.



## Why Is the Internet Moving to a "Secure by Default" Model?


Many people do not understand that HTTP is inherently unsecure. When you connect over HTTP, which is an unencrypted and unauthenticated protocol, any server could be providing you with a response—and it may not be the one you want to talk to. That means when you visit "http://www.MyFavoriteWebsite.com," you may actually be talking to another server pretending to be your favorite site. That's due to a lack of authentication, which makes it as easy for servers to impersonate, or "spoof" each other, as it is to write the wrong name on a nametag and pretend to be someone else. Even worse, because HTTP is unencrypted, anyone else involved in the connection – such as the many ISPs your data travels over to reach its destination—can read all the data being sent between your computer and the server.

HTTPS solves both of these issues. Your website's SSL certificate provides cryptographically verifiable proof of your identity—verified with industry standard methods and then digitally "signed" by a CA (such as DigiCert). This provides the authentication which makes it impossible for any other server to impersonate or spoof you. The SSL/TLS protocol provides the encryption, so no one else but the computer/server at the other end of the connection can read the data being transmitted.

The modern web is an essential part of the daily lives of billions of people. It is no surprise that both these security properties—encryption and authentication—are important for everything from a simple Google search, to checking your email, and online banking/ecommerce.

The reasons for promoting HTTPS use now are clear. Hackers can exploit unencrypted HTTP for all manner of purposes—from simple snooping to data theft and site manipulation. HTTP is especially dangerous for pages with login or payment forms. An attacker can use a “man-in-the-middle” attack to intercept passwords, cookies, personal, and even credit card information as it flows across the network, without users seeing or even suspecting it.

Being a small or midsize business does not make an organization any less of a target than a large enterprise. For example, insights from the Symantec Internet Security Threat Report 2017 indicate that more than



400 businesses are targeted by BEC scams every day, with small and medium-sized businesses being the most targeted.

400 businesses are targeted by BEC scams (a form of low-tech financial fraud where spoofed emails are sent to financial staff by scammers pretending to be the CEO or senior management) every day, with small- and medium-sized businesses being the most targeted.<sup>6</sup> The fact is, hackers run programs that automatically perform searches

for targets that are misconfigured or that contain vulnerabilities they can exploit. Your customers' credit card information is just as enticing as Amazon's—more so, if it's easy for cybercriminals to obtain.

Google's own research shows that its new labels are more likely to make users turn away from an unencrypted website.

Today's browser companies know how important encryption is to privacy and security, which is why they are taking steps to make HTTP warnings more obvious. Google's research shows that its new labels are effective at warning users of HTTP's insecurity—making them more likely to turn away from an insecure website. As a result, these changes will have a significant impact on e-commerce domains without an SSL/TLS certificate.

## The Value of Advanced Website Security

Many organizations have been gambling with their website's security, hoping they would get (and stay) lucky. But now that Google and others are making it obvious to users when connections are not secure, it's more important than ever to upgrade to HTTPS. HTTP is going to be the exception rather than the rule, and it's not the kind of distinction you want for your website.

Users who see the “Not Secure” label next to your web address may stop in the middle of the

## Why HTTPS Is Essential to the Future of Your Website

sign-up process, abandon their shopping cart, or simply stop reading and close the tab. Some will immediately associate your domain with security risk and find a more secure alternative.<sup>8</sup>

SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are secure protocols that help secure network communications. The use of these protocols is paired with SSL/TLS certificates, which provide unique identification to websites. Having a valid SSL/TLS certificate is key to having Chrome and other browsers identify your site as providing a valid HTTPS connection, and therefore as being "Secure."

HTTPS and SSL/TLS have always been fundamental security protocols. But thanks to the importance placed on security by collaborative organizations (such as the IETF) that design internet standards, and the requirements of major tech firms, you now receive many more benefits for deploying HTTPS.

The main benefits of using HTTPS can be summarized into five main groups: security, trust, performance, functionality, and SEO. Where are all these benefits coming from?

As already stated, HTTPS' core design provides security in the form of authentication and encryption. Performance comes from HTTP/2, the new version of the website communication protocol, which can massively reduce webpage load times and is only available when using HTTPS. Improved functionality due to Chrome and Firefox's requirement to use HTTPS with "powerful" features such as geo-location, webcam access, Service Workers, and many more.

You will enjoy increased user trust because secure sites not only avoid the negative "Not Secure" label, but also receive a green padlock icon with a "Secure" label. Finally, since 2014, Google has

treated HTTPS as a signal in their search results, meaning that you can enjoy higher ranked search results.

