Why website security that's "good enough" soon won't be

Raising the standards of trust: Chrome is one of the first browsers to do it. It won't be the last.

Symantec Website Security™

Introduction

Having an 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 certificates provide a measure of trust for your users and customers, especially when a certificate is issued by a reputable Internet security company, known as a Certificate Authority (CA).

The latest changes to the Google Chrome browser 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. That's because as of January 2017, if your site is collecting passwords or credit card information, Chrome will begin labeling sites as "Not secure" if the site is not encrypted.[1] Even if you don't process financial transactions, this new label will appear clearly in the address bar—and could have a significant impact on user engagement. It won't be long before all websites will be subject to the same warnings.

While this new advanced website security standard goes into effect with the Chrome 56 release, Chrome is not the only browser discouraging use of unencrypted HTTP. Firefox Developer Edition displays a lock icon with a red strike-through in the address bar when a page containing a password field does not have an HTTPS connection.[2] This feature was added to Firefox Beta in September 2016, setting it on the path to general release.[3]

Ultimately all businesses will be impacted by these new warnings, regardless of the type of content on their websites. Whether a small business, midsize organization, or enterprise, they can also start taking advantage of the benefits of a secure site now, including higher search engine rankings, the ability to leverage HTTP/2 performance enhancements, and the ability to prevent third-party ad inserts, resulting in a better user experience.

The solution for domain owners is straightforward: Upgrade to an encrypted website by procuring an SSL/TLS certificate that meets users' high expectations for privacy and lets customers know your site is safe. But there are many ways to accomplish this task, and not all of them are created equal. This paper provides more detail on Google's short-term and long-term plans, explores the value of advanced website security, and outlines the features to look for in an SSL/TLS certificate.

How Chrome Is Changing

Due to the sensitive nature of password and credit card information, Chrome's new warning labels are targeting unencrypted pages with those fields first. The "Not secure" label will appear in the address bar, directly in front of the URL. This label will appear after the encircled "i" that currently appears in the address bar of HTTP pages—an icon that links to a dropdown that states, "Your connection to this website is not private."

But Chrome isn't going to stop with warnings for password and credit card fields. According to Google, these changes are part of a longer-term plan to label all unencrypted sites as "Not secure," whether you capture user information or not.[4] Eventually, all HTTP sites will be flagged as "Not secure" and will display the same red triangle icon currently used to indicate a broken HTTPS website. Over time and across all popular browsers, the "HTTPS Everywhere" approach will become the norm—table stakes for doing business online—and unencrypted sites will be the glaring exceptions.

Why is Google making these changes now?

HTTP was first developed in 1989, and the first definition of the protocol, HTTP/1.1, has been in common use since 1997.[5] In fact, the protocol wasn't updated until HTTP/2 was standardized in 2015. But the reasons for promoting HTTPS use now are clear—encryption has a direct impact on the security and privacy of users who are browsing or conducting transactions online. Hackers can exploit unencrypted HTTP for all manner of purposes—from simple snooping to data theft and site manipulation. As a result, HTTP is especially dangerous for pages with login, information sharing and payment forms, as these are particularly vulnerable to "man-in-the-middle" attacks. An attacker can 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 2016 indicate that small businesses experienced 65% of all spear phishing attacks recorded in 2015.[6] The fact is, hackers run programs that systematically 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.

Today's browser companies know how important encryption is to privacy and security, which is why they are taking steps to make the HTTP warnings more obvious. Recent research has shown that users disregard cybersecurity warnings at very high rates, especially when the warnings interrupt their workflow.[7] But Google's own research shows that its new labels are more likely to make users turn away from an unencrypted website. As a result, these changes will have a significant impact on domain owners without an SSL/TLS certificate.

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

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 sites are not encrypted, 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.

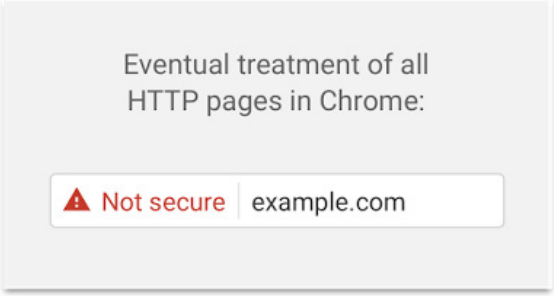
Users who see the "Not secure" label next to your web address may stop in the middle of the sign-up process, abandon their shopping cart, or simply stop reading and close the tab. Some will immediately associate your domain with security risk and find a more secure alternative. Google says that more than half of Chrome's desktop page loads are now served over a secure network, but according to Google's Transparency Report, only one-third of the top 100 non-Google websites are currently using HTTPS by default.[8]

SSL (Secure Sockets Layer) and its successor, TLS (Transport Layer Security), are encryption protocols that help secure network communications. Whether SSL or TLS, the use of these protocols is identified and verified via digital SSL/TLS certificates. The SSL/TLS certificate is the key to having Chrome and other browsers view your site as correctly encrypted and therefore as "Secure." It also allows information about the domain owner's verification to be displayed to visitors when they click on the browser's padlock symbol or trust mark.

Encrypted sites not only avoid the negative "Not secure" label, but also enjoy other benefits. The most popular browsers support the latest HTTP/2 protocol only over TLS, which means sites using HTTP/2 benefit from both full-site encryption and performance enhancements (including the associated search-engine boost) inherent to the new protocol.

Sites that have correctly configured HTTPS certificates will also be given more prominence, with the word "Secure" appearing next to the padlock in the address bar, and encrypted sites will continue to receive special SEO treatment. In addition, encryption helps you keep control over your site, preventing ISPs and Wi-Fi hotspots from inserting ads that can distract your users, slow down your site's performance, and negatively impact your search engine ranking. Advanced website security helps you maintain control of the user experience and design by securing your site's pages, cookies, APIs, and sessions.