Let's not underestimate the importance of security. HTTPS and SSL/TLS helps you keep control over your site, preventing ISPs and Wi-Fi Hotspots from inserting ads that can distract your users, and slow down your site's performance.

Some organizations and online merchants may still be concerned that an SSL/TLS certificate will have a significant negative impact on a site's performance. This is a misconception carried on from earlier decades when encryption was taxing on a computer's resources. But these days, thanks to new internet technologies (such as HTTP/2) that require HTTPS, many benchmarks actually show a performance increase when using SSL/TLS.<sup>10</sup>

Eventual treatment of all HTTP pages in Chrome:



▲ Not Secure | example.com

Users who see the "Not Secure" label next to your web address may stop in the middle of the sign-up process, abandon their shopping cart, or simply stop reading and close the tab.

# Types of SSL/TLS Certificates

You can obtain SSL/TLS certificates any number of ways, but it's important to know that not all certificates are the same. You may find companies or organizations that offer SSL/TLS certificates at a very low cost—or even for free—but these certificates are not necessarily equivalent to certificates purchased through reputable internet security companies.

All public websites will want to avoid “self-signed certificates,” which are generated internally as opposed to having been issued by a CA. These cannot be effectively used with web browsers. Other sites use a domain-validated certificate, the most entry-level SSL/TLS certificate available. It

can be issued very quickly, and the only verification check performed is to ensure that the applicant owns the domain. No other checks are done to ensure the website is operated by a valid business entity.

By contrast, a fully authenticated SSL/TLS certificate is an appropriate first step to building online security and customer trust. Taking slightly longer to issue, these certificates are granted only after the organization passes a number of validation procedures and checks to confirm the existence of the business, the ownership of the domain, and the user's authority to apply for the certificate.

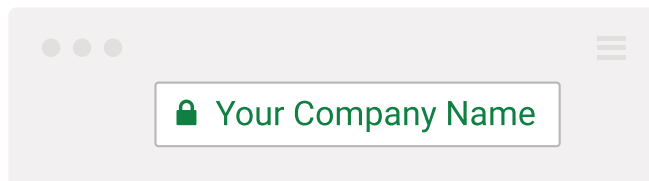
Certificate Type	Description	Recommended for	HTTPS encrypted?	Padlock displayed?	Domain validated?	Address validated?	Identity validation
EV	The highest level of authentication of the business by the Certificate Authority	Websites handling payment information and other sensitive data.	✓	✓	✓	✓	Strong
OV	A more secure step where the Certificate Authority vets the business before certificate issuance.	Public-facing websites dealing with less sensitive information.	✓	✓	✓	✓	Good
DV	The lowest level of authentication.	For situations only where trust and credibility have low risk, where a consumer is not directly involved.	✓	✓	✓	✗	None

## Finding the Right SSL Certificate

Given that SSL/TLS certificates are quickly becoming a non-negotiable part of today's internet, it's important that all website owners get a fully authenticated SSL/TLS certificate and deploy HTTPS on their website. DigiCert offers multiple SSL/TLS certificate options, all fully authenticated, across two major categories:

- **Organization Validation (OV) certificates** provide authentication of your business, giving your visitors confirmation they are interacting with a legitimate entity and not an anonymous website.
- **Extended Validation (EV) certificates** provide the highest level of authentication and receives a unique identifier in web browsers known as the "green address bar," which displays the organization's registered name to the left of the URL, and is exclusive to EV certificates. This enhanced certificate is recommended for websites where user trust is of the utmost importance—such as websites handling cardholder data (CHD), personally identifiable information (PII), and other sensitive data.

In addition, all SSL/TLS certificates provide a UI icon in web browsers: A padlock icon indicating that the user has a secure connection with your website. This not only provides vital information to users that they are browsing privately and can safely enter sensitive information into your website, but also bestows trust that you take user security seriously.



DigiCert's high-assurance certificates use enterprise-class encryption across all products, protecting users at every point—from browsing to buying. Multi-Domain/Wildcard SSL certificates are available for protecting multiple subdomains under one certificate.

### Additional features include:

- Free 24/7 support via phone, live chat, and email from a workforce of trained experts
- SSL/TLS certificate management tools
- Unified Communications support, allowing multiple domain names to be protected with a single certificate for applications like Microsoft Exchange
- 100% browser and system compatibility
- Installation assistance, including a step-by-step server-specific installation guides



## Why DigiCert?

Advanced website security is critical to your online success. Having a high-assurance certificate from a trusted Internet security provider like DigiCert can boost your business reputation as well as your SEO ranking—and help keep Chrome and other browsers from mislabeling your site as “Not Secure.” It can also help ensure that your site is compliant, increasing search engine visibility, as well as providing your customers with a consistent site experience and helping to ensure the integrity of their visit.