Some online merchants may still be concerned that an SSL/TLS certificate will have a significant negative impact on the site's performance. While encrypted sites do typically require more resources than unencrypted sites, the impact on today's CPUs and networks is negligible—and has been for several years.[9] In fact, recent benchmark tests have shown that performance of HTTPS sites is now faster than HTTP in some cases.[10]



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.

For example, some sites use a "self-signed certificate" they have generated internally as opposed to having been issued the certificate by a CA. This does not hold the same weight as a fully authenticated and verified SSL/TLS certificate. Other sites use a domain-validated certificate, which is 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 owner of the domain is 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 CHD, PII, 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

SSL/TLS Certificate Solutions from Symantec

Given that SSL/TLS certificates are quickly becoming a non-negotiable for today's website owners, it's important that your organization be issued a fully authenticated SSL/TLS certificate. Symantec offers five different SSL/TLS certificate options, all fully authenticated, across two major categories:

- **Organization Validation (OV) certificates,** in which the business is vetted before the certificate is issued. This certificate is recommended for public-facing websites that handle less sensitive information.

- **Extended Validation (EV) certificates,** the highest level of authentication of the business. This enhanced certificate is recommended for websites handling cardholder data (CHD), personally identifiable information (PII), and other sensitive data.

In addition, SSL/TLS certificates provide a visual cue in green: A padlock, padlock or type in the browser, indicating that the certificate holder has been verified and that there is a higher probability that online trust can be established.

Symantec's high-assurance certificates use enterprise-class encryption across all products, protecting users at every point—from browsing to buying. The Pro SSL products offer ECC encryption for the strongest security, and Wildcard SSL certificates are available for protecting multiple subdomains under one certificate.

All Symantec SSL/TLS certificates carry a minimum warranty of $1.5 million, and all carry the widely recognized Norton Secured trust mark. Additional features include:

- Free 24/7 support via web and email from a workforce of trained experts, with extended support plans available
- Daily malware scanning
- SSL/TLS certificate management tools
- DSA (Digital Signature Algorithm) certificates for compliance with certain government agencies
- Unified communications support, allowing multiple domain names to be protected with a single certificate for applications like Microsoft Exchange
- Near 100% browser and system compatibility
- Installation assistance, including a step-by-step server-specific installation wizard
- Automatic certificate renewal
- Expiration protection, including a 30-day renewal grace period

Why Symantec?

Advanced website security is critical to your online success. Having a high-assurance certificate from a trusted Internet security provider like Symantec Website Security 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.

The Norton Secured Seal that accompanies Symantec's SSL/TLS certificates is the #1 most recognized trust mark on the web today.[11] It's seen almost one billion times per day in 170 countries, and studies have shown that 90% of customers are likely to continue an online purchase when they view the Norton Secured Seal during the checkout process–more than any other seal. That's why 90% of the Fortune 500 and 96 of the world's 100 largest financial institutions depend on Symantec to safeguard their websites, and why we secure 81% of the world's e-commerce revenue.[12]

On top of the peace of mind that Symantec's SSL/TLS certificates provide, Symantec's customer support for both SMB and Enterprises is unmatched in the industry. In recognition, the company was recently awarded the North America Frost & Sullivan's 2016 Award for Customer Value Leadership.[13]

To learn more about SSL/TLS certificate solutions from Symantec, please visit **www.symantec.com/ssl-certificates** or call **1-866-893-6565.**

Symantec Website Security

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] Mozilla Firefox Beta version 50.0 release notes, September 20, 2016. https://www.mozilla.org/en-US/firefox/50.0beta/releasenotes

[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

[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/

[11] "A Mark of Trust," *Symantec*. https://www.symantec.com/page.jsp?id=seal-transition

[12] Sources: Internal customer analysis against: Forbes Global 2000 list published in 2015, Internet Retailer Top 500 Guide 2015 Edition, Internet Retailer Europe Top 500 2015 Edition, Internet Retailer Latin America Top 500 Guide 2015 Edition, comScore Analysis 2016, Thomson Reuters Top 100 Global Innovators Award, 2015. comScore Analysis with top ecommerce organizations. comScore Analysis of Global Internet Traffic.

[13] "Frost & Sullivan Applauds the Breadth of Symantec's Security Solutions As Well As Collaborations with Customers and Peers to Provide Customized Tools," *Frost & Sullivan*, August 23, 2016. http://ww2.frost.com/news/press-releases/frost-sullivan-applauds-breadth-symantecs-security-solutions-well-collaborations-customers-and-peers-provide-customized-tools

For global offices and contact numbers, please visit our website.

For product information in the U.S., call:
1-866-893-6565 or 1-520-477-3111

Symantec World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com/ssl

For product information in Asia Pacific, call:
Australia: +61 3 9674 5500
New Zealand: +64 9 9127 201
Singapore: +65 6622 1638
Hong Kong: +852 30 114 683

Symantec Website Security Solutions Pty Ltd:
3/437 St Kilda Road, Melbourne, 3004
ABN: 88 088 021 603
www.symantec.com/en/aa/ssl-certificates

For product information in the Americas (Non-U.S.), call:
Mexico: 554 738 0448
Brazil: 800 038 0598

For product information in the U.K., call:
0800 032 2101 or +44 (0) 208 6000 740

Symantec (UK) Limited.
350 Brook Drive
Green Park, Reading
Berkshire, RG2 6UH UK
www.symantec.co.uk/ssl

For product information in Europe, call:
+353 1 793 9053 or +41 (0) 26 429 7929
Germany: 0800 128 1000
France: 0800 90 43 51
Spain: 900 93 1298

Follow Us:

Symantec Website Security™