DigiCert certificates are a common choice amongst Forbes' Global 2000, securing a total of 26 billion connections every day. Our systems have

reliably performed at 99.99% uptime and we back that technical expertise with 24/7 live customer support and an average customer rating of 4.96/5 stars.

As a Certificate Authority that is always focused on innovating and looking forward, DigiCert provides the tools you need to effectively manage, automate, and scale your SSL certificates, and support your other PKI needs. As the Internet of Things adopts secure computing, you will want a CA partner that can support these emerging fields.

## Sources

1 Schechter, Emily, "Moving towards a more secure web," Google Security Blog, September 8, 2016. <https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html>

2 Vyas, Tanvi, "No More Passwords over HTTP, Please!" Mozilla, January 28, 2016. <https://blog.mozilla.org/tanvi/2016/01/28/no-more-passwords-over-http-please>

3 Lynch, Vincent, "Safari Warns about Unsecure Logins." DigiCert, March 30, 2018. <https://www.digicert.com/blog/safari-warns-about-unsecure-logins/>

4 Schechter, Emily, "Moving towards a more secure web," Google Security Blog, September 8, 2016. <https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html>

5 Fielding, R., et al., "Hypertext Transfer Protocol – HTTP/1.1," Internet Engineering Task Force, January 1997. <https://tools.ietf.org/html/rfc2068>

6 "Internet Security Threat Report 2016," Symantec, April 2016. [https://resource.elq.symantec.com/LP=2899?inid=symc\\_threat-report\\_istr\\_to\\_leadgen\\_form\\_LP-2899\\_ISTR21-report-main](https://resource.elq.symantec.com/LP=2899?inid=symc_threat-report_istr_to_leadgen_form_LP-2899_ISTR21-report-main)

7 Hachman, Mark, "Blame it on your brain: Researchers discover why we ignore PC security warnings," PCWorld, August 22, 2016. <http://www.pcworld.com/article/3109952/windows/blame-it-on-your-brain-researchers-discover-why-we-ignore-pc-security-warnings.html>

8 Wiener-Bronner, Danielle, "Google will soon call out websites for not being secure," CNNMoney, September 9, 2016. <http://money.cnn.com/2016/09/08/technology/google-chrome-flag-non-secure-sites>

9 Wenninger, Sascha, "Why You Shouldn't be Afraid of SSL Performance," SAP Blog, June 23, 2013. <https://blogs.sap.com/2013/06/23/whos-afraid-of-ssl/>

10 Jackson, Brian, "Analyzing HTTPS Performance Overhead," KeyCDN, September 27, 2016. <https://www.keycdn.com/blog/https-performance-overhead/>

To learn more about SSL/TLS certificate solutions from DigiCert, please visit [digicert.com](https://www.digicert.com) or call one of the following numbers:

DigiCert SSL Retail Phone Number for NAM: 1.866.893.6565

Symantec SSL Retail Phone Number for NAM: 1.866.893.6565

GeoTrust SSL Retail Phone Number for NAM: 1.866.511.4141

Thawte SSL Retail Phone Number for NAM: 1.888.484.298

DigiCert retail customers (UK): +44 (0) 208.6000.740

French: +41.26.429.77.24

Spanish: 900.931.298

German: +49.69.3807.89081

### Lehi

2801 North Thanksgiving Way Suite 500  
Lehi, UT 84043  
USA

### Mountain View

487 E. Middlefield  
Buildings K & J  
Mountain View, CA 94043  
USA

### United Kingdom

88 Wood Street, Suite 1001 & 1002  
London EC2V 7RS England

### Switzerland

Balexert Tower, 18 Avenue Louis-Casai  
Unites 01 and 30CH-1209  
Geneva, Switzerland

### Cape Town

Gateway Bldg. (3rd, 4th, & 5th floors)  
Century Blvd & Century Way 1  
Century City, Cape Town 7441  
South Africa

### Australia

437 St. Kilda Road  
Level 3, Unit 4.01  
Melbourne VIC 3004  
Australia

### China

23F/Taikang Financial Tower  
38 East Third Ring Road  
Chaoyang District, Beijing, 100026  
China

### Japan

Ginza 3-Chome  
5F Okura Bekkan  
3-4-1 Ginza Chuo-ku  
Tokyo 104-0061  
Japan

### India

10th Floor-RMZ Eco World, Sarjapur,  
Marathalli Outer Ring Road  
Devarabeesanahalli Village  
Bangalore, India 560103

© 2018 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.

**digicert**<sup>®</sup